УТВЕРЖДАЮ
Заместитель директора
ФМС России

М.Л. Тюркин
« » ___________ 2007 г.

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ЦЕНТРАЛЬНОГО БАНКА
ДАННЫХ УЧЕТА ИНОСТРАННЫХ ГРАЖДАН, ВРЕМЕННО
ПРЕБЫВАЮЩИХ И ВРЕМЕННО ИЛИ ПОСТОЯННО
ПРОЖИВАЮЩИХ В РОССИЙСКОЙ ФЕДЕРАЦИИ ДО 2012 ГОДА

Листов 106

СОГЛАСОВАНО
Начальник ЦБС
ФСБ России

В.С. Горбачев
«__» ___________ 2007 г.

СОГЛАСОВАНО
Заместитель директора
ФСТЭК России

А.Е. Гапонов
«__» ___________ 2007 г.

Москва 2007
СОГЛАСОВАНО

Генеральный директор
ЗАО «Ай-Теко»

В.В. Подшивалов
« » __________ 2007 г.

СОГЛАСОВАНО

Генеральный директор
ЗАО НИП «ИНФОРМЗАЩИТА»

В.Ю. Гайкович
«__» __________ 2007 г.

СОГЛАСОВАНО

Директор по корпоративным проектам
ЗАО «Ай-Теко»

А.А. Калайдя
«__» __________ 2007 г.

СОГЛАСОВАНО

Руководитель проекта
ЗАО НИП «ИНФОРМЗАЩИТА»

В.Ф. Минаев
«__» __________ 2007 г.

СОГЛАСОВАНО

Заместитель начальника отдела
ФМС России

С.В. Бабкин
«__» __________ 2007 г.
I АННОТАЦИЯ

В настоящем документе описана концепция создания системы обеспечения информационной безопасности автоматизированной системы1 Центрального банка данных по учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации, в том числе участников Государственной программы по оказанию содействия добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом2.

В документе приводится описание состава, структуры, целей создания и использования АС ЦБД УИГ, основные цели и задачи по защите информации в АС ЦБД УИГ. В документе также устанавливается структура системы защиты информации АС ЦБД УИГ как совокупности организационных, технических и иных мер защиты, определяются требования по реализации данных мер.

Настоящий документ является неотъемлемой частью организационно-нормативного обеспечения ФМС России по вопросам защиты информации в АС ЦБД УИГ.

1 Далее – «АС».
2 Далее – «ЦБД УИГ».
<table>
<thead>
<tr>
<th>Глава</th>
<th>Разделы</th>
<th>Страница</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Аннотация</td>
<td>3</td>
</tr>
<tr>
<td>II</td>
<td>Введение</td>
<td>7</td>
</tr>
<tr>
<td>III</td>
<td>Общие положения</td>
<td>10</td>
</tr>
<tr>
<td>3.1</td>
<td>Назначение и статус Концепции</td>
<td>10</td>
</tr>
<tr>
<td>3.2</td>
<td>Область применения</td>
<td>10</td>
</tr>
<tr>
<td>IV</td>
<td>Особенности обеспечения информационной безопасности АС ЦБД УИГ</td>
<td>12</td>
</tr>
<tr>
<td>V</td>
<td>Основные принципы обеспечения информационной безопасности</td>
<td>13</td>
</tr>
<tr>
<td>VI</td>
<td>Объект защиты</td>
<td>14</td>
</tr>
<tr>
<td>6.1</td>
<td>Сведения, подлежащие защите</td>
<td>14</td>
</tr>
<tr>
<td>6.2</td>
<td>Структура, состав и размещение основных элементов АС ЦБД УИГ. Технологии обработки и передачи информации</td>
<td>14</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Структура АС ЦБД УИГ</td>
<td>14</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Функциональная схема АС ЦБД УИГ</td>
<td>16</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Техническое и программное обеспечение АС ЦБД УИГ</td>
<td>17</td>
</tr>
<tr>
<td>6.3</td>
<td>Категории пользователей АС ЦБД УИГ</td>
<td>20</td>
</tr>
<tr>
<td>6.4</td>
<td>Требуемые категории и классы защищённости АС ЦБД УИГ</td>
<td>21</td>
</tr>
<tr>
<td>VII</td>
<td>Цели и задачи обеспечения информационной безопасности</td>
<td>24</td>
</tr>
<tr>
<td>7.1</td>
<td>Интересы субъектов информационных отношений, затрагиваемые при эксплуатации АС ЦБД УИГ</td>
<td>24</td>
</tr>
<tr>
<td>7.2</td>
<td>Цели обеспечения информационной безопасности</td>
<td>24</td>
</tr>
<tr>
<td>7.3</td>
<td>Основные задачи обеспечения информационной безопасности АС ЦБД УИГ</td>
<td>25</td>
</tr>
<tr>
<td>7.4</td>
<td>Пути достижения целей обеспечения информационной безопасности</td>
<td>26</td>
</tr>
<tr>
<td>VIII</td>
<td>Модель угроз и нарушителя информационной безопасности АС ЦБД УИГ</td>
<td>28</td>
</tr>
<tr>
<td>8.1</td>
<td>Угрозы безопасности информации и их источники</td>
<td>28</td>
</tr>
<tr>
<td>8.2</td>
<td>Нарушители информационной безопасности АС ЦБД УИГ</td>
<td>29</td>
</tr>
<tr>
<td>8.3</td>
<td>Пересмотр модели угроз и нарушителя ИБ АС ЦБД УИГ</td>
<td>30</td>
</tr>
<tr>
<td>IX</td>
<td>Структура системы обеспечения информационной безопасности АС ЦБД УИГ</td>
<td>31</td>
</tr>
<tr>
<td>X</td>
<td>Меры, методы и средства обеспечения информационной безопасности АС ЦБД УИГ</td>
<td>34</td>
</tr>
<tr>
<td>10.1</td>
<td>Правовые (законодательные) меры защиты информации</td>
<td>34</td>
</tr>
<tr>
<td>10.2</td>
<td>Морально-этические меры защиты информации</td>
<td>34</td>
</tr>
<tr>
<td>10.3</td>
<td>Организационные (административные) меры защиты информации</td>
<td>34</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Регламентация допуска внешних пользователей к АС ЦБД УИГ</td>
<td>36</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Регламентация допуска внутренних пользователей к АС ЦБД УИГ</td>
<td>37</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Регламентация доступа на территорию, в здания и помещения ФМС России</td>
<td>39</td>
</tr>
<tr>
<td>10.3.4</td>
<td>Регламентация процессов, связанных с эксплуатацией и сопровождением АС ЦБД УИГ</td>
<td>40</td>
</tr>
<tr>
<td>10.3.5</td>
<td>Регламентация действий в случае нештатных ситуаций</td>
<td>41</td>
</tr>
<tr>
<td>10.3.6</td>
<td>Подготовка персонала в вопросах обеспечения ИБ</td>
<td>42</td>
</tr>
<tr>
<td>10.3.7</td>
<td>Регламентация распределения ролей персонала по доступу к АС ЦБД УИГ</td>
<td>43</td>
</tr>
<tr>
<td>10.3.8</td>
<td>Регламентация работы удостоверяющего центра ФМС России</td>
<td>44</td>
</tr>
<tr>
<td>10.4</td>
<td>Технические (программные/программно-аппаратные) меры защиты информации</td>
<td>46</td>
</tr>
</tbody>
</table>
10.4.1 Требования к средствам идентификации и аутентификации пользователей АС ЦБД УИГ ................................................................. 46
10.4.2 Требования к обеспечению информационной безопасности к основным техническим средствам АС ЦБД УИГ, расположенным за пределами государственной границы Российской Федерации ................................................. 47
10.4.3 Требования к средствам разграничения доступа к информационным ресурсам АС ЦБД УИГ ......................................................... 47
10.4.4 Требования к средствам обеспечения и контроля целостности программных и информационных ресурсов АС ЦБД УИГ .................................................................................................................. 48
10.4.5 Требования к средствам антивирусной защиты .......................................................................................................................... 49
10.4.6 Требования к средствам мониторинга и регистрации событий безопасности ...................................................................................... 49
10.4.7 Требования к ИБ при использовании информационно-аналитической подсистемы АС ЦБД УИГ .......................................................... 50
10.4.8 Требования к ИБ при использовании подсистемы хранения данных ............................................................................................ 50
10.4.9 Требования к ИБ при использовании подсистемы резервного копирования и восстановления данных ............................................. 51
10.4.10 Требования к ИБ при использовании подсистемы ведомственной электронной почты АС ЦБД УИГ .................................................... 52
10.4.11 Требования к ИБ при использовании подсистемы ведомственной телефонной связи АС ЦБД УИГ ......................................................... 52
10.4.12 Требования к ИБ при использовании подсистемы мониторинга и управления ............................................................................. 53
10.4.13 Требования к ИБ при использовании подсистемы сервисного обслуживания заявок пользователей АС ЦБД УИГ ............................................. 54
10.4.14 Требования к ИБ при использовании подсистемы представления общедоступной информации из АС ЦБД УИГ в сеть общего пользования «Интернет» .......................................................... 55
XI УПРАВЛЕНИЕ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ .......................................................... 57
XII АНАЛИЗ РИСКОВ .............................................................................................................................................................................. 60
XIII ПРЕДСТАВЛЕНИЕ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ ИЗ АС ЦБД УИГ В СЕТЬ ОБЩЕГО ПОЛЬЗОВАНИЯ «ИНТЕРНЕТ» ................................................................. 62
XIV СИСТЕМА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ ................................................................. 63
XV АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ .......................................................................................... 65
XVI ПОРЯДОК АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ АС ЦБД УИГ ...................................................................................... 67
XVII ПОРЯДОК РЕАЛИЗАЦИИ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ ........................................ 69
ПРИЛОЖЕНИЕ 1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ .......................................................................................................................... 75
ПРИЛОЖЕНИЕ 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ................................................................................................................................. 78
ПРИЛОЖЕНИЕ 3. НОРМАТИВНАЯ ПРАВОВАЯ БАЗА РАЗРАБОТКИ КОНЦЕПЦИИ .......................................................... 82
ПРИЛОЖЕНИЕ 4. НОРМАТИВНО-ТЕХНИЧЕСКАЯ БАЗА РАЗРАБОТКИ КОНЦЕПЦИИ .......................................................... 85
ПРИЛОЖЕНИЕ 5. ШАБЛОН ЗАПРОСА НА ПРЕДОСТАВЛЕНИЕ ДОСТУПА ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЯМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ АС ЦБД УИГ ......................................................... 87
ПРИЛОЖЕНИЕ 6. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЯМ К РЕСУРСАМ АС ЦБД УИГ ......................................................... 90
ПРИЛОЖЕНИЕ 7. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК РАЗГРАНИЧЕНИЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ТЕРИТОРИЮ, В ЗДАНИЯ И ПОМЕЩЕНИЯ ................................................................. 92
ПРИЛОЖЕНИЕ 8. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК ПРОВЕДЕНИЯ ЭКСПЛУАТАЦИИ, ОБСЛУЖИВАНИЯ, РЕМОНТА И МОДИФИКАЦИИ АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ АС ЦБД УИГ .......................................................... 94
ПРИЛОЖЕНИЕ 9. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК ДЕЙСТВИЙ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНОЙ СИТУАЦИИ В АС ЦБД УИГ .......................................................... 96
ПРИЛОЖЕНИЕ 10. ТИПОВОЙ ПЕРЕЧЕНЬ ТРЕБОВАНИЙ К ПОДГОТОВКЕ ПЕРСОНАЛА В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИБ ................................................................. 98

ПРИЛОЖЕНИЕ 11. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ МЕХАНИЗМЫ РАСПРЕДЕЛЕНИЯ РОЛЕЙ СОТРУДНИКОВ СИСТЕМЫ ФМС РОССИИ ПО ДОСТУПУ К РЕСУРСАМ АС ЦБД УИГ ............................................................................................................. 100

ПРИЛОЖЕНИЕ 12. ПЛАН-ПРОСПЕКТ АКТА ФМС РОССИИ, ОПРЕДЕЛЯЮЩЕГО РЕГЛАМЕНТ РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ФМС РОССИИ .................................................................................................................. 102

ПРИЛОЖЕНИЕ 13. ПЛАН-ПРОСПЕКТ «ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ АКТИВОВ» ................................................................. 104

ПРИЛОЖЕНИЕ 14. ПЛАН-ПРОСПЕКТ «ОТЧЕТА ОБ ОЦЕНКЕ РИСКОВ» ............................................................................. 105

ПРИЛОЖЕНИЕ 15. ПЛАН-ПРОСПЕКТ «ПЛана обработки Рисков» ................................................................. 106
В ВВЕДЕНИЕ

В соответствии с требованиями законодательства Российской Федерации, должны обеспечиваться сбор и консолидация информации об иностранных гражданах и лицах без гражданства, находящихся в Российской Федерации. Данная информация формируется федеральными органами исполнительной власти и организациями, оформляющими въездные и выездные документы иностранных граждан, осуществляющими их регистрацию при пересечении государственной границы Российской Федерации и по месту пребывания или проживания, а также определяющими регламент пребывания данных лиц.

АС ЦБД УИГ создана с целью реализации требований по сбору и консолидации информации об иностранных гражданах. АС ЦБД УИГ представляет собой специализированную межведомственную автоматизированную систему, пользователями и поставщиками информации при ведении которой являются:

− заинтересованные федеральные органы государственной власти, их территориальные органы (структурные подразделения);
− органы государственной власти субъектов Российской Федерации;
− Администрация Президента Российской Федерации;
− Центральный банк Российской Федерации;
− Счетная палата Российской Федерации;
− Центральная избирательная комиссия Российской Федерации;
− Генеральная прокуратура Российской Федерации.

Ответственность за ведение АС ЦБД УИГ возложена на Федеральную миграционную службу. ФМС России обеспечивает бесперебойную эксплуатацию программных и технических средств АС ЦБД УИГ, а также осуществляет сбор, хранение, обработку и представление пользователям информации об иностранных гражданах.

Основными целями создания и использования АС ЦБД УИГ являются:

− обеспечение национальной безопасности Российской Федерации и общественной безопасности в сфере миграции;

1 Далее – «иностранные граждане».
2 Далее – «ФОИВ».
3 Далее – «ФМС России».
– обеспечение прав и законных интересов граждан Российской Федерации, а также иностранных граждан;

– формирование полной, достоверной и актуальной информации о перемещениях иностранных граждан, необходимой для оценки миграционной ситуации на территории Российской Федерации, выработки и реализации мер, направленных на регулирование миграционных процессов на территории Российской Федерации.

АС ЦБД УИГ для достижения указанных целей обеспечивает выполнение следующих функций:

– автоматизация сбора, обработки, хранения и представления данных об иностранных гражданах;

– обеспечение доступа к консолидированным данным по учету иностранных граждан сотрудникам ФМС России, ее территориальных органов и иных входящих в структуру ФМС России организаций и подразделений¹;

– предоставление информации из базы данных пользователям иных органов государственной власти;

– представление открытой информации в сеть Интернет;

– обеспечение внутриведомственного обмена электронными сообщениями между пользователями АС ЦБД УИГ;

– обеспечение централизованного сбора, учета и хранения заявок пользователей АС ЦБД УИГ на разрешение проблем, возникающих при эксплуатации АС.

АС ЦБД УИГ относится к ключевым системам информационной инфраструктуры Российской Федерации.

________________________

¹ Далее – «система ФМС». 
Особенность обеспечения информационной безопасности связана со спецификой информации, обрабатываемой в АС ЦБД УИГ. Данная информация является конфиденциальной и содержит персональные данные. Разглашение информации, хранимой и обрабатываемой в АС ЦБД УИГ, может нанести ущерб обладателям данной информации (в частности, иностранным гражданам). Кроме того, пользователи АС ЦБД УИГ заинтересованы в получении своевременного доступа к информации из АС ЦБД УИГ, и временное отсутствие такого доступа может привести к затруднениям в решении задач, возложенных на ФМС России. С учетом перечисленных проблем, законодательством Российской Федерации были установлены следующие требования по защите АС ЦБД УИГ:

– должна быть обеспечена защита от несанкционированного доступа информации, хранимой, обрабатываемой и передаваемой в АС ЦБД УИГ;

– должна быть обеспечена бесперебойная эксплуатация программно-технического комплекса АС ЦБД УИГ в соответствии с техническим заданием АС ЦБД УИГ.

ФМС России, являясь оператором АС ЦБД УИГ, определяет и реализует комплекс мер по защите АС ЦБД УИГ. Обеспечение необходимого уровня защиты невозможно без организационной и административной поддержки со стороны руководства ФМС России, направленной на установление требований, норм и правил по защите АС ЦБД УИГ и обеспечение контроля реализации данных требований. Одним из важнейших аспектов административной поддержки является разработка и внедрение организационно-нормативных документов, регламентирующих вопросы защиты информации в АС ЦБД УИГ. «Концепция информационной безопасности автоматизированной системы центрального банка данных учета иностранных граждан, временно прибывающих и постоянно проживающих в Российской Федерации» является основополагающим нормативным документом ФМС России по защите информации в АС ЦБД УИГ.

---

1 Далее – «ИБ».
2 Далее – «НСД».
3 Далее – «Концепция».
III ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Назначение и статус Концепции

Настоящая Концепция определяет систему взглядов на проблему обеспечения информационной безопасности АС ЦБД УИГ. Концепция представляет собой систематизированное изложение целей и задач защиты, основных принципов построения системы защиты, требований к организационным и техническим мерам защиты информации в АС ЦБД УИГ.

Целями разработки и применения Концепции являются:

– определение стратегии построения, реализации и дальнейшего развития системы обеспечения информационной безопасности АС ЦБД УИГ;

– формирование требований по защите АС ЦБД УИГ, единых для ФМС России и всех ее территориальных органов (структурных подразделений).

Концепция разработана на основе анализа угроз ИБ для подлежащих защите ресурсов АС ЦБД УИГ с учетом современного состояния и ближайших перспектив развития АС ЦБД УИГ, а также положений действующего законодательства Российской Федерации и нормативно-технических документов, регламентирующих вопросы защиты информации в АС ЦБД УИГ.

Концепция является документом верхнего уровня в системе организационно-нормативного обеспечения защиты информации в АС ЦБД УИГ. Организационно-нормативные документы нижнего уровня создаются в развитие Концепции, определяя и уточняя процедуры и порядки, направленные на реализацию положений Концепции. Структура нормативного обеспечения ИБ АС ЦБД УИГ определена в разделе 10.3.

3.2 Область применения

Концепция является обязательной для применения в Центральном аппарате¹ ФМС России и ее территориальных органах, в которых размещены технические и программные компоненты АС ЦБД УИГ. Ознакомление с Концепцией и учет ее положений обязательны для сотрудников ЦА ФМС России и территориальных органов ФМС России, осуществляющих:

– администрирование и сопровождение (в том числе ремонт и обслуживание) компонентов АС ЦБД УИГ;

¹ Далее – «ЦА».
– организацию и проведение работ по защите информации в АС ЦБД УИГ (в том числе работ по физической защите АС ЦБД УИГ).

Организационно-нормативные, эксплуатационные и проектные документы ФМС России по вопросам эксплуатации, администрирования и сопровождения АС ЦБД УИГ должны формироваться с учетом положений Концепции и не противоречить им.
IV ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АС ЦБД УИГ

Построение системы обеспечения информационной безопасности АС ЦБД УИГ осуществляется с учетом особенностей АС ЦБД УИГ (архитектуры, состава программных и технических средств и т. д.) и специфики деятельности ФМС России. Основными особенностями, значимыми для построения системы обеспечения ИБ, являются:

— территориальная распределенность. АС ЦБД УИГ является территориально-распределенной автоматизированной системой, что приводит к возникновению трудностей по обеспечению управления и контроля функционирования АС ЦБД УИГ;

— сложность эксплуатации высокотехнологического оборудования. В состав АС ЦБД УИГ входят технические средства различных типов, работающие под управлением разнообразных программных средств. Проведение работ по администрированию и сопровождению данных средств требует привлечения высококвалифицированного персонала;

— межведомственный информационный обмен. Поставщиками информации и пользователями АС ЦБД УИГ, помимо ФМС России, являются иные федеральные органы государственной власти, их территориальные органы и т. д. В задачи ФМС России входит обеспечение нормальной эксплуатации поставщиками и пользователями программных и технических компонентов АС ЦБД УИГ. В то же время подключение поставщиков информации и пользователей к АС ЦБД УИГ не должно приводить к снижению уровня защищенности ресурсов АС ЦБД УИГ;

— необходимость межведомственного согласования документации. Для координации работ по созданию и внедрению АС ЦБД УИГ была создана Межведомственная комиссия по координации работ федеральных органов исполнительной власти. В функции данной комиссии входит координация деятельности ФОИВ по созданию и внедрению АС ЦБД УИГ. Комиссия осуществляет межведомственное согласование проектной документации на АС ЦБД УИГ, в том числе в части обеспечения ИБ;

— нехватка профессионально подготовленных кадров. В ряде территориальных органов ФМС России возникают сложности с подбором персонала, имеющего достаточную квалификацию для выполнения функций по администрированию, сопровождению и защите информации в АС ЦБД УИГ.
V ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности АС ЦБД УИГ должно осуществляться в соответствии со следующими принципами:

− законность – построение системы обеспечения ИБ с учетом требований законодательства Российской Федерации в сфере обеспечения ИБ, нормативно-технических документов ФСТЭК России и ФСБ России;

− непрерывность – реализация мер обеспечения ИБ в форме непрерывного процесса, охватывающего все этапы жизненного цикла АС ЦБД УИГ; обеспечение постоянной организационной и технической поддержки применения защитных мер;

− адекватность мер защиты – планирование мер обеспечения ИБ исходя из наиболее актуальных на текущий момент угроз ИБ; проведение постоянного анализа состояния АС ЦБД УИГ с целью своевременного обнаружения возникновения новых угроз ИБ;

− обязательность контроля – обеспечение своевременного выявления и пресечения действий, направленных на нарушение установленных правил и требований обеспечения ИБ АС ЦБД УИГ, принятие мер по устранению выявленных недостатков в системе обеспечения ИБ;

− знание своих служащих – проведение тщательного подбора персонала на должности, связанные с доступом к ресурсам АС ЦБД УИГ; осуществление контроля выполнения служащими своих обязанностей по обеспечению ИБ;

− персонификация ролей – проведение четкого распределения ролей сотрудников ФМС России по управлению активами и выполнению мер обеспечения ИБ, позволяющего в случае любого нарушения ИБ четко определить или свести к минимуму круг подозреваемых лиц;

− минимизация полномочий – предоставление сотрудникам ФМС России минимальных привилегий по доступу к ресурсам АС ЦБД УИГ, необходимых для выполнения сотрудниками своих должностных обязанностей;

− отслеживание и анализ инцидентов – принятие мер, направленных на предотвращение инцидентов ИБ, их своевременное обнаружение, устранение негативных последствий от их возникновения и оценку последствий; создание нормативно-правовой и доказательной базы по расследованию инцидентов ИБ.
VI ОБЪЕКТ ЗАЩИТЫ

6.1 Сведения, подлежащие защите

Информация, содержащаяся в АС ЦБД УИГ, представляет собой совокупность сведений в электронном виде (базы данных, файлы в электронном виде и т. д.)

Перечень видов информации, поступающей в ЦБД УИГ от поставщиков информации, определен Приказом МВД России, МИД России, ФСБ России, Минэкономразвития России и Мининформсвязи России от 10.03.2006 г. № 148/2562/98/62/25 «О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации». Детализированный перечень видов информации в ЦБД УИГ устанавливается «Объединенным базовым реквизитным составом информации, содержащейся в ЦБД УИГ».

Поставщиками информации в АС ЦБД УИГ являются МВД России, ФМС России, МИД России, ФСБ России. Поставщики осуществляют передачу информации для занесения в АС ЦБД УИГ с использованием одной из следующих технологий:

− на электронных или бумажных носителях почтой в порядке, установленном для информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну;

− в режиме электронной почты по защищенным линиям связи;

− непосредственным взаимодействием информационных систем поставщиков с АС ЦБД УИГ или установкой Абонентских пунктов на территории поставщиков информации.

В соответствии с указанным выше Приказом, вся информация в АС ЦБД УИГ является конфиденциальной и содержит персональные данные иностранных граждан.

6.2 Структура, состав и размещение основных элементов АС ЦБД УИГ. Технологии обработки и передачи информации

6.2.1 Структура АС ЦБД УИГ

АС ЦБД УИГ функционирует на трех уровнях в соответствии с организационно-штатным делением ФМС России:

− федеральный уровень;

− региональный уровень;
– территориальный уровень.

Федеральный уровень АС ЦБД УИГ представляет собой программно-аппаратный комплекс, развернутый в ЦА ФМС России, в котором аккумулируется информация с регионального и территориального уровней АС ЦБД УИГ. АС ЦБД УИГ федерального уровня является защищенным сегментом локальной вычислительной сети ЦА ФМС России.

Региональный уровень АС ЦБД УИГ представляет собой совокупность программно-аппаратных комплексов, развернутых в территориальных органах ФМС России. Объекты регионального уровня подключены к ПАК-Центр по защищенным линиям связи. В состав ПАК-Регион входят локальные вычислительные сети и выделенные автоматизированные рабочие места пользователей. В зависимости от требований к объемам хранимых данных и иных особенностей функционирования территориальных органов ФМС России, выделяют четыре типа программно-аппаратных комплексов: ПАК-Регион-1, ПАК-Регион-2, ПАК-Регион-3, ПАК-Регион-4.

Территориальный уровень АС ЦБД УИГ представляет собой выделенные защищенные АРМ пользователей, размещенные в территориальных органах ФМС России и выполняющие функции приема, обработки и передачи информации.

Объекты АС ЦБД УИГ всех уровней объединены в единую автоматизированную систему с помощью сетей передачи данных.

Структура АС ЦБД УИГ представлена на Рис. 1.

---

1 Далее – «ПАК-Центр».
2 Далее – «ЛВС».
3 Далее – «ПАК-Регион».
4 Далее – «АРМ».
6.2.2 Функциональная схема АС ЦБД УИГ

По функциональному назначению АС ЦБД УИГ разделена на следующие основные подсистемы:

– информационно-аналитическая подсистема 1 – подсистема, реализующая основной функционал АС ЦБД УИГ в части учета и контроля иностранных граждан, построенная на базе системы управления базами данных 2 Oracle 10g и специального программного обеспечения 3;

– подсистема хранения данных 4 – подсистема, предназначенная для организации хранения и предоставления своевременного доступа к данным;

– подсистема резервного копирования и восстановления данных 5 – подсистема, предназначенная для организации процессов копирования и восстановления данных;

– подсистема ведомственной электронной почты 6 – подсистема, предназначенная для обеспечения обмена электронными сообщениями между пользователями АС ЦБД УИГ и построенная на базе программного обеспечения 7 CommuniGate Pro 5.3 for Solaris;

1 Далее – «ИАП».
2 Далее – «СУБД».
3 Далее – «СПО».
4 Далее – «ПХД».
5 Далее – «ПРКВД».
6 Далее – «ПВЭП».
7 Далее – «ПО».  

Рис. 1. Структура АС ЦБД УИГ
– подсистема ведомственной телефонной связи\(^1\) – подсистема, предназначенная для организации взаимодействия пользователей АС ЦБД УИГ с помощью средств телефонной связи и построенная на основе ПО Avaya IP Office Administration Applications;

– подсистема мониторинга и управления\(^2\) – подсистема, предназначенная для управления и мониторинга работы программных и технических компонентов АС ЦБД УИГ, построенная на базе продуктов семейства Tivoli;

– подсистема сервисного обслуживания заявок пользователей\(^3\) – подсистема, предназначенная для организации централизованного обобщения и учета заявок пользователей АС ЦБД УИГ на обслуживание и разрешение возникающих у них проблем, построенная на основе ПО CA Unicenter ServicePlus Service Desk;

– подсистема представления общеупотребимой информации из АС ЦБД УИГ в сеть общего пользования Интернет\(^4\) – подсистема, предназначенная для предоставления доступа заинтересованным лицам к сведениям АС ЦБД УИГ, не содержащим конфиденциальной информации, через сеть Интернет;

– подсистема информационной безопасности\(^5\) – подсистема, предназначенная для обеспечения информационной безопасности всех подсистем, элементов и компонентов АС ЦБД УИГ;

– подсистема удостоверяющего центра\(^6\) – подсистема, обеспечивающая возможность применения в АС ЦБД УИГ средств электронной цифровой подписи\(^7\).

**6.2.3 Техническое и программное обеспечение АС ЦБД УИГ**

В состав ПАК-Центр входят следующие основные компоненты:

1. Кластер серверов IBM pSeries 690 под управлением операционной системы\(^8\) AIX 5.3. На серверах установлены серверные компоненты основных подсистем АС ЦБД УИГ, определенных в п. 6.2.1 и п. 6.2.2, включая:

– СУБД Oracle 10g Standard Edition;

\(^1\) Далее – «ПВТС».
\(^2\) Далее – «ПМУ».
\(^3\) Далее – «ПСО».
\(^4\) Далее – «ППНИ».
\(^5\) Далее – «ПИБ».
\(^6\) Далее – «подсистема УЦ».
\(^7\) Далее – «ЭЦП».
\(^8\) Далее – «ОС».
– специальное программное обеспечение¹ «Мигрант-1»;

2. Управляющий сервер IBM pSeries 630 под управлением ОС AIX 5.3, на котором установлено ПО IBM Tivoli;

3. Ленточная библиотека IBM 3504;

4. Система хранения данных IBM Total Storage DS 4500.

5. Программно-аппаратный комплекс УЦ АС ЦБД УИГ.

Архитектура ПАК-Центр представлена на Рис. 2.

¹ Далее – «СПО».

Рис. 2. Архитектура ПАК-Центр

В состав типового ПАК-Регион входят следующие основные компоненты:

1. Кластер серверов Fujitsu Siemens PrimePower 250 под управлением ОС Solaris 9. На серверах установлены серверные компоненты всех подсистем АС ЦБД УИГ, определенных в п. 6.2.1 и п. 6.2.2 (кроме ППНИ и подсистемы УЦ);

2. Ленточная библиотека Fujitsu-Siemens Computers MTC9084;

3. Система хранения данных Hitachi Data Systems AMS 500.

Типовая архитектура ПАК-Регион представлена на Рис. 3.
В качестве специального программного обеспечения в серверных комплексах ПАК-Центр и ПАК-Регион применяется программный комплекс\(^1\) «Мигрант-1». В настоящее время осуществляется ввод в эксплуатацию новой версии СПО «Мигрант-2», предоставляющего расширенный функционал в сравнении с предыдущей версией СПО.

АРМы пользователей реализуются на базе защищенных персональных компьютеров с архитектурой Intel, работающих под управлением специальной сертифицированной ОС «Атликс», имеющей встроенные СКЗИ. На этапе опытной эксплуатации допускается использование ОС Windows XP SP 2, Secure Pack Rus 0.1. На АРМ пользователя установлены:

– модуль криптопровайдера «Удостоверяющий центр “КриптоПро УЦ”»;

– «тонкий» клиент ПК «Мигрант-1», с помощью которого осуществляется доступ к серверу приложений СПО.

Взаимодействие клиента СПО с сервером приложений осуществляется по защищенному соединению. Для организации защищенного соединения используется закрытый ключ, хранящийся на смарт-карте пользователя, и открытый ключ, хранящийся в списке сертификатов пользователей на сервере приложений. Защита соединения осуществляется с помощью библиотеки криптопровайдера «КриптоПро».

\(^1\) Далее – «ПК».
Система генерации и проверки сертификатов пользователей реализуется на базе Удостоверяющего центра, развернутого на Федеральном уровне АС ЦБД УИГ.

Система антивирусной защиты на базе продуктов имеющих сертификат соответствия требованиям информационной безопасности ФСБ России.

Размещение серверного оборудования осуществляется в модульных комнатах Lampertz либо в серверных помещениях, оснащенных следующими системами:

– система бесперебойного питания;
– система пожаротушения;
– система видеонаблюдения;
– система кондиционирования;
– система контроля доступа.

Для связи федерального, регионального и территориального уровней АС ЦБД УИГ используются следующие сети передачи данных:

– единая информационно-телекоммуникационная сеть органов внутренних дел Российской Федерации;
– арендованные у компаний-провайдеров каналы связи.

Подключение ПАК-Центр и ПАК-Регион к внешним сетям передачи данных осуществляется через сертифицированный ФСТЭК России межсетевой экран Cisco Firewall PIX 525, при этом шифрование передаваемой информации обеспечивается средствами криптоМаршрутизатора «Атликс-VPN».

6.3 Категории пользователей АС ЦБД УИГ

Исходя из особенностей строения и функционирования АС ЦБД УИГ, допущенным к ней физическим лицам предоставляются различные полномочия по доступу к информационным, программным, техническим и другим ресурсам АС ЦБД УИГ. Эти лица могут быть разделены на следующие четыре категории:

1. Категория I – технический персонал АС ЦБД УИГ. К данной категории относятся:

– специалисты по обслуживанию технических средств, сопровождению общего и специального ПО;
– администраторы, осуществляющие настройку технических и программных средств в составе АС ЦБД УИГ;
– администраторы информационной безопасности, осуществляющие настройку технических и программных средств защиты информации АС ЦБД УИГ;

2. Категория II – внутренние пользователи АС ЦБД УИГ. К данной категории относятся сотрудники структурных подразделений системы ФМС России, являющиеся зарегистрированными пользователями АС ЦБД УИГ и осуществляющие доступ к АС ЦБД УИГ из локальной вычислительной сети ФМС России;

3. Категория III – внешние пользователи АС ЦБД УИГ. К данной категории относятся уполномоченные лица заинтересованных ФОИВ и иных организаций, получивших доступ к АС ЦБД УИГ на основании заключенного с ФМС России соглашения об информационном обмене;

4. Категория IV – другие физические лица. Все лица данной категории имеют доступ в помещения с установленными в них техническими средствами АС ЦБД УИГ, но не являются зарегистрированными пользователями или инженерно-техническим персоналом АС ЦБД УИГ. К данной категории относятся:

– обслуживающий персонал ФМС России, производящий работы в помещениях, в которых размещается оборудование АС ЦБД УИГ;

– другие сотрудники подразделений ФМС России, имеющие доступ в помещения, в которых размещается оборудование АС ЦБД УИГ;

– уполномоченный персонал специальных служб Российской Федерации;

– посетители подразделений ФМС России – физические лица, имеющие право разового доступа в контролируемую зону АС ЦБД УИГ;

– уполномоченный персонал подрядных организаций, имеющий на основании контрактов и соглашений право на модификацию информационных ресурсов общего доступа.

6.4 Требуемые категории и классы защищенности АС ЦБД УИГ

В целях дифференцированного подхода к защите информации производится классификация АС ЦБД УИГ по требованиям защищенности от несанкционированного доступа к информации и аттестация объектов информатизации на соответствие предъявленным требованиям. Класс защищенности устанавливается на основе Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», и

1 Далее – «НСД».
2 Утвержден решением председателя Гостехкомиссии России от 30.03.1992 г.
«Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)»¹, исходя из следующих особенностей АС ЦБД УИГ:

– категории хранимой и обрабатываемой в АС ЦБД УИГ информации;

– уровень полномочий пользователей АС ЦБД УИГ по доступу к конфиденциальной информации;

– режим обработки данных в АС (коллективный или индивидуальный).

С учетом характера обрабатываемой в АС ЦБД УИГ информации, АС ЦБД УИГ классифицирована по классу защищенности 2Б. Класс 2Б установлен в соответствии с актом классификации АС ЦБД УИГ утверждённым директором ФМС России от 29.12.2005 года на этап опытной эксплуатации АС ЦБД УИГ. На начальном этапе должна быть проведена аттестация всех объектов информатизации в составе АС ЦБД УИГ (ПАК-Центр и ПАК-Регион) для подтверждения выполнения требований к классу защищенности 2Б.

Подключение новых ПАК к АС ЦБД УИГ допускается только после их аттестации по классу 2Б.

Аттестация объектов информатизации АС ЦБД УИГ по классу 2Б на этапе опытной эксплуатации позволит:

- гарантировать отсутствие гальванических соединений основных технических средств связи АС ЦБД УИГ с локальными вычислительными сетями ФМС России и сетями общего пользования;

- провести планомерное обучение личного состава системы ФМС россии по направлению: «Безопасность информационных технологий»;

- разработать необходимую организационно-распорядительную документацию в области обеспечения информационной безопасности АС ЦБД УИГ;

- внедрить сертифицированные ФСТЭК России средства разграничения доступа к информации содержащейся в АС ЦБД УИГ;

- создать инфраструктуру УЦ АС ЦБД УИГ.

В дальнейшем, в связи с необходимостью разграничения доступа пользователей к информации в АС ЦБД УИГ необходимо провести классификацию и аттестацию АС ЦБД УИГ по классу 1Г.

¹ Утверждены приказом Гостехкомиссии России от 30.08.2002 г. № 282.
Для обеспечения возможности аттестации по классу 1Г в АС ЦБД УИГ должны быть внедрены механизмы разграничения доступа к информации на основе сертифицированных ФСТЭК России средств защиты информации.

В соответствии с Указом Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», применяемые в АС ЦБД УИГ средства криптографической защиты информации¹ должны быть сертифицированы ФСБ России. До начала эксплуатации сертифицированных СКЗИ должно быть получено заключение ФСБ России о корректности встраивания СКЗИ в соответствующее программное обеспечение.

Класс применяемых в АС ЦБД УИГ СКЗИ устанавливается на основе нормативных правовых актов² ФСБ России с учетом действующей в ФМС России модели нарушителя ИБ АС ЦБД УИГ (см. п. 8.2). Поскольку на этапе опытной эксплуатации АС ЦБД УИГ определен нарушитель категории Н2 (до конца 2008 года), далее Н3, то:

- СКЗИ, применяемые для защиты от нарушителя, должны быть сертифицированы ФСБ России по классу не ниже чем КС2 до конца 2008 года, и КС3 далее;

- СКЗИ, применяемые для защиты от внешнего нарушителя, должны быть сертифицированы ФСБ России по классу не ниже чем КВ2.

¹ Далее – «СКЗИ».
² Далее – «НПА».
VII ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1 Интересы субъектов информационных отношений, затрагиваемые при эксплуатации АС ЦБД УИГ

Субъектами информационных отношений при эксплуатации АС ЦБД УИГ являются:

– федеральные органы государственной власти, их территориальные органы, Администрация Президента Российской Федерации и иные органы и подразделения, являющиеся пользователями АС ЦБД УИГ;

– иностранные граждане как субъекты персональных данных;

– иные юридические и физические лица, задействованные в процессах создания и функционирования АС ЦБД УИГ (разработчики отдельных компонентов АС ЦБД УИГ, пользователи информации, обслуживающий персонал и т. д.)

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

– конфиденциальности (сохранения в тайне) определенной части информации;

– достоверности (полноты, точности, адекватности, целостности) информации;

– защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

– своевременного доступа (за приемлемое для них время) к необходимой им информации;

– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

– защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации).

7.2 Цели обеспечения информационной безопасности

Стратегической целью обеспечения информационной безопасности АС ЦБД УИГ является защита интересов субъектов информационных отношений, возникающих при функционировании АС ЦБД УИГ. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:
− доступности обрабатываемой информации для зарегистрированных пользователей (т. е. устойчивого функционирования АС ЦБД УИГ, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое время);

− конфиденциальности информации, хранимой и обрабатываемой в АС ЦБД УИГ;

− целостности информации, хранимой и обрабатываемой в АС ЦБД УИГ;

− достоверности информации, хранимой в АС ЦБД УИГ.

7.3 Основные задачи обеспечения информационной безопасности АС ЦБД УИГ

Для достижения основных целей обеспечения ИБ система защиты АС ЦБД УИГ должна обеспечивать решение следующих задач:

− выявление уязвимостей в АС ЦБД УИГ, которые могут представлять угрозу ИБ информации;

− уведомление о фактах реализации угроз информационной безопасности АС ЦБД УИГ соответствующих администраторов, обнаружение, нейтрализация и локализация воздействия угроз ИБ;

− обеспечение криптографической защиты информации при использовании различных систем передачи данных в соответствии с требованиями по защите конфиденциальной информации;

− обеспечение защиты информации в АС ЦБД УИГ от несанкционированного доступа с помощью средств защиты информации, не препятствующих возможности последующей аттестации АС ЦБД УИГ;

− управление доступом к защищаемой информации;

− восстановление работоспособности средств защиты информации в случае сбоя или аварии технических средств АС ЦБД УИГ, а также после воздействия угроз ИБ;

− регистрация событий и попыток НСД к защищаемой информации и несанкционированного воздействия на нее;

− обеспечение контроля функционирования средств и системы защиты информации, немедленное реагирование на их выход из строя;

− организация и обеспечение функционирования разрешительной системы допуска пользователей системы к работе с защищаемой информацией и ее носителями;

− накопление опыта решения проблем информационной безопасности;
– подтверждение авторства и контроль целостности передаваемых электронных сообщений (документов) с использованием средств электронной цифровой подписи1 на основе сертификатов ключей подписи, выдаваемых удостоверяющим центром;

– обеспечение централизованного контроля целостности ПО, установленного на серверах и АРМ АС ЦБД УИГ;

– обеспечение доставки электронных сообщений (документов) с учетом требований, предъявляемых к АС ЦБД УИГ при обмене с органами государственной власти и другими внешними абонентами.

7.4 Пути достижения целей обеспечения информационной безопасности

Достижение поставленных целей защиты и решение перечисленных в п. 7.3 задач достигаются:

– применением физических и технических (программных, программно-аппаратных) средств защиты ресурсов АС ЦБД УИГ и непрерывной административной поддержкой их использования;

– защитой сведений в АС ЦБД УИГ путем использования разрешенных к применению в Российской Федерации средств криптографической и технической защиты, включая средства защиты от несанкционированного доступа;

– применением средств электронной цифровой подписи для обеспечения юридической значимости и невозможности отрицания факта направления и (или) получения сведений;

– регламентацией процессов обработки подлежащей защите информации с применением технических и программных средств (действий сотрудников структурных подразделений системы ФМС России, использующих АС ЦБД УИГ, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС ЦБД УИГ);

– предупреждением попадания конфиденциальной информации на носители и в файлы, доступ к которым не разграничивается, а также запрещением передачи информации ограниченного распространения по незащищенным каналам связи;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-нормативных документов ФМС России по вопросам защиты информации в АС ЦБД УИГ;

– созданием в системе ФМС России подразделений, ответственных за организацию технической и криптографической защиты информации;

1 Далее – «ЭЦП».
– назначением и подготовкой сотрудников ФМС России на роли, связанные с защитой информации в АС ЦБД УИГ;

– наделением каждого пользователя (сотрудника подразделения системы ФМС России) полномочиями по доступу к ресурсам АС ЦБД УИГ на минимально необходимый для выполнения функциональных обязанностей срок;

– четким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими технические и программные средства АС ЦБД УИГ, требований организационно-нормативных документов ФМС России по вопросам защиты информации;

– персональной ответственностью лиц, участвующих в информационном обмене в АС ЦБД УИГ, за полноту и достоверность сведений, их своевременную передачу и изменение, а также хранение и уничтожение в установленном порядке;

– строгим учетом всех подлежащих защите ресурсов АС ЦБД УИГ (информации, программных средств, серверов, АРМ и т. д.);

– постоянным контролем за соблюдением сотрудниками подразделений системы ФМС России – пользователями АС ЦБД УИГ – требований по обеспечению ИБ;

– аттестацией АС ЦБД УИГ на соответствие требованиям защищенности от НСД по требованиям ФСТЭК России;

– применением сертифицированных ФСБ России средств криптографической защиты информации;

– юридической защитой интересов ФМС России при взаимодействии с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;

– проведением постоянного анализа эффективности и достаточности применяемых мер и средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации в АС ЦБД УИГ при развитии системы.
8.1 Угрозы безопасности информации и их источники

Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Основные угрозы ИБ, направленные на АС ЦБД УИГ, в конечном итоге оказывают влияние на безопасность сведений, хранимых и обрабатываемых в АС, и приводят к нарушению конфиденциальности, целостности или доступности информации.

Выделяют три основных типа угроз в зависимости от способа их создания:

– природные (пожары, осадки, наводнения и т. д.);

– технические (отключения или колебания электропитания и других средств обеспечения, отказы и сбои аппаратных и программных средств, электромагнитные излучения и наводки и т. д.);

– созданные людьми (перехват, хищение, уничтожение, блокирование, модификация информации, отказ от информации).

Угрозы ИБ подразделяются также на преднамеренные (умышленные) и непреднамеренные (случайные) угрозы.

Преднамеренные угрозы ИБ преследуют цель нанесения ущерба информационным, программным, техническим и иным ресурсам АС ЦБД УИГ.

Непреднамеренные угрозы ИБ связаны со случайными действиями пользователей, ошибками операторов, программистов, управленческого персонала и службы персонала.

Основными целями реализации угроз ИБ в АС ЦБД УИГ могут являться:

– утечка (хищение) конфиденциальной информации;

– уничтожение конфиденциальной информации;

– блокирование конфиденциальной информации;

– модификация конфиденциальной информации;

– нарушение функционирования элементов или узлов технических или программных средств, АС ЦБД УИГ в целом.
8.2 Нарушители информационной безопасности АС ЦБД УИГ

**Нарушитель** — это лицо, предпринявшее попытку реализации угрозы информационной безопасности АС ЦБД УИГ, независимо от предпосылок и используемых методов и средств. Попытка реализации угроз ИБ называется **атакой.**

По признаку принадлежности к АС ЦБД УИГ всех нарушителей можно разделить на две группы:

– внешние нарушители — физические лица, не имеющие права доступа в контролируемую зону;

– внутренние нарушители — физические лица, имеющие право доступа в контролируемую зону.

Внешний нарушитель может осуществлять атаки на АС ЦБД УИГ только с территории, расположенной вне контролируемой зоны, по внешним каналам связи. Возможности внешнего нарушителя по воздействию на АС ЦБД УИГ зависят от типов используемых в АС ЦБД УИГ каналов связи и степени их защищенности.

Возможности внутреннего нарушителя зависят от действующих в пределах контролируемой зоны ограничительных факторов, основным из которых является реализация комплекса режимных и организационно-технических мер по предотвращению и пресечению несанкционированных действий в АС ЦБД УИГ.

На текущий момент в АС ЦБД УИГ выделены следующие типы нарушителей ИБ в соответствии с классификацией ФСБ России:

– нарушитель (тип Н5) — нарушитель (группа нарушителей), осуществляющий создание методов и средств реализации атак, а также реализующий атаки с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа СКЗИ и подсистем криптографической защиты информации;

– нарушитель (тип Н2) — нарушитель, не являющийся пользователем средств вычислительной техники, на которых реализованы СКЗИ и ПТЗИ (группа нарушителей, среди которых есть по крайней мере один указанный внутренний нарушитель), самостоятельно осуществляющий создание методов и средств реализации атак, а также самостоятельно реализующий атаки;

– нарушитель (тип Н3) — нарушитель, являющийся пользователем СВТ, на которых реализованы АИС (группа нарушителей, среди которых есть, по крайней мере, один из

1 Далее — «ПКЗИ». 
нарушителей типа Н₂ и Н₁), самостоятельно осуществляющий (-ая) создание методов и средств реализации атак, а также самостоятельно реализующий (-ая) атаки.

8.3 Пересмотр модели угроз и нарушителя ИБ АС ЦБД УИГ

Текущая модель угроз и нарушителя ИБ АС ЦБД УИГ приведена в документе «ДШСК.0029-ТА Автоматизированная система центрального банка данных учета иностранных граждан. Подсистема информационной безопасности. Модель угроз информационной безопасности и действий нарушителя» и используется в качестве основы при разработке и построении системы обеспечения ИБ АС ЦБД УИГ. Для обеспечения актуальности модели должен осуществляться регулярный пересмотр модели с периодичностью не реже чем один раз в три года.

Внеплановый пересмотр модели угроз и нарушителя должен осуществляться в случаях:

– измени́ния законодательства Российской Федерации, нормативных правовых актов ФМС России, приводящих к изменению категорий пользователей АС ЦБД УИГ, состава программных и технических средств в составе АС ЦБД УИГ;

– существенных изменений в технологии обработки информации АС ЦБД УИГ, влияющих на состав угроз ИБ.
IX СТРУКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ

Обеспечение достаточного уровня защищенности информации в АС ЦБД УИГ требует комплексного подхода и осуществляется путем реализации совокупности мер обеспечения ИБ по следующим направлениям:

− правовые меры защиты;
− морально-этические меры защиты;
− организационные меры защиты;
− технические меры защиты.

В разделе X приводится характеристика данных мер и устанавливаются требования к составу и содержанию мер по каждому из направлений.

Необходимым условием построения эффективной системы обеспечения ИБ АС ЦБД УИГ является четкое распределение обязанностей по планированию и реализации защитных мер между различными подразделениями и должностными лицами ФМС России.

Основные обязанности по организации и координации применения технических и организационных мер защиты в АС ЦБД УИГ должны быть возложены:

− в ЦА ФМС России – на сотрудников Отдела технической защиты информации1 Управления по вопросам информационно-аналитического обеспечения ФМС России2;
− в территориальных органах ФМС России – на сотрудников подразделений, ответственных за организацию технической и криптографической защиты информации3.

Сотрудники ОТЗИ УИАО ФМС России осуществляют:

− планирование мер защиты информации, применяемых на федеральном, региональном и территориальном уровнях АС ЦБД УИГ;
− организацию применения мер защиты информации в АС ЦБД УИГ на федеральном уровне;
− контроль и оценку эффективности применяемых мер защиты информации в АС ЦБД УИГ;
− контроль действий пользователей и администраторов АС ЦБД УИГ (сотрудников ЦА ФМС России) на предмет соблюдения установленных требований по защите информации;

1 Далее – «ОТЗИ».
2 Далее – «УИАО ФМС России».
3 Далее – «подразделение ОТКЗИ».
– периодические проверки выполнения технических мер защиты информации в территориальных органах ФМС России;
– организацию проведения служебных расследований по фактам нарушения правил обеспечения ИБ и возникновения инцидентов ИБ;
– обучение пользователей АС ЦБД УИГ правилам работы со средствами защиты информации в составе АС ЦБД УИГ;
– ведение учета используемых СКЗИ, эксплуатационной и технической документации к ним;
– ведение учета пользователей, допущенных к работе с СКЗИ;
– техническое обслуживание применяемых средств защиты информации, в том числе СКЗИ;
– поддержку функционирования Удостоверяющего центра ФМС России;
– мониторинг применяемых СКЗИ и контроль настроек АС ЦБД УИГ;
– аттестацию объектов информатизации АС ЦБД УИГ (после получения аттестата аккредитации ФСТЭК России на право аттестации); 
– маркировку средств защиты информации и основных средств вычислительной техники АС ЦБД УИГ защитными голографическими знаками их учет и контроль использования знаков в системе ФМС России.

Сотрудники подразделения ОТКЗИ территориальных органов осуществляют:
– организацию применения мер защиты информации на региональном и территориальном уровнях АС ЦБД УИГ;
– контроль и оценку эффективности применяемых мер защиты информации в АС ЦБД УИГ;
– контроль действий пользователей и администраторов АС ЦБД УИГ (сотрудников соответствующих территориальных органов ФМС России) на предмет соблюдения установленных требований по защите информации;
– организацию проведения служебных расследований по фактам нарушения правил обеспечения ИБ и возникновения инцидентов ИБ;
– маркировку средств защиты информации и основных средств вычислительной техники АС ЦБД УИГ защитными голографическими знаками их учет и контроль.

Обязанности по управлению настройками и сопровождению специализированных и штатных средств защиты АС ЦБД УИГ должны быть возложены:
– в ЦА ФМС России – на сотрудников Информационного центра (исключая обязанности по управлению Удостоверяющим центром);

– в территориальных органах ФМС России – на сотрудников подразделения по информационным технологиям, ответственного за обеспечение функционирования АС ЦБД УИГ³.

³ Далее – «ИТ-подразделение». 
X МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ

10.1 Правовые (законодательные) меры защиты информации

Правовые (законодательные) меры защиты заключаются в применении действующих в Российской Федерации законодательных и подзаконных актов, руководящих и нормативно-технических документов для определения прав, обязанностей и ответственности лиц, участвующих в эксплуатации и сопровождении АС ЦБД УИГ. Правовые меры защиты определяют развитие системы обеспечения ИБ АС ЦБД УИГ и являются сдерживающим фактором для потенциальных нарушителей информационной безопасности ИБ.

10.2 Морально-этические меры защиты информации

Морально-этические меры защиты основываются на сложившихся в ФМС России и обществе в целом нормах поведения. Эти нормы не являются обязательными, как нормативные акты, однако их несоблюдение обычно ведет к падению авторитета человека, группы лиц или организации. В связи с этим сложившиеся нормы поведения могут сдерживать потенциальных нарушителей от нарушений ИБ, отрицательно воспринимающихся в обществе.

10.3 Организационные (административные) меры защиты информации

Организационные (административные) меры защиты – это меры организационного характера, позволяющие регламентировать процессы функционирования АС ЦБД УИГ, использования ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз ИБ или снизить размер потерь в случае их реализации.

Организационные меры защиты базируются на комплексе организационно-нормативных документов ФМС России, регламентирующих вопросы защиты информации при эксплуатации, сопровождении и администрировании АС ЦБД УИГ.

В состав организационно-нормативных документов АС ЦБД УИГ входят документы двух уровней:

– первый уровень – документы, единые для ЦА и всех территориальных органов ФМС России;
– второй уровень – документы, специфичные для ЦА и территориальных органов.

Документы первого уровня разрабатываются ОТЗИ УИАО ФМС России (по согласованию с заинтересованными подразделениями ФМС России) или внешними подрядными организациями и доводятся до всех территориальных органов ФМС России. Документы второго уровня разрабатываются подразделениями ОТЗИ территориальных органов самостоятельно либо на основе типового документа, предоставленного ОТЗИ УИАО ФМС России.

К документам первого уровня относятся настоящая Концепция, а также нормативные правовые акты ФМС России, регламентирующие и определяющие:

– порядок регистрации внешних пользователей и (или) поставщиков сведений и подключения их к АС ЦБД УИГ;
– порядок обращения со сведениями конфиденциального характера, хранимыми и обрабатываемыми в АС ЦБД УИГ;
– процессы функционирования удостоверяющего центра ФМС России;
– порядок проведения анализа рисков информационной безопасности;
– порядок сбора доказательств и проведения расследования инцидентов ИБ;
– порядок предоставления открытой информации в сеть общего пользования «Интернет»;
– требования по обучению персонала АС ЦБД УИГ в вопросах обеспечения информационной безопасности.

К документам второго уровня относятся нормативные правовые акты ФМС России, регламентирующие и определяющие:

– порядок предоставления доступа внутренним пользователям к АС ЦБД УИГ;
– порядок допуска сотрудников и посетителей на территорию, в здания и помещения подразделения ФМС России;
– процессы проведения эксплуатации, обслуживания, ремонта и модификации программных и технических ресурсов АС ЦБД УИГ;
– порядок действий обслуживающего персонала и пользователей при возникновении нештатной ситуации в АС ЦБД УИГ;
– порядок распределения ролей персонала по доступу к АС ЦБД УИГ и механизмы доверия к персоналу;
– инструкции по эксплуатации, администрированию и сопровождению программных и технических средств АС ЦБД УИГ.
Данные документы разрабатываются с учетом положений по ИБ, изложенных в разделах 10.3.1-10.3.8. За основу при разработке документов могут быть взяты план-проресекты, приведенные в Приложениях 6-12.

Встроенные средства беспроводного доступа входящие в состав основных технических средств, применяемых в составе системы управления ТКО, используемой в составе АС ЦБД УИГ, удаляются или их функционирование аппаратно блокируется.

Средства защиты информации и основные технические средства АС ЦБД УИГ должны быть защищены от несанкционированного вскрытия корпусов специальными защитными голограмфическими знаками.

В случае необходимости проведения регламентных работ или работ по техническому обслуживанию требующих вскрытие корпусов оборудования, вскрытие корпусов должно производиться по согласованию с ОТЗИ УИАО ФМС России в ЦА ФМС России и сотрудниками подразделений ОТКЗИ в территориальных органах ФМС России.

10.3.1 Регламентация допуска внешних пользователей к АС ЦБД УИГ

Внешними пользователями АС ЦБД УИГ являются уполномоченные лица ФОИВ, их территориальных органов, иных организаций и структур согласно постановлению Правительства Российской Федерации от 14.02.2007 г. № 94 «О государственной системе миграционного учета». Подключение внешних пользователей должно осуществляться только после заключения соглашения об информационном обмене сведениями между ФМС России и пользователем, определяющего:

– режим информационного обмена сведениями;

– порядок информационного обмена сведениями, в том числе между территориальными органами и (или) структурными подразделениями сторон;

– права и обязанности сторон (в том числе обязательства по неразглашению сведений конфиденциального характера);

– условия использования электронной цифровой подписи при осуществлении информационного обмена сведениями;

– порядок разрешения и (или) ограничения доступа к передаваемым поставщиком сведениям;

– основания и условия расторжения соглашения.
При подключении пользователей должен быть составлен протокол, определяющий требования к средствам защиты объекта информатизации, подключаемого к АС ЦБД УИГ. Требования к средствам защиты должны быть согласованы с требованиями по защите от несанкционированного доступа, предъявляемым к АС класса защищенности 2Б (либо 1Г после аттестации АС ЦБД УИГ данному классу защищенности).

Подключение пользователей должно осуществляться только после проверки соблюдения требований по технической защите информации, определяемых протоколом, сотрудниками ОТЗИ УИАО ФМС России либо подразделений ОТКЗИ территориальных органов ФМС России. Приобретение и внедрение средств защиты информации, направленных на реализацию установленных требований, осуществляется за счет пользователя.

Для осуществления доступа к АС ЦБД УИГ внешнему пользователю должен быть выдан сертификат ключа подписи в порядке, определенном в п. 10.3.8.

Порядок предоставления внешнему пользователю сведений из АС ЦБД УИГ должен предусматривать следующие фазы:

1. Передача пользователем запроса на получение сведений из АС ЦБД УИГ, подписанного ЭЦП пользователя;
2. Передача пользователю необходимых сведений из АС ЦБД УИГ, подписанных ЭЦП уполномоченного должностного лица ФМС России. Подлинность ЭЦП означает, что переданные пользователю сведения соответствуют запросу пользователя и содержатся в АС ЦБД УИГ;
3. Передача пользователем квитка, подписанного ЭЦП пользователя, подтверждающего факт получения запрошенных сведений из АС ЦБД УИГ и обязательство обеспечить защиту данных сведений.

Права доступа пользователей должны немедленно аннулироваться в случае расторжения соглашения между внешним пользователем и ФМС России.

В соответствии с постановлением правительства Российской Федерации от 14.02.2007 г. № 94 «О государственной информационной системе миграционного учета», должен быть разработан межведомственный нормативный правовой акт, определяющий порядок регистрации внешних пользователей и подключения к АС ЦБД УИГ.

10.3.2 Регламентация допуска внутренних пользователей к АС ЦБД УИГ

Внутренними пользователями АС ЦБД УИГ являются сотрудники подразделений системы ФМС России. В ЦА и каждом территориальном органе ФМС России должно быть назначено лицо, ответственное за управление доступом внутренних пользователей к АС ЦБД УИГ, должностью не
ниже начальника отдела. Данное лицо принимает решение о целесообразности подключения внутренних пользователей из ЦА ФМС России или соответствующего территориального органа ФМС России к АС ЦБД УИГ исходя из должностных обязанностей конкретного должностного лица.

Подключение внутренних пользователей к АС ЦБД УИГ должно осуществляться на основании письменного запроса, подготовленного непосредственным руководителем должностного лица. Запрос должен оформляться в соответствии с шаблоном, приведенным в Приложении 5. Запрос на предоставление доступа должен быть согласован с лицом, ответственным за управление доступом к АС ЦБД УИГ, а также с руководителем ОТЗИ УИАО ФМС России в ЦА ФМС России или с руководителем соответствующего подразделения ОТКЗИ в территориальном органе ФМС России. Согласование осуществляется в форме проставления визы на документе.

В случае, если привилегии доступа необходимы пользователю на непродолжительный период времени (например, для проведения регламентных работ), в заявке должен быть указан срок предоставления доступа.

Доступ пользователям к АС ЦБД УИГ должен предоставляться только после подписания пользователем обязательства о неразглашении сведений конфиденциального характера, хранимых и обрабатываемых в АС ЦБД УИГ.

Права доступа пользователей к АС ЦБД УИГ должны немедленно аннулироваться в случаях:

– истечения срока, на который данные права были предоставлены;

– увольнения сотрудника или перевода на другую должность, не требующую доступа к АС ЦБД УИГ.

Должен быть разработан нормативный правовой акт ФМС России, определяющий порядок предоставления доступа внутренним пользователям к АС ЦБД УИГ. План-проспект данного НПА приведен в Приложении 6.

Права доступа внутренних пользователей к АС ЦБД УИГ могут быть аннулированы в случае выявления нарушений данными лицами требований по обеспечению ИБ, определенных в организационно-нормативных документах ФМС России, законодательных и подзаконных актах по защите информации, нормативно-технических документах ФСБ России и ФСТЭК России.
10.3.3 Регламентация доступа на территорию, в здания и помещения ФМС России

Должна быть обеспечена охрана территорий и зданий, в которых размещены технические средства АС ЦБД УИГ.

Должен быть реализован пропускной режим для допуска на территорию и в здания ФМС России, в которых размещены объекты АС ЦБД УИГ, предусматривающий:

– доступ сотрудников ФМС России по магнитным картам, удостоверениям или иным документам, подтверждающим право доступа;

– доступ посетителей только после предъявления документа, удостоверяющего личность, и только в сопровождении сотрудника ФМС России;

– регистрацию входа и выхода посетителей.

Доступ представителям коммерческих организаций в помещения ФМС России, в которых размещены технические средства АС ЦБД УИГ, для проведения обслуживания технических средств и иных работ, должен предоставляться только после:

1. Подписания представителем организации обязательства о неразглашении сведений конфиденциального характера ФМС России;

2. Подготовки начальником ОТЗИ УИАО ФМС России или подразделения ОТКЗИ соответствующего территориального органа ФМС России справки о допуске представителя коммерческой организации к техническим средствам АС ЦБД УИГ.

В случае невозможности организации пропускного режима (например, если соответствующим подразделением ФМС России ведется прием и работа с гражданами) должны быть приняты иные меры, направленные на предотвращение несанкционированного доступа к техническим средствам АС ЦБД УИГ, по согласованию с ОТЗИ УИАО ФМС России.

Все помещения ФМС России, в которых размещены технические средства АС ЦБД УИГ (сервера, АРМы пользователей, коммутаторы и т. д.), должны быть оснащены замками и средствами сигнализации.

Все серверные помещения должны быть дополнительно оснащены электронными замками и системами видеонаблюдения, позволяющими контролировать все рабочее пространство помещений.

Должен быть составлен перечень лиц, имеющих доступ в серверные помещения. В перечень включаются только те сотрудники, доступ которых необходим для выполнения должностных обязанностей. Перечень должен быть утвержден лицом, ответственным за организацию физической защиты территории, зданий и помещений ФМС России, и
пересматриваться с периодичностью один раз в полгода. Перечни должны быть размещены в местах, доступных для лиц, работающих в серверных помещениях (например, с внутренней стороны дверей).

В каждом помещении, в котором размещены технические средства АС ЦБД УИГ и осуществляется обработка конфиденциальной информации, должен быть назначен ответственный за помещение. По окончании рабочего дня помещения должны сдаваться под охрану ответственными за помещения с включением сигнализации и с отметкой в книге приема и сдачи помещений.

Должен быть разработан нормативный правовой акт ФМС России, определяющий порядок разграничения и управления доступом на территорию, в здания и помещения ФМС России, в которых размещены технические средства АС ЦБД УИГ. План-проспект НПА приведен в Приложении 7.

Подключение пользователей к АС ЦБД УИГ должно осуществляться на основании межведомственного приказа утверждающего порядок регистрации и подключения пользователей и (или) поставщиков сведений.

10.3.4 Регламентация процессов, связанных с эксплуатацией и сопровождением АС ЦБД УИГ

С целью предотвращения рисков информационной безопасности АС ЦБД УИГ в ходе управления и эксплуатации АС ЦБД УИГ необходим постоянный учет вопросов обеспечения ИБ и оценка производимых действий в АС ЦБД УИГ с точки зрения безопасности.

Все изменения в конфигурации АС ЦБД УИГ (установка новых аппаратных или программных компонентов, перемещение компонентов и т. д.) должны проводиться только по согласованию с сотрудниками ОТЗИ УИАО ФМС России в ЦА ФМС России и подразделений ОТКЗИ в территориальных органах ФМС России. Данные лица должны проводить оценку влияния предлагаемых изменений на уровень защиты информации в АС ЦБД УИГ.

Планирование изменений в конфигурации АС ЦБД УИГ должно осуществляться таким образом, чтобы минимизировать возможное негативное влияние на работу пользователей АС ЦБД УИГ.

После проведения изменений в конфигурации АС ЦБД УИГ лицами, проводившими изменения, должна быть выполнена проверка функционирования АС ЦБД УИГ, в том числе проверка работоспособности средств защиты информации.
Конфигурация АС ЦБД УИГ (состав и размещение технических и программных средств) должна быть документирована. При внесении изменений в конфигурацию АС ЦБД УИГ соответствующие изменения должны быть внесены в документацию на АС ЦБД УИГ.

Сотрудниками ОТЗИ УИАО ФМС России и подразделений ОТКЗИ в территориальных органах ФМС России должен проводиться периодический контроль внесения изменений в конфигурацию АС ЦБД УИГ в части отсутствия несанкционированно подключенного оборудования, несанкционированно установленных программных средств и т. д.

Должно обеспечиваться защищенное хранение дистрибутивов программных средств АС ЦБД УИГ и документации на данные средства. Хранение может осуществляться в электронном виде либо на внешних носителях. Должны существовать как минимум две копии всех дистрибутивов и документации, хранимые раздельно. Должны осуществляться периодические проверки работоспособности носителей дистрибутивов.

Должны быть назначены сотрудники, в обязанности которых входит поддержка пользователей: помощь при выявлении ошибок и сбоев в работе технических и программных средств АС ЦБД УИГ, консультации по вопросам эксплуатации АС ЦБД УИГ. Контактная информация данных сотрудников должна быть доведена до всех пользователей АС ЦБД УИГ.

Должны быть разработаны инструкции для всех категорий сотрудников, задействованных в процессах эксплуатации и сопровождении АС ЦБД УИГ, определяющие:

– состав действий по управлению и эксплуатации компонентами АС ЦБД УИГ;
– условия выполнения каждого действия (перечень событий, при наступлении которых необходимо совершить определенное действие, требования к периодичности выполнения операций).

Должен быть разработан нормативный правовой акт ФМС России, определяющий порядок взаимодействия сотрудников ФМС России по вопросам обеспечения ИБ при эксплуатации и сопровождении АС ЦБД УИГ. План-проспект данного НПА приведен в Приложении 8.

10.3.5 Регламентация действий в случае нештатных ситуаций

Должен быть проведен анализ основных нештатных ситуаций, которые могут возникнуть при эксплуатации и сопровождении АС ЦБД УИГ. На основе результатов анализа должен быть определен перечень нештатных ситуаций, которые могут нанести ущерб ФМС России и иным субъектам информационных отношений, возникающих при эксплуатации АС ЦБД УИГ.

Для каждого вида нештатных ситуаций из перечня должны быть определены меры и средства по предотвращению возникновения данных ситуаций, а также действия по
восстановлению работоспособности АС ЦБД УИГ и устранению последствий нештатных ситуаций.

Должен быть разработан нормативный правовой акт ФМС России, определяющий последовательность действий и обязанности сотрудников для всех основных типов нештатных ситуаций и всех категорий сотрудников (пользователь, администратор и т. д.). План-проспект данного НПА ФМС России приведен в Приложении 9. НПА должен в обязательном порядке рассматривать следующие нештатные ситуации:

− пожар в помещениях, в которых размещены технические средства АС ЦБД УИГ;
− прорыв трубопровода;
− нарушение функционирования технических или программных компонентов АС ЦБД УИГ, приводящее к невозможности использования сервисов АС ЦБД УИГ;
− утечка и (или) порча ключевой информации.

Все сотрудники, участвующие в восстановлении работоспособности АС ЦБД УИГ в случае нештатной ситуации, должны быть ознакомлены с НПА в части, их касающейся. С периодичностью не реже чем один раз в год должна осуществляться проверка действий сотрудников при возникновении нештатных ситуаций.

10.3.6 Подготовка персонала в вопросах обеспечения ИБ

Источником ряда актуальных для АС ЦБД УИГ угроз ИБ являются сотрудники ФМС России, реализующие данные угрозы по незнанию или злому умыслу. Для снижения рисков реализации данных угроз необходимо проводить:

− тщательный подбор персонала на должности, связанные с администрированием и сопровождением АС ЦБД УИГ;
− мероприятия по повышению осведомленности пользователей и администраторов АС ЦБД УИГ в вопросах обеспечения ИБ.

Все новые сотрудники, в должностные обязанности которых входит эксплуатация, сопровождение или администрирование АС ЦБД УИГ, должны быть ознакомлены под подпись с организационно-нормативными документами по защите информации в АС ЦБД УИГ в части, их касающейся.

Доступ к сведениям конфиденциального характера АС ЦБД УИГ должен предоставляться сотрудникам ФМС России и представителям коммерческих организаций только после подписания обязательства о неразглашении сведений конфиденциального характера.
Пользователи АС ЦБД УИГ должны обладать знаниями и навыками по использованию программных и технических средств, достаточными для выполнения возложенных на них обязанностей по защите информации в АС ЦБД УИГ. В случае отсутствия у пользователей таких знаний/навыков сотрудниками ОТЗИ УИАО ФМС России и подразделений ОТКЗИ территориальных органов ФМС России должны быть организованы мероприятия по обучению пользователей.

Обучение сотрудников, выполняющих функции по администрированию и сопровождению АС ЦБД УИГ, на курсах по обеспечению ИБ (управление специализированными и встроенными средствами защиты информации, изучение актуальных угроз ИБ, изучение лучших практик по обеспечению ИБ) должно осуществляться на ежегодной основе.

Должны быть документированы требования к подготовке персонала в вопросах обеспечения ИБ, достаточные для выполнения установленных мер и требований по ИБ. Требования должны определяться дифференцированно для различных категорий персонала АС ЦБД УИГ, определенных в п. 10.3.7. Типовой перечень требований приведен в Приложении 10.

10.3.7 Регламентация распределения ролей персонала по доступу к АС ЦБД УИГ

В ЦА ФМС России и в каждом территориальном органе ФМС России должны быть выделены следующие роли персонала по эксплуатации, администрированию и контролю функционирования АС ЦБД УИГ:

1. Администратор АС ЦБД УИГ, осуществляющий:
   – обеспечение функционирования и настройку основных технических средств и систем в составе АС ЦБД УИГ;
   – управление привилегиями доступа пользователей к АС ЦБД УИГ;
   – мониторинг функционирования АС ЦБД УИГ;

2. Администратор информационной безопасности АС ЦБД УИГ, осуществляющий:
   – управление специализированными средствами защиты в составе АС ЦБД УИГ;
   – контроль настроек штатных средств защиты АС ЦБД УИГ (операционных систем, СУБД);
   – контроль привилегий доступа пользователей к АС ЦБД УИГ;
   – анализ журналов регистрации;
   – учет носителей ключевой информации и контроль их использования;

3. Пользователь АС ЦБД УИГ, осуществляющий эксплуатацию АС ЦБД УИГ.
Роли должны быть возложены на конкретных должностных лиц ФМС России. В должностных инструкциях данных лиц должны быть отражены права, обязанности и полномочия по выполнению соответствующих ролей.

Руководителями подразделений должен осуществляться контроль выполнения сотрудниками возложенных на них ролей.

Должен быть разработан нормативный правовой акт ФМС России, определяющий механизмы распределения ролей сотрудников ФМС России по доступу к АС ЦБД УИГ и порядок контроля выполнения сотрудниками предписанных функций. План-проспект НПА приведен в Приложении 11.

10.3.8 Регламентация работы удостоверяющего центра ФМС России

В соответствии с п. 32 «Положения о государственной информационной системе миграционного учета», утвержденного постановлением Правительства Российской Федерации от 14.02.2007 г. № 94, обработка, хранение и обмен электронными документами в АС ЦБД УИГ должны осуществляться с использованием электронной цифровой подписи.

Средства ЭЦП должны основываться на применении криптографических преобразований с использованием закрытых ключей. Криптографические алгоритмы, используемые для формирования ЭЦП, должны соответствовать требованиям законодательства Российской Федерации.

С целью обеспечения административной и технической поддержки использования ЭЦП в ЦА ФМС России должен быть создан удостоверяющий центр, выполняющий следующие основные функции:

− изготовление сертификатов ключей подписей пользователей АС ЦБД УИГ;

− создание ключей ЭЦП по обращению пользователей АС ЦБД УИГ;

− приостановление и возобновление действия сертификатов ключей подписей, а также их аннулирование;

− ведение реестра сертификатов ключей подписей, обеспечение их актуальности и возможности свободного доступа к нему пользователей АС ЦБД УИГ;

− выдача сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии.

− УЦ должен быть сертифицирован в соответствии с временными требованиями к информационной безопасности удостоверяющих центров ФСБ России и аттестован в соответствии
с ГОСТ Р ИСО/МЭК 15408-2002 в системе сертификации средств защиты информации ФСТЭК России.

Должны быть назначены администраторы УЦ из числа сотрудников ОТЗИ УИАО ФМС России, осуществляющие поддержку функционирования УЦ.

Изготовление ключевых документов для пользователей АС ЦБД УИГ и формирование запросов на сертификат может осуществляться администраторами УЦ, сотрудниками подразделений ОТКЗИ территориальных органов ФМС России либо самостоятельно пользователями АС ЦБД УИГ. Администраторам УЦ и сотрудникам подразделений ОТКЗИ должно быть запрещено делать копии и хранить закрытые ключи подписи пользователей АС ЦБД УИГ. Хранение вышедших из эксплуатации сертификатов должно быть организовано в соответствии с регламентом работы Удостоверяющего центра АС ЦБД УИГ.

Регламент работы УЦ АС ЦБД УИГ должен быть согласован с Центром безопасности связи ФСБ России.

В случае прекращения использования ключей ЭЦП должно осуществляться уничтожение информации на носителях ключевой информации.

До предоставления доступа пользователю АС ЦБД УИГ к сервисам УЦ должно быть заключено соглашение между пользователем и УЦ, определяющее:

− обязанности пользователя по защите ключевых носителей и сохранению в тайне паролей доступа к ключевым носителям;

− согласие пользователя считать закрытый ключ своим (в случае если генерацию ключа осуществляли администраторы УЦ либо сотрудники подразделений ОТКЗИ территориальных органов ФМС России).

Хранение ключей подписей должно осуществляться на смарт-картах. Пользователям должно быть запрещено делать неучтенные копии ключевых носителей.

На смарт-карте должны быть указаны следующие идентификационные данные:

− фотоизображение владельца ключевого носителя;

− фамилия имя отчество владельца ключевого носителя;

− должность владельца ключевого носителя;

− учетный номер ключевого носителя (номер карты);

− номер сертификата владельца ключевого носителя;

− дата выпуска электронной цифровой подписи владельца ключевого носителя;
- срок действия сертификата владельца ключевого носителя;
- условные обозначения области допуска к сведениям АС ЦБД УИГ и помещениям ФМС России владельца ключевого носителя если карта имеет в своем составе RFID чип.

Идентификационные данные могут наноситься на тонкий пластик, имеющий клейкую основу. При этом, пластиковое покрытие должно плотно приклеиваться к ключевому носителю.

В случае использования пластикового покрытия на ключевой носитель должна наклеиваться гологрмма, которая должна скреплять ключевой носитель с пластиковым покрытием и разрушаться, при несанкционированном снятии пластикового покрытия.

Ключевой носитель типа смарт-карта должен иметь сертификат ФСТЭК России для использования в автоматизированных системах, обрабатывающих конфиденциальную информацию не содержащей сведений, составляющих государственную тайну.

Должна осуществляться ежегодная смена открытых и закрытых ключей подписей пользователей АС ЦБД УИГ.

В соответствии с постановлением правительства Российской Федерации от 14.02.2007 г. № 94 «О государственной информационной системе миграционного учета», должен быть разработан межведомственный нормативный правовой акт, определяющий состав и порядок действий по управлению, сопровождению и эксплуатации УЦ. План-проект НПА приведен в Приложении 12.

10.4 Технические (программные/программно-аппаратные) меры защиты информации

10.4.1 Требования к средствам идентификации и аутентификации пользователей АС ЦБД УИГ

Все внутренние и внешние пользователи АС ЦБД УИГ, включая сетевых и системных администраторов, администраторов баз данных и т. п., должны иметь уникальный идентификатор для доступа к АС ЦБД УИГ с целью обеспечения контроля выполнения операций пользователями.

Доступ пользователю к АС ЦБД УИГ и ее подсистемам не должен предоставляться без прохождения процедуры аутентификации пользователя. Аутентификация пользователя должна производиться с использованием закрытых ключей, хранение которых осуществляется на смарт-картах.

1 Требования данного раздела не относятся к подсистеме представления общедоступной информации из АС ЦБД УИГ в сеть общего пользования «Интернет». 
Пользовательские пароли должны иметь длину не менее шести символов. Программными средствами должна обеспечиваться невозможность выбора пользователями паролей, не удовлетворяющих установленному ограничению по длине.

10.4.2 Требования к обеспечению информационной безопасности к основным техническим средствам АС ЦБД УИГ расположенным за пределами государственной границы Российской Федерации

В соответствии с Указом Президента Российской Федерации от 22 июня 2006 года № 637 «О мерах по оказанию содействия добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом» на ФМС России возложена задача по учету персональных данных участников Государственной программы по оказанию содействия добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом.

Обеспечение информационной безопасности основных технических средств АС ЦБД УИГ, расположенных за пределами государственной границы Российской Федерации должно осуществляться в соответствии с отдельной моделью угроз и нарушителя согласованной в установленном порядке с СВР России, МИД России, ФСБ России.

Средства криптографической защиты информации должны быть сертифицированы по уровню, предусматривающему защиту информации от иностранных технических разведок.

10.4.3 Требования к средствам разграничения доступа к информационным ресурсам АС ЦБД УИГ

АС ЦБД УИГ должна обеспечивать возможность выбора и назначения пользователям привилегий доступа к информации и сервисам АС ЦБД УИГ.

Контроль доступа пользователей в соответствии с назначенными привилегиями должен осуществляться средствами общего и специального программного обеспечения, поддерживаемого механизмами идентификации и аутентификации пользователей при входе в АС ЦБД УИГ.

Пользователи, администраторы, обслуживающий персонал должны иметь минимально необходимые привилегии на своих АРМ. Пользователям не должны предоставляться права локальных администраторов на АРМ. Все исключения из данного правила должны быть документированы и согласованы с подразделением по защите информации (ОТЗИ УИАО в ЦА ФМС России и подразделениями ОТКЗИ в территориальных органах ФМС России).
Технические процедуры разграничения доступа должны основываться на принципе «запрещено все, что явно не разрешено».

В настоящее время разграничение доступа пользователей к различным частям баз данных АС ЦБД УИГ осуществляется средствами СУБД Oracle на ПАК-Центр и ПАК-Регион. Однако данное ПО не является сертифицированным по требованиям защиты информации. В связи с планируемой аттестацией АС ЦБД УИГ по классу 1Г в системе сертификации средств защиты информации РОСС RU.0001.01БИ00 в дальнейшем должно быть обеспечено разграничение доступа к АС ЦБД УИГ с использованием сертифицированных средств защиты. Возможны следующие пути реализации данного требования:

− проведение сертификации СУБД Oracle ПАК-Центр и ПАК-Регион;
− создание отдельных хранилищ данных для сведений различных уровней конфиденциальности;
− создание защищенной технологии доступа.

10.4.4 Требования к средствам обеспечения и контроля целостности программных и информационных ресурсов АС ЦБД УИГ

Должны применяться средства электронной цифровой подписи для обеспечения целостности электронных документов при их хранении, обработке и передаче по каналам связи в АС ЦБД УИГ.

Применяемые средства ЭЦП должны быть сертифицированы в ФСБ России и основываться на криптографических алгоритмах, определяемых российскими государственными стандартами. При загрузке системы должна осуществляться проверка целостности системных компонентов и успешность загрузки применяемых в АС ЦБД УИГ программных средств защиты информации. Проверка целостности системных компонент должна осуществляться средствами контроля целостности из состава сертифицированных ФСБ России АПМДЗ и встроенными механизмами сертифицированных ФСБ России операционных систем.

Разработка и отладка программных компонентов АС ЦБД УИГ не должна проводиться на серверах и АРМ АС ЦБД УИГ, находящихся в опытной или постоянной эксплуатации. При отладке и тестировании не должны использоваться реальные данные из АС ЦБД УИГ.

Для обеспечения возможности восстановления информационных ресурсов в случае нарушения целостности должно осуществляться резервное копирование ресурсов в соответствии с требованиями раздела 10.4.9.
Должно осуществляться периодическое тестирование работоспособности средств защиты информации в АС ЦБД УИГ. При тестировании должны проводиться попытки преодоления средств защиты информации.

10.4.5 Требования к средствам антивирусной защиты

В соответствии с пунктом 4.2. «Модели угроз информационной безопасности и действий нарушителя АС ЦБД УИГ» в АС ЦБД УИГ должно обеспечиваться активное (сканирование) и пассивное (мониторинг в режиме реального времени) обнаружение вирусов и иного вредоносного ПО на серверах и АРМ пользователей АС ЦБД УИГ (при наличии технических возможностей).

Должна обеспечиваться автоматическая антивирусная проверка всех почтовых сообщений, проходящих через почтовые сервера АС ЦБД УИГ (при наличии технических возможностей).

В случае обнаружения вирусов должно осуществляться лечение или удаление зараженных файлов.

Должны быть предприняты технические меры, направленные на снижение вероятности отключения антивирусных систем.

Должно осуществляться регулярное обновление антивирусных баз. Загрузка обновлений должна осуществляться из Антивирусного центра ФСБ России или источников, определенных соответствующими производителями средств антивирусной защиты, по мере выхода обновлений. Обновление антивирусных баз данных должно осуществляться централизованно от федерального уровня до территориального уровня АС ЦБД УИГ по защищенным линиям связи.

10.4.6 Требования к средствам мониторинга и регистрации событий безопасности

Должна обеспечиваться возможность регистрации следующих событий в АС ЦБД УИГ:

− вход/выход пользователей в АС ЦБД УИГ;
− запуск/завершение программ и процессов;
− попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
− попытки доступа программных средств к АРМ, серверам, внешним устройствам АРМ (принтерам, сканерам и т. д.), каналам связи.

В параметрах регистрации должны указываться:

− дата и время возникновения события;
− идентификатор субъекта доступа (пользователя, программного средства);
– идентификатор объекта доступа (файла, программного средства);
– в случае попытки доступа или запуска программного средства – результат (успешный/неуспешный).

Применяемые средства мониторинга должны основываться на клиент-серверной архитектуре. Серверная часть устанавливается на управляющие сервера в ЦА ФМС России и территориальных органах ФМС России, клиентская часть – на контролируемые сервера и АРМ в подразделениях ФМС России всех уровней.

Средства мониторинга должны предоставлять возможности:
– сбора данных о конфигурации технических и программных средств АС ЦБД УИГ;
– контроля функционирования компонентов АС ЦБД УИГ;
– сбора, хранения и анализа данных о событиях в АС ЦБД УИГ;
– оповещения администратора о критичных событиях в АС ЦБД УИГ.

Применяемые средства мониторинга должны предоставлять возможность централизованного определения параметров мониторинга и сбора информации о произошедших событиях на центральном узле мониторинга.

10.4.7 Требования к ИБ при использовании информационно-аналитической подсистемы АС ЦБД УИГ

Должна обеспечиваться круглосуточная работа информационно-аналитической подсистемы.

ИАП не должна иметь единой точки отказа. ИАП должна реализовываться на основе кластера. В случае сбоя одного из узлов кластера выполнение критичных сервисов ИАП должно автоматически переводиться на другой узел кластера.

Распределение сервисов по узлам кластера должно осуществляться таким образом, чтобы обеспечить равномерную загрузку серверов.

10.4.8 Требования к ИБ при использовании подсистемы хранения данных

Должна обеспечиваться круглосуточная работа ПХД и обеспечение доступа к хранимым данным для других подсистем АС ЦБД УИГ (ИАП, ПВЭП, ПСО, ПМУ и др.)

Архитектура ПХД не должна иметь единой точки отказа. Должно осуществляться дублирование критических для работы подсистемы ресурсов (блоков питания, дисковых массивов и т. д.).
Должно осуществляться регулярное резервное копирование хранимых данных в соответствии с требованиями пункта 10.4.9.

Должно обеспечиваться разграничение доступа к данным ПХД в соответствии с требованиями пункта 10.4.3.

10.4.9 Требования к ИБ при использовании подсистемы резервного копирования и восстановления данных

Должно осуществляться регулярное резервное копирование информационных ресурсов АС ЦБД УИГ. Резервное копирование должно осуществляться автоматически без прекращения работы прикладных задач.

Сотрудниками Информационного центра в ЦА и ИТ-подразделений в территориальных органах ФМС России должны быть разработаны и документированы Планы резервного копирования информационных ресурсов АС ЦБД УИГ, определяющие:

− состав ресурсов, подлежащих резервному копированию;
− время и периодичность резервного копирования;
− методы резервного копирования (применяемые программные и технические средства);
− типы носителей резервных копий.

Периодичность резервного копирования должна определяться на основе анализа возможных последствий от нарушения целостности и доступности ресурсов с учетом частоты модификации ресурсов.

В качестве носителей резервных копий должны использоваться ленточные либо дисковые носители.

Планы резервного копирования должны быть согласованы с соответствующими подразделениями по защите информации (ОТЗИ УИАО в ЦА и подразделениями ОТКЗИ в территориальных органах ФМС России)

Резервные копии информационных ресурсов должны храниться в специально выделенных местах. Уровень защиты резервных копий должен быть не ниже уровня защиты данных и программного обеспечения, которые подвергаются резервному копированию.

Должно быть создано хранилище резервных копий, территориально удаленное от места размещения основных ресурсов АС ЦБД УИГ. В данное хранилище должны помещаться полные резервные копии информации АС ЦБД УИГ ПАК-Центр и ПАК-Регион с периодичностью не реже чем один раз в месяц.
Должно производиться периодическое тестовое восстановление данных из резервных копий с целью контроля корректности восстановления данных и определения времени, затрачиваемого на процедуры восстановления.

Должен быть реализован механизм внесения меток в резервные копии информации ЦБД УИГ, позволяющий в случае утечки информации, хранимой на носителе резервной копии, определить дату создания соответствующей резервной копии.

10.4.10 Требования к ИБ при использовании подсистемы ведомственной электронной почты АС ЦБД УИГ

Передача почтовых сообщений по каналам связи, проходящим по неконтролируемой территории, должна осуществляться в зашифрованном виде. Шифрование данных должно осуществляться на сетевом или прикладном уровнях с использованием сертифицированных ФСБ России средств криптографической защиты информации. При использовании каналов передачи общего пользования СКЗИ должны соответствовать требованиям к средствам криптографической защиты информации по классу не ниже КВ2.

В соответствии с требованиями п. 10.4.5. должна осуществляться антивирусная проверка передаваемых в ПВЭП сообщений.

Должна осуществляться проверка подлинности адресов отправителей писем, посылаемых внутренними пользователями АС ЦБД УИГ.

10.4.11 Требования к ИБ при использовании подсистемы ведомственной телефонной связи АС ЦБД УИГ

Подсистема ведомственной телефонной связи должна быть построена на основе цифровых учрежденческих АТС и цифровых соединительных линий на базе телекоммуникационной инфраструктуры АС ЦБД УИГ с использованием сервисов IP-телефонии.

Должна осуществляться автоматическая регистрация всех вызовов, инициированных в ПВТС.

Должен осуществляться мониторинг функционирования ПВТС. В ЦА ФМС России и территориальных органах ФМС России должны быть назначены сотрудники, ответственные за осуществление мониторинга и устранение неисправностей и сбоев в работе ПВТС.

Должен обеспечиваться контроль того, что сотрудники ФМС России не используются линии связи ПВТС для передачи данных с помощью модема и подключения к сети Интернет.
10.4.12 Требования к ИБ при использовании подсистемы мониторинга и управления

Управляющие сервера в ПМУ должны быть установлены и функционировать на федеральном и региональном уровнях АС ЦБД УИГ. Клиентские компоненты ПМУ должны быть установлены на серверах и АРМ федерального, регионального и территориального уровней АС ЦБД УИГ.

В ЦА ФМС России и всех территориальных органах ФМС России должны быть назначены сотрудники, осуществляющие управление ПМУ и ответственные за разрешение выявленных при мониторинге проблем. В случае невозможности разрешения проблем в территориальном органе информация о проблеме должна передаваться на уровень выше.

В рамках мониторинга в обязательном порядке должны осуществляться регистрация и анализ следующих сведений:

− о запуске и остановке системных сервисов;
− о входе и выходе пользователей (дата, имя сервиса, с использованием которого осуществляется вход/выход);
− о подключенных к АС ЦБД УИГ пользователях;
− о функционировании web-сервисов (имя пользователя, характер обращения, откуда осуществляется подключение, объем переданных данных);
− о сетевых подключениях к серверам в составе АС ЦБД УИГ;
− о текущем состоянии портов;
− о работе системы резервного копирования (дата начала и окончания резервного копирования, статус процесса).

На основе данных мониторинга должен осуществляться анализ первопричин возникновения проблем в функционировании АС ЦБД УИГ.

При использовании ПМУ для автоматизации распространения и установки программного обеспечения должно осуществляться предварительное тестирование данного ПО для проверки отсутствия негативного влияния на работоспособность АС ЦБД УИГ.

Должна быть обеспечена защита журналов регистрации событий от несанкционированного доступа, изменения и удаления. Доступ к журналам должны иметь администраторы ИБ АС ЦБД УИГ.
Администраторам АС ЦБД УИГ должно быть запрещено несанкционированно вносить изменения или очищать содержимое журналов регистрации.

Постоянный либо временный доступ к журналам аудита должен предоставляться сотрудникам ОТЗИ УИАО и подразделений ОТКЗИ территориальных органов ФМС России для осуществления периодического контроля и анализа событий ИБ в АС ЦБД УИГ.

Должна быть обеспечена защита настроек средств мониторинга от несанкционированного изменения.

Выходящие за пределы контролируемой зоны каналы удаленного управления ТКО, используемым в составе АС ЦБД УИГ, должны быть защищены с помощью СКЗИ, сертифицированных ФСБ России по классу не ниже КВ2.

Удаленная модификация программного обеспечения ТКО и системы управления ТКО должна осуществляться с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КС2 (до 2008 и КС3 – после).

Настройки мультипROTокольного оборудования (маршрутизаторов, коммутаторов и т.п.), используемые протоколы передачи данных, управления и маршрутизации и конфигурации ПО ТКО и системы управления ТКО, а также состав средств диагностики и управления ТКО, используемым в составе АС ЦБД УИГ должны быть определены в отдельном документе и, согласованы с Центром безопасности связи ФСБ России.

10.4.13 **Требования к ИБ при использовании подсистемы сервисного обслуживания заявок пользователей АС ЦБД УИГ**

Подсистема сервисного обслуживания заявок пользователей АС ЦБД УИГ должна обеспечивать надежную и своевременную передачу заявок пользователей на разрешение возникающих проблем и решение иных вопросов, связанных с эксплуатацией АС ЦБД УИГ.

В ЦА ФМС России и территориальных органах должны быть назначены лица, ответственные за рассмотрение и реагирование на заявки пользователей. Для каждого типа заявок должны быть определены и документированы требования к времени реакции на заявку.

ПСО должна предоставлять возможность генерации отчетов по заявкам пользователей, отражающих количество заявок различного типа, сформированных за определенный период времени, среднее время регистрации и обработки заявок и иные параметры.

Должен осуществляться регулярный анализ генерируемых отчетов сотрудниками ИЦ, ОТЗИ УИАО, ИТ-подразделений и подразделений ОТКЗИ территориальных органов ФМС России.
с целью планирования мер по предотвращению инцидентов ИБ, повышению надежности функционирования АС ЦБД УИГ и улучшению качества обслуживания пользователей.

10.4.14 Требования к ИБ при использовании подсистемы представления общедоступной информации из АС ЦБД УИГ в сеть общего пользования «Интернет»

Подсистема представления общедоступной информации из АС ЦБД УИГ в сеть общего пользования «Интернет» (web-портал) должна размещаться в открытом сегменте АС ЦБД УИГ и быть физически изолирована от защищенного сегмента АС ЦБД УИГ. Репликация данных между сегментами должна осуществляться сотрудниками ЦА ФМС России. Для информации, подлежащей передаче из защищенного сегмента в открытый сегмент, должна быть обеспечена целостность, достоверность и неотказуемость с применением сертифицированных СКЗИ, предназначенных для использования в системах класса АК3.

Передача сведений из защищенного сегмента АС ЦБД УИГ в web-портал может осуществляться следующими способами:

- на отчуждаемых носителях информации;
- с использованием устройства сопряжения разнокатегорийных сетей (шлюза).

При этом разработка данного устройства (шлюза) для передачи информации в ППНИ АС ЦБД УИГ должна выполняться по отдельному техническому заданию, согласованному с Центром безопасности связи ФСБ России.

Возможность использования данного устройства (шлюза) в ППНИ АС ЦБД УИГ должна подтверждаться соответствующим заключением Центра безопасности связи ФСБ России.

Должен быть определен перечень лиц из числа сотрудников ЦА ФМС России, ответственных за информационное наполнение web-портала (изменение его содержимого). Доступ к web-порталу с привилегиями изменения его содержимого должен предоставляться только указанным лицам. Изменение содержимого web-портала должно осуществляться указанными лицами из сегмента ЛВС ППНИ. При этом не допускается использование сети Интернет или других открытых каналов связи для осуществления указанной деятельности.

Перед использованием web-портала пользователь должен уведомляться о том, что передаваемые ему сведения:

- носят справочных характер;
- будут доставлены по открытым каналам связи;

Базовый реквизитный состав сведений, предоставляемых в web-портал должен быть определен в отдельном документе, согласованным с заказчиками системы и не содержать
сведений ограниченного доступа. Механизм функционирования ППНИ и предоставления сведений в web-портал должен быть в установленном порядке согласован с ФСБ России и ФСТЭК России.
XI УПРАВЛЕНИЕ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Управление системой обеспечения ИБ заключается в целенаправленном воздействии на различные компоненты системы обеспечения ИБ (организационные, технические, программные и пр.) для повышения надежности защиты информации в процессе ее обработки, хранения и передачи.

Цели управления системой обеспечения ИБ определяются в зависимости от этапа жизненного цикла АС ЦБД УИГ.

На этапе создания АС ЦБД УИГ целями управления системой обеспечения ИБ являются:

− организация и координация взаимодействия разработчиков АС ЦБД УИГ, сотрудников ФМС России, ответственных за принятие решения в области защиты информации, с целью планирования оптимальной структуры обеспечения ИБ;

− выработка согласованных решений по организационным, техническим и иным мерам защиты информации, необходимым при эксплуатации, сопровождении и администрировании АС ЦБД УИГ;

На этапе ввода в действие АС ЦБД УИГ целями управления системой обеспечения ИБ являются:

− обеспечение контроля за реализацией предусмотренных на этапе создания АС ЦБД УИГ мер защиты информации и корректностью применения защитных механизмов;

− создание эффективной организационной структуры, обеспечивающей комплексное решение задач ИБ при функционировании АС ЦБД УИГ, в том числе подразделений по защите информации, оснащенных необходимыми программными и техническими средствами управления и контроля.

На этапе эксплуатации АС ЦБД УИГ целями управления системой обеспечения ИБ являются:

− обеспечение реализации предусмотренных на этапе создания АС ЦБД УИГ требований и мер обеспечения ИБ;

− пресечение и выявление инцидентов ИБ, связанных с эксплуатацией и сопровождением АС ЦБД УИГ;

− своевременное выявление изменений в актуальных угрозах ИБ и совершенствование системы обеспечения ИБ.
Управление системой обеспечения ИБ заключается в реализации комплекса информационных, управляющих и вспомогательных функций.

Информационные функции направлены на контроль состояния системы защиты АС ЦБД УИГ и включают:

– проверку соответствия системы обеспечения ИБ предъявленным к ней требованиям, зафиксированным в организационно-нормативных документах ФМС России по защите информации, а также установленным при аттестации АС ЦБД УИГ;

– информирование лиц, ответственных за координацию и реализацию мер защиты в АС ЦБД УИГ, о возникновении в АС ЦБД УИГ событий, способных привести к нарушению ИБ.

Управляющие функции направлены на поддержку и совершенствование системы обеспечения ИБ АС ЦБД УИГ и включают:

– планирование процедур по эксплуатации, администрированию и сопровождению АС ЦБД УИГ с учетом требований по защите информации;

– выявление уязвимостей в АС ЦБД УИГ и их оперативное устранение;

– учет, хранение и выдачу ключей, паролей, ключевых носителей;

– администрирование и сопровождение средств разграничения доступа и иных средств защиты.

Реализуются также вспомогательные функции, к которым относятся:

– учет всех операций, выполняемых в АС ЦБД УИГ с защищаемой информацией;

– формирование отчетных документов и сбор статистических данных по происходящих в АС ЦБД УИГ событиям с целью анализа и выявления потенциальных каналов утечки информации.

Реализацию информационных, управляющих и вспомогательных функций обеспечивают:

– в ЦА ФМС России – сотрудники ОТЗИ УИАО ФМС России и сотрудники Информационного центра;

– в территориальном органе – сотрудники подразделения ОТКЗИ и ИТ-подразделения территориального органа.

Распределение информационных, управляющих и вспомогательных функций между сотрудниками указанных подразделений осуществляется в соответствии с приведенным в разделе IX перечнем обязанностей данных сотрудников по защите информации АС ЦБД УИГ. Установленные функции, обязанности и полномочия сотрудников в части управления системой
обеспечения ИБ должны быть документированы в должностных инструкциях сотрудников и положениях о подразделениях.
XII  АНАЛИЗ РИСКОВ

В основе планирования и реализации мер обеспечения ИБ в АС ЦБД УИГ должен лежать подход, основанный на анализе рисков реализации угроз ИБ. Такой подход предусматривает проведение регулярной оценки рисков ИБ и принятие мер по снижению рисков до приемлемого уровня.

Для создания методической базы проведения анализа рисков сотрудниками ОТЗИ УИАО ФМС России либо внешними подрядными организациями должна быть разработана методика анализа рисков ИБ, определяющая:

− процедуры идентификации и классификации активов ФМС России;
− критерии категорирования угроз и уязвимостей;
− правила вычисления значений рисков;
− критерии обработки рисков;
− распределение функций и ответственности сотрудников ФМС России по проведению анализа и оценки рисков.

При разработке методики должен быть проведен предварительный анализ уже существующих методик анализа рисков (в том числе методик, предусматривающих применение средств автоматизации процесса анализа рисков) с точки зрения возможности и целесообразности их применения в ФМС России.

Аналит рисков должен проводиться ежегодно на основе разработанной Методики силами ОТЗИ УИАО ФМС России и подразделениями ОТКЗИ территориальных органов ФМС России или с привлечением внешнего исполнителя. Анализ должен также осуществляться при проведении существенных изменений в АС ЦБД УИГ. Ответственность за организацию проведения анализа рисков должна быть возложена на ОТЗИ УИАО ФМС России.

Работы по проведению анализа и оценки рисков должны предусматривать следующие этапы:

− определение активов, рассматриваемых в рамках процесса анализа рисков;
− определение ценности активов;
− определение угроз, направленных на данные активы;
− вычисление рисков на основе полученных оценок угроз и уязвимостей и ценности актива;
− выбор защитных мер, направленных на снижение рисков;
– вычисление планируемых остаточных рисков после применения защитных мер.

По результатам анализа рисков должны быть оформлены следующие отчетные документы:
– «Перечень защищаемых активов»;
– «Отчет об оценке рисков»;
– «План обработки рисков».

«Перечень защищаемых активов» должен быть утвержден руководством ФМС России и доведен до сведения лиц, использующих данные активы при эксплуатации, администрировании или сопровождении АС ЦБД УИГ.

План-проспекты отчетных документов приведены в Приложениях 13-15.
**XIII ПРЕДСТАВЛЕНИЕ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ ИЗ АС ЦБД УИГ В СЕТЬ ОБЩЕГО ПОЛЬЗОВАНИЯ «ИНТЕРНЕТ»**

Должны быть назначены лица, ответственные за информационное наполнение web-портала, из числа сотрудников ЦА ФМС России. Данные лица должны осуществлять контроль того, что:

− размещаемая на web-портале информация достоверна;

− информация не содержит персональных данных;

− предоставление информации в сеть общего пользования «Интернет» не должно нарушать какие-либо требования законодательства Российской Федерации и договорных обязательств ФМС России, в том числе требования по обеспечению конфиденциальности информации и защите авторских прав.

Действия администраторов по изменению содержания web-портала должны осуществляться только по согласованию с ответственными лицами.

Должен быть разработан нормативный правовой акт ФМС России, определяющий порядок представления общедоступной информации из АС ЦБД УИГ в сеть общего пользования «Интернет», в том числе:

− реквизитный состав размещаемой на web-портале информации;

− требования к периодичности обновления информации;

− распределение обязанностей должностных лиц ЦА ФМС России по подготовке, согласованию и публикации информации на web-портале.

Технические меры обеспечения ИБ при предоставлении общедоступной информации из АС ЦБД УИГ должны соответствовать требованиям раздела 10.4.12.
XIV СИСТЕМА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ

Под мониторингом ИБ понимается процесс регулярного (периодического) или постоянного наблюдения за событиями ИБ в АС ЦБД УИГ с целью своевременного выявления и реагирования на действия, которые привели либо могут привести к реализации угроз ИБ.

Мониторинг событий ИБ должен включать:
− мониторинг сетевой активности;
− мониторинг событий доступа к защищаемым информационным ресурсам АС ЦБД УИГ;
− мониторинг системной активности;
− мониторинг сбоев в работе АС ЦБД УИГ;
− мониторинг содержания потоков информации (в частности, контроль отсутствия вирусов в электронных почтовых сообщениях).

В ЦА ФМС России и каждом территориальном органе ФМС России должен быть определен и документирован перечень параметров функционирования АС ЦБД УИГ, подлежащих мониторингу. Для всех параметров должны быть определены значения/диапазоны значений, свидетельствующие:

1. О нормальном функционировании АС ЦБД УИГ;
2. Об угрозе возникновения нештатной ситуации или инцидента ИБ (например, если зафиксированные параметры свидетельствуют о высокой загрузке аппаратных компонентов АС ЦБД УИГ);
3. О возникновении нештатной ситуации или инцидента ИБ.

Перечень параметров, подлежащих мониторингу, а также допустимые значения параметров должны быть согласованы с ОТЗИ УИАО в ЦА и подразделениями ОТКЗИ в территориальных органах ФМС России.

Состав действий администраторов при выявлении отклонений в значениях параметров должен быть документирован в инструкциях по управлению и эксплуатации компонентов АС ЦБД УИГ (в соответствии с п. 10.3.4), а также в НПА ФМС России, определяющем порядок действий при возникновении нештатной ситуации в АС ЦБД УИГ (в соответствии с п. 10.3.5).

Администраторы АС ЦБД УИГ и администраторы ИБ АС ЦБД УИГ должны осуществлять сбор и обобщение информации о фактах выхода параметров мониторинга за пределы нормы для
своевременного планирования мер по предотвращению инцидентов ИБ и нештатных ситуаций, увеличению производительности АС ЦБД УИГ и т. д.

Администраторы АС ЦБД УИГ и администраторы ИБ АС ЦБД УИГ по запросу сотрудников ОТЗИ УИАО и подразделений ОТКЗИ территориальных органов ФМС России должны предоставлять собранные данные по фактам выходам параметров мониторинга за установленные диапазоны.

Факты выявления нештатных ситуаций и инцидентов ИБ в рамках мониторинга должны документироваться соответствующими администраторами АС ЦБД УИГ с указанием:

– выявленных значений параметров мониторинга;
– причин возникновения нештатной ситуации или инцидента ИБ;
– предпринятых действий по устранению последствий нештатной ситуации или инцидента ИБ.

Отчеты об инцидентах ИБ и нештатных ситуациях должны предоставляться сотрудникам ОТЗИ УИАО в ЦА ФМС России и подразделений ОТКЗИ в территориальных органах ФМС России.

Должен быть разработан нормативно-правовой акт ФМС России, определяющий порядок расследования инцидентов ИБ, возникающих в АС ЦБД УИГ. НПА должен определять:

– распределение ролей между должностными лицами подразделений системы ФМС России по организации и проведению расследований инцидентов ИБ;
– требования к формированию доказательной базы по инцидентам ИБ в соответствии с требованиями законодательства Российской Федерации.
XV АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ

С целью обеспечения контроля за состоянием системы ИБ АС ЦБД УИГ должен проводиться периодический аудит информационной безопасности АС ЦБД УИГ. Целями аудита ИБ являются:

− проверка выполнения требований, мер и процедур по обеспечению ИБ в АС ЦБД УИГ, определяемых настоящей Концепцией, иными организационно-нормативными документами ФМС России по защите информации, а также законами, подзаконными актами и нормативно-техническими документами ФСБ России и ФСТЭК России;

− оценка защищенности АС ЦБД УИГ от угроз ИБ.

Аудит ИБ должен проводиться не реже чем один раз в год и охватывать как ЦА ФМС России, так и (выборочно) территориальные органы ФМС России.

Ответственность за организацию и координацию работ по аудиту ИБ АС ЦБД УИГ должна быть возложена на ОТЗИ УИАО ФМС России. Исполнителем работ по аудиту могут являться сотрудники ОТЗИ УИАО ФМС России (внутренний аудит) либо внешние исполнители (внешний аудит). В качестве внешних исполнителей выступают независимые эксперты по информационной безопасности.

Работы по аудиту должны проводиться на основе предварительно разработанного плана аудита, определяющего:

− границы аудита (состава технических, программных компонентов, информационных ресурсов АС ЦБД УИГ и категорий персонала, подлежащих проверке);

− перечень лиц, участвующих в проведении аудита, с указанием функций данных лиц по аудиту;

− методы и механизмы проведения аудита;

− сроки проведения аудита.

План аудита должен быть согласован с руководителем УИАО и утвержден руководством ЦА или соответствующего территориального органа ФМС России.

В ходе аудита должны применяться различные методы и механизмы получения информации, такие как:

− использование специализированного ПО для выявления несанкционированных изменений в конфигурации программных и технических средств АС ЦБД УИГ;

− использование разного рода инструментов визуального просмотра и экспертизы программного обеспечения и технических средств АС ЦБД УИГ;
− использование специализированного ПО для анализа журналов регистрации событий безопасности, анализа защищенности серверов;

− ручная проверка конфигурации программных и технических средств (визуальная проверка без применения специализированных средств анализа конфигурации);

− экспертиза (изучение) организационно-нормативной, проектной и эксплуатационной документации на АС ЦБД УИГ;

− наблюдение, визуальный осмотр.

Аудиторам должны быть предоставлены привилегии доступа к ресурсам АС ЦБД УИГ, достаточные для выполнения работ в соответствии с утвержденным планом аудита. Доступ аудиторов к техническим средствам АС ЦБД УИГ должен осуществляться в присутствии лиц, ответственных за данные средства.

По результатам аудита должен быть составлен отчет об аудите, содержащий описание проделанной работы, выводы по результатам аудита и рекомендации по устранению выявленных в ходе аудита несоответствий. Отчет об аудите должен быть предоставлен на ознакомление руководству ФМС России.
XVI ПОРЯДОК АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ АС ЦБД УИГ

Программно-аппаратные комплексы, входящие в состав АС ЦБД УИГ, территориально распределены и находятся в подразделениях ФМС России различных уровней. В связи с этим проведение аттестации всех объектов информатизации АС ЦБД УИГ потребует значительных временных затрат специалистов, проводящих аттестацию, и, следовательно, существенных финансовых затрат. Для снижения затрат, связанных с проведением аттестации объектов автоматизации АС ЦБД УИГ, должно быть создано специальное структурное подразделение в ЦА ФМС России, имеющее право аттестации объектов информатизации. Создание такого подразделения позволит:

– сократить материальные затраты, связанные с проведением аттестации объектов информатизации (поскольку исчезнет необходимость привлечения сторонних организаций для проведения аттестации);

– упростить процедуры взаимодействия лиц, инициирующих проведение аттестации, с аттестующим органом.

Кроме того, по мере дальнейшего развития информационных технологий в ФМС России создаваемое подразделение сможет осуществлять аттестацию новых внедряемых автоматизированных систем.

До начала деятельности по аттестации объектов информатизации подразделение ФМС России должно получить аттестат аккредитации ФСТЭК России на право аттестации объектов информатизации в системе сертификации средств защиты информации РОСС RU.0001.01БИ00.

Проведение выделенным подразделением аттестации объекта информатизации АС ЦБД УИГ должно осуществляться в соответствии со следующим общим порядком:

1. Принятие решения руководством ФМС России о проведении аттестации объекта информатизации;

2. Создание аттестационной комиссии для подготовки и проведения аттестации;

3. Предварительное ознакомление аттестующего подразделения с объектом информатизации;

4. Разработка аттестующим подразделением программы и методики проведения аттестационных испытаний;

5. Проведение аттестационных испытаний объекта информатизации в соответствии с разработанными программой и методикой;

6. Подготовка аттестующим подразделением протоколов испытаний;
7. Подготовка аттестующим подразделением заключения по результатам аттестационных испытаний, содержащего:

− вывод о возможности (или невозможности) выдачи аттестата соответствия;
− перечень выявленных недостатков и несоответствий (если недостатки или несоответствия имеются);
− рекомендации по устранению выявленных недостатков и несоответствий;

8. Выдача аттестата соответствия (в случае положительного заключения по результатам аттестационных испытаний).

В ходе аттестационных испытаний должны осуществляться следующие мероприятия:

− проверка соответствия представленных исходных данных реальным условиям размещения, монтажа и эксплуатации средств вычислительной техники объекта информатизации;
− проверка состояния организации работ и выполнения организационных и технических требований по защите информации;
− оценка правильности классификации объекта информатизации;
− оценка полноты и уровня разработки организационно-нормативной, проектной и эксплуатационной документации, оценка уровня подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации;
− испытания технических средств объекта информатизации, отдельных средств и систем защиты на соответствие требованиям по защите информации от НСД.

На подразделение по аттестации, помимо проведения аттестационных испытаний, должно быть также возложено осуществление периодического контроля за эксплуатацией аттестованных объектов информатизацией на предмет соблюдения установленных требований по защите информации.
Реализация Концепции должна осуществляться на основе утвержденных конкретных программ и планов, которые уточняются с периодичностью один раз в полгода с учетом:

− новых требований законов Российской Федерации, подзаконных актов в области защиты информации, нормативно-технических документов ФСБ России и ФСТЭК России, а также организационно-нормативных документов ФМС России по вопросам обеспечения ИБ;

− реальных потребностей в средствах защиты информации;

− объемов финансирования, выделяемых на защиту информации АС ЦБД УИГ.

Перечень первоочередных мероприятий, направленных на реализацию настоящей Концепции, приведен в Табл. 1. Проведение данных мероприятий может быть возложено на внешнего исполнителя либо осуществляться силами ОТЗИ УИАО ФМС России и подразделений ОТКЗИ территориальных органов ФМС России с привлечением администраторов АС ЦБД УИГ, администраторов информационной безопасности АС ЦБД УИГ и иных специалистов. Сроки, необходимые для реализации мероприятий, и финансовые затраты определяются при разработке более конкретных программ и планов по согласованию с выбранным исполнителем работ.

Табл. 1. Перечень мероприятий

<table>
<thead>
<tr>
<th>№</th>
<th>Наименование мероприятия</th>
<th>Комментарии</th>
<th>Ссылки1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Разработка комплекса организационно-нормативных документов по защите информации АС ЦБД УИГ первого уровня</td>
<td>Должны быть разработаны НПА ФМС России, определяющие: регламент работы удостоверяющего центра ФМС России</td>
<td>п. 10.3.8, Приложение 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>требования к подготовке персонала в вопросах обеспечения информационной безопасности</td>
<td>п. 10.3.6, Приложение 10</td>
</tr>
</tbody>
</table>

1 Приводятся ссылки на пункты Концепции, в соответствии с требованиями которых должна осуществляться реализация мероприятий
<table>
<thead>
<tr>
<th>№</th>
<th>Наименование мероприятия</th>
<th>Комментарии</th>
<th>Ссылки</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>порядок предоставления открытой информации в сеть общего пользования «Интернет»</td>
<td>п. XIII</td>
<td></td>
</tr>
<tr>
<td></td>
<td>методику анализа рисков информационной безопасности</td>
<td>п. XIII</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Разработка комплекса организационно-нормативных документов по защите информации АС ЦБД УИГ второго уровня для ЦА ФМС России</td>
<td>Должны быть разработаны НПА ФМС России, действие которых распространяется на ЦА ФМС России, определяющие:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>порядок предоставления доступа внутренним пользователям к ресурсам АС ЦБД УИГ</td>
<td>п. 10.3.1, Приложение 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>порядок разграничения и управления доступом на территорию, в здания и помещения ФМС России</td>
<td>п. 10.3.3, Приложение 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>порядок проведения эксплуатации, обслуживания, ремонта и модификации аппаратных и программных ресурсов АС ЦБД УИГ</td>
<td>п. 10.3.4, Приложение 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>порядок действий при возникновении нештатной ситуации в АС ЦБД УИГ</td>
<td>п. 10.3.5, Приложение 9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>механизмы распределения ролей сотрудников ФМС России по доступу к АС ЦБД УИГ</td>
<td>п. 10.3.6, Приложение 11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>инструкции по эксплуатации, администрированию и сопровождению компонентов АС ЦБД УИГ</td>
<td>п. 10.3.4</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Разработка комплекса организационно-нормативных документов по защите</td>
<td>Должны быть разработаны следующие документы для территориальных органов ФМС России:</td>
<td></td>
</tr>
<tr>
<td>№</td>
<td>Наименование мероприятия</td>
<td>Комментарии</td>
<td>Ссылки</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>информации АС ЦБД УИГ второго уровня для всех территориальных органов ФМС России</td>
<td>порядок предоставления доступа внешним пользователям к ресурсам АС ЦБД УИГ</td>
<td>п. 10.3.1, определяется в соответствии с постановлением Правительства Российской Федерации от 14.02.2007 № 94.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>порядок предоставления доступа внутренним пользователям к ресурсам АС ЦБД УИГ</td>
<td>10.3.2, Приложение 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>порядок разграничения и управления доступом на территорию, в здания и помещения ФМС России</td>
<td>п. 10.3.3, Приложение 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>порядок проведения эксплуатации, обслуживания, ремонта и модификации аппаратных и программных ресурсов АС ЦБД УИГ</td>
<td>п. 10.3.4, Приложение 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>порядок действий при возникновении нештатной ситуации в АС ЦБД УИГ</td>
<td>п. 10.3.5, Приложение 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>механизмы распределения ролей сотрудников ФМС России по доступу к АС ЦБД УИГ</td>
<td>п. 10.3.6, Приложение 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>инструкции по эксплуатации, администрированию и сопровождению компонентов АС ЦБД УИГ</td>
<td>п. 10.3.4</td>
</tr>
<tr>
<td>№</td>
<td>Наименование мероприятия</td>
<td>Комментарии</td>
<td>Ссылки</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 4. | Внедрение в ЦА ФМС России и территориальных органах ФМС России разработанного комплекса документов | Должны осуществляться:  
  − возложение ролей администратора АС ЦБД УИГ и администратора ИБ АС ЦБД УИГ на конкретных должностных лиц;  
  − ознакомление сотрудников с разработанным комплектом организационно-нормативных документов;  
  − внедрение определяемых документами процедур по эксплуатации, администрированию и сопровождению АС ЦБД УИГ | пп. 10.3.6, 10.3.7 |
| 5. | Развертывание в ЦА ФМС России удостоверяющего центра                                       | Должны быть проведены:  
  − назначение администраторов УЦ;  
  − установка и настройка программных и технических компонентов УЦ;  
  − создание службы доставки ключей ЭЦП;  
  − разработка регламента УЦ и его согласование с ФСБ России;  
  − сертификация УЦ по требованиям ФСБ России;  
  − аттестация УЦ по требованиям ФСТЭК России. | п. 10.3.8 |
<table>
<thead>
<tr>
<th>№</th>
<th>Наименование мероприятия</th>
<th>Комментарии</th>
<th>Ссылки¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Создание в ЦА ФМС России подразделения, имеющего право аттестации объекта информатизации</td>
<td>Должны быть проведены: &lt;br&gt;− разработка организационно-распорядительной документации, регулирующей вопросы функционирования данного подразделения; &lt;br&gt;− получение подразделением ФМС России аттестата аккредитации ФСТЭК России на право аттестации объектов информатизации</td>
<td>п. XVI</td>
</tr>
<tr>
<td>7.</td>
<td>Подготовка и проведение аттестации объектов информатизации АС ЦБД УИГ по классу защищенности 2Б</td>
<td></td>
<td>п. XVI</td>
</tr>
<tr>
<td>8.</td>
<td>Проведение анализа рисков в соответствии с разработанной методикой анализа рисков</td>
<td></td>
<td>п. XII</td>
</tr>
<tr>
<td>9.</td>
<td>Разработка и реализация в АС ЦБД УИГ механизма внесения меток в резервные копии информации АС ЦБД УИГ</td>
<td></td>
<td>п. 10.4.9</td>
</tr>
<tr>
<td>10.</td>
<td>Реализация системы разграничения доступа в АС ЦБД УИГ с использованием сертифицированных ФСТЭК России средств защиты информации</td>
<td></td>
<td>п. 10.4.3</td>
</tr>
<tr>
<td>11.</td>
<td>Подготовка и проведение аттестации объектов информатизации АС ЦБД УИГ по классу защищенности 1Г</td>
<td></td>
<td>п. XVI</td>
</tr>
</tbody>
</table>

¹ Ссылки на нормативные документы.
<table>
<thead>
<tr>
<th>№</th>
<th>Наименование мероприятия</th>
<th>Комментарии</th>
<th>Ссылки&lt;sup&gt;1&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Проведение тематических исследований по оценки корректности встраивания СКЗИ в СПО АС ЦБД и экспертиза проведенных исследований Центром безопасности связи ФСБ России</td>
<td></td>
<td>П. 10.4.1.</td>
</tr>
<tr>
<td>13</td>
<td>Проведение работ по установке криптосредств и создание органов криптозащиты</td>
<td></td>
<td>П. 10.4.1.</td>
</tr>
</tbody>
</table>
| 14 | Проведение работ по настройке подсистемы мониторинга и управления. Настройка ТКО. | Должны быть проведены:  
- разработка порядка, определяющего настройки мультипротокольного оборудования (маршрутизаторов, коммутаторов и т.п.), используемые протоколы передачи данных, управления и маршрутизации и конфигурации ПО ТКО и системы управления ТКО, а также состав средств диагностики и управления ТКО, используемым в составе АС ЦБД УИГ должны быть определены в отдельном документе;  
- согласование порядка с Центром безопасности связи ФСБ России. | П. 10.4.11 |
ПРИЛОЖЕНИЕ 1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

<table>
<thead>
<tr>
<th>АРМ</th>
<th>Автоматизированное рабочее место</th>
</tr>
</thead>
<tbody>
<tr>
<td>АС</td>
<td>Автоматизированная система</td>
</tr>
<tr>
<td>Гостехкомиссия</td>
<td>Государственная техническая комиссия при Президенте Российской Федерации</td>
</tr>
<tr>
<td>РОССИИ</td>
<td>Федерации</td>
</tr>
<tr>
<td>АТС</td>
<td>Автоматическая телефонная станция</td>
</tr>
<tr>
<td>ИАП</td>
<td>Информационно-аналитическая подсистема</td>
</tr>
<tr>
<td>ИБ</td>
<td>Информационная безопасность</td>
</tr>
<tr>
<td>Иностранные</td>
<td>Иностранные граждане и лица без гражданства, находящиеся в Российской Федерации</td>
</tr>
<tr>
<td>ИТ</td>
<td>Информационные технологии</td>
</tr>
<tr>
<td>ЛВС</td>
<td>Локальная вычислительная сеть</td>
</tr>
<tr>
<td>МВД России</td>
<td>Министерство внутренних дел Российской Федерации</td>
</tr>
<tr>
<td>МИД России</td>
<td>Министерство иностранных дел Российской Федерации</td>
</tr>
<tr>
<td>Минздравсоцразвития</td>
<td>Министерство здравоохранения и социального развития Российской Федерации</td>
</tr>
<tr>
<td>Мининформсвязи</td>
<td>Министерство информационных технологий и связи Российской Федерации</td>
</tr>
<tr>
<td>Минобороны России</td>
<td>Министерство обороны Российской Федерации</td>
</tr>
<tr>
<td>Минобрнауки России</td>
<td>Министерство образования и науки Российской Федерации</td>
</tr>
<tr>
<td>Минтранс России</td>
<td>Министерство транспорта Российской Федерации</td>
</tr>
<tr>
<td>Минэкономразвития</td>
<td>Министерство экономического развития и торговли Российской Федерации</td>
</tr>
<tr>
<td>МЧС России</td>
<td>Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий</td>
</tr>
<tr>
<td>НПА</td>
<td>Нормативно-правовой акт</td>
</tr>
<tr>
<td>НСД</td>
<td>Несанкционированный доступ</td>
</tr>
<tr>
<td>Сокращение</td>
<td>Полное название</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>ОПО</td>
<td>Общее программное обеспечение</td>
</tr>
<tr>
<td>ОС</td>
<td>Операционная система</td>
</tr>
<tr>
<td>ОТЗИ</td>
<td>Отдел технической защиты информации</td>
</tr>
<tr>
<td>ПАК</td>
<td>Программно-аппаратный комплекс</td>
</tr>
<tr>
<td>ПАК-Регион</td>
<td>Региональный уровень АС ЦБД УИГ</td>
</tr>
<tr>
<td>ПАК-Центр</td>
<td>Федеральный уровень АС ЦБД УИГ</td>
</tr>
<tr>
<td>ПВЭП</td>
<td>Подсистема ведомственной электронной почты</td>
</tr>
<tr>
<td>ПВТС</td>
<td>Подсистема ведомственной телефонной связи</td>
</tr>
<tr>
<td>ПИБ</td>
<td>Подсистема информационной безопасности</td>
</tr>
<tr>
<td>ПК</td>
<td>Программный комплекс</td>
</tr>
<tr>
<td>ПКЗИ</td>
<td>Подсистема криптографической защиты информации</td>
</tr>
<tr>
<td>ПМУ</td>
<td>Подсистема мониторинга и управления</td>
</tr>
<tr>
<td>ПО</td>
<td>Программное обеспечение</td>
</tr>
<tr>
<td>Подразделение</td>
<td>Подразделение, ответственное за организацию технической и криптографической защиты информации</td>
</tr>
<tr>
<td>ППНИ</td>
<td>Подсистема представления неконфиденциальной информации ЦБД УИГ в сети общего пользования «Интернет»</td>
</tr>
<tr>
<td>ПРКВД</td>
<td>Подсистема резервного копирования и восстановления данных</td>
</tr>
<tr>
<td>ПСО</td>
<td>Подсистема сервисного обслуживания заявок</td>
</tr>
<tr>
<td>ПХД</td>
<td>Подсистема хранения данных</td>
</tr>
<tr>
<td>РД</td>
<td>Руководящий документ</td>
</tr>
<tr>
<td>СПО</td>
<td>Специальное программное обеспечение</td>
</tr>
<tr>
<td>СУБД</td>
<td>Система управления базами данных</td>
</tr>
<tr>
<td>ТКО</td>
<td>телекоммуникационное оборудование</td>
</tr>
<tr>
<td>УИАО</td>
<td>Управление по вопросам информационно-аналитического обеспечения</td>
</tr>
<tr>
<td>УЦ</td>
<td>Удостоверяющий центр</td>
</tr>
<tr>
<td>ФАПСИ</td>
<td>Федеральное агентство правительственной связи и информации при Президенте Российской Федерации</td>
</tr>
<tr>
<td>Сокращение</td>
<td>Полное наименование</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>ФМС России</td>
<td>Федеральная миграционная служба</td>
</tr>
<tr>
<td>ФОИВ</td>
<td>Федеральные органы исполнительной власти</td>
</tr>
<tr>
<td>ФСБ России</td>
<td>Федеральная служба безопасности Российской Федерации</td>
</tr>
<tr>
<td>ФСКН России</td>
<td>Федеральная служба Российской Федерации по контролю за оборотом наркотиков</td>
</tr>
<tr>
<td>ФСТЭК России</td>
<td>Федеральная служба по техническому и экспортному контролю</td>
</tr>
<tr>
<td>ЦА</td>
<td>Центральный аппарат ФМС России</td>
</tr>
<tr>
<td>ЦБД УИГ</td>
<td>Центральный банк данных по учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации, в том числе участников Государственной программы по оказанию содействия добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом</td>
</tr>
<tr>
<td>ЭЦП</td>
<td>Электронная цифровая подпись</td>
</tr>
<tr>
<td>АПМДЗ</td>
<td>Аппаратно-программный модуль доверенной загрузки</td>
</tr>
</tbody>
</table>
ПРИЛОЖЕНИЕ 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 г. № 282).

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности (Руководящий документ (РД) Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термы и определения»).

Безопасность информации — состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз (РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термы и определения»).

Владелец сертификата ключа подписи — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы) (Федеральный закон от 10.01.2002 г. №1-ФЗ «Об электронной цифровой подписи»).

Доступ к информации — возможность получения информации и ее использования (Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Закрытый ключ электронной цифровой подписи — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи (Федеральный закон от 10.01.2002 г. №1-ФЗ «Об электронной цифровой подписи»).

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термы и определения»).
Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока (Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»). Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию (Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»). Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации) (Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»). Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами (РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения»). Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных (Федеральный закон Российской от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом (РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения»).
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 (Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»).

Средство криптографической защиты информации — 1) Реализующие криптографические алгоритмы преобразования информации, аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи включая СКЗИ; 2) Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; 3) Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; 4) Аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации (Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»).

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее (ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»).


Целостность информации — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения) (РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения»).
Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (Федеральный закон от 10.01.2002 г. №1-ФЗ «Об электронной цифровой подписи»).

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме (Федеральный закон от 10.01.2002 г. №1-ФЗ «Об электронной цифровой подписи»).
ПРИЛОЖЕНИЕ 3. НОРМАТИВНАЯ ПРАВОВАЯ БАЗА РАЗРАБОТКИ КОНЦЕПЦИИ

Нормативную правовую базу разработки и обеспечения функционирования АС ЦБД УИГ в области обеспечения ИБ составляют следующие документы:

1. Законы и подзаконные акты, устанавливающие требования по защите информации в Российской Федерации, в том числе:


– Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон Российской Федерации от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи»;


1 Собрание законодательства Российской Федерации, 2005, № 52 (1 ч.), ст. 5573.
2 Собрание законодательства Российской Федерации, 2006, № 31 (1 ч.), ст. 3448.
3 Собрание законодательства Российской Федерации, 2006, № 31 (1 ч.), ст. 3451.
5 Собрание законодательства Российской Федерации, 2006, № 30, ст. 3285.
7 Собрание законодательства Российской Федерации, 2002, № 52 (1 ч.), ст. 5140; 2005, № 19, ст. 1752.
– Указ Президента Российской Федерации от 12.05.2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»

– Указ Президента Российской Федерации от 3 марта 2006 г. № 175 «О внесении изменений в Указ Президента Российской Федерации от 12 мая 2004 г. № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

– Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;

– Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Постановление Правительства Российской Федерации от 15.08.2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;

– Постановление Правительства Российской Федерации от 23.09.2002 г. № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

2. Подзаконные акты, регламентирующие вопросы функционирования АС ЦБД УИГ, а также устанавливающие функции и полномочия ФМС России по обеспечению эксплуатации АС ЦБД УИГ:

– Указ Президента Российской Федерации от 19.07.2004 г. № 928 «Вопросы Федеральной миграционной службы»;

– Постановление Правительства Российской Федерации от 06.04.2005 г. № 186 «Об утверждении Положения о создании, ведении и использовании центрального банка данных по


4 Собрание законодательства Российской Федерации, 2006, № 34, ст. 3691.

5 Собрание законодательства Российской Федерации, 2002, № 39, ст. 3792.

учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации»1;

– Постановление Правительства Российской Федерации от 14.02.2007 г. № 94 «О государственной информационной системе миграционного учета»2;

– Приказ МВД России, МИД России, ФСБ России, Минэкономразвития России и Мининформсвязи России от 10.03.2006 г. № 148/2562/98/62/25 «О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации»3;


1 Собрание законодательства Российской Федерации, 2005, № 15, ст. 1348.
2 Собрание законодательства Российской Федерации, 2007, №8 (1 ч.), ст. 1012.
3 Зарегистрирована в Министерстве юстиции Российской Федерации 31 марта 2006 г., регистрационный № 7652
ПРИЛОЖЕНИЕ 4. НОРМАТИВНО-ТЕХНИЧЕСКАЯ БАЗА
РАЗРАБОТКИ КОНЦЕПЦИИ

Нормативно-техническую базу разработки и обеспечения функционирования АС ЦБД УИГ в области обеспечения ИБ составляют следующие документы:

1. Нормативно-технические и методические документы по информационной безопасности, утвержденные федеральными органами государственного управления в соответствии с их компетенцией:

   – Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»1;

   – Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»2;

   – Приказ ФСБ России от 9.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»3;

   – Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»4;

   – Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)5;

2. Нормативно-правовые акты ФМС России;

   – Приказ ФМС России от 24.03.2006 г. № 103 «О мерах по технической и криптографической защите автоматизированных информационных систем ФМС России»;

1 Утвержден решением председателя Гостехкомиссии России от 30.03.1992 г.
2 Утвержден решением председателя Гостехкомиссии России от 04.06.1999 г. № 114.
3 Зарегистрирован в Министерстве юстиции Российской Федерации 3 марта 2005 г., регистрационный № 6382.
4 Зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г., регистрационный № 2848.
5 Утверждены приказом Гостехкомиссии России от 30.08.2002 г. № 282.
Приказ ФМС России от 14.03.2007 г. № 48 «О мерах по защите информации в системе ФМС России»;

Распоряжение ФМС России от 15.12.2006 г. № МС-1/11-21000 «О проведении аттестационных испытаний федерального и территориального уровней ПАК АС ЦБД УИГ»;

Распоряжение ФМС России от 01.03.2007 г. № МС-1/11-3286 «О создании подразделений по защите информации в системе ФМС России».

3. Нормативно-технические документы:

− ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
− ГОСТ 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении»;
− ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;
− ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»;
− ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
− ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

4. Проектно-техническая документация на АС ЦБД УИГ:

− ДШСК.42 5500 9.012-ТЗ АС ЦБД УИГ. Техническое задание. – Москва, 2005 г.;
− ДШСК.42 5500 9.020 Частное техническое задание. Автоматизированная система центрального банка данных учета иностранных граждан. Подсистема информационной безопасности. Частное техническое задание;
− ДШСК.42 5500 9.026 Частное техническое задание. Автоматизированная система центрального банка данных учета иностранных граждан. Подсистема сервисного обслуживания. Частное техническое задание;
− ДШСК.50 6900 4.001 Частное техническое задание. Автоматизированная система центрального банка данных учета иностранных граждан. Прикладная подсистема. Частное техническое задание;
− ДШСК.0029-ТА Автоматизированная система центрального банка данных учета иностранных граждан. Подсистема информационной безопасности. Модель угроз информационной безопасности и действий нарушителя.
ПРИЛОЖЕНИЕ 5. ШАБЛОН ЗАПРОСА НА ПРЕДОСТАВЛЕНИЕ ДОСТУПА ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЯМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ АС ЦБД УИГ

Начальнику Отдела/Управления

(резолюция начальника отдела/управления)

ЗАЯВКА

на предоставление доступа к информационным ресурсам АС ЦБД УИГ

Прошу зарегистрировать пользователем (исключить из списка пользователей, изменить полномочия пользователя) АС

____________________________________________________________________________________

(ненужное зачеркнуть)

____________________________________________________________________________________

(должность с указанием подразделения)

____________________________________________________________________________________

(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)

(ненужное зачеркнуть)

dля решения задач:

____________________________________________________________________________________

(список задач согласно формуляров задач)

____________________________________________________________________________________

на следующих рабочих станциях (РС):

____________________________________________________________________________________

(перечень условных наименований РС подразделения согласно их формуляров)

____________________________________________________________________________________

Начальник

(наименование заказывающего подразделения)

«___» _____________ 200__ г. ______________________________________________________________________________________

(подпись) (фамилия)
ЗАДАНИЕ
на внесение изменений в списки пользователей АС

Администраторам средств защиты серверов и баз данных

_________________________________________
(фамилии и инициалы исполнителей)

Администратору средств защиты от НСД

_________________________________________
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей серверов и баз данных

Начальник отдела информационного обеспечения ___________ ___________
«___» _____________ 200__ г.

Произвести изменения в списках пользователей указанных РС

Начальник отдела информационного обеспечения ___________ ___________
«___» _____________ 200__ г.
Обратная сторона заявки

Присвоено имя __________________________ (персональный идентификатор Touch Memory номер __________________________ ) и предоставлены полномочия, необходимые для решения следующих задач на следующих РС:

<table>
<thead>
<tr>
<th>Наименование АРМ</th>
<th>Наименование задачи</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Администратор АС ЦБД УИГ __________________________

(подпись, фамилия)

«___» _____________ 200___ г.

Администратор ИБ АС ЦБД УИГ __________________________

(подпись, фамилия)

«___» _____________ 200___ г.

Имя, персональный идентификатор Touch Memory, личные ключевые дискеты и начальные значения паролей получил, о порядке смены пароля при первом входе в систему проинструктирован

Пользователь __________________________

(подпись, фамилия)

«___» _____________ 200___ года
ПРИЛОЖЕНИЕ 6. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЯМ К РЕСУРСАМ АС ЦБД УИГ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Раздел определяет цели разработки и использования данной Инструкции. Приводится перечень подразделений и должностных лиц, на которых распространяется действие данной Инструкции.

2 ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И КОНТРОЛЯ ДОСТУПА К РЕСУРСАМ АС ЦБД УИГ

2.1 Порядок предоставления, изменения и прекращения прав доступа к ресурсам АС ЦБД УИГ

Раздел устанавливает процедуры подготовки запросов на предоставление доступа к ресурсам АС ЦБД УИГ, согласования запросов и принятия решений о предоставлении доступа к ресурсам АС ЦБД УИГ. Устанавливаются требования по прекращению доступа пользователей в случаях увольнения сотрудников, перевода на другую должность, нарушения требований по защите информации и пр.

2.2 Порядок хранения запросов на предоставление доступа к ресурсам АС ЦБД УИГ

Раздел устанавливает порядок хранения запросов на предоставление доступа к ресурсам АС ЦБД УИГ (как в электронном, так и в бумажном виде) с целью обеспечения контроля за предоставленными привилегиями доступа.

2.3 Порядок осуществление контроля привилегий доступа к ресурсам АС ЦБД УИГ

Раздел содержит требования к периодичности и механизмам проведения контроля предоставленных привилегий доступа. Устанавливаются также требования к периодическому пересмотру предоставленных привилегий доступа и отмене ставших ненужными привилегий.
3 РОЛИ И ОТВЕТСТВЕННОСТЬ

В данном разделе определяются роли должностных лиц по предоставлению и контролю доступа к ресурсам АС ЦБД УИГ, а также ответственность за соблюдение данной Инструкции.
ПРИЛОЖЕНИЕ 7. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК РАЗГРАНИЧЕНИЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ТЕРРИТОРИЮ, В ЗДАНИЯ И ПОМЕЩЕНИЯ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Раздел определяет цели разработки и использования данной Инструкции. Определяется сфера применения документа, приводится перечень подразделений и должностных лиц, на которых распространяется действие данной Инструкции.

2 ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ ДОСТУПА

В данном разделе приводится краткая характеристика основных технических мер и средств, которые могут использоваться для разграничения и контроля доступа сотрудников и посетителей на территорию, в здания и помещения (турникеты, замки на дверях, системы контроля доступа и т. д.) Определяются требования к применению данных средств.

3 ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА НА ТЕРРИТОРИЮ, В ЗДАНИЯ И ПОМЕЩЕНИЯ

3.1 Порядок допуска сотрудников

Определяется порядок доступа сотрудников на территорию, в здания и помещения, устанавливается порядок выдачи сотрудникам удостоверений, пропусков, магнитных карт и иных подобных документов.

Устанавливается порядок формирования перечня выделенных помещений и списка сотрудников, допущенных в данные помещения.

3.2 Порядок допуска посетителей

Устанавливается порядок доступа посетителей на территорию, в здания и помещения. Определяются требования по регистрации фактов входа и выхода посетителей. Также регламентируется порядок доступа сторонних лиц в выделенные помещения (например, для проведения обслуживания технических средств).
4 КОНТРОЛЬ ДОСТУПА

Данный раздел содержит описание мер, направленных на своевременное выявление фактов несанкционированного доступа на территорию, в здания и помещения. Устанавливаются требования к назначению лиц, ответственных за выделенные помещения, регламентируются обязанности данных лиц.

5 РОЛИ И ОТВЕТСТВЕННОСТЬ

В данном разделе определяются роли сотрудников подразделений по организации разграничения и контроля физического доступа сотрудников и посетителей, а также ответственность за соблюдение требований данной Инструкции.
ПРИЛОЖЕНИЕ 8. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК ПРОВЕДЕНИЯ ЭКСПЛУАТАЦИИ, ОБСЛУЖИВАНИЯ, РЕМОНТА И МОДИФИКАЦИИ АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ АС ЦБД УИГ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Данный раздел устанавливает цели разработки и применения данной Инструкции, определяет перечень подразделений и должностных лиц, на которых распространяется действие данной Инструкции.

2 ПОРЯДОК ПРОВЕДЕНИЯ МОДИФИКАЦИИ АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ АС ЦБД УИГ

2.1 Документирование состава аппаратных и программных средств АС ЦБД УИГ

Раздел устанавливает перечень разрабатываемой на АС ЦБД УИГ документации, которая должна определять состав, схемы физического и логического размещения аппаратных и программных компонентов АС ЦБД УИГ. Устанавливаются также требования по поддержке документации в актуальном состоянии.

2.2 Подготовка и проведение модификаций аппаратных и программных средств АС ЦБД УИГ

В данном разделе устанавливаются процедуры планирования, согласования, предварительного тестирования и проведения модификаций аппаратных и программных средств АС ЦБД УИГ. Определяются меры, направленные на предотвращение сбоев в работе АС ЦБД УИГ после проведения модификаций и обеспечение возможности отката изменений.

3 ПОРЯДОК РЕМОНТА И ОБСЛУЖИВАНИЯ АППАРАТНЫХ СРЕДСТВ АС ЦБД УИГ

Регламентируется порядок проведения ремонта, технического обслуживания и вывода из эксплуатации аппаратных средств АС ЦБД УИГ. Определяются меры по предотвращению несанкционированного доступа к информационным ресурсам АС ЦБД УИГ при передаче
аппаратных средств в ремонт, списании компонентов аппаратных средств, а также при допуске сторонних лиц для проведения обслуживания компонентов АС ЦБД УИГ.

4 ПОРЯДОК ЭКСПЛУАТАЦИИ АППАРАТНЫХ И ПРОГРАММНЫХ СРЕДСТВ АС ЦБД УИГ

В данном разделе устанавливаются требования к согласованию администраторами АС ЦБД УИГ действий, оказывающих существенное влияние на безопасность информационных ресурсов АС ЦБД УИГ, с сотрудниками подразделений по защите информации. Приводятся требования по разработке инструкций, определяющих основные эксплуатационные процедуры, и даются ссылки на действующие инструкции по администрированию и сопровождению АС ЦБД УИГ.

5 РОЛИ И ОТВЕТСТВЕННОСТЬ

Определяются роли должностных лиц по реализации и контролю реализации процессов эксплуатации, сопровождения, ремонта, управления конфигурацией АС ЦБД УИГ, а также ответственность за соблюдение требований данной Инструкции.
ПРИЛОЖЕНИЕ 9. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ ПОРЯДОК ДЕЙСТВИЙ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНОЙ СИТУАЦИИ В АС ЦБД УИГ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Раздел определяет цели разработки и использования данной Инструкции, перечень подразделений и должностных лиц, на которых распространяется действие Инструкции.

2 ВИДЫ НЕШТАТНЫХ СИТУАЦИЙ

Раздел содержит перечень и краткое описание нештатных ситуаций, которые могут возникнуть при эксплуатации АС ЦБД УИГ и нанести ущерб пользователям АС ЦБД УИГ и иным субъектам информационных отношений.

3 МЕРЫ ПО ПРЕДОТВРАЩЕНИЮ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ

В разделе определяются основные меры по предотвращению возникновения нештатных ситуаций и минимизации ущерба от их возникновения (такие меры как установка средств кондиционирования, пожаротушения, пожарной сигнализации, резервное копирование, резервирование аппаратных средств и т.д.).

4 ПОРЯДОК ДЕЙСТВИЙ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНОЙ СИТУАЦИИ

Раздел определяет порядок действий пользователей АС ЦБД УИГ, администраторов, обслуживающего персонала при возникновении нештатных ситуаций различных видов. В разделе содержится контактная информация лиц, к которым необходимо обращаться пользователям при возникновении нештатных ситуаций.
5 РОЛИ И ОТВЕТСТВЕННОСТЬ

В данном разделе определяются роли должностных лиц по планированию и проведению мероприятий на случай нештатной ситуации, а также ответственность за соблюдение требований данной Инструкции.
ПРИЛОЖЕНИЕ 10. ТИПОВОЙ ПЕРЕЧЕНЬ ТРЕБОВАНИЙ К ПОДГОТОВКЕ ПЕРСОНАЛА В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИБ

1 ТРЕБОВАНИЯ К ПОДГОТОВКЕ АДМИНИСТРАТОРОВ АС ЦБД УИГ

Администраторы АС ЦБД УИГ должны обладать следующими знаниями и навыками по защите информации:

1. В части общих вопросов обеспечения информационной безопасности:
   - знать основные угрозы и пути реализации угроз информационной безопасности в автоматизированных системах;
   - знать основные технологии и механизмы защиты информации, включая:
     • обеспечение безопасности средствами ОС;
     • сетевую безопасность;
     • криптографическую защиту информации;

2. В части обеспечения защиты информации в АС ЦБД УИГ:
   - знать основные положения законов и подзаконных актов Российской Федерации, организационно-нормативных документов ФМС России в части, касающейся сопровождения и защиты информации в АС ЦБД УИГ;
   - знать и понимать технологию функционирования АС ЦБД УИГ, в том числе принципов работы программных и технических средств защиты АС ЦБД УИГ;
   - иметь навыки эксплуатации и администрирования штатных и специализированных средств защиты, входящих в состав АС ЦБД УИГ (в части компонентов АС ЦБД УИГ, администрирование и сопровождение которых возложено на соответствующего администратора АС ЦБД УИГ).
2 ТРЕБОВАНИЯ К ПОДГОТОВКЕ АДМИНИСТРАТОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АС ЦБД УИГ

Администраторы информационной безопасности АС ЦБД УИГ должны обладать следующими знаниями и навыками по защите информации:

1. В части общих вопросов обеспечения информационной безопасности:
   − знать основные положения законов и подзаконных актов Российской Федерации, нормативно-технических документов ФСБ России и ФСТЭК России, а также международных стандартов по защите информации;
   − знать основные угрозы и пути реализации угроз информационной безопасности;
   − знать основные технологии защиты информации, программные и технические средства защиты информации, а также методы обнаружения попыток несанкционированного доступа к ресурсам автоматизированной системы.

2. В части обеспечения защиты информации в АС ЦБД УИГ:
   − знать основные положения законов и подзаконных актов Российской Федерации, организационно-нормативных документов ФМС России в части, касающейся защиты информации в АС ЦБД УИГ;
   − знать и понимать технологию функционирования АС ЦБД УИГ, в том числе принципов работы программных и технических средств защиты АС ЦБД УИГ;
   − иметь навыки эксплуатации и администрирования штатных и специализированных средств защиты, входящих в состав АС ЦБД УИГ (в части компонентов АС ЦБД УИГ, управление и контроль управления которых возложен на данного сотрудника).

3 ТРЕБОВАНИЯ К ПОДГОТОВКЕ ПОЛЬЗОВАТЕЛЕЙ АС ЦБД УИГ

Пользователи АС ЦБД УИГ должны:

− знать требования организационно-нормативных документов ФМС России по эксплуатации и защите информации в АС ЦБД УИГ, действие которых на них распространяется;
− знать и понимать меры и требования по обеспечению ИБ при эксплуатации АС ЦБД УИГ, реализация которых возложена на пользователей;
− уметь использовать средства защиты, установленные на АРМ пользователя (средства формирования и проверки ЭЦП, средства шифрования и пр.)
ПРИЛОЖЕНИЕ 11. ПЛАН-ПРОСПЕКТ ИНСТРУКЦИИ, ОПРЕДЕЛЯЮЩЕЙ МЕХАНИЗМЫ РАСПРЕДЕЛЕНИЯ РОЛЕЙ СОТРУДНИКОВ СИСТЕМЫ ФМС РОССИИ ПО ДОСТУПУ К РЕСУРСАМ АС ЦБД УИГ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Раздел определяет цели разработки и использования данной Инструкции. Устанавливается перечень подразделений/должностных лиц, которые должны руководствоваться требованиями данной Инструкции.

2 ПОДБОР ПЕРСОНАЛА

Определяется порядок подбора и приема персонала на должности, связанные с эксплуатацией, обслуживанием и сопровождением АС ЦБД УИГ. Распределяется ответственность за формирование требований к новым сотрудникам в зависимости от должности сотрудника и проведение проверки соответствия сотрудника предъявленным требованиям. Устанавливаются повышенные требования к отбору персонала на ключевые должности по управлению АС ЦБД УИГ.

3 ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННО-НОРМАТИВНому ОБЕСПЕЧЕНИЮ

Устанавливаются требования по документированию ролей и обязанностей сотрудников, связанных с управлением и эксплуатацией компонентов АС ЦБД УИГ, в должностных инструкциях, положениях о подразделениях и иных организационно-нормативных документах. Определяется порядок ознакомления сотрудников с соответствующими документами в части, их касающейся.

4 ПРОВЕРКИ СОТРУДНИКОВ

Определяются механизмы проверок сотрудников с целью оценки качества выполнения ролей и анализа лояльности сотрудников.
5 РОЛИ И ОТВЕТСТВЕННОСТЬ

В данном разделе определяются обязанности должностных лиц по управлению ролями персонала в части доступа к ресурсам АС ЦБД УИГ, а также ответственность за соблюдение требований данной Инструкции.
ПРИЛОЖЕНИЕ 12. ПЛАН-ПРОСПЕКТ АКТА ФМС РОССИИ, ОПРЕДЕЛЯЮЩЕГО РЕГЛАМЕНТ РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ФМС РОССИИ

1 ОБЩИЕ ПОЛОЖЕНИЯ

В данном разделе содержится краткое описание содержания данного акта, назначения и области действия. Приводится характеристика структуры УЦ и контактная информация лиц, ответственных за обеспечение функционирования УЦ.

Приводится перечень функций, обязанностей и прав лиц, участвующих в поддержке функционирования УЦ, а также обязанности и ответственность пользователей УЦ. Определяются требования к периодичности и механизмам проверки соблюдения положений данного акта при эксплуатации и поддержке функционирования УЦ.

2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

В данном разделе устанавливаются правила формирования имен владельцев и издателей сертификатов. Определяется порядок регистрации пользователей, требования по проверке идентичности личности.

3 ЭКСПЛУАТАЦИОННЫЕ ТРЕБОВАНИЯ

Раздел определяет требования к основным процедурам, связанным с эксплуатацией и поддержкой функционирования УЦ, в том числе к процедурам:

− изготовления, выдачи, приостановления действия и аннулирования сертификатов;

− проверки статуса сертификатов;

− генерации записей и анализу событий безопасности, связанных с функционированием УЦ;

− архивирования данных, обрабатываемых в УЦ;

− восстановления работоспособности УЦ после сбоев.
4 ФИЗИЧЕСКИЙ, ПРОЦЕДУРНЫЙ И ПЕРСОНАЛЬНЫЙ КОНТРОЛЬ БЕЗОПАСНОСТИ

Данный раздел устанавливает требования по обеспечению безопасности на физическом уровне (разграничение доступа к техническим средствам УЦ, обеспечение помещений, в которых размещены технические средства УЦ, электроснабжением и кондиционированием, предотвращение несанкционированного доступа к носителям информации или их повреждения), процедурном уровне (разграничение ролей и полномочий обслуживающего персонала УЦ), а также на уровне персонала (определение требований к квалификации сотрудников, к проведению подготовки и переподготовки обслуживающего персонала).

5 ТЕХНИЧЕСКИЙ КОНТРОЛЬ БЕЗОПАСНОСТИ

Раздел определяет требования к техническим мерам защиты при генерации, распространении ключей, хранении и уничтожении ключевых носителей, хранении и использовании активационных данных (паролей). Устанавливаются требования к составу сервисов безопасности, предоставляемых удостоверяющим центром, а также требования к средствам обеспечения надежности функционирования УЦ.

6 СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКИ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

Данный раздел определяет номера версий и перечень полей сертификатов и списков аннулированных сертификатов.

7 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К АДМИНИСТРИРОВАНИЮ

Данный раздел устанавливает требования к проведению периодического анализа и пересмотра данного документа. Определяются механизмы публикации данного документа и оповещения заинтересованных лиц об изменениях в этом документе.

8 ПРИЛОЖЕНИЕ ПОЛЬЗОВАТЕЛЬСКОЕ СОГЛАШЕНИЕ

В данном разделе приводится шаблон соглашения, заключаемого с пользователем до начала предоставления ему сервисов УЦ и определяющего обязанности и права пользователя при пользовании сервисами УЦ.
ПРИЛОЖЕНИЕ 13. ПЛАН-ПРОСПЕКТ «ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ АКТИВОВ»

ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ АКТИВОВ

<table>
<thead>
<tr>
<th>№</th>
<th>Наименование актива</th>
<th>Описание актива</th>
<th>Местоположение актива</th>
<th>Владелец актива</th>
<th>Ценность актива</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ПРИЛОЖЕНИЕ 14. ПЛАН-ПРОСПЕКТ «ОТЧЕТА ОБ ОЦЕНКЕ РИСКОВ»

ОТЧЕТ ОБ ОЦЕНКЕ РИСКОВ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Раздел определяет исполнителя работ по анализу рисков, устанавливает цели проведения анализа рисков АС ЦБД УИГ.

2 КРАТКАЯ ХАРАКТЕРИСТИКА АС ЦБД УИГ

В данном разделе приводится краткое описание особенностей АС ЦБД УИГ, значимых при проведении анализа рисков ИБ АС ЦБД УИГ.

3 МЕТОДИКА ПРОВЕДЕНИЯ АНАЛИЗА РИСКОВ

Приводится описание применявшейся методики анализа и оценки рисков.

4 АНАЛИЗ РИСКОВ ИБ АС ЦБД УИГ

В разделе содержится описание модели АС ЦБД УИГ, применявшейся при проведении анализа рисков. Приводятся основные результаты и выводы по оценке рисков ИБ АС ЦБД УИГ.

5 РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ ОБЕСПЕЧЕНИЯ ИБ

В данном разделе приводятся основные рекомендации по снижению рисков реализации угроз ИБ.

ПРИЛОЖЕНИЕ. РЕЗУЛЬТАТЫ АНАЛИЗА И ОЦЕНКИ РИСКОВ

В данном разделе приводится сводная таблица оценки рисков по следующему шаблону:

<table>
<thead>
<tr>
<th>№</th>
<th>Актив</th>
<th>Угроза</th>
<th>Уязвимость</th>
<th>Риск актива</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## ПРИЛОЖЕНИЕ 15. ПЛАН-ПРОСПЕКТ «ПЛАНА ОБРАБОТКИ РИСКОВ»

### ПЛАН ОБРАБОТКИ РИСКОВ

<table>
<thead>
<tr>
<th>№</th>
<th>Уязвимость</th>
<th>Угроза</th>
<th>Актив</th>
<th>Уровень риска</th>
<th>Защитные меры</th>
<th>Остаточный уровень риска</th>
<th>Ответственное лицо</th>
<th>Срок выполнения</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>