ДИАЛОГОВАЯ ИНФОРМАЦИОННАЯ СИСТЕМА «НООСФЕРА»
Техническая защита информации от несанкционированного доступа

КОНЦЕПЦИЯ
ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ДИАЛОГОВЫМ ПРОГРАММНЫМ КОМПЛЕКСОМ «С ОТКРЫТЫМ КОДОМ»

Шифр: «КСЗ от НСД 3.КЦД.2/2 в ДИС 3.КЦД.5/7»

Руководитель проекта

А.А. Прималенный

ООО «КРЫМСКОЕ АЭРОКОСМИЧЕСКОЕ АГЕНТСТВО»
(Лицензиат Администрации государственной службы специальной связи и защиты информации Украины)
город Севастополь
2011 год

1. Руководитель проекта:

Председатель ООО «Крымское аэрокосмическое агентство»,
кандидат географических наук А. А. Прималенный

2. Соисполнители проекта:

Генеральный директор ООО «Крымское аэрокосмическое агентство»,
кандидат технических наук А. П. Котов

Главный инженер ООО «Крымское аэрокосмическое агентство»,
кандидат технических наук А. Н. Ларионов

Главный технолог
ООО «Крымское аэрокосмическое агентство» В. В. Ляхов

Главный геодезист
ООО «Крымское аэрокосмическое агентство» Л. П. Жоголева

Юрисконсульт
ООО «Крымское аэрокосмическое агентство» В. Н. Ладыка

3. Консультанты проекта:

Начальник Управления
Государственного Департамента специальной связи
и защиты информации Украины в г. Севастополе,
полковник Госспецсвязи Ф. И. Егоров

Декан факультета общественно-политического развития
Национальной Академии государственного управления
При Президенте Украины
доктор наук государственного управления А. И. Семенченко

Советник по научной работе
Председателя Всеукраинского общественного объединения
«Украинская служба спасения» (ВГО УСП),
кандидат технических наук Г. А. Клименко

Материалы настоящей Концепции раскрывают принципиальные основы актуальности и новизны диалоговой информационной системы «Ноосфера» с дуализмом программных функций комплекса защиты информации от несанкционированного доступа:

- «открытый код обращения к программному комплексу» из неконтролируемой среды с различной политикой безопасности (открытость доступа – до 3.КЦД.2 не выше Г-2),
- «ограничение доступа программным комплексом к авторизованным данным и процессам третьих лиц» с непрерывной обработкой массивов запросов с различными критериями, уровнями и функциями услуг безопасности (ограничение доступа – до 3.КЦД.5 не ниже Г-7),
- возможностью адаптации программного комплекса к вычислительным системам стандартных автоматизированных систем классов «1», «2», «3», «4» субъектов «обратной связи» и присущих им способам и системам передачи/приема данных.

1. Область применения и регламентации

1.1. ДИС «Ноосфера» (*версия Г-2*) применяется в компьютерных системах электронных приемных со-интегральной системы местного электронного правления (как неотъемлемой части электронного правительства Украины) и субъектов «обратной связи», функционирующих в режиме:

1) «открытого» доступа граждан и их объединений к публичной и государственной информации;
2) необходимостью защиты «открытых» сведений, принадлежащих:
   - другим гражданам и их объединениям;
   - должностным лицам государственных и коммунальных органов власти и их учреждений;
   - обществу (публичная информация);
   - государству.

1.2. Принципы настоящей Концепции обеспечения защиты информации (далее – Концепция) ДИС «Ноосфера» от несанкционированного доступа (далее – НСД) регламентирует вопросы:

1) определения совокупности требований по одновременной восьмиуровневой защите объектов ДИС от НСД (далее – эшелоны), обеспечивающих в условиях «обратной связи» с пользователями из неконтролируемой среды и с данными различной конфиденциальности:
   - беспрепятственный непрерывный множественный доступ к объектам (до критерия Г-2),
   - максимальный уровень услуг безопасности по защите «открытых» персональных данных, публичной информации и сведений, принадлежащих государству (до критерия Г-7);
2) создания защищенных компонентов ДИС «Ноосфера» и средств их защиты от НСД;
3) оценки защищенности ДИС «Ноосфера»;
4) пригодности ДИС «Ноосфера» для удовлетворения запросов потребителей.

1.3. Заданные технологические требования обеспечивают прямое взаимодействие с «одномашинными - однопользовательскими» и «многомашинными – многопользовательскими» конфигурациями КС внешних пользователей с различной политикой безопасности и защитой среды передачи информации по уровням:

1) КС Головного узла обратной связи Главы государства;
2) КС узлов обратной связи государственных органов;
3) КС узлов обратной связи различных ветвей и административных уровней органов государственной власти;
4) КС узлов обратной связи органов местного самоуправления;
5) КС предприятий финансовой сферы;
6) КС справочных и поисковых систем;
7) КС нечеткого множества электронных офисов домашних и/или товарных хозяйств участников обратной связи в лице собственников земельных участков (застройщиков в лице граждан и их объединений, коммунальных и государственных учреждений) как информационно-коммуникационных центров внутри протокола связи «ДИС «Ноосфера» (для АС-3);
8) КС нечеткого множества участников обратной связи в лице граждан и их объединений вне протокола связи «ДИС «Ноосфера» (для АС-3).

Информационная концепция области применения ДИС в местном электронном правлении и взаимодействия ДИС с КС (внешними источниками/приемниками) пользователей неконтролируемой среды приведены на рис. 1.

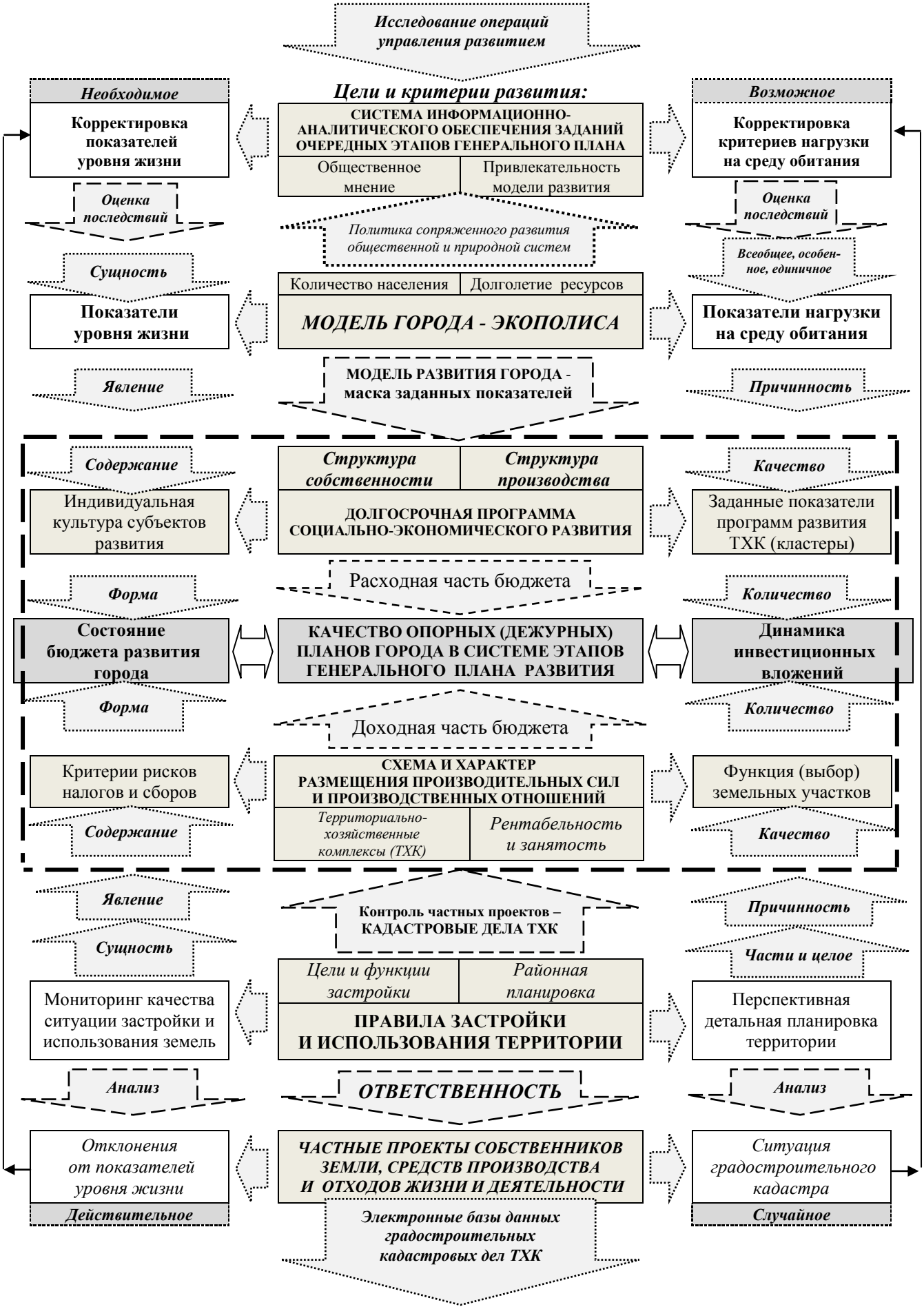


Рис. 1. Информационная концепция области применения ДИС и взаимодействия ДИС с КС внешних источников/приемников пользователей неконтролируемой среды в местном электронном правлении

2. Нормативные ссылки

При разработке настоящего документа использованы следующие нормативно-правовые акты, стандарты и нормативные документы:

- Конституция Украины, п.п. 31, 32.
- Закон Украины «О внесении изменений в Закон Украины «Об информации».
- Закон Украины «О защите информации в автоматизированных системах».
- Закон Украины «О научно-технической информации».
- Закон Украины «О государственной тайне».
- Закон Украины «О доступе к публичной информации».
- Закон Украины «О защите персональных данных».
- Указ Президента «О новой редакции Стратегии национальной безопасности Украины».
- Постановление Кабинета министров Украины «Концепция технической зашиты информации в Украине».
- Постановление Кабинета министров Украины «О внесении изменений в некоторые постановления Кабинета Министров Украины по вопросам доступа к информации».
- Постановление Кабинета министров Украины «О Порядке предания огласке в сети Интернет информации о деятельности органов исполнительной власти».
- Положение о порядке осуществления криптографической защиты информации в Украине.
- НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа.
- НД ТЗИ 2.5-004-99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа.
- НД ТЗИ 2.5-005-99. Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа.
- Международные договоры Украины, которые касаются сферы информационных отношений.

3. Определения

В настоящем документе используются термины и определения, соответствующие и установленные в нормативных документах:

- ✓ ГОСТ-34-320-96 Межгосударственный стандарт «Концепции и терминология для концептуальной схемы и информационной базы. Информационные технологии. Система стандартов по базам данных».
- ✓ ГОСТ 19781-90 Единая система программной документации. Обеспечение систем обработки информации программное. Термины и определения.
- ✓ НД ТЗИ 1.1-003-99 «Терминология в области защиты информации в компьютерных системах от несанкционированного доступа».
- ✓ НД ТЗИ 2.5-004-99 «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа».
- ✓ НД ТЗИ 2.5-005-99 «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа».
- ✓ НД ТЗИ 3.7-001-99 Методические указания по разработке технического задания на создание комплексной системы защиты информации в автоматизированной системе. С изменением №1, утвержденным приказом ГСТСЗИ СБ Украины от 18.06.2002 г. № 37.
- ✓ НД ТЗИ 1.4-001-2000 Типовое положение о службе защиты информации в автоматизированной системе.
- ✓ НД ТЗИ 1.1-002-99 Общие положения относительно защиты информации в компьютерных системах от несанкционированного доступа.
- ✓ НД ТЗИ 3.6-001-2000 Техническая защита информации. Компьютерные системы. Порядок создания, внедрения, сопровождения и модернизации средств технической защиты информации от несанкционированного доступа.
- ✓ ГСТУ 3396 0-96 Защита информации. Техническая защита информации. Основные положения.
- ✓ ГСТУ 3396 1-96 Защита информации. Техническая защита информации. Порядок проведения работ.
- ✓ ГСТУ 3396.2-97 Защита информации. Техническая защита информации. Термины и определения.
- ✓ Порядок защиты государственных информационных ресурсов в информационно - телекоммуникационных системах. (Приказ ГСТСЗИ СБ Украины от 24.12.2001 г. № 76, зарегистрировано в Министерстве юстиции Украины 11.01.2002 г. за №27/6315).

4. Обозначения и сокращения

В настоящем документе используются следующие обозначения и сокращения:

АС — автоматизированная система;
БД — база данных;
В/В — ввод/вывод;
ВС — вычислительная система;
ДИС — диалоговая информационная система «Ноосфера» (версия Г-2);
КС — компьютерная система;
КСЗ — комплекс средств защиты;
КСЗИ — комплексная система защиты информации;
ЛВС — локальная вычислительная сеть;
НД — нормативный документ;
НД ТЗИ — нормативный документ технической защиты информации;
НСД — несанкционированный доступ;
ОС — операционная система;
ПЗУ — постоянное запоминающее устройство;
ПО — программное обеспечение;
ПРД — правила разграничения доступа;
ПЭМИН — побочное электромагнитное излучение и наводки;
ТЗИ — техническая защита информации;
ЭВМ — электронно-вычислительная машина.

Обозначения услуг безопасности:

Конфиденциальность:
КД — доверительная конфиденциальность;
КА — административная конфиденциальность;
КО — повторное использование объектов;
КК — анализ скрытых каналов;
КВ — конфиденциальность при обмене.

Целостность:
ЦД — доверительная целостность;
ЦА — административная целостность;
ЦО — откат;
ЦВ — целостность при обмене.

Доступность:
ДР — использование ресурсов;
ДС — устойчивость к отказам;
ДЗ — горячая замена;
ДВ — восстановление после сбоев.

Наблюдаемость:
НР — регистрация;
НИ — идентификация и аутентификация;
НК — достоверный канал;
НО — разграничение обязанностей;
НЦ — целостность КСЗ;
НТ — самотестирование;
НВ — аутентификация при обмене;
НА — аутентификация отправителя;
НП — аутентификация получателя.

5. Постановка проблемы зашиты информации в ДИС от НСД

5.1 Общие положения

Современная правовая основа защиты информации, информационные ресурсы, обрабатываемые КС в процессе «обратной связи», регламентируют обязательность «открытости» информации государственных и публичных учреждений для населения.

В то же время для государственных и публичных сведений устанавливаются повышенные требования к организации защиты «открытой» информации, принадлежащей государству и/или имеющей статус конфиденциальности (ограниченной публичности).

Не менее конкретные требования выставлены и к защите персональных данных физических лиц, которые возможно собирать «только о себе» с запретом ознакомления о персональных данных «третьих физических лиц». Это касается и «третьих юридических лиц», например служащих различных учреждений и организаций, когда различные ситуации гражданско-правового характера принуждают граждан делиться с ними такой информацией «о себе». Как и служащих предоставлять информацию гражданам о своих функциональных обязанностях и связанных с этим особенностей их служебной деятельности.

При этом даже «открытая» информация, принадлежащая субъектам «обратной связи», например, при оказании административных услуг государственными или муниципальными органами власти гражданам или юридическим лицам, представляет собой не только определенную ценность, но и может использоваться для дезинформации путем ее модификации или утаивания.

Такие воздействия, как и бездействие по защите «открытых» данных, могут являться причиной материальных ущербов за счет снижения ценности этих информационных ресурсов. А также могут являться неблагоприятными. Всякое же потенциально возможное неблагоприятное воздействие является угрозой.

Ответственность за исключение подобных угроз требует от владельцев автоматизированных систем организации защиты информации путем создания и поддержания в работоспособном состоянии системы мер как технических (инженерных, программно-аппаратных), так и нетехнических (правовых, организационных), позволяющих предотвратить и/или затруднить возможность реализации угроз.

Важнейшим фактором противодействия и снижения потенциального ущерба владельцев информации является исключение несанкционированного доступа к обрабатываемой информации и сохранение заданных информации свойств автоматизированной системой, ее обрабатывающей.

В данном случае обработка информации в автоматизированных системах области применения производится техническими и технологическими средствами ДИС (*версия Г-2*), что требует наличия в структуре программного обеспечения комплекса средств защиты.

Система принятия указанных мер по защите информации свойствами ДИС в совокупности с организационными мероприятиями создания АС является искомой комплексной системой защиты информации от НСД.

В свою очередь, требования к политике безопасности, обязанной исключить противоречие «открытости доступа» при наивысшем функциональном профиле защищенности, определяют задачу проектирования и эксплуатации КСЗ ДИС от НСД как нестандартную «по сути» с обязательностью ее реализации стандартными методами в рамках НД ТЗИ.

5.2 Основные направления защиты

ДИС (*версия Г-2*) предназначена для обслуживания автоматизированной системы класса «3», представляющую собой организационно-техническую систему, объединяющую вычислительную систему, физическую среду, персонал и обрабатываемую информацию.

Принято выделять следующие основные направления технической защиты информации, которая обрабатывается вычислительной системой АС:

1) защита обрабатываемой информации от несанкционированного доступа;
2) защита информации от утечки по техническим каналам.

В связи с сущностью ДИС как совокупности прикладного, инструментального, операционного программного обеспечения:

1) является предметом рассмотрения построение комплекса средств защиты от НСД как свойств ДИС, взаимодействующей с вычислительной системой АС;
2) не являются предметом рассмотрения:
   - организационные и физические меры защиты, включая защиту от НСД к компонентам вычислительной системы АС,
   - защита от утечки по техническим каналам и через ВЧ - навязывание;
   - повреждение или уничтожение информации средствами электромагнитного воздействия.
3) в случае влияния нетехнических аспектов организации защиты информации на оценку технической защищенности, в Концепции им уделяется необходимое и достаточное внимание.

Таким образом, для КСЗ ДИС в проблеме защиты информации от НСД методологически следует выделить два направления:

1) оценка защищенности информации КСЗ ДИС от НСД в функционирующей ВС АС-3;
2) оценка комплекса средств защиты КСЗ ДИС от НСД вне конкретной среды эксплуатации.

Конечной целью всех реализуемых мероприятий по защите информации КСЗ ДИС (*версия Г-2*) от НСД является обеспечение безопасности информации:

1) при ее обработке с применением в АС-3;
2) на всех стадиях собственного жизненного цикла;
3) на всех технологических этапах обработки информации.

Жизненный цикл КСЗ ДИС от НСД включает:

1. Планирование разработки.
2. Определение требований.
3. Проектирование.
4. Реализация и тестирование.
5. Выпуск.
6. Эксплуатация.
7. Завершение разработки.

Для гарантии зашиты информации от НСД в АС-3, которую обслуживает ДИС (*версия Г-2*), должно быть выполнено проектирование АС с целью интеграции средств защиты, предоставляемых каждым компонентом, в единый комплекс средств защиты от определенных угроз.

Комплекс средств защиты должен быть сертифицирован (в целом или по компонентам).

6. Концепция обеспечения защиты информации

6.1 Основные угрозы информации

Зависимость заданного в разработке качества работы КСЗ ДИС от НСД от качества работы остальных элементов КСЗ и определенных угроз субъективного и объективного характера АС, требует описания угроз как для КСЗ, так и существующих зависимостей:

1) информация существует в виде формализованных данных, пригодных для обработки, где в соответствии с ДСТУ 2226-93 в настоящей Концепции под обработкой понимается:
   - обработка информации как назначение (передача данных из неконтролируемой среды),
   - обработка данных как процедуры ввода, вывода, поиска, сбора, использование, хранения, накопления и тиражирования,

   где термины:
   - ✓ «обработка» как назначение и «обработка» как процедура являются омонимами;
   - ✓ «информация» из неконтролируемой среды подразумевает «передачу данных»;
   - ✓ «информация», обрабатываемая контролируемой средой, является синонимом «данных»;
2) информация для своего существования всегда требует наличия носителя:
   - в качестве носителя информации может выступать поле или вещество;
   - в некоторых случаях в качестве носителя информации может рассматриваться человек.
3) потеря информацией своей ценности (нарушение безопасности информации) может произойти вследствие перемещения или изменения физических свойств носителя;
4) при анализе проблемы зашиты от НСД информации, которая может циркулировать в КС, как правило, рассматриваются лишь информационные объекты, служащие приемниками/источниками информации, и информационные потоки (порции перемещаемой между объектами информации) безотносительно к физическим характеристикам их носителей;
5) угрозы обрабатываемой ДИС в АС информации зависят от характеристик ВС, физической среды, персонала и обрабатываемой информации;
6) угрозы могут иметь:
   - объективную природу, например, изменение условий физической среды (пожары, наводнения и т.п.) или отказ элементов ВС;
   - субъективную природу, например, ошибки персонала или действия злоумышленника;
7) угрозы, имеющие субъективную природу, могут быть случайными либо преднамеренными;
8) попытка реализации угрозы является атакой, где из всего множества способов классификации угроз в настоящей концепции принимается классификация угроз по результату их воздействия на информацию:
   - нарушение конфиденциальности информации вследствие несоблюдения установленных правил ознакомления с ней;
   - нарушение целостности информации вследствие несоблюдения установленных правил ее модификации и/или удаления,
   - нарушение доступности информации вследствие утраты возможности ознакомления с информацией или ее модификациями в соответствии с установленными правилами в течение любого определенного (малого) промежутка времени.

9) Угрозы могут воздействовать на информацию не непосредственно, а опосредовано: например, потеря КСЗ управляемости может привести к неспособности КСЗ обеспечивать защиту информации и, как результат, к потере определенных свойств обрабатываемой информации.

6.2 Политика безопасности информации

6.2.1 Концептуальные особенности политики безопасности информации

1. Под политикой безопасности информации следует понимать набор законов, правил, ограничений, рекомендаций и т.д., регламентирующих порядок обработки информации и направленных на защиту информации от определенных угроз.

2. В соответствии с настоящей Концепцией термин «политика безопасности» методологически применяется к КСЗ в ДИС по двум направлениям:

1) оценка защищенности информации ДИС в функционирующей ВС ***в связи***:
   - с назначением ДИС «*версии Г-2*» для эксплуатации в комплекте с ВС в АС-3, «привязанных» к выделенным помещениям, как фактору косвенных угроз для НСД в ДИС;
   - с требованиями учета существующих зависимостей КСЗ ДИС от качества единого комплекса средств защиты информации в АС-3 для тиражирования типовым комплексом;

2) оценка комплекса средств защиты ДИС вне конкретной среды эксплуатации, что обусловлено условиями тиражирования ДИС с КСЗ как типового программного комплекса, эксплуатируемого ВС АС-3 (*версии Г-2*) с адекватной технологической платформой.

3. Для ДИС требования указанных направлений удовлетворяются:

1) определением профиля безопасности защиты информации с необходимым и достаточным числом политик безопасности информации как наборов соответствующих функций услуг безопасности (далее – профиль безопасности);

2) формированием «политики безопасности информации» как совокупности «политик безопасности информации, реализуемых услугами» в соответствии с установленным профилем безопасности; далее указанные термины применяются в следующем виде:
   - «политика безопасности информации» - «политика безопасности»,
   - «политика безопасности информации, реализуемая услугой» - «политика услуги»,
   - «услуга политики безопасности» - «услуга безопасности».

4. Как следствие, политика безопасности должна:

1) для ДИС (как программного комплекса) определять ресурсы, нуждающиеся в защите, в том числе, устанавливать категории информации «не выше открытой информации» с учетом правового статуса пользователей;

2) для ДИС (как компонента ВС АС), дополнительно учитывать основные угрозы для ВС и персонала, ответственность которого должна быть персонифицирована.

3) часть политики безопасности, требующая по существу назначения ДИС регламентации правил доступа и процессов к ресурсам, регламентируется правилами разграничения доступа.

5. Учитывая особенность назначения ДИС по обслуживанию со-интегральной системы местного электронного правления Украины к выбору профиля функциональной защищенности КСЗ, как особенным свойствам ДИС, предъявляются наивысшие требования в рамках НД ТЗИ Украины.

6.2.2 Выбор профиля функциональной защищенности

1. Выбор профиля производится с учетом следующих факторов влияния внешней среды:

1) ДИС (версия *Г-2*) предназначена для автоматизации «обратной связи» между государственными учреждениями органов власти, органами местного самоуправления, гражданами и их объединениями, землепользователями и территориально-хозяйственными комплексами (ТХК):
   - по обращениям за административными услугами с заявлениями, жалобами и предложениями,
   - по управлению бюджетной политикой административных единиц (АТЕ) как совокупности ТХК,
   - по поддержке градостроительного кадастра и генерального плана развития по отчетам ТХК,
   - по контролю управления проектами застройки и эксплуатации земельных участков ТХК,
   - по учету доходов и расходов целевых средств на развитие административных территорий,
   - по другим прикладным аспектам общественных отношений в области применения ДИС.

2) Данная конфигурация по обмену потоками информации указанных категорий пользователей и различием в политике безопасности их собственных источников и/или приемников информации определяет ДИС как КСЗ «полного профиля» и программный комплекс для ВС АС-3 (табл. 1 - 3):

Таблица 1

Функциональные критерии услуг безопасности в составе 4-х групп (столбцов) (с гарантиями)

1. Конфиденциальность	**2. Целостность**	**3. Доступность**	**4. Наблюдаемость**	Критерии гарантий услуг безопасности

Таблица 2

Структура услуг безопасности по 5-ти строкам наборов функций политик услуг

1.1 Доверительная конфиденциальность	2.1 Доверительная целостность	3.1 Использование ресурсов	4.1.1 Регистрация	4.1.2 Контроль гарантий	1. Строка наборов функций запросов
1.2 Административная конфиденциальность	2.2 Административная целостность	3.2 Устойчивость к отказам	4.2.1 Идентификация и аутентификация	4.2.2. Достоверный канал	2. Строка наборов функций допусков
1.3 Повторное использование объектов	2.3 Откат	3.3 Горячая замена	4.3.1 Разграничение обязанностей	4.3.2 Целостность КСЗ	3. Строки наборов функций объектов
1.4 Анализ скрытых каналов	2.4 Не проектируется	3.4 Восстановление после сбоев	4.4.1 Самотестирование	4.4.2 Аутентификация при обмене	4. Строки наборов функций надзора
1.5 Конфиденциальность при обмене	2.5 Целостность при обмене	3.5 Не проектируется	4.5.1 Аутентификация отправителя	4.5.2 Аутентификация получателя	5. Строки наборов функций связи

Таблица 3

Уровни услуг безопасности по столбцам функциональных критериев и строкам политики услуг

Таблица 3.1

Доверительная конфиденциальность	Доверительная целостность	Использование ресурсов	Регистрация	Контроль гарантий	Строка «**Запрос**» по уровням услуг
КД-1	**ЦД-1**	**ДР-1**	**НР-1**	**Г-1,2**	Строка-1
КД-2	**ЦД-2**	**ДР-2**	**НР-2**	**Г-3**	Строка-1
КД-3	**ЦД-3**	**ДР-3**	**НР-3**	**Г-4**	Строка-1
КД-4	**ЦД-4**		**НР-4**	**Г-5**	Строка-1
			НР-5	**Г-6,7**	Строка-1

Таблица 3.2

Административная конфиденциальность	Административная целостность	Устойчивость к отказам	Идентификация и аутентификация	Достоверный канал	Строка «**Допуск**» по уровням услуг
КА-1	**ЦА-1**	**ДС-1**	**НИ-1**	**НК-1**	Строка-2
КА-2	**ЦА-2**	**ДС-2**	**НИ-2**	**НК-2**	Строка-2
КА-3	**ЦА-3**	**ДС-3**	**НИ-3**		Строка-2
КА-4	**ЦА-4**				Строка-2

Таблица 3.3

Повторное использование объектов	Откат	Горячая замена	Разграничение обязанностей	Целостность КСЗ	Строка «**Объект**» по уровням услуг
КО-1	**ЦО-1**	**ДЗ-1**	**НО-1**	**НЦ-1**	Строка-3
	ЦО-2	**ДЗ-2**	**НО-2**	**НЦ-2**	Строка-3
		ДЗ-3	**НО-3**	**НЦ-3**	Строка-3

Таблица 3.4

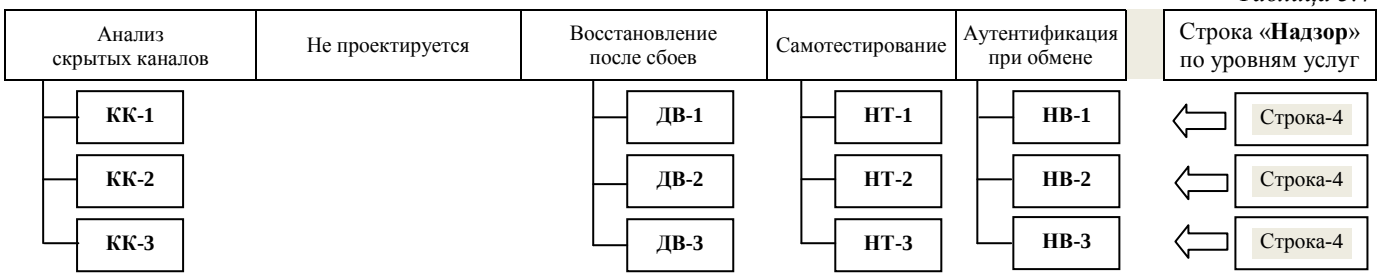
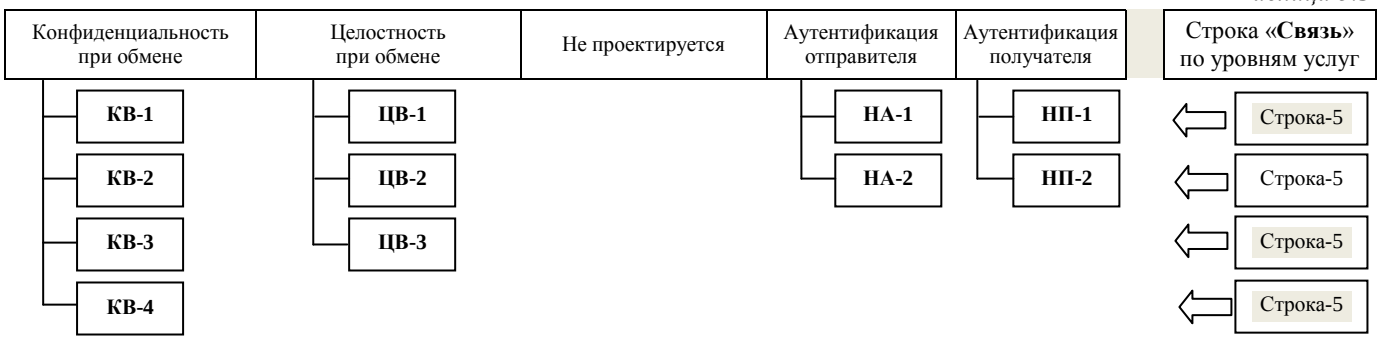


Таблица 3.5



3) Наборы функций услуг безопасности формируются на каждом уровне каждой услуги безопасности в соответствии с НД ТЗИ 2.05-004-99 «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа».

6.2.3. Организация структуры политики безопасности

Политика безопасности ДИС для данной конфигурации должна удовлетворять требованиям:

1. Защита государственной и публичной информации в классах АС определяется по НД ТЗИ:
   1) А-1 – стандартные функциональные профили защищенности в КС, входящих в состав АС, предназначенных для автоматизации деятельности органов государственной власти;
   2) А-2 – стандартные функциональные профили защищенности в КС, входящих в состав АС, предназначенных для автоматизации банковской деятельности;
   3) А-3 – стандартные функциональные профили защищенности в КС, входящих в состав АС управления технологическими процессами;
   4) А-4 – стандартные функциональные профили защищенности в КС, входящих в состав справочно-поисковых систем.
2. Защита персональных данных в классах АС опирается на требования НД ТЗИ с учетом:
   1) требований (дуализма) идентификации и аутентификации пользователей:
      - «не авторизованные пользователи» «вне протокола связи КС» с «открытым ключом» - уровень на внешнем эшелоне (Г-1) и 7-м эшелоне (Г-2) защиты КСЗ,
      - «авторизованные пользователи» – уровень на конкретном эшелоне защиты КСЗ;
   2) данные о пользователях, объектах и процессах КС, не должны становиться «открытыми» в результате допуска.
3. Двойственность «организации» и «последствий» «открытого доступа» в КС исключается:
   1) обеспечением доступа к объектам АС «без распознавания» за счет проектирования необходимых условий беспрепятственной доступности не выше уровня критерия гарантий Г-2;
   2) способностью защиты персональных данных (объектов КС) данного пользователя на наивысшем уровне критерия гарантий Г-7 (по эшелонам иерархии КСЗ):
   3) «встречным» функционированием «минимального набора функций доверительной конфиденциальности» и «максимального набора функций административной конфиденциальности административной» с реализацией критерия наблюдения за взаимодействием (табл. 4):

Табл. 4

Эшелоны организации защиты от НСД из неконтролируемой среды

Эшелон защиты	Действия административные	Действия доверительные	Форма документа	Регистрация
8-й - внешний эшелон	Получение информации субъектом (заявителем из неконтролируемой среды)	Просмотр содержания паспорта объекта без активного управления поведением WEB-страницы	Документ (бланк формы) в растровом изображении	Гость без регистрации
7-й эшелон	Передача информации / прием информации между объектом и субъектом	Возможность управления (воздействия на отображение содержимого) поведением WEB-страницы (пассивная обратная связь);	Конвертор бланка формы ✓ с растровым изображением императивной части (требования формы бланка по аутентификации заявителя) ✓ функциональными полями: - для аутентификации (заполнения) заявителем личности - запроса по сути заявления.	Внешний анализ
6-й эшелон	Конвертация текущих синтезированных сведений в формат, используемый субъектом	Возможность осуществить управление созданием содержимого WEB-страницы - ввести запрос и получить динамически заполненный ответ (активная обратная связь).	Дескриптор бланка формы: ✓ с лексическим именем бланка ✓ заполненными заявителем функциональными полями аутентификации личности ✓ незаполненными функциональными полями запроса по сути заявления	Защищенный журнал
5-й эшелон	Персонификация текущих субъектов	Регулируются администратором	Декодер полей лексического объекта на уникальные коды	Сигнализация об опасности
4-й эшелон	Синтез текущих сведений	Регулируются администратором	Дескриптор с полями запроса на уникальных кодах	Детальная регистрация
3-й эшелон	Персонификация текущих процессов	Регулируются администратором	Рескриптор с заполненными полями запроса	Анализ в реальном времени
2-й эшелон	Назначение атрибутов и значений объектов, субъектов и процессов	Регулируются разработчиком	Базы данных ДИС	В реальном времени
1-й эшелон	Декомпозиция исходных данных	Регулируются разработчиком	Данные ДИС	В реальном времени
Эталон КСЗ	Надзор за КСЗ и реагирование	Регулируются разработчиком	Надзор за СУБМ и СУБД и реагирование	В реальном времени

4. Методологически прием устранения двойственности требования к доступности в ДИС, исходя из «встречной» организации защиты от НСД, в этом случае требует (табл. 5 – 8):

Таблица 5

Формирование функционального профиля необходимых условий защищенности от НСД при неавторизованном доступе к объектам

Номер профиля	<=>	Перечень необходимых условий для беспрепятственного допуска как базового уровня функциональных услуг безопасности КС										Функциональные критерии по группам
3.КЦД.НУ, *Г-1*	=	КД-1		КА-1		**КО-1**		КК-1		КВ-1		Конфиденциальность
Внешний ***ЭШЕЛОН*** *КСЗ КС*		ЦД-1		ЦА-1		ЦО-1		-		ЦВ-1		Целостность
		ДР-1		ДС-1		ДЗ-1		ДВ-1		-		Доступность
		НР-1	**Г-1**	**НИ-1**	**НК-1**	**НО-1**	НЦ-1	НТ-1	**НВ-1**	НА-1	НП-1	Наблюдаемость

Таблица 6

Формирование иерархии уровней стандартных функциональных профилей защищенности и критериев гарантий до 3.КЦД.5, Г-6

Номер профиля	<=>	Перечень уровней функциональных услуг безопасности КСЗ									Функциональные критерии по группам
											Таблица 6.1
3.КЦД.1, *Г-2*	=	**КД-2**		*КА-1*		***КО-1***		*КК-1*		***КВ-1***	Конфиденциальность
7-й ЭШЕЛОН КСЗ ДИС		***ЦД-1***		*ЦА-1*		***ЦО-1***		-		***ЦВ-1***	Целостность
		ДР-1		*ДС-1*		*ДЗ-1*		***ДВ-1***		-	Доступность
		НР-2	**Г-2**	**НИ-2**	***НК-1***	**НО-2**	**НЦ-2**	**НТ-2**	***НВ-1***	*НА-1*	*НП-1*	Наблюдаемость
											Таблица 6.2
3.КЦД.2, *Г-3*	=	***КД-2***		**КА-2**		***КО-1***		*КК-1*		**КВ-2**	Конфиденциальность
6-й ЭШЕЛОН КСЗ ДИС		***ЦД-1***		**ЦА-2**		*ЦО-1*		-		**ЦВ-2**	Целостность
		ДР-1		*ДС-1*		*ДЗ-1*		***ДВ-1***		-	Доступность
		НР-2	**Г-3**	***НИ-2***	***НК-1***	***НО-2***	***НЦ-2***	***НТ-2***	***НВ-1***	*НА-1*	*НП-1*	Наблюдаемость
											Таблица 6.3
3.КЦД.3, *Г-4*	=	***КД-2***		***КА-2***		***КО-1***		**КК-1**		**КВ-3**	Конфиденциальность
5-й ЭШЕЛОН КСЗ КС		**ЦД-2**		**ЦА-3**		**ЦО-2**		-		***ЦВ-2***	Целостность
		ДР-2		***ДС-1***		***ДЗ-1***		**ДВ-2**		-	Доступность
		НР-3	**Г-4**	***НИ-2***	***НК-1***	***НО-2***	**НЦ-3**	***НТ-2***	**НВ-2**	*НА-1*	*НП-1*	Наблюдаемость
											Таблица 6.4
3.КЦД.4, *Г-5*	=	**КД-3**		**КА-3**		***КО-1***		***КК-1***		***КВ-3***	Конфиденциальность
4-й ЭШЕЛОН КСЗ КС		**ЦД-3**		***ЦА-3***		***ЦО-2***		-		***ЦВ-2***	Целостность
		ДР-3		**ДС-2**		**ДЗ-2**		***ДВ-2***		-	Доступность
		НР-4	**Г-5**	***НИ-2***	***НК-1***	**НО-3**	***НЦ-3***	***НТ-2***	***НВ-2***	**НА-1**	**НП-1**	Наблюдаемость
											Таблица 6.5
3.КЦД.5, *Г-6*	=	**КД-4**		**КА-4**		***КО-1***		**КК-2**		**КВ-4**	Конфиденциальность
3-й ЭШЕЛОН КСЗ ДИС		**ЦД-4**		**ЦА-4**		***ЦО-2***		-		***ЦВ-3***	Целостность
		ДР-3		**ДС-3**		**ДЗ-3**		**ДВ-3**		-	Доступность
		НР-5	**Г-6**	***НИ-2***	***НК-2***	***НО-3***	***НЦ-3***	***НТ-2***	***НВ-2***	***НА-1***	***НП-1***	Наблюдаемость

Примечание: в связи с обязательностью автоматизации КСЗ (от уровня критерия Г-4) политика услуги ЦД с ЦД-1 в профиле 3.КЦД.3 повышается до ЦД-2 и в профиле 3.КЦД.4 – до ЦД-3.

Таблица 7

Формирование сверх стандартного функционального профиля защищенности КСЗ - 3.КЦД.6, Г-7

Номер профиля	<=>	Перечень уровней функциональных услуг как необходимых условий политики безопасности - элементы функциональных критериев КСЗ									Функциональные критерии по группам
3.КЦД.6, Г-7	=	***КД-4***		***КА-4***		***КО-1***		**КК-3**		***КВ-4***	Конфиденциальность
2-й ЭШЕЛОН КСЗ ДИС		***ЦД-4***		***ЦА-4***		***ЦО-2***		-		***ЦВ-3***	Целостность
		ДР-3		***ДС-3***		***ДЗ-3***		***ДВ-3***		-	Доступность
		НР-5	**Г-7**	**НИ-3**	***НК-2***	***НО-3***	***НЦ-3***	**НТ-3**	**НВ-3**	**НА-2**	**НП-2**	Наблюдаемость

1-й ЭШЕЛОН КСЗ ДИС

Таблица 8

Принципы объектного ориентирования базы данных по единству свойств объектов и нормализации структуры связей концептуальной схемы и информационной базы

Социальное управление	**Методология науки**	**Методология деятельности**	**Динамико-стохастическое моделирование**	**Познание**	**Знание**	**Мышление**	**Стили мышления**	**Уровни (формы) мышления**	**Интерфейсы электронного гиппокампа и конверторы дескрипции**	**Модули систем управления**	**Правила формирования**	**Язык логики**	**Защищенный ВЭБ – сервер ин - страниц АРМ города**
Целевые функции	Принятие решения	Структура деятельности	Системное описание искомого	Сущее	Единство и противоположность	Общее	Оптимизационный	Диалектическая логика	Рамка таблицы	Риски и выгоды обитания в данном месте	Требования учета свойств	S_1, S_2, S_3	Процессор распознавания задач
Предмет деятельности	Оценка последствий	Логическая организация	Информационная концепция	Проявление	Качество	Модель связей	Причинно-следственный (детерминизм)	Формальная логика	Шапка таблицы	Сложная проблемная	Типы показателей	<=>	Процессор управления
Проблемные области	Прогноз	Методы	Формализация	Содержание	Количество	Особенное	Диалектико-алгоритмический (синтез)	Логика науки	Колонки таблицы	Проблемная	Научные направления	P**	Процессор программ
Предметные области	Анализ	Средства	Алгоритм	Форма	Отрицание отрицания	Единичное	Фрактально-голографический (декомпозиция во времени)	Логика классов	Строки таблицы	Сложная предметная	Научные разделы	P*	Процессор процедур
Задачи	Исследование	Технологическая карта	Программа	Критерии	Сценарии развития	Отражение	Вихревой (декомпозиция в пространстве)	Логика 2-го порядка	Поля множеств	Предметная	Свойства	P	Процессор процессов
Сферы подготовки решений	Развитие	Этап	Стохастика в объеме основных свойств	Статистика	Аксиомы	Репрезентативность	Модель (терм, предикат)	Логика 1-го порядка	Наполнение полей	Состояние в пространстве	Скорость изменения состояний	Логические связки	Процессор команд
Сущности Сущего *(атомы баз данных)*	Субъекты, Объекты, Связи	Исследование операций	Верификация	Ограничения по качеству	Вывод	Мысли	Эмоции	Логика 0-го порядка	Правила наполнения полей	Допуски по вероятности рескрипции	Реальное время	Алфавит логики	Процессор данных

С У Б М И К Р О С С - А С С Е М Б Л Е Р (С К С З - Н С Д)

С У Б Д И Б А З Ы Д А Н Н Ы Х (С К С З - Н С Д)

Атом – файл	Атом – файл	Атом – файл	Атом – файл	Атом - файл	Атом – файл	Атом – файл	Атом – файл	Атом – файл	Атом – файл	Атом – файл	Атом – файл	Атом – файл	Атом – файл

Таблица 9

Структура эталона КСЗ в ДИС от НСД
с функциями «третьей независимой стороны»

Номер СФПЗ / Политика услуги	З.КЦД. НУ	З.КЦД.1	З.КЦД.2	З.КЦД.3	З.КЦД.4	З.КЦД.5	З.КЦД.6
1.1 **КД**	КД-1	КД-2	КД-2	КД-2	КД-3	КД-4	КД-4
1.2 **КА**	КА-1	КА-1	КА-2	КА-2	КА-3	КА-4	КА-4
1.3 **КО**	КО-1	КО-1	КО-1	КО-1	КО-1	КО-1	КО-1
1.4 **КК**	КК-1	КК-1	КК-1	КК-2	КК-2	КК-2	КК-3
1.5 **КВ**	КВ-1	КВ-1	КВ-2	КВ-3	КВ-3	КВ-4	КВ-4
2.1 **ЦД**	ЦД-1	ЦД-1	ЦД-2	ЦД-3	ЦД-4	ЦД-4	ЦД-4
2.2 **ЦА**	ЦА-1	ЦА-1	ЦА-2	ЦА-3	ЦА-3	ЦА-4	ЦА-4
2.3 **ЦО**	ЦО-1	ЦО-1	ЦО-1	ЦО-2	ЦО-2	ЦО-2	ЦО-2
2.4 Не проектируется	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.5 **ЦВ**	ЦВ-1	ЦВ-1	ЦВ-2	ЦВ-2	ЦВ-2	ЦВ-3	ЦВ-3
3.1 **ДР**	ДР-1	ДР-1	ДР-1	ДР-2	ДР-2	ДР-3	ДР-3
3.2 **ДС**	ДС-1	ДС-1	ДС-1	ДС-2	ДС-2	ДС-3	ДС-3
3.3 **ДЗ**	ДЗ-1	ДЗ-1	ДЗ-1	ДЗ-1	ДЗ-2	ДЗ-3	ДЗ-3
3.4 **ДВ**	ДВ-1	ДВ-1	ДВ-1	ДВ-2	ДВ-2	ДВ-3	ДВ-3
3.5 Не проектируется	*0*	*0*	*0*	*0*	*0*	*0*	*0*
4.1.1 **НР**	НР-1	НР-2	НР-2	НР-3	НР-4	НР-5	НР-5
4.1.2 ***Г***	*Г-1*	*Г-2*	*Г-3*	*Г-4*	*Г-5*	*Г-6*	*Г-7*
4.2.1 **НИ**	НИ-1	НИ-1	НИ-2	НИ-2	НИ-2	НИ-2	НИ-3
4.2.2 **НК**	НК-1	НК-1	НК-1	НК-2	НК-2	НК-2	НК-2
4.3.1 **НО**	НО-1	НО-2	НО-2	НО-3	НО-3	НО-3	НО-3
4.3.2 **НЦ**	НЦ-1	НЦ-2	НЦ-2	НЦ-3	НЦ-3	НЦ-3	НЦ-3
4.4.1 **НТ**	НТ-1	НТ-2	НТ-2	НТ-2	НТ-2	НТ-2	НТ-3
4.4.2 **НВ**	НВ-1	НВ-1	НВ-1	НВ-2	НВ-2	НВ-2	НВ-3
4.5.1. **НА**	НА-1	НА-1	НА-1	НА-2	НА-2	НА-2	НА-2
4.5.2 **НП**	НП-1	НП-1	НП-1	НП-2	НП-2	НП-2	НП-2

5. В соответствии с требованиями НД ТЗИ, начиная с уровня Г-4, система управления конфигурацией КСЗ ДИС от НСД должна базироваться на автоматизированных средствах. Для достижения цели и, исходя из наличия в столбце «Наблюдение» двух колонок, в целях достижения линейной зависимости строк политики услуг (таблица 10):

1) в столбцы критериев «конфиденциальность», «целостность», «доступность» вводятся дополнительно 2-е колонки с определителем колонок равном нулю;
2) не проектируемые услуги безопасности выражаются с определителем строк равных нулю.

Таблица 10

Матрица эталона автоматизированного КСЗ в ДИС от НСД
с функциями «третьей независимой стороны»

Номер СФПЗ / Политика услуги	**3.КЦД. НУ**	**3.КЦД.1**	**3.КЦД.2**	**3.КЦД.3**	**3.КЦД.4**	**3.КЦД.5**	**3.КЦД.6**
1.1.1 КД	**КД-1**	**КД-2**	**КД-2**	**КД-2**	**КД-3**	**КД-4**	**КД-4**
1.1.2 КД	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1.2.1 КА	**КА-1**	**КА-1**	**КА-2**	**КА-2**	**КА-3**	**КА-4**	**КА-4**
1.2.2 КА	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1.3.1 КО	**КО-1**	**КО-1**	**КО-1**	**КО-1**	**КО-1**	**КО-1**	**КО-1**
1.3.2 КО	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1.4.1 КК	**КК-1**	**КК-1**	**КК-1**	**КК-2**	**КК-2**	**КК-2**	**КК-3**
1.4.2 КК	*0*	*0*	*0*	*0*	*0*	*0*	*0*
1.5.1 КВ	**КВ-1**	**КВ-1**	**КВ-2**	**КВ-3**	**КВ-3**	**КВ-4**	**КВ-4**
1.5.2 КВ	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.1.1 ЦД	**ЦД-1**	**ЦД-1**	**ЦД-2**	**ЦД-3**	**ЦД-4**	**ЦД-4**	**ЦД-4**
2.1.2 ЦД	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.2.1 ЦА	**ЦА-1**	**ЦА-1**	**ЦА-2**	**ЦА-3**	**ЦА-3**	**ЦА-4**	**ЦА-4**
2.2.2 ЦА	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.3.1 ЦО	**ЦО-1**	**ЦО-1**	**ЦО-1**	**ЦО-2**	**ЦО-2**	**ЦО-2**	**ЦО-2**
2.3.2 ЦО	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.4 1 ***не проектируется***	**0**	**0**	**0**	**0**	**0**	**0**	**0**
2.4 2 не проектируется	*0*	*0*	*0*	*0*	*0*	*0*	*0*
2.5.1 ЦВ	**ЦВ-1**	**ЦВ-1**	**ЦВ-2**	**ЦВ-2**	**ЦВ-2**	**ЦВ-3**	**ЦВ-3**
2.5.2 ЦВ	*0*	*0*	*0*	*0*	*0*	*0*	*0*
3.1.1 ДР	**ДР-1**	**ДР-1**	**ДР-1**	**ДР-2**	**ДР-2**	**ДР-3**	**ДР-3**
3.1.2 ***ДР***	*0*	*0*	*0*	*0*	*0*	*0*	*0*
3.2.1 ДС	**ДС-1**	**ДС-1**	**ДС-1**	**ДС-2**	**ДС-2**	**ДС-3**	**ДС-3**
3.2.2 ДС	*0*	*0*	*0*	*0*	*0*	*0*	*0*
3.3.1 ДЗ	**ДЗ-1**	**ДЗ-1**	**ДЗ-1**	**ДЗ-1**	**ДЗ-2**	**ДЗ-3**	**ДЗ-3**
3.3.2 ДЗ	*0*	*0*	*0*	*0*	*0*	*0*	*0*
3.4.1 **ДВ**	ДВ-1	ДВ-1	ДВ-1	ДВ-2	ДВ-2	ДВ-3	ДВ-3
3.4.2 ДВ	*0*	*0*	*0*	*0*	*0*	*0*	*0*
3.5.1 ***не проектируется***	**0**	**0**	**0**	**0**	**0**	**0**	**0**
3.5 2 *не проектируется*	**0**	**0**	**0**	**0**	**0**	**0**	**0**
4.1.1 **НР**	НР-1	НР-2	НР-2	НР-3	НР-4	НР-5	НР-5
4.1.2 ***Г***	*Г-1*	*Г-2*	*Г-3*	*Г-4*	*Г-5*	*Г-6*	*Г-7*
4.2.1 **НИ**	НИ-1	НИ-1	НИ-2	НИ-2	НИ-2	НИ-2	НИ-3
4.2.2 **НК**	НК-1	НК-1	НК-1	НК-2	НК-2	НК-2	НК-2
4.3.1 **НО**	НО-1	НО-2	НО-2	НО-3	НО-3	НО-3	НО-3
4.3.2 **НЦ**	НЦ-1	НЦ-2	НЦ-2	НЦ-3	НЦ-3	НЦ-3	НЦ-3
4.4.1 **НТ**	НТ-1	НТ-2	НТ-2	НТ-2	НТ-2	НТ-2	НТ-3
4.4.2 **НВ**	НВ-1	НВ-1	НВ-1	НВ-2	НВ-2	НВ-2	НВ-3
4.5.1. **НА**	НА-1	НА-1	НА-1	НА-2	НА-2	НА-2	НА-2
4.5.2 **НП**	НП-1	НП-1	НП-1	НП-2	НП-2	НП-2	НП-2

Примечание: Матрица эталона автоматизированного КСЗ ДИС от НСД далее расширяется до конструкторов профилей защищенности по уровням политики услуг и технологий КСЗ ДИС..

6.3 Комплекс средств зашиты и объекты ДИС

1. Идеология структуры КСЗ ДИС от НСД (*версия Г-2*) как системы неотъемлемых свойств авторского программного комплекса обработки информации в корне отличается от проекта «стороннего контроля» множеств компонентов и данных «в черном ящике программного комплекса третьего разработчика»:

1) «наружный» КСЗ для стороннего программного комплекса является своеобразным межсетевым экраном «от внешних пользователей с другой политикой безопасности», заданной этим «внешним» для операционной системы и ПЗУ «фильтром»,
2) внешнее ограничение заданных возможностей назначения и области применения стороннего программного комплекса не исключает возможность их «враждебного использования»;
3) обслуживание «наружным» КСЗ сторонних программных комплексов, поставляемых в виде операционных систем, опирается в этом случае не более чем «доменную организацию» обработки информации без атомарной основы запоминания и распознавания образов файлов, независимо от логической конфигурации пространства сущностей и пространства высказываний, ими хранимых в виде данных;
4) данная практика защиты информации от НСД не дает возможности организации доверительного доступа/получения информации с более высоким уровнем конфиденциальности или делает такой доступ «условным».

2. Исключение противоречивости КСЗ «открытости обратной связи» власти и населения достигается за счет разработки собственного программного комплекса с построением структуры свойств КСЗ, исходя из внутренних принципов назначения и области применения ДИС:

1) автоматизированное управление непрерывной обработки массивов «открытой» информации из неконтролируемой среды с различной политикой безопасности не выше Г-2 и ограничением доступа к персональным данным до 3.КЦД.5, Г-7;
2) сфера электронных приемных со-интегральной системы местного электронного правления как неотъемлемой части электронного правительства Украины, функционирующих в режиме «открытого» доступа граждан к публичной и государственной информации с одновременной необходимостью защиты «открытых» сведений, принадлежащих другим гражданам, должностным лицам, обществу (публичная информация), государству.

3. Создание ДИС со свойствами КСЗ от НСД основано на паспортизации свойств компонентов:

1) атомы-файлы, независимо от логической конфигурации хранимых ими данных,
2) минимальное множество пассивных объектов: «Пользователь», «Процесс», «Объект» (здесь термины «объект» и «пассивный объект» воспринимается как омонимы).
3) органичная спецификация функциональности политик услуг и технологической карты.

4. Доменная структура распознавания образов свойств в иерархии уникального кода: Общее, каталоги, справочники, списки высказываний 2-го, 1-го и 0-го порядков, позволяет однозначно учитывать, маркировать и контролировать логически организованные компоненты КСЗ:

1) как специально предназначенные для реализации политики безопасности,
2) как могущие влиять на безопасность «опосредовано» через качество обеспечения функционирования компонентов первого типа.
3) компоненты, не задействованные на данном уровне политики какой-либо услуги.

5. Разработке структуры свойств пассивных объектов с возможностью маркировки их авторской аутентификации под контролем эталона делают возможной поставку и эксплуатацию ДИС с КСЗ:

- вне конкретной среды эксплуатации ДИС (типовая версия),
- для конкретной среды АС-3 (адаптация типовой версии).

6. Совместимость КСЗ ДИС с ВС АС достигается на технологической платформе (табл. 11):

Таблица 11

Технические характеристики технологической платформы реализации диалоговой информационной системы «НООСФЕРА» (ДИС «Ноосфера»)

№	Наименование	Описание
1	Доступ пользователя к системе	Локальный для однопользовательских или удаленный в многопользовательской.
2	Система взаимодействия	Многопользовательская система: сервер - клиенты. Однопользовательская система: сервер + клиент.
3	Клиентская часть	1. Удаленный доступ - WEB-интерфейс. Любая ОС с доступом через браузер, поддерживающий протокол HTTP и FTP. 2. Локальный доступ - Операционная система Windows.
4	Серверная часть	Распределенная система обработки данных на основе ОС Linux, Windows
5	Сервер баз данных	Поддержка баз данных в форматах: СУБД Firebird и/или Access
6	Сервер WEB доступа	ОС Linux или Windows.
7	Сервер обработки	ОС Windows сервер.
8	Формат обмена данных	Внутренний формат с конвертацией данных (поддержка обмена данными с клиентом в формате данных клиента).
9	Каналы связи сервер-клиент	Локальная или глобальная сеть, поддерживающая работу протокола TC/IP.
10	Защита данных	Защита на всех уровнях технологии обработки без возможности несанкционированного получения данных.
11	Минимальные типовые требования к оборудованию клиентской части удаленного доступа.	Любой ПК, обеспечивающий выход в сеть Интернет с использованием типового браузера и отображение графических данных 256 цветов с разрешением минимум 800x600 dpi (при получении ответов с графической информацией).
12	Минимальные типовые требования к оборудованию клиентской части локального доступа.	Типовой ПК, обеспечивающий выход в сеть Интернет с использованием типового браузера и отображение графических данных 256 цветов с разрешением минимум 800x600 dpi (при получении ответов с графической информацией). А также: Системный блок средней производительности: CPU 2 x 3 GHz, RAM 2 Gb, LAN 1x1000 Mbit, HDD 1x500 Gb
13	Типовые требования к оборудованию серверной части удаленного доступа.	WEB-сервер средней производительности: CPU 4 x 3 GHz, RAM 8 Gb, LAN 3x1000 Mbit, HDD 2x320 Gb scsi, Сервер обработки средней производительности: CPU 4 x 3 GHz, RAM 16 Gb, LAN 3x1000 Mbit, HDD 2x320 Gb scsi, Сервер баз данных средней производительности: CPU 4 x 3 GHz, RAM 16 Gb, LAN 3x1000 Mbit, HDD 6x320 Gb scsi
14	Пропускная способность каналов связи к серверу	Средняя пиковая нагрузка: Символьный режим около 1,2 Мбит/с, Графический режим около 16 Мбит/с
15	Режим работы серверной части	Круглосуточно
16	Зависимость от других информационных систем	Другие информационные системы могут использоваться как поставщики или потребители информации. Технология работы с данными обеспечивает в "неблагоприятных информационных условиях" полную автономию системы с "ручным" вводом данных.
17	Программная продукция и база данных	Программное обеспечение (ПО) и база данных (БД) в форме: 1. Исполняемых файлов под ОС Windows (сервер обработки). 2. Исполняемых скриптов, файлов конфигурации типового ПО (WEB-сервер). 3. Структура БД в формате СУБД Firebird и/или Access (сервер баз данных). 4. Установленные библиотеки GDI+ для построения векторной графики

Примечания:

1. Данный вид технологической платформы ДИС «Ноосфера» представлен под существующую практику сбора и манипулирования данными в отраслях, ведомствах и органов местного самоуправления Украины, при этом:
   - выбор технологической платформы определяется возможностями заказчика и текущим наличием уже имеющихся у заказчика программных и аппаратных средств;
   - минимальные требования к аппаратному обеспечению определяются объемом обрабатываемых данных и количеством запросов клиентов, обслуживаемых в реальном времени.
2. При формировании более высоких требований проблемных областей управления и наличии возможностей у такого заказчика, технологическая платформа ДИС «Ноосфера» способна к развитию ее информационной базы и концептуальной схемы без ограничений пределами иностранных технологий управления развитием.

6.4 Определение несанкционированного доступа

1. Под НСД следует понимать доступ к информации с использованием средств, включенных в состав ДИС (поставка) и/или ДИС в ВС АС (эксплуатация):
   1) нарушающие установленные правила разграничения доступа (как базовое понятие);
   2) нарушение ПРД за счет качества функционирования средств, входящими в состав КСЗ, поскольку система НД ТЗИ в области защиты информации от НСД в АС охватывает круг вопросов, связанных с созданием и поддержкой в работоспособном состоянии системы мер, которые направлены на обеспечение соблюдения требований политики безопасности информации при ее обработке в КС.
2. НСД может осуществляться:
   1) с использованием совокупности программно-аппаратного обеспечения, включенного в ДИС при разработке или системным администратором АС в процессе эксплуатации, и входящих в утвержденную конфигурацию ДИС,
   2) с использованием программно-аппаратных средств, включенных в состав ДИС злоумышленником.
3. К основным способам НСД относятся:
   1) непосредственное обращение к объектам с целью получения определенного вида доступа;
   2) создание программно-аппаратных средств, выполняющих обращение к объектам в обход средств защиты;
   3) модификация средств защиты, позволяющая осуществить НСД;
   4) внедрение в ДИС или в ВС АС программных или аппаратных механизмов, нарушающих предполагаемую структуру и функции ДИС и позволяющих осуществить НСД.

6.5 Модель нарушителя

В качестве нарушителя рассматривается лицо, которое может получить доступ к работе с включенными в состав КС средствами. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами КС.

Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый последующий уровень включает в себя функциональные возможности предыдущего:

- первый уровень определяет самый низкий уровень возможностей ведения диалога в ДИС — возможность запуска фиксированного набора задач (программ), реализующих заранее предусмотренные функции по обработке информации;
- второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации;
- третий уровень определяется возможностью управления функционированием КС, т.е. воздействием на базовое программное обеспечение системы, а также на состав и конфигурацию ее оборудования;
- четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт аппаратных компонентов КС, вплоть до включения в состав КС собственных средств с новыми функциями по обработке информации.

Предполагается, что в своем уровне нарушитель - это специалист высшей квалификации, имеющий полную информацию об АС, ДИС и КСЗ.

Такая классификация нарушителей является полезной для использования:

- в процессе оценки рисков,
- анализа уязвимости системы,
- эффективности существующих и планируемых мер защиты
- определения ответных мер по отношению к нарушителю.

7 Основные принципы обеспечения защиты информации

7.1 Планирование зашиты и управление системой защиты

1. В соответствии с требованиями данной Концепции обеспечения защиты информации от НСД (*версия Г-2*), планирование защиты и управления ДИС предполагает два уровня развития:

1) вне конкретной среды эксплуатации ДИС (типовая версия),
2) для конкретной среды АС-3 (адаптация типовой версии).

2. Принципы разработки ДИС исключают противоречие типовой версии Г-2 условиям адаптации данного программного комплекса со свойствами защиты информации от НСД на все типы АС, удовлетворяющие техническим характеристикам технологической платформы ДИС, более того:

1) создание средств защиты, которые могли бы эффективно противостоять вероятным угрозам и обеспечивали бы в дальнейшем соблюдение политики безопасности при обработке информации, является основной целью создания КСЗИ АС;
2) требования к жизненным циклам типовой версии КСЗ ДИС и КСЗИ АС идентичны;
3) создание КСЗИ начинается с анализа объекта защиты и возможных угроз, которые в КСЗ ДИС учитываются созданием наивысшего (полного) профиля защищенности информации с наивысшими гарантиями критериев (для ДИС) от начала разработки ДИС;
4) требования по проектированию АС с целью интеграции средств защиты, предоставляемых каждым компонентом, включают КСЗ ДИС от НСД в единый комплекс средств защиты от определенных угроз;
5) разработка спецификаций функциональности политики безопасности КСЗ ДИС от НСД в составе функциональных спецификаций политик услуг безопасности (с перечнем и описанием) и технологических режимов на различных уровнях политик услуг безопасности не противоречат политике безопасности КСЗИ АС и обосновывают технологические возможности применения ДИС в ВС АС по ее назначению и области применения;
6) разработка КСЗ ДИС как общего и целостного спектра стационарных профилей защищенности информации обеспечивают возможность для КСЗИ АС:
   - выполнения на всех (любых) этапах сборки и подготовки данных как исходных данных для их анализа на следующем этапе обработки данных;
   - уточнения начальных условий и возврата на более ранние этапы по множеству компонентов в интересах множества пользователей;
   - манипулирования свойствами подлежащих (или возможных) защите ресурсов путем маркировки свойства аутентификации пользователей, процессов и отсылок на право авторства в искомых ресурсах.

3. Определение стоимости КСЗ ДИС от НСД на стоимости КСЗИ АС не отражается, поскольку является свойством ДИС как программного комплекса, что облегчает расчеты сопоставимости КСЗИ от размеров возможных ущербов и позволяет направить высвобожденные средства на усиление остальных мероприятий КСЗИ в соответствии с НД ТЗИ.

4. Сформулированное единство политики безопасности КСЗ ДИС и КСЗИ АС не усложняет порядок составления плана защиты АС, в том числе по описанию последовательности и содержания всех стадий и этапов жизненного цикла КСЗИ и их соответствию стадиям и этапам жизненного цикла АС.

7.2 Основные принципы управления доступом в ДИС

7.2.1 Непрерывная защита

1. Защита информации в ДИС должна обеспечиваться на протяжении всего ее существования.

2. С момента создания объекта ДИС или его импорта в систему и вплоть до его уничтожения или экспорта из системы все запросы на доступ к объекту и объекта на доступ к другим объектам должны контролироваться КСЗ:

1) абсолютно все запросы на доступ к объектам должны контролировались КСЗ,
2) не должно существовать возможности получить к объекту доступ в обход КСЗ,
3) первым условием защиты объектов ДИС является способность КСЗ обеспечивать собственную целостность и управляемость.

3. Особое значение имеет правило паспортизации объекта внутри ДИС как начальное условие его существования для КСЗ (по наименованию и декомпозиции свойств как атрибутов доступа).

7.2.2 Атрибуты доступа

1. Атрибут доступа - это термин, используемый для описания любой информации, используемой при управлении доступом, связанной с пользователями, процессами или пассивными объектами (***далее термины «объект» и «пассивный объект» воспринимается как синонимы***).

2. Атрибуты доступа объекта являются частью его представления в ДИС как его свойства, при этом соответствие атрибутов доступа и объекта (как идентичных и адекватных свойства):

1) признается явным при наличии достоверной информации об объекте,
2) признается неявным при необходимости распознавания образа (свойства) объекта, допуск к которому обеспечивается с оформлением «паспорта тревоги» и присвоении временных кодов (лексического, уникального и декодированного).

3. Реализации политики безопасности КСЗ ДИС на базе паспортизации (реляционная база):

1) обеспечивает изоляцию объектов внутри сферы управления;
2) гарантирует разграничение:
   - запросов доступа,
   - управление потоками информации между объектами;
3) имеет связь с информацией об атрибутах доступа, позволяющей:
   - идентифицировать объекты,
   - проверять легальность доступа (пользователей, процессов).

4. Реализация политики безопасности обеспечивается назначением КСЗ набора функций услуг безопасности по каждому из множеств запросов пользователей и процессов:

1) от момента попытки получения доступа к пассивным объектам ДИС (в том числе о других пользователях, процессах и объектах);
2) от уровня авторизации запроса на конкретном эшелоне защиты КСЗ.

5. Отображение функциональности ДИС в пространство, в котором не рассматриваются права собственности:

1) по инициативе ДИС не производится,
2) при необходимости анализа отображений объектов без прав собственности учитывает их аргументы доступа как «нераспознанных объектов».

6. Для отображения функциональности ДИС в пространство используется табличная матрица отсылок аргументов доступа пользователей, процессов и пассивных объектов к свойствам их авторизации с полнотой насыщения ответа информацией в зависимости от объема запроса.

7.2.3 Доверительное и административное управление доступом

1. Под доверительным управлением понимается разрешение КСЗ ДИС доступа обычным пользователям управлять (доверие управлением) потоками информации между другими пользователями и объектами своего домена (например, на основании права владения объектами) без административного вмешательства.

2. Под административным управлением понимается разрешение КСЗ управлять потоками информации между пользователями и объектами только специально авторизованным пользователям (процессам).

3. Маркировка свойства авторства в паспорте объектов позволяет:

1) при административном управлении доступом к объектам внутри системы гарантирует исключение изменения потоков информации, установленных администратором, со стороны обычных пользователей;
2) при доверительном управлении доступом система его реализации позволяет обычному пользователю модифицировать, в том числе создавать и уничтожать новые потоки информации внутри системы.

4. Создание дополнительных потоков информации может быть вызвано:

1) модификацией атрибутов доступа пользователя, процесса или пассивного объекта;
2) созданием новых объектов (включая копирование существующих);
3) экспортом или импортом объектов.

5. Под системой требований к созданию дополнительных потоков информации понимается:

1) Постоянство атрибутов доступа:
   - при реализации системой административного управления доступом обычный пользователь не должен иметь возможность изменять атрибуты доступа объекта, в том числе передавать другому пользователю свои полномочия по доступу к существующему объекту;
   - при реализации системой доверительного управления доступом возможно предоставление обычному пользователю права изменять атрибуты доступа принадлежащего ему объекта.
2) Создание новых объектов:
   - если система реализует административное управление доступом и политика потоков информации, созданная администратором, определяет, что два пользователя не могут разделять информацию, то ни один из них не должен быть способен:
     - создать объект, доступный другому пользователю;
     - скопировать объект с нарушением правил определения (задания) атрибутов доступа и присвоения скопированному объекту этих атрибутов.
   - если система реализует доверительное управление доступом и политика безопасности это определяет, возможность предоставления обычному пользователю права устанавливать атрибуты доступа для вновь создаваемого объекта, в том числе с указанием пользователей, которые могут иметь права доступа к объекту.
3) Экспорт и импорт объектов:
   - если система реализует административное управление доступом, то атрибуты доступа объекта должны сохраняться при его экспорте на внешний носитель с дополнительными правилами присвоения атрибутов доступа импортируемому объекту;
   - если система реализует доверительное управление доступом, то возможны:
     - экспорт объектов без сохранения атрибутов доступа;

- импорт обычным пользователем объекта, с последующим присвоением ему атрибутов доступа по усмотрению пользователя;

➢ в соответствии с политикой доверительного и административного управления доступом атрибуты доступа объекта при выполнении некоторых операций, например, при его резервном копировании, должны сохраняться при восстановлении объекта из резервной копии, то его атрибуты доступа также должны быть восстановлены.

7.2.4 Обеспечение персональной ответственности

1. Каждый сотрудник из персонала АС, эксплуатирующей ДИС, должен быть ознакомлен с необходимыми положениями политики безопасности КСЗ ДИС и нести персональную ответственность за их соблюдение.

1) Политика безопасности должна устанавливать обязанности сотрудников, в особенности имеющих административные полномочия, и виды ответственности за неисполнение этих обязанностей, как правило, в рамках организационных мер безопасности.
2) Политика безопасности должна рассматривать пользователя ДИС не как физическое лицо, а как объект, которому присущи определенные атрибуты и поведение.

2. Эффективность организационных мер обеспечивается поддержкой со стороны ДИС, где КСЗ обеспечивает регистрацию:

1) действий объектов-пользователей по использованию ресурсов системы,
2) других действий и событий, которые тем или иным образом могут повлиять на соблюдение реализуемой КС политики безопасности.

3. КСЗ ДИС предоставляет имеющим административные полномочия пользователям возможность:

1) просматривать и анализировать данные регистрации, представляемые в виде журналов регистрации,
2) выявлять опасные с точки зрения политики безопасности события,
3) устанавливать их причины и пользователей, ответственных за нарушения политики безопасности.

7.3 Услуги безопасности

1. Обеспечение безопасности информации достигается через определение политикой безопасности КСЗ к каким объектам применяется услуга, по отношению к которой определенное подмножество объектов называется защищенными объектами.

2. Каждая услуга представляет собой набор функций, позволяющих противостоять некоторому множеству угроз за счет определенных технологических режимов данных наборов функций на каждом уровне безопасности.

3. Структура обеспечения безопасности информации КСЗ ДИС представлена в иерархии спецификаций функциональности:

1) Набор функциональных услуг стандартных профилей защищенности информации по критериям (Приложение 1).
2) Конструктор профилей защищенности по уровням критериев политики услуг КСЗ ДИС (Приложение 2).
3) Матрица технологических заданий по реализации политики услуг безопасности КСЗ ДИС (Приложение 3).
4) Набор функциональных услуг стандартных профилей защищенности информации по политике услуг КСЗ в ДИС (Приложение 4).
5) Конструктор технологических режимов по реализации услуг безопасности КСЗ ДИС (Приложение 5).

4. Структура услуг безопасности КСЗ ДИС представлена в таблице 10 «Матрица эталона автоматизированного КСЗ ДИС от НСД с функциями «третьей независимой стороны».

5. При поставке ДИС в виде программного комплекса заказчик выставляет разработчику требования к функциональности ДИС и КСЗ на уровне гарантий договора поставки.

6. При установке ДИС на ВС АС заказчик обязан самостоятельно:

1) согласовать разработчику техническое задание на адаптацию и инсталляцию ДИС (со свойствами КСЗ) на ВС АС по НД ТЗИ 3.6-001-2000 для КСЗ с уровнем критериев гарантий Г-2:
   - набора функциональных услуг внешнего профиля защищенности «от рисков открытого доступа» необходимыми условиями 3.КЦД.НУ (Г-1) инсталлируются как внешний (8-й) эшелон защиты во всех вариантах поставок и в эксплуатации ДИС;
   - наборов функциональных услуг профилей защищенности для аутентифицированных запросов из неконтролируемой среды после контроля допуска необходимыми условиями 3.КЦД.НУ (Г-1):
     - на уровне «пассивного управления объектами», как 7-го эшелона защиты объектов, КСЗ реализуется в виде профиля 3.КЦД.1, Г-1,
     - на уровне «активного управления объектами», как 6-го эшелона защиты объектов, КСЗ реализуется в виде профиля 3.КЦД.2, Г-2;
2) осуществить приемку КСЗ ДИС в составе АС силами заказчика (для версии Г-2 государственная экспертиза не проводится).

7. Передача в администрирование стандартных профилей защиты информации КСЗ для заказчика производится в следующем порядке:

1) КСЗ ДИС от НСД на уровень гарантий КСЗИ в АС относится по версии Г-2 3.КЦД.2,
2) КСЗ ДИС от НСД сдается непосредственно заказчику на основании тестовых испытаний,
3) профиль КСЗ 3.КЦД.5, Г-6 является внутренним ресурсом КСЗ ДИС от НСД,
4) профиль КСЗ 3.КЦД.6, Г-7 является контрольным ресурсом разработчика.

8. На рис. 2 представлена структура стандартного функционального профиля защищенности КСЗ

3.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, КВ-4,
ЦД-4, ЦА-4, ЦО-2, ЦВ-3,
ДР-3, ДС-3, ДЗ-3, ДВ-3,
НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1} , -

с внутренним резервом ДИС до 3.КЦД.6, Г-7, обслуживающей автоматизированные системы класса 3 (*версия Г-2*) с повышенными требованиями к обеспечению конфиденциальности, целостности и доступности обрабатываемой информации из незащищенной среды (Критерии):

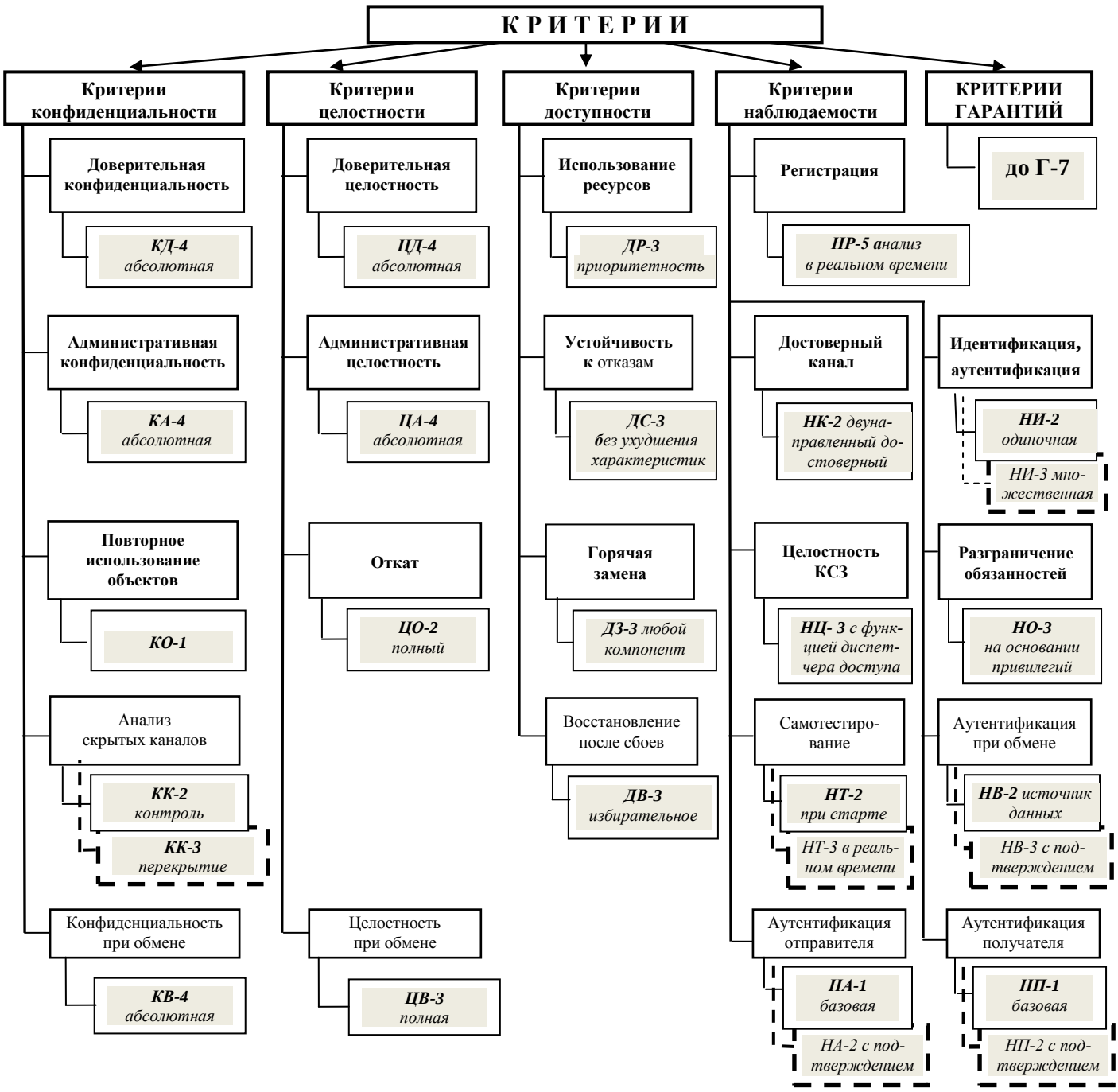


Рис. 2 Структура стандартного функционального профиля защищенности 3.КЦД.5,6 (Г-6,**7)**

7.4 Гарантии

1. Дополнительно к функциональным критериям, позволяющим оценить наличие услуг безопасности в ДИС, Критерии (политики безопасности КСЗ) содержат также критерии гарантий, позволяющих оценить корректность реализации услуг.

2. Критерии гарантий включают требования по семи уровням гарантий:
   - ✓ к архитектуре КСЗ,
   - ✓ к среде разработки,
   - ✓ к последовательности разработки,
   - ✓ к испытаниям КСЗ,
   - ✓ к среде функционирования,
   - ✓ к эксплуатационной документации, -

формирующих конкретную структуру требований к критериям гарантий безопасности КСЗ ДИС, достигаемых в процессе разработки (приложение 6).

3. Иерархия уровней гарантий отражает постепенно нарастающую степень уверенности в том, что предоставляемые услуги позволяют противостоять определенным угрозам, что реализующие их механизмы, в свою очередь, корректно реализованы и могут обеспечить ожидаемую потребителем степень защищенности информации при эксплуатации ДИС в составе АС.

4. Гарантии обеспечиваются как в процессе разработки, так и в процессе оценки:

1) в процессе разработки выполнение гарантий обеспечивается действиями разработчика;

2) в процессе оценки контроль выполнения гарантий обеспечиваются:
   - ➢ путем проверки соблюдения разработчиком требований Критериев, анализа документации, процедур разработки и поставки,
   - ➢ другими действиями экспертов, проводящих оценку.

7. Последовательность иерархии действий позволяет сконструировать матрицу иерархии технологических режимов разработки по уровням гарантий безопасности КСЗ ДИС (приложение 7).

8 Основные принципы реализации программно-технических средств

8.1 Функции и механизмы зашиты

1. Основными задачами комплекса средств защиты объектов в ДИС являются:
   1) изоляция объектов КС внутри сферы управления,
   2) проверка всех запросов доступа к объектам,
   3) регистрация запросов и результатов их проверки и/или выполнения.

2. Решение задач защиты объектов КСЗ опирается на паспортизацию и маркировку достаточного и необходимого количества списков свойств любой элементарной функции любой из услуг, реализуемой КСЗ, где любая из этих функций одновременно может относиться (иметь свойства) к функциям:
   1) изоляции, проверки или регистрации,
   2) обеспечения конфиденциальности, целостности и доступности информации,
   3) управляемости КСЗ,
   4) наблюдаемости действий пользователей.

3. При маркировке свойств каждой функции необходимо указывать ее свойства реализации:
   1) одним или более внутренними программными механизмами ДИС,
   2) для реализации в составе единого программного механизма нескольких услуг.

4. Реализация механизмов защиты ДИС учитывает их методическое различие:
   1) программные или аппаратные средства,
   2) криптографические преобразования,
   3) различные методы проверки полномочий и т.п.

5. Выбор методов и механизмов разработчиком преследует цели реализации функций защиты в соответствии с декларируемой политикой безопасности и требованиями гарантий.

8.2 Реализация комплекса средств защиты

1. КСЗ обеспечивает непрерывную защиту объектов ДИС от НСД следующим образом:
   1) КСЗ исключает возможность получения доступа к объектам ДИС в обход КСЗ,
   2) КСЗ контролирует и пресекает попытки взлома и несанкционированной модификации,
   3) базовые программные механизмы КСЗ, реализующие политику безопасности, не являются субъектами для несанкционированной модификации или замены.

2. КСЗ имеет модульную структуру:
   1) на уровне архитектуры ДИС реализован как набор относительно независимых частей.
   2) каждая из этих частей взаимодействует с другими частями посредством хорошо определенных интерфейсов.

3. КСЗ спроектирован как набор логических групп программного обеспечения, где каждая логическая группа решает определенные задачи.
   1) для простейших случаев сходные функции (свойства) сосредоточены в определенных исходных файлах.
   2) для более сложных по рискам ситуаций используется скрытие данных, инкапсуляции и других механизмов, позволяющих получить уверенность, что каждый модуль решает единственную задачу и все данные, которыми он оперирует, либо определены внутри и доступны как локальные, либо передаются в качестве параметров или схожим образом.
   3) любое взаимодействие между компонентами осуществляется только через известные и описанные каналы (интерфейсы).
   4) КСЗ спроектирован как набор групп функций (слоев), которые взаимодействуют только с соседними нижним и верхним слоями.

8.3 Концепция диспетчера доступа

1. При реализации КСЗ используется концепция диспетчера доступа, которая является наиболее проработанной теоретически и проверенной на практике из всех возможных методов.

2. Диспетчер доступа характеризуется тремя атрибутами:

1) обеспечение непрерывной и полной защиты:
   - всегда активен,
   - контролирует все запросы доступа к любому защищенному объекту, который подвергается воздействию.
2) Достоверность:
   - является защищенным от модификации путем программной изоляцией домена КСЗ от доменов остальных процессов.
   - контроль изоляции процессов друг от друга является отдельной задачей КСЗ.
3) небольшие размеры:
   - код (реализация) разборчив и способен к проверке в процессе оценки;
   - включает минимальный необходимый набор программных механизмов, непосредственно реализующих проверку легальности запросов доступа и их регистрацию;
   - использованы типовые принципы организации для всех эшелонов (слоев) КСЗ.

3. Главная цель диспетчера доступа — обеспечение известной точки прохождения всех запросов внутри ДИС и достижение гарантии того, что потоки информации между объектами-пользователями, объектами-процессами и пассивными объектами отвечают требованиям политики безопасности, при этом:

1) диспетчер доступа служит барьером между информацией, к которой хочет получить доступ пользователь, и самим пользователем.
2) диспетчер доступа разрешает или запрещает доступ в соответствии с тем, является ли запрос авторизованным на основании проверки атрибутов доступа пользователя, процесса и пассивного объекта,
3) диспетчер доступа «герметизирует» каждый объект путем отключения отсылок его паспортных свойств от одного объекта ко всем объектам ДИС, что поддерживается принципом организации реляционных объектно-ориентированных систем,
4) диспетчер доступа препятствует доступу к объектам в обход механизмов защиты,
5) диспетчер доступа обеспечивает проверку наличия у пользователя и/или процесса прав доступа к объекту и регистрацию происходящих событий.

Спецификация функциональности № 1. Набор функциональных услуг стандартных профилей защищенности информации КСЗ ДИС *Приложение 1*

Номер строки *(по колонкам)*	Наименование компонентов и элементов уровней функциональных критериев услуг КСЗ КС	Код критерия базовый	*Код минимум критерия*	Развитие КСЗ по уровням (строкам) требований к функциональным критериям услуг					*Код максимум критерия*
				1	**2**	**3**	**4**	**5**	
1. Справочник - столбец компонента «Критерии конфиденциальности» ***(колонки 1, 2)***									
1.1.1	**Доверительная конфиденциальность**	**КД**	***от КД-1***	+	+	+	+	=	***до КД-4***
1.1.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
1.2.1	**Административная конфиденциальность**	**КА**	***от КА-1***	+	+	+	+	=	***до КА-4***
1.2.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
1.3.1	**Повторное использование объектов**	**КО**	***от К0-1***	+	=	=	=	=	***до КО-1***
1.3.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
1.4.1	**Анализ скрытых каналов**	**КК**	***от КК-1***	+	+	+	=	=	***до КК-3***
1.4.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
1.5.1	**Конфиденциальность при обмене**	**КВ**	***от КВ-1***	+	+	+	+	=	***до КВ-4***
1.5.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
2. Справочник - столбец компонента «Критерии целостности» ***(колонки 1, 2)***									
2.1.1	**Доверительная целостность**	**ЦД**	***от ЦД-1***	+	+	+	+	=	***до ЦД-4***
2.1.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
2.2.1	**Административная целостность**	**ЦА**	***от ЦА-1***	+	+	+	+	=	***до ЦА-4***
2.2.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
2.3.1	**Откат**	**ЦО**	***от ЦО-1***	+	+	=	=	=	***до ЦО-2***
2.3.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
2.4.1	***Элемент критерия не проектируется***	-	-	***нет***	***нет***	***нет***	***нет***	***нет***	**отсутствует**
2.4.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
2.5.1	**Целостность при обмене**	**ЦВ**	***от ЦВ-1***	+	+	+	=	=	***до ЦВ-3***
2.5.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
3. Справочник - столбец компонента «Критерии доступности» ***(колонки 1, 2)***									
3.1.1	**Использование ресурсов**	**ДР**	***от ДР-1***	+	+	+	=	=	***до ДР-3***
3.1.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
3.2.1	**Устойчивость к отказам**	**ДС**	***от ДС-1***	+	+	+	=	=	***до ДС-3***
3.2.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
3.3.1	**Горячая замена**	**ДЗ**	***от ДЗ-1***	+	+	+	=	=	***до ДЗ-3***
3.3.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
3.4.1	**Восстановление после сбоев**	**ДВ**	***от ДВ-1***	+	+	+	=	=	***до ДВ-3***
3.4.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
3.5.1	***Элемент критерия не проектируется***	-	-	-	-	-	-	-	**отсутствует**
3.5.2	*Элемент критерия не проектируется*	-	-	*нет*	*нет*	*нет*	*нет*	*нет*	-
4. Справочник – столбец компонента «Критерии наблюдаемости» ***(колонки 1, 2)***									
4.1.1	**Регистрация**	**НР**	***от НР-1***	+	+	+	+	+	***до НР-5***
4.1.2	*Отсылка к НД ТЗИ 2.5-004-99 «10..Критерии гарантий»*	***Г***	***от Г-1***	***Г-2***	***Г-3***	***Г-4***	***Г-5***	***Г-6***	***до Г-7***
4.2.1	**Идентификация и аутентификация**	**НИ**	***от НИ-1***	+	+	+	=	=	***до НИ-3***
4.2.2	**Достоверный канал**	**НК**	***от НК-1***	+	+	=	=	=	***до НК-2***
4.3.1	**Разграничение обязанностей**	**НО**	***от НО-1***	+	+	+	=	=	***до НО-3***
4.3.2	**Целостность КСЗ**	**НЦ**	***от НЦ-1***	+	+	+	=	=	***до НЦ-3***
4.4.1	**Самотестирование**	**НТ**	***от НТ-1***	+	+	+	=	=	***до НТ-3***
4.4.2	**Аутентификация при обмене**	**НВ**	***от НВ-1***	+	+	+	=	=	***до НВ-3***
4.5.1	**Аутентификация отправителя**	**НА**	***от НА-1***	+	+	=	=	=	***до НА-2***
4.5.2	**Аутентификация получателя**	**НП**	***от НП-1***	+	+	+	=	=	***до НП-2***

Спецификация функциональности № 2. *Приложение 2*

Конструктор профилей защищенности по уровням критериев политики услуг КСЗ ДИС

Требования к функциональным критериям услуг на уровне 1 (база).

№ строки *(в столбцах)*	Наименование элементов (из компонентов) функциональных критериев услуг КСЗ КС	Код уровня	Код элемента	Требования к функциональным критериям услуг *(с матричным кодированием строк по колонкам столбцов)*	Необходимые условия по НД ТЗИ
1. Справочники - столбцы компонента «Критерии конфиденциальности» (колонки: 1, 2)					
1.1.1	**Доверительная конфиденциальность**	**КД-1**	**1.1.1.1**	**Минимальная доверительная конфиденциальность**	**НИ-1**
1.1.2	*Элемент критерия не проектируется*		*1.1.2.0*		-
1.2.1	**Административная конфиденциальность**	**КА-1**	**1.2.1.1**	**Минимальная административная конфиденциальность**	**НО-1, НИ-1**
1.2.2	*Элемент критерия не проектируется*		*1.2.2.0*		-
1.3.1	**Повторное использование объектов**	**КО-1**	**1.3.1.1**	**Повторное использование объектов**	***нет***
1.3.2	*Элемент критерия не проектируется*		*1.3.2.0*		-
1.4.1	**Анализ скрытых каналов**	**КК-1**	**1.4.1.1**	**Выявление скрытых каналов**	**КО-1, Г-3**
1.4.2	*Элемент критерия не проектируется*		*1.4.2.0*		-
1.5.1	**Конфиденциальность при обмене**	**КВ-1**	**1.5.1.1**	**Минимальная конфиденциальность при обмене**	***нет***
1.5.2	*Элемент критерия не проектируется*		*1.5.2.0*		-
2. Справочники – столбцы компонента «Критерии целостности» (колонки: 1, 2)					
2.1.1	**Доверительная целостность**	**ЦД-1**	**2.1.1.1**	**Минимальная доверительная целостность**	**НИ-1**
2.1.2	*Элемент критерия не проектируется*		*2.1.2.0*		-
2.2.1	**Административная целостность**	**ЦА-1**	**2.2.1.1**	**Минимальная административная целостность**	**НО-1, НИ-1**
2.2.2	*Элемент критерия не проектируется*		*2.2.2.0*		-
2.3.1	**Откат**	**ЦО-1**	**2.3.1.1**	**Ограниченный откат**	**НИ-1**
2.3.2	***Элемент критерия не проектируется***		*2.3.2.0*		
2.4.1	***Элемент критерия не проектируется***	**-**	**2.4.2.0**	***Элемент критерия не проектируется (компонент не задан)***	**-**
2.4.2	*Элемент критерия не проектируется*		*2.4.2.0*		-
2.5.1	**Целостность при обмене**	**ЦВ-1**	**2.5.1.1**	**Минимальная целостность при обмене**	***нет***
2.5.2	*Элемент критерия не проектируется*		*2.5.2.0*		-
3. Справочники – столбцы компонента «Критерии доступности» (колонки: 1, 2)					
3.1.1	**Использование ресурсов**	**ДР-1**	**3.1.1.1**	**Квоты**	**НО-1**
3.1.2	*Элемент критерия не проектируется*		*3.1.2.0*		-
3.2.1	**Устойчивость к отказам**	**ДС-1**	**3.2.1.1**	**Устойчивость при ограниченных отказах**	**НО-1**
3.2.2	*Элемент критерия не проектируется*		*3.2.2.0*		-
3.3.1	**Горячая замена**	**ДЗ-1**	**3.3.1.1**	**Модернизация**	**НО-1**
3.3.2	*Элемент критерия не проектируется*		*3.3.2.0*		
3.4.1	**Восстановление после сбоев**	**ДВ-1**	**3.4.1.1**	**Ручное восстановление**	**НО-1**
3.4.2	*Элемент критерия не проектируется*		*3.4.2.0*		-
3.5.1	*Элемент критерия не проектируется*	**-**	**3.5.1.0**	***Элемент критерия не проектируется (компонент не задан)***	**-**
3.5.2	*Элемент критерия не проектируется*		*3.5.2.0*		-
4. Справочники – столбцы компонента «Критерии наблюдаемости» (колонки: 1, 2)					
4.1.1	**Регистрация**	**НР-1**	**4.1.1.1**	**Внешний анализ**	**НИ-1**
4.1.2	***Требования критериев гарантий***	***Г-1, Г-2***	***4.1.2.1***	***Отсылка к НД ТЗИ 2.5-004-99 «10. Критерии гарантий»***	**-**
4.2.1	**Идентификация и аутентификация**	**НИ-1**	**4.2.1.1**	**Внешняя идентификация и аутентификация**	***нет***
4.2.2	**Достоверный канал**	**НК-1**	**4.2.2.1**	**Однонаправленный достоверный канал**	***нет***
4.3.1	**Разграничение обязанностей**	**НО-1**	**4.3.1.1**	**Выделение администратора**	**НИ-1**
4.3.2	**Целостность КСЗ**	**НЦ-1**	**4.3.2.1**	**КСЗ с контролем целостности**	**НР-1, НО-1**
4.4.1	**Самотестирование**	**НТ-1**	**4.4.1.1**	**Самотестирование по запросу**	**НО-1**
4.4.2	**Идентификация и аутентификация при обмене**	**НВ-1**	**4.4.2.1**	**Аутентификация узла**	***нет***
4.5.1	**Аутентификация отправителя**	**НА-1**	**4.5.1.1**	**Базовая аутентификация отправителя**	**НИ-1**
4.5.2	**Аутентификация получателя**	**НП-1**	**4.5.2.1**	**Базовая аутентификация получателя**	**НИ-1**

Требования к функциональным критериям услуг на уровне 2 (1).

№ строки *(в столбцах)*	Наименование элементов (из компонентов) функциональных критериев услуг КСЗ КС	Код уровня	Код в матрице	Требования к функциональным критериям услуг *(с матричным кодированием строк по колонкам столбцов)*	Необходимые условия
1.1.1	**Доверительная конфиденциальность**	**КД-2**	**1.1.1.2**	**Базовая доверительная конфиденциальность**	**НИ-1**
1.1.2	*Элемент критерия не проектируется*		*1.1.2.0*		-
1.2.1	**Административная конфиденциальность**	**КА-2**	**1.2.1.2**	**Базовая административная конфиденциальность**	**НО-1, НИ-1**
1.2.2	*Элемент критерия не проектируется*		*1.2.2.0*		-
1.3.1	**Повторное использование объектов**	***КО-1***	**1.3.1.2**	***Повторное использование объектов***	***Нет***
1.3.2	*Элемент критерия не проектируется*		*1.3.2.0*		-
1.4.1	**Анализ скрытых каналов**	**КК-2**	**1.4.1.2**	**Контроль скрытых каналов**	**КО-1, Г-3**
1.4.2	*Элемент критерия не проектируется*		*1.4.2.0*		
1.5.1	**Конфиденциальность при обмене**	**КВ-2**	**1.5.1.2**	**Базовая конфиденциальность при обмене**	***Нет***
1.5.2	*Элемент критерия не проектируется*		*1.5.2.0*		-
1. Справочники – столбцы компонента «Критерии целостности» (колонки: 1, 2)					
2.1.1	**Доверительная целостность**	**ЦД-2**	**2.1.1.2**	**Базовая доверительная целостность**	**НИ-1**
2.1.2	*Элемент критерия не проектируется*		*2.1.2.0*		-
2.2.1	**Административная целостность**	**ЦА-2**	**2.2.1.2**	**Базовая административная целостность**	**НО-1, НИ-1**
2.2.2	*Элемент критерия не проектируется*		*2.2.2.0*		-
2.3.1	**Откат**	**ЦО-2**	**2.3.1.2**	**Полный откат**	**НИ-1**
2.3.2	*Элемент критерия не проектируется*		*2.3.2.0*		-
2.4.1	*Элемент критерия не проектируется*	-	**2.4.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	-
2.4.2	*Элемент критерия не проектируется*		*2.4.2.0*		-
2.5.1	**Целостность при обмене**	**ЦВ-2**	**2.5.1.2**	**Базовая целостность при обмене**	***Нет***
2.5.2	*Элемент критерия не проектируется*		*2.5.2.0*		-
3. Справочники – столбцы компонента «Критерии доступности» (колонки: 1, 2)					
3.1.1	**Использование ресурсов**	**ДР-2**	**3.1.1.2**	**Пресечение захвата ресурсов**	**НО-1**
3.1.2	*Элемент критерия не проектируется*		*3.1.2.0*		-
3.2.1	**Устойчивость к отказам**	**ДС-2**	**3.2.1.2**	**Устойчивость с ухудшением характеристик обслуживания**	**НО-1**
3.2.2	*Элемент критерия не проектируется*		*3.2.2.0*		
3.3.1	**Горячая замена**	**ДЗ-2**	**3.3.1.2**	**Ограниченная горячая замена**	**НО-1**
3.3.2	*Элемент критерия не проектируется*		*3.3.2.0*		-
3.4.1	**Восстановление после сбоев**	**ДВ-2**	**3.4.1.2**	**Автоматизированное восстановление**	**НО-1**
3.4.2	*Элемент критерия не проектируется*		*3.4.2.0*		-
3.5.1	***Элемент критерия не проектируется***	-	**3.5.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	-
3.5.2	*Элемент критерия не проектируется*		*3.5.2.0*		-
4. Справочники – столбцы компонента «Критерии наблюдаемости» (колонки: 1, 2)					
4.1.1	**Регистрация**	**НР-2**	**4.1.1.2**	**Защищенный журнал**	**НИ-1**
4.1.2	***Требования критериев гарантий***	***Г - 3***	***4.1.2.2***	***Отсылка к НД ТЗИ 2.5-004-99 «10. Критерии гарантий»***	-
4.2.1	**Идентификация и аутентификация**	**НИ-2**	**4.2.1.2**	**Одиночная идентификация и аутентификация**	***Нет***
4.2.2	**Достоверный канал**	**НК-2**	**4.2.2.2**	**Двунаправленный достоверный канал**	***Нет***
4.3.1	**Разграничение обязанностей**	**НО-2**	**4.3.1.2**	**Разграничение обязанностей администратора**	**НИ-1**
4.3.2	**Целостность КСЗ**	**НЦ-2**	**4.3.2.2**	**КСЗ с гарантируемой целостностью**	**НР-1, НО-1**
4.4.1	**Самотестирование**	**НТ-2**	**4.4.1.2**	**Самотестирование при старте**	**НО-1**
4.4.2	**Идентификация и аутентификация при обмене**	**НВ-2**	**4.4.2.2**	**Аутентификация источника данных**	***Нет***
4.5.1	**Аутентификация отправителя**	**НА-2**	**4.5.1.2**	**Аутентификация отправителя с подтверждением**	**НИ-1**
4.5.2	**Аутентификация получателя**	**НП-2**	**4.5.2.2**	**Аутентификация получателя с подтверждением**	**НИ-1**

Требования к функциональным критериям услуг на уровне 3 (2,1).

№ строки *(в столбцах)*	Наименование элементов (из компонентов) функциональных критериев услуг КСЗ КС	Код уровня	Код в матрице	Требования к функциональным критериям услуг *(с матричным кодированием строк по колонкам столбцов)*	Необходимые условия
1. Справочники - столбцы компонента «Критерии конфиденциальности» (колонки: 1, 2)					
1.1.1	**Доверительная конфиденциальность**	**КД-3**	**1.1.1.3**	**Полная доверительная конфиденциальность**	**НИ-1**
1.1.2	*Элемент критерия не проектируется*		*1.1.2.0*		-
1.2.1	**Административная конфиденциальность**	**КА-3**	**1.2.1.3**	**Полная административная конфиденциальность**	**НО-1, НИ-1**
1.2.2	*Элемент критерия не проектируется*		*1.2.2.0*		-
1.3.1	**Повторное использование объектов**	***КО-1***	**1.3.1.3**	***Повторное использование объектов***	***Нет***
1.3.2	*Элемент критерия не проектируется*		*1.3.2.0*		-
1.4.1	**Анализ скрытых каналов**	**КК-3**	**1.4.1.3**	**Перекрытие скрытых каналов**	**КО-1, Г-3**
1.4.2	*Элемент критерия не проектируется*		*1.4.2.0*		-
1.5.1	**Конфиденциальность при обмене**	**КВ-3**	**1.5.1.3**	**Полная конфиденциальность при обмене**	***нет***
1.5.2	*Элемент критерия не проектируется*		*1.5.2.0*		
2. Справочники – столбцы компонента «Критерии целостности» (колонки: 1, 2)					
2.1.1	**Доверительная целостность**	**ЦД-3**	**2.1.1.3**	**Полная доверительная целостность**	**НИ-1**
2.1.2	*Элемент критерия не проектируется*		*2.1.2.0*		-
2.2.1	**Административная целостность**	**ЦА-3**	**2.2.1.3**	**Полная административная целостность**	**НО-1, НИ-1**
2.2.2	*Элемент критерия не проектируется*		*2.2.2.0*		-
2.3.1	**Откат**	***ЦО-2***	**2.3.1.3**	***Полный откат***	**НИ-1**
2.3.2	*Элемент критерия не проектируется*		*2.3.2.0*		-
2.4.1	***Элемент критерия не проектируется***	**-**	**2.4.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	**-**
2.4.2	*Элемент критерия не проектируется*		*2.4.2.0*		-
2.5.1	**Целостность при обмене**	**ЦВ-3**	**2.5.1.3**	**Полная целостность при обмене**	***нет***
2.5.2	*Элемент критерия не проектируется*		*2.5.2.0*		-
3. Справочники – столбцы компонента «Критерии доступности» (колонки: 1, 2)					
3.1.1	**Использование ресурсов**	**ДР-3**	**3.1.1.3**	**Приоритетность захвата ресурсов**	**НО-1**
3.1.2	*Элемент критерия не проектируется*		*3.1.2.0*		
3.2.1	**Устойчивость к отказам**	**ДС-3**	**3.2.1.3**	**Устойчивость без ухудшения характеристик обслуживания**	**НО-1**
3.2.2	*Элемент критерия не проектируется*		*3.2.2.0*		
3.3.1	**Горячая замена**	**ДЗ-3**	**3.3.1.3**	**Горячая замена любого компонента**	**НО-1**
3.3.2	*Элемент критерия не проектируется*		*3.3.2.0*		
3.4.1	**Восстановление после сбоев**	**ДВ-3-**	**3.4.1.3**	**Избирательное восстановление**	**НО-1**
3.4.2	*Элемент критерия не проектируется*		*3.4.2.0*		-
3.5.1	***Элемент критерия не проектируется***	**--**	**3.5.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	**-**
3.5.2	*Элемент критерия не проектируется*		*3.5.2.0*		-
4. Справочники – столбцы компонента «Критерии наблюдаемости» (колонки: 1, 2)					
4.1.1	**Регистрация**	**НР-3**	**4.1.1.3**	**Сигнализация об опасности**	**НИ-1**
4.1.2	***требованиям критериев гарантий***	***Г – 4***	***4.1.2.3***	***Отсылка к НД ТЗИ 2.5-004-99 «10. Критерии гарантий»***	**-**
4.2.1	**Идентификация и аутентификация**	**НИ-3**	**4.2.1.3**	**Множественная идентификация и аутентификация**	***нет***
4.2.2	**Достоверный канал**	**НК-2**	**4.2.2.3**	***Двунаправленный достоверный канал***	***нет***
4.3.1	**Разграничение обязанностей**	**НО-2**	**4.3.1.3**	**Разграничение обязанностей администратора**	**НИ-1**
4.3.2	**Целостность КСЗ**	**НЦ-2**	**4.3.2.3**	**КСЗ с функциями диспетчера доступа**	**НР-1, НО-1**
4.4.1	**Самотестирование**	**НТ-2**	**4.4.1.3**	**Самотестирование при старте**	**НО-1**
4.4.2	**Идентификация и аутентификация при обмене**	**НВ-2**	**4.4.2.3**	**Аутентификация источника данных**	***нет***
4.5.1	**Аутентификация отправителя**	***НА-2***	**4.5.1.3**	***Аутентификация отправителя с подтверждением***	**НИ-1**
4.5.2	**Аутентификация получателя**	***НП-2***	**4.5.2.3**	***Аутентификация получателя с подтверждением***	**НИ-1**

Требования к функциональным критериям услуг на уровне 4 (3,2,1).

№ строки *(в столбцах)*	Наименование элементов (из компонентов) функциональных критериев услуг КСЗ КС	Код уровня	Код в матрице	Требования к функциональным критериям услуг *(с матричным кодированием строк по колонкам столбцов)*	Необходимые условия
1. Справочники - столбцы компонента «Критерии конфиденциальности» (колонки: 1, 2)					
1.1.1	**Доверительная конфиденциальность**	**КД-4**	**1.1.1.4**	**Абсолютная доверительная конфиденциальность**	**НИ-1**
1.1.2	*Элемент критерия не проектируется*		*1.1.2.0*		-
1.2.1	**Административная конфиденциальность**	**КА-4**	**1.2.1.4**	**Абсолютная административная конфиденциальность**	**НО-1, НИ-1**
1.2.2	*Элемент критерия не проектируется*		*1.2.2.0*		-
1.3.1	**Повторное использование объектов**	***КО-1***	**1.3.1.4**	***Повторное использование объектов***	***нет***
1.3.2	*Элемент критерия не проектируется*		*1.3.2.0*		-
1.4.1	**Анализ скрытых каналов**	***КК-3***	**1.4.1.4**	***Перекрытие скрытых каналов***	**КО-1, Г-3**
1.4.2	*Элемент критерия не проектируется*		*1.4.2.0*		-
1.5.1	**Конфиденциальность при обмене**	**КВ-4**	**1.5.1.4**	**Абсолютная конфиденциальность при обмене**	***нет***
1.5.2	*Элемент критерия не проектируется*		*1.5.2.0*		
2. Справочники – столбцы компонента «Критерии целостности» (колонки: 1, 2)					
2.1.1	**Доверительная целостность**	**ЦД-4**	**2.1.1.4**	**Абсолютная доверительная целостность**	**НИ-1**
2.1.2	*Элемент критерия не проектируется*		*2.1.2.0*		-
2.2.1	**Административная целостность**	**ЦА-4**	**2.2.1.4**	**Абсолютная административная целостность**	**НО-1, НИ-1**
2.2.2	*Элемент критерия не проектируется*		*2.2.2.0*		-
2.3.1	**Откат**	***ЦО-2***	**2.3.1.4**	***Полный откат***	**НИ-1**
2.3.2	*Элемент критерия не проектируется*		*2.3.2.0*		-
2.4.1	***Элемент критерия не проектируется***	**-**	**2.4.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	**-**
2.4.2	*Элемент критерия не проектируется*		*2.4.2.0*		-
2.5.1	**Целостность при обмене**	***ЦВ-3***	**2.5.1.4**	***Полная целостность при обмене***	***нет***
2.5.2	*Элемент критерия не проектируется*		*2.5.2.0*		-
3. Справочники – столбцы компонента «Критерии доступности» (колонки: 1, 2)					
3.1.1	**Использование ресурсов**	***ДР-3***	**3.1.1.4**	***Приоритетность захвата ресурсов***	**НО-1**
3.1.2	*Элемент критерия не проектируется*		*3.1.2.0*		
3.2.1	**Устойчивость к отказам**	***ДС-3***	**3.2.1.4**	***Устойчивость без ухудшения характеристик обслуживания***	**НО-1**
3.2.2	*Элемент критерия не проектируется*		*3.2.2.0*		
3.3.1	**Горячая замена**	***ДЗ-3***	**3.3.1.4**	***Горячая замена любого компонента***	**НО-1**
3.3.2	*Элемент критерия не проектируется*		*3.3.2.0*		
3.4.1	**Восстановление после сбоев**	***ДВ-3***	**3.4.1.4**	***Избирательное восстановление***	**НО-1**
3.4.2	*Элемент критерия не проектируется*		*3.4.2.0*		-
3.5.1	***Элемент критерия не проектируется***	**-**	**3.5.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	**-**
3.5.2	*Элемент критерия не проектируется*		*3.5.2.0*		-
4. Справочники – столбцы компонента «Критерии наблюдаемости» (колонки: 1, 2)					
4.1.1	**Регистрация**	**НР-4**	**4.1.1.4**	**Детальная регистрация**	**НИ-1**
4.1.2	***Требования критериев гарантий***	***Г - 5***	***4.1.2.4***	***Отсылка к НД ТЗИ 2.5-004-99 «10. Критерии гарантий»***	**-**
4.2.1	**Идентификация и аутентификация**	***НИ-3***	**4.2.1.4**	***Множественная идентификация и аутентификация***	***нет***
4.2.2	**Достоверный канал**	***НК-2***	**4.2.2.4**	***Двунаправленный достоверный канал***	***нет***
4.3.1	**Разграничение обязанностей**	***НО-2***	**4.3.1.4**	***Разграничение обязанностей администратора***	**НИ-1**
4.3.2	**Целостность КСЗ**	***НЦ-2***	**4.3.2.4**	***КСЗ с функциями диспетчера доступа***	**НР-1, НО-1**
4.4.1	**Самотестирование**	***НТ-2***	**4.4.1.4**	***Самотестирование при старте***	**НО-1**
4.4.2	**Идентификация и аутентификация при обмене**	***НВ-2***	**4.4.2.4**	***Аутентификация источника данных***	***нет***
4.5.1	**Аутентификация отправителя**	***НА-2***	**4.5.1.4**	***Аутентификация отправителя с подтверждением***	**НИ-1**
4.5.2	**Аутентификация получателя**	***НП-2***	**4.5.2.4**	***Аутентификация получателя с подтверждением***	**НИ-1**

Требования к функциональным критериям услуг на уровне 5 (4,3,2,1).

№ строки *(в столбцах)*	Наименование элементов (из компонентов) функциональных критериев услуг КСЗ КС	Код уровня	Код в матрице	Требования к функциональным критериям услуг *(с матричным кодированием строк по колонкам столбцов)*	Необходимые условия
1. Справочники - столбцы компонента «Критерии конфиденциальности» (колонки: 1, 2)					
1.1.1	**Доверительная конфиденциальность**	***КД-4***	**1.1.1.5**	***Абсолютная доверительная конфиденциальность***	**НИ-1**
1.1.2	*Элемент критерия не проектируется*		*1.1.2.0*		-
1.2.1	**Административная конфиденциальность**	***КА-4***	**1.2.1.5**	***Абсолютная административная конфиденциальность***	**НО-1, НИ-1**
1.2.2	*Элемент критерия не проектируется*		*1.2.2.0*		-
1.3.1	**Повторное использование объектов**	***КО-1***	**1.3.1.5**	***Повторное использование объектов***	***нет***
1.3.2	*Элемент критерия не проектируется*		*1.3.2.0*		-
1.4.1	**Анализ скрытых каналов**	***КК-3***	**1.4.1.5**	***Перекрытие скрытых каналов***	**КО-1, Г-3**
1.4.2	*Элемент критерия не проектируется*		*1.4.2.0*		-
1.5.1	**Конфиденциальность при обмене**	***КВ-4***	**1.5.1.5**	***Абсолютная конфиденциальность при обмене***	***нет***
1.5.2	*Элемент критерия не проектируется*		*1.5.2.0*		
2. Справочники – столбцы компонента «Критерии целостности» (колонки: 1, 2)					
2.1.1	**Доверительная целостность**	***ЦД-4***	**2.1.1.5**	***Абсолютная доверительная целостность***	**НИ-1**
2.1.2	*Элемент критерия не проектируется*		*2.1.2.0*		-
2.2.1	**Административная целостность**	***ЦА-4***	**2.2.1.5**	***Абсолютная административная целостность***	**НО-1, НИ-1**
2.2.2	*Элемент критерия не проектируется*		*2.2.2.0*		-
2.3.1	**Откат**	***ЦО-2***	**2.3.1.5**	***Полный откат***	**НИ-1**
2.3.2	*Элемент критерия не проектируется*		*2.3.2.0*		-
2.4.1	***Элемент критерия не проектируется***	-	**2.4.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	-
2.4.2	*Элемент критерия не проектируется*		*2.4.2.0*		-
2.5.1	**Целостность при обмене**	***ЦВ-3***	**2.5.1.5**	***Полная целостность при обмене***	***нет***
2.5.2	*Элемент критерия не проектируется*		*2.5.2.0*		-
3. Справочники – столбцы компонента «Критерии доступности» (колонки: 1, 2)					
3.1.1	**Использование ресурсов**	***ДР-3***	**3.1.1.5**	***Приоритетность захвата ресурсов***	**НО-1**
3.1.2	*Элемент критерия не проектируется*		*3.1.2.0*		
3.2.1	**Устойчивость к отказам**	***ДС-3***	**3.2.1.5**	***Устойчивость без ухудшения характеристик обслуживания***	**НО-1**
3.2.2	*Элемент критерия не проектируется*		*3.2.2.0*		
3.3.1	**Горячая замена**	***ДЗ-3***	**3.3.1.5**	***Горячая замена любого компонента***	**НО-1**
3.3.2	*Элемент критерия не проектируется*		*3.3.2.0*		
3.4.1	**Восстановление после сбоев**	***ДВ-3***	**3.4.1.5**	***Избирательное восстановление***	**НО-1**
3.4.2	*Элемент критерия не проектируется*		*3.4.2.0*		-
3.5.1	***Элемент критерия не проектируется***	-	**3.5.1.0**	***Элемент критерия не проектируется (отсутствует компонент)***	-
3.5.2	*Элемент критерия не проектируется*		*3.5.2.0*		-
4. Справочники – столбцы компонента «Критерии наблюдаемости» (колонки: 1, 2)					
4.1.1	**Регистрация**	**НР-5**	**4.1.1.5**	**Анализ в реальном времени**	**НИ-1**
4.1.2	***Требования критериев гарантий***	***Г-6, Г-7***	***4.1.2.5***	***Отсылка к НД ТЗИ 2.5-004-99 «10. Критерии гарантий»***	-
4.2.1	**Идентификация и аутентификация**	***НИ-3***	**4.2.1.5**	***Множественная идентификация и аутентификация***	***нет***
4.2.2	**Достоверный канал**	***НК-2***	**4.2.2.5**	***Двунаправленный достоверный канал***	***нет***
4.3.1	**Разграничение обязанностей**	***НО-2***	**4.3.1.5**	***Разграничение обязанностей администратора***	**НИ-1**
4.3.2	**Целостность КСЗ**	***НЦ-2***	**4.3.2.5**	***КСЗ с функциями диспетчера доступа***	**НР-1, НО-1**
4.4.1	**Самотестирование**	***НТ-2***	**4.4.1.5**	***Самотестирование при старте***	**НО-1**
4.4.2	**Идентификация и аутентификация при обмене**	***НВ-2***	**4.4.2.5**	***Аутентификация источника данных***	***нет***
4.5.1	**Аутентификация отправителя**	***НА-2***	**4.5.1.5**	***Аутентификация отправителя с подтверждением***	**НИ-1**
4.5.2	**Аутентификация получателя**	***НП-2***	**4.5.2.5**	***Аутентификация получателя с подтверждением***	**НИ-1**

Спецификация функциональности № 3. *Приложение 3*

Матрица технологических заданий по реализации политики услуг безопасности КСЗ ДИС

КД-**1**. Минимальная доверительная конфиденциальность	КД-**2**. Базовая доверительная конфиденциальность	КД-**3**. Полная доверительная конфиденциальность	КД-**4**. Абсолютная доверительная конфиденциальность
(код элемента 1.1.1.1)	(код элемента 1.1.1.2)	(код элемента 1.1.1.3)	(код элемента 1.1.1.4)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ			
1.1.1.1.**1** Политика доверительной конфиденциальности, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится	1.1.1.2.**7** <=> 1.1.1.1.**1**	1.1.1.3.**13** Политика доверительной конфиденциальности, реализуемая КСЗ, должна относиться ко всем объектам КС	1.1.1.4.**19** <=> 1.1.1.3.**13**
1.1.1.1.**2** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта	1.1.1.2.**8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя защищенного объекта	1.1.1.3.**14** <=> 1.1.1.2.8	1.1.1.4.**20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя, процесса и защищенного объекта
1.1.1.1.**3** Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ на основании атрибутов доступа пользователя, инициирующего запрос, и объекта	1.1.1.2.**9** <=> 1.1.1.1.**3**	1.1.1.3.**15** <=> 1.1.1.1.**3**	1.1.1.4.**21** <=> 1.1.1.1.**3**
1.1.1.1.**4** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретные процессы и/или группы процессов, которые имеют право получать информацию от объекта	1.1.1.2.**10** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право получать информацию от объекта	1.1.1.3.**16** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права получать информацию от объекта	1.1.1.4.**22** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права получать информацию от объекта
1.1.1.1.**5** не проектируется	1.1.1.2.**11** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс	1.1.1.3.**17** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс	1.1.1.4.**23** <=> 1.1.1.3.**17**
1.1.1.1.**6** Права доступа к каждому защищенному объекту должны устанавливаться в момент его создания или инициализации. Как часть политики доверительной конфиденциальности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте	1.1.1.2.**12** <=> 1.1.1.1.**6**	1.1.1.3.**18** <=> 1.1.1.1.**6**	1.1.1.4.**24** <=> 1.1.1.1.**6**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**		НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, НИ-1**	

Столбец-справочник **1** «Критерии конфиденциальности»:

Строка-справочник **2.1** «Административная конфиденциальность»
Строка-справочник 2.2 – не проектируется (с учетом в матрице)

КА-**1** .Минимальная административная конфиденциальность	КА-**2.** Базовая административная конфиденциальность	КА-**3**. Полная административная конфиденциальность	КА-**4**. Абсолютная административная конфиденциальность
(код элемента 1.2.1.1)	(код элемента 1.2.1.2)	(код элемента 1.2.1.3)	(код элемента 1.2.1.4)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ			
1.2.1.1.**1** Политика административной конфиденциальности, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится	1.2.1.2.**7** <=> 1.2.1.1.**1**	1.2.1.3.**13** Политика административной конфиденциальности, реализуемая КСЗ, должна относиться ко всем объектам КС	1.2.1.4.**19** <=> 1.2.1.3.**13**
1.2.1.1.**2** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта	1.1.1.2.**8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя и защищенного объекта	1.2.1.3.**14** <=> 1.1.1.2.**8**	1.2.1.4.**20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя, процесса и защищенного объекта
1.2.1.1.**3** Запросы на изменение прав доступа должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или от пользователей, которым предоставлены соответствующие полномочия	1.1.1.2.**9** <=> 1.2.1.1.**3**	1.2.1.3.**15** <=> 1.2.1.1.**3**	1.2.1.4.**21** <=> 1.2.1.1.**3**
1.2.1.1.**4** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретные процессы и/или группы процессов, которые имеют право получать информацию от объекта	1.2.1.2.**10** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей и/или группы пользователей, которые имеют право получать информацию от объекта	1.2.1.3.**16** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права получать информацию от объекта	1.2.1.4.**22** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права получать информацию от объекта
1.2.1.1.**5** не проектируется	1.2.1.2.**11** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс	1.2.1.3.**17** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс	1.2.1.4.**23** <=> 1.2.1.3.**17**
1.2.1.1.**6** Права доступа к каждому защищенному объекту должны устанавливаться в момент его создания или инициализации. Как часть политики административной конфиденциальности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте	1.2.1.2.**12** <=> 1.2.1.1.**6**	1.2.1.3.**18** <=> 1.2.1.1.**6**	1.2.1.4.**24** <=> 1.2.1.1.**6**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1, НИ-1**		НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, НО-1, НИ-1**	

Столбец-справочник **1** «Критерии конфиденциальности»: Строка-справочник **3.1** «Повторное использование объектов»
Строка-справочник 3.2 – не проектируется (с учетом в матрице)

КО-1. Повторное использование объектов
(код элемента 1.3.1.1)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ
1.3.1.1.**1** Политика повторного использования объектов, реализуемая КСЗ, должна относиться ко всем объектам КС. Прежде чем пользователь или процесс сможет получить в свое распоряжение освобожденный другим пользователем или процессом объект, установленные для предыдущего пользователя или процесса права доступа к данному объекту должны быть отменены.Прежде чем пользователь или процесс сможет получить в свое распоряжение освобожденный другим пользователем или процессом объект, вся содержащаяся в данном объекте информация должна стать недоступной.
НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**

Столбец-справочник **1** «Критерии конфиденциальности»: Строка-справочник **4.1** «Анализ скрытых каналов»
Строка-справочник 4.2 – не проектируется (с учетом в матрице)

КК-**1**. Выявление скрытых каналов	КК-**2**. Контроль скрытых каналов	КК-**3.** Перекрытие скрытых каналов
(код элемента 1.4.1.1)	(код элемента 1.4.1.2)	(код элемента 1.4.1.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
1.4.1.1.**1** Должен быть выполнен анализ скрытых каналов	1.4.1.2.**4** <=> 1.4.1.1.**1**	1.4.1.3.**7** <=> 1.4.1.1.**1**
1.4.1.1.**2** Все скрытые каналы, существующие в аппаратном и программном обеспечении, а также в программах ПЗУ, должны быть документированы. Должна быть документирована максимальная пропускная способность каждого обнаруженного скрытого канала, полученная на основании теоретической оценки или измерений. Для скрытых каналов, которые могут использоваться совместно, должна быть документирована совокупная пропускная способность.	1.4.1.2.**5** <=> 1.4.1.1.**2**	1.4.1.3.**8** Все (утвержденное подмножество) обнаруженные при анализе скрытые каналы должны быть устранены
1.4.1.1.**3** не проектируется	**1.4.1.2.6** КСЗ должен обеспечивать регистрацию использования утвержденного подмножества обнаруженных скрытых каналов	1.4.1.3.**9** не проектируется
НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, Г-3**	НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, НР-1, Г-3**	НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, Г-3**

Столбец-справочник **1** «Критерии конфиденциальности»: Строка-справочник **5.1** «Конфиденциальность при обмене»

Строка-справочник 5.2 – не проектируется (с учетом в матрице)

КВ-1 .Минимальная конфиденциальность при обмене	**КВ-2. Базовая конфиденциальность при обмене**	**КВ-3. Полная конфиденциальность при обмене**	**КВ-4. Абсолютная конфиденциальность при обмене**
(код элемента 1.5.1.1)	(код элемента 1.5.1.2)	(код элемента 1.5.1.3)	(код элемента 1.5.1.4)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ			
1.5.1.1.**1** Политика конфиденциальности при обмене, реализуемая КСЗ, должна определять множество объектов и интерфейсных процессов, к которым она относится	1.5.1.2.**9** <=> 1.5.1.1.**1**	1.5. 1.3.**17** Политика конфиденциальности при обмене, реализуемая КСЗ, должна относиться ко всем объектам и существующим интерфейсным процессам	1.5.1.4.**25** <=> 1.5.1.3.**17**
1.5.1.1.**2** Политика конфиденциальности при обмене, реализуемая КСЗ, должна определять уровень защищенности, который обеспечивается используемыми механизмами, и способность пользователей и/или процессов управлять уровнем защищенности	1.5. 1.2.**10** <=> 1.5.1.1.**2**	1.5. 1.3.**18** <=> 1.5.1.1.**2**	1.5.1.4.**26** <=> 1.5.1.1.**2**
1.5.1.1.3 КСЗ должен обеспечивать защиту от непосредственного ознакомления с информацией, содержащейся в передаваемом объекте	**1.5.1.2.11** <=> 1.5.1.1.**3**	**1.5.1.3.19** <=> 1.5.1.1.**3**	**1.5.1.4.27** <=> 1.5.1.1.**3**
1.5.1.1.**4** не проектируется	1.5.1.2.**12** Запросы на присвоение или изменение уровня защищенности должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или пользователей, имеющих соответствующие полномочия	1.5.1.3.**20** <=> 1.5.1.2.**12**	1.5.1.4.**28** <=> 1.5.1.2.**12**
1.5.1.1.**5** не проектируется	1.5.1.2.**13** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса	1.5.1.3.**21** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса и приемника объекта	1.5.1.4.**29** <=> 1.5.1.3.**21**
1.5.1.1.**6** не проектируется	1.5.1.2.**14** Запросы на импорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса	1.5.1.3.**22** Запросы на импорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса и источника объекта	1.5.1.4.**30** <=> 1.5.1.3.**22**
1.5.1.1.**7** не проектируется	1.5.1.2.**15** не проектируется	1.5.1.3.**23** Представление защищенного объекта должно быть функцией атрибутов доступа интерфейсного процесса, самого объекта, а также его источника и приемника	1.5.1.4.**31** <=> 1.5.1.3.**23**
1.5.1.1.**8** не проектируется	1.5.1.2.**16** <=> 1.5.1.1.**8**	1.5.1.3.**24** <=> 1.5.1.1.**8**	1.5.1.4.**32** Политика конфиденциальности при обмене должна включать описание информации, которую можно получить путем совместного анализа ряда полученных объектов. Должен быть выполнен анализ скрытых каналов обмена. Все обнаруженные скрытые каналы обмена и максимальная пропускная способность каждого из них должны быть документированы. Должна быть обеспечена регистрация использования утвержденного подмножества обнаруженных скрытых каналов, их частичное перекрытие или исключение
НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1, НВ-1**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1, НВ-1, НР-1, Г-3**

Столбец-справочник **2** «Критерии целостности»:

Строка-справочник **1.1** «Доверительная целостность»
Строка-справочник 1.2 – не проектируется (с учетом в матрице)

ЦД-1. Минимальная доверительная целостность	**ЦД-2. Базовая доверительная целостность**	**ЦД-3. Полная доверительная целостность**	**ЦД-4. Абсолютная доверительная целостность**
(код элемента 2.1.1.1)	(код элемента 2.1.1.2)	(код элемента 2.1.1.3)	(код элемента 2.1.1.4)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ			
2.1.1.1.**1** Политика доверительной целостности, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится	2.1.1.2.**7** <=> 2.1.1.1.**1**	2.1.1.3.**13** Политика доверительной целостности, реализуемая КСЗ, должна относиться ко всем объектам КС	2.1.1.4.**19** <=> 2.1.1.3.**13**
2.1.1.1.**2** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя и защищенного объекта	2.1.1.2.**8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта	2.1.1.3.**14** <=> 2.1.1.2.**8**	2.1.1.4.**20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса, пользователя и защищенного объекта
2.1.1.1.**3** Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ на основании атрибутов доступа пользователя, инициирующего запрос, и объекта	2.1.1.2.**9** <=> 2.1.1.1.**3**	2.1.1.3.**15** <=> 2.1.1.1.**3**	2.1.1.4.**21** <=> 2.1.1.1.**3**
2.1.1.1.**4** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право модифицировать объект	2.1.1.2.**10** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретные процессы и/или группы процессов, которые имеют право модифицировать объект	2.1.1.3.**16** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретные процессы (и группы процессов), которые имеют, а также тех, которые не имеют права модифицировать объект	2.1.1.4.**22** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права модифицировать объект
2.1.1.1.**5** не проектируется	2.1.1.2.**11** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс	2.1.1.3.**17** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс	2.1.1.4.**23** <=> 2.1.1.3.**17**
2.1.1.1.**6** Права доступа к каждому защищенному объекту должны устанавливаться в момент его создания или инициализации. Как часть политики доверительной целостности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте	2.1.1.2.**12** <=> 2.1.1.1.**6**	2.1.1.3.**18** <=> 2.1.1.1.**6**	2.1.1.4.**24** <=> 2.1.1.1.**6**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**		НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, НИ-1**	

Столбец-справочник **2** «Критерии целостности»:

Строка-справочник **2.1** «Административная целостность»
Строка-справочник 2.2 – не проектируется (с учетом в матрице)

ЦА-1. Минимальная административная целостность	**ЦА-2. Базовая административная целостность**	**ЦА-3. Полная административная целостность**	**ЦА-4. Абсолютная административная целостность**
(код элемента 2.2.1.1)	(код элемента 2.2.1.2)	(код элемента 2.3.1.3)	(код элемента 2.3.1.4)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ			
2.2.1.1.**1** Политика административной целостности, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится	2.2.1.2.**7** <=> 2.2.1.1.**1**	2.2.1.3.**13** Политика административной целостности, реализуемая КСЗ, должна относиться ко всем объектам КС	2.2.1.4.**19** <=> 2.2.1.3.**13**
2.2.1.1.**2** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя и защищенного объекта	2.2.1.2.**8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта	2.2.1.3.**14** <=> 2.2.1.2.**8**	2.2.1.4.**20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса, пользователя и защищенного объекта
2.2.1.1.**3** Запросы на изменение прав доступа должны обрабатываться КСЗ только в том случае, если они поступают от администратора или от пользователей, которым предоставлены соответствующие полномочия	2.2.1.2.**9** <=> 2.2.1.1.**3**	2.2.3.**15** <=> 2.2.1.1.**3**	2.2.1.4.**21** <=> 2.2.1.1.**3**
2.2.1.1.**4** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей и/или группы пользователей, которые имеют право модифицировать объект	2.2.1.2.**10** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретные процессы и/или группы процессов, которые имеют право модифицировать объект	2.2.1.3.**16** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретные процессы (и группы процессов), которые имеют, а также тех, которые не имеют права модифицировать объект	2.2.1.4.**22** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права модифицировать объект
2.2.1.1.**5** не проектируется	2.2.1.2.**11** КСЗ должен давать администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс	2.2.1.3.**17** КСЗ должен давать администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс	2.2.1.4.**23** <=> 2.2.1.3.**17**
2.2.1.1.**6** Права доступа к каждому защищенному объекту должны устанавливаться в момент его создания или инициализации. Как часть политики административной целостности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте	2.2.1.2.**12** <=> 2.2.1.1.**6**	2.2.1.3.**18** <=> 2.2.1.1.**6**	2.2.1.4.**24** <=> 2.2.1.1.**6**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1, НИ-1**		НЕОБХОДИМЫЕ УСЛОВИЯ: **КО-1, НО-1, НИ-1**	

Столбец-справочник **2** «Критерии целостности»: Строка-справочник **3.1** «Откат»
Строка-справочник 3.2 – не проектируется (с учетом в матрице)

ЦО-1. Ограниченный откат	**ЦО-2. Полный откат**
(код элемента 2.3.1.1)	(код элемента 2.3.1.2)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ	
2.3.1.1.**1** Политика отката, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится	2.3.1.2.**3** <=> 2.3.1.1.**1**
2.3.1.1.**2** Должны существовать автоматизированные средства, которые позволяют авторизованному пользователю или процессу откатить или отменить определенный набор (множество) операций, проведенных над защищенным объектом за определенный промежуток времени	2.3.1.2.**4** Должны существовать автоматизированные средства, которые позволяют авторизованному пользователю или процессу откатить или отменить все операции, проведенные над защищенным объектом за определенный промежуток времени
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**	

Столбец-справочник **2** «Критерии целостности»:

Строка-справочник **4.1** - не проектируется (с учетом в матрице)

Строка-справочник 4.2 - не проектируется (с учетом в матрице)

Столбец-справочник **2** «Критерии целостности»:

Строка-справочник **5.1** «Целостность при обмене»

Строка-справочник 5.2 – не проектируется (с учетом в матрице)

ЦВ-1. Минимальная целостность при обмене	**ЦВ-2. Базовая целостность при обмене**	**ЦВ-3. Полная целостность при обмене**
(код элемента 2.3.1.1)	(код элемента 2.3.1.2)	(код элемента 2.3.1.2)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
2.4.1.1.**1** Политика целостности при обмене, реализуемая КСЗ, должна определять множество объектов КС и интерфейсных процессов, к которым она относится, степень защищенности, обеспечиваемую используемыми механизмами, и способность пользователей и/или процессов управлять степенью защищенности	2.4.1.2.**7** <=> 2.4.1.1.**1**	2.4.1.3.**13** <=> 2.4.1.1.**1**
2.4.1.1.**2** КСЗ должен обеспечивать возможность обнаружения нарушения целостности информации, содержащейся в передаваемом объекте	2.4.1.2.**8** КСЗ должен обеспечивать возможность обнаружения нарушения целостности информации, содержащейся в передаваемом объекте, а также фактов его удаления или дублирования	2.4.1.3.**14** <=> 2.4.1.2.**8**
2.4.1.1.**3** не проектируется	2.4.1.2.**9** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса	2.4.1.3.**15** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса и приемника объекта
2.4.1.1.**4** не проектируется	2.4.1.2.**10** Запросы на экспорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса	2.4.1.3.**16** Запросы на экспорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса и источника объекта
2.4.1.1.**5** не проектируется	2.4.1.2.**11** Запросы на присвоение или изменение уровня защищенности должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или пользователей, которым предоставлены соответствующие полномочия	2.4.1.3.**17** <=> 2.4.1.2.**11**
2.4.1.1.**6** не проектируется	2.4.1.2.**12** <=> 2.4.1.1.**6**	2.4.1.3.**18** Представление защищенного объекта должно быть функцией атрибутов доступа интерфейсного процесса, самого объекта, а также его источника и приемника
НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1, НВ-1**

Столбец-справочник **3** «Критерии доступности»: Строка-справочник **1.1** «Использование ресурсов»
Строка-справочник 1.2 – не проектируется (с учетом в матрице)

ДР-1. Квоты	**ДР-2. Пресечение захвата ресурсов**	**ДР-3. Приоритетность использования ресурсов**
(код элемента 3.1.1.1)	(код элемента 3.1.1.2)	(код элемента 3.1.1.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
3.1.1.1.**1** Политика использования ресурсов, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится	3.1.1.2.**5** Политика использования ресурсов, реализуемая КСЗ, должна относиться ко всем объектам КС	3.1.1.3.**9** <=> 3.1.1.2.**5**
3.1.1.1.**2** Политика использования ресурсов должна определять ограничения, которые можно накладывать, на количество данных объектов (объем ресурсов), выделяемых отдельному пользователю	3.1.1.2.**6** <=> 3.1.1.1.**2**	3.1.1.3.**10** Политика использования ресурсов должна определять ограничения, которые можно накладывать, на количество данных объектов (объем ресурсов), выделяемых отдельному пользователю и произвольным группам пользователей
3.1.1.1.**3** Запросы на изменение установленных ограничений должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или от пользователей, которым предоставлены соответствующие полномочия	**3.1.1.2.7** <=> 3.1.1.1.**3**	3.1.1.3.**11** <=> 3.1.1.1.**3**
3.1.1.1.**4** не проектируется	3.1.1.2.**8** Должна существовать возможность устанавливать ограничения таким образом, чтобы КСЗ имел возможность предотвратить действия, которые могут привести к невозможности доступа других пользователей к функциям КСЗ или защищенным объектам. КСЗ должен контролировать такие действия, осуществляемые со стороны отдельного пользователя	3.1.1.3.**12** Должна существовать возможность устанавливать ограничения таким образом, чтобы КСЗ имел возможность предотвратить действия, которые могут привести к невозможности доступа других пользователей к функциям КСЗ или защищенным объектам. КСЗ должен контролировать такие действия, осуществляемые со стороны отдельного пользователя и произвольных групп пользователей
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**		

Столбец-справочник **3** «Критерии доступности»: Строка-справочник **2.1** «**Устойчивость к отказам**»
Строка-справочник 2.2 – не проектируется (с учетом в матрице)

ДС-1. Устойчивость при ограниченных отказах	**ДС-2. Устойчивость с ухудшением характеристик обслуживания**	**ДС-3. Устойчивость без ухудшения характеристик обслуживания**
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
3.2.1.1.**1** Разработчик должен провести анализ отказов компонентов КС	3.2.1.2.**6** <=> 3.2.1.1.**1**	3.2.1.3.**11** <=> 3.2.1.1.**1**
3.2.1.1.**2** Политика устойчивости к отказам, реализуемая КСЗ, должна определять множество компонентов КС, к которым она относится, и типы их отказов, после которых КС в состоянии продолжать функционирование	3.2.1.2.**7** Политика устойчивости к отказам, реализуемая КСЗ, должна относиться ко всем компонентам КС	3.2.1.3.**12** <=> 3.2.1.2.**7**
3.2.1.1.**3** Должны быть четко указаны уровни отказов, при превышении которых отказы приводят к снижению характеристик обслуживания или недоступности услуги	3.2.1.2.**8** <=> 3.2.1.1.**3**	3.2.1.3.**13** <=> 3.2.1.1.**3**
3.2.1.1.**4** Отказ одного защищенного компонента не должен приводить к недоступности всех услуг, а должен в худшем случае проявляться в снижении характеристик обслуживания	3.2.1.2.**9** <=> 3.2.1.1.**4**	3.2.1.3.**14** Отказ одного защищенного компонента не должен приводить к недоступности всех услуг или к снижению характеристик обслуживания
3.2.1.1.**5** КСЗ должен быть способен ставить в известность администратора об отказе любого защищенного компонента	3.2.1.2.**10** <=> 3.2.1.1.**5**	3.2.1.3.**15** <=> 3.2.1.1.**5**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**		

Столбец-справочник **3** «Критерии доступности»: Строка-справочник 3**.1** «**Горячая замена**»
Строка-справочник 3.2 – не проектируется (с учетом в матрице)

ДЗ-1. Модернизация	**ДЗ-2. Ограниченная горячая замена**	**ДЗ-3. Горячая замена любого компонента**
3.3.1.1.**1** Политика горячей замены, реализуемая КСЗ, должна определять политику проведения модернизации КС	3.3.1.2.**3** Политика горячей замены, реализуемая КСЗ, должна определять множество компонентов КС, которые могут быть заменены без прерывания обслуживания	3.3.1.3.**5** Политика горячей замены, реализуемая КСЗ, должна обеспечивать возможность замены любого компонента без прерывания обслуживания
3.3.1.1.**2** Администратор или пользователи, которым предоставлены соответствующие полномочия, должны иметь возможность провести модернизацию (upgrade) КС. Модернизация КС не должна приводить к необходимости заново производить инсталляцию КС или к прерыванию выполнения КСЗ функций защиты	3.3.1.2.**4** Администратор или пользователи, которым предоставлены соответствующие полномочия, должны иметь возможность заменить любой защищенный компонент	3.3.1.3.**6** <=> 3.3.1.2.**4**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1, ДС-1**	

Столбец-справочник **3** «Критерии доступности»: Строка-справочник 4**.1** «**Восстановление после сбоев**»
Строка-справочник 4.2 – не проектируется (с учетом в матрице)

ДВ-1. Ручное восстановление	**ДВ-2. Автоматизированное восстановление**	**ДВ-3. Избирательное восстановление**
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
3.4.1.1.**1** Политика восстановления, реализуемая КСЗ, должна определять множество типов отказов КС и прерываний обслуживания, после которых возможен возврат в известное защищенное состояние без нарушения политики безопасности. Должны быть четко указаны уровни отказов, при превышении которых необходима повторная инсталляция КС	3.4.1.2.**5** <=> 3.4.1.1.**1**	3.4.1.3.**9** <=> 3.4.1.1.**1**
3.4.1.1.**2** После отказа КС или прерывания обслуживания КСЗ должен перевести КС в состояние, из которого вернуть ее к нормальному функционированию может только администратор или пользователи, которым предоставлены соответствующие полномочия	3.4.1.2.**6** После отказа КС или прерывания обслуживания КСЗ должен быть способен определить, могут ли быть использованы автоматизированные процедуры для возврата КС к нормальному функционированию безопасным образом. Если такие процедуры могут быть использованы, то КСЗ должен быть способен выполнить их и вернуть КС к нормальному функционированию	3.4.1.3.**10** После любого отказа КС или прерывания обслуживания, не приводящих к необходимости заново инсталлировать КС, КСЗ должен быть способен выполнить необходимые процедуры и безопасным образом вернуть КС к нормальному функционированию или, в худшем случае, функционированию в режиме с ухудшенными характеристиками обслуживания
3.4.1.1.**3** не проектируется	3.4.1.2.**7** Если автоматизированные процедуры не могут быть использованы, то КСЗ должен перевести КС в состояние, из которого вернуть ее к нормальному функционированию может только администратор или пользователи, которым предоставлены соответствующие полномочия	3.4.1.3.**11** <=> 3.4.1.2.7
3.4.1.1.4 Должны существовать ручные процедуры, с помощью которых можно безопасным образом вернуть КС к нормальному функционированию	3.4.1.2.**8** <=> 3.4.1.1.**4**	3.4.1.3.**12** Должны существовать ручные процедуры, с помощью которых можно безопасным образом вернуть КС из режима с ухудшенными характеристиками обслуживания в режим нормального функционирования
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**		

Столбец-справочник **3** «Критерии доступности»: Строка-справочник 5**.1** «Горячая замена» (с учетом в матрице)
Строка-справочник 5.2 – не проектируется (с учетом в матрице)

Столбец-справочник **4** «Критерии наблюдаемости»: Строка-справочник 1**.1** «Регистрация»

НР-1. Внешний анализ	**НР-2. Защищенный журнал**	**НР-3. Сигнализация об опасности**	**НР-4. Детальная регистрация**	**НР-5. Анализ в реальном времени**
(код элемента 4.1.1.1)	(код элемента 4.1.1.2)	(код элемента 4.1.1.3)	(код элемента 4.1.1.4)	(код элемента 4.1.1.5)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ				
4.1.1.1.**1** Политика регистрации, реализуемая КСЗ, должна определять перечень регистрируемых событий	4.1.1.2.**7** <=> 4.1.1.1.**1**	4.1.1.3.**13** <=> 4.1.1.1.**1**	4.1.1.4.**19** <=> 4.1.1.1.**1**	4.1.1.5.**25** <=> 4.1.1.1.**1**
4.1.1.1.**2** КСЗ должен быть способен осуществлять регистрацию событий, имеющих непосредственное отношение к безопасности	4.1.1.2.**8** <=> 4.1.1.1.**2**	4.1.1.3.**14** <=> 4.1.1.1.**2**	4.1.1.4.**20** КСЗ должен быть способен осуществлять регистрацию событий, имеющих непосредственное или косвенное отношение к безопасности	4.1.1.5.**26** <=> 4.1.1.4.**20**
4.1.1.1.**3** Журнал регистрации должен содержать информацию о дате, времени, месте, типе и успешности или неуспешности каждого зарегистрированного события. Журнал регистрации должен содержать информацию, достаточную для установления пользователя, процесса и/или объекта, имевших отношение к каждому зарегистрированному событию	4.1.1.2.**9** <=> 4.1 1.1.**3**	4.1.1.3.**15** <=> 4.1.1.1.**3**	4.1.1.4.**21** <=> 4.1.1.1.**3**	4.1.1.5.**27** <=> 4.1.1.1.**3**
4.1.1.1.**4** КСЗ должен быть способен передавать журнал регистрации в другие системы с использованием определенных механизмов защиты	4.1.1.2.**10** КСЗ должен обеспечивать защиту журнала регистрации от несанкционированного доступа, модификации или разрушения. Администраторы и пользователи, которым предоставлены соответствующие полномочия, должны иметь в своем распоряжении средства просмотра и анализа журнала регистрации	4.1.1.3.**16** <=> 4.1.1.2.**10**	4.1.1.4.**22** <=> 4.1.1.2.**10**	4.1.1.5.**28** <=> 4.1.1.2.**10**
4.1.1.1.**5** не проектируется	4.1.1.2.**11** <=> 4.1.1.1.**5**	4.1.1.3.**17** КСЗ должен быть способен контролировать единичные или повторяющиеся регистрируемые события, которые могут свидетельствовать о прямых (существенных) нарушениях политики безопасности КС. КСЗ должен быть способен немедленно информировать администратора о превышении порогов безопасности и, если регистрируемые опасные события повторяются, осуществить неразрушающие действия по пресечению повторения этих событий	4.1.1.4.**23** <=> 4.1.1.3.**17**	4.1.1.5.**29** <=> 4.1.1.3.**17**
4.1.1.1.**6** не проектируется	4.1.1.2.**12** <=> 4.1.1.1.**6**	4.1.1.3.**18** <=> 4.1.1.1.**6**	4.1.1.4.**24** <=> 4.1.1.1.**6**	4.1.1.5.**30** КСЗ должен быть способен выявлять и анализировать несанкционированные действия в реальном времени
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1, НО-1**			

Столбец-справочник **4** «Критерии наблюдаемости»: Строка-справочник 1**.2** Отсылка к требованиям критериев гарантий к НД ТЗИ 2.5-004-99 «10. КРИТЕРИИ ГАРАНТИЙ»

Г-1	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**	**Независимая третья сторона**
Необходимые условия (без кода)	(код элемента) 4.1.2.**1**	(код элемента) 4.1.2.**2**	(код элемента) 4.1.2.**3**	(код элемента) 4.1.2.**4**	(код элемента) 4.1.2.**5**	(не задается) Критерии максимальные	(не задается) Препроцессор контролер
Адаптация	*Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ*						***Инсталляция***
3.КЦД. Б	3.КЦД.1	3.КЦД.2	3.КЦД.3	3.КЦД.4	3.КЦД.5	3.КЦД.5/1	Эталон

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **2.1** «Идентификация и аутентификация»

НИ-1. Внешняя идентификация и аутентификация	**НИ-2. Одиночная идентификация и аутентификация**	**НИ-3. Множественная идентификация и аутентификация**
(код элемента 4.2.1.1)	(код элемента 4.2.1.2)	(код элемента 4.2.1.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
4.2.1.1.**1** Политика идентификации и аутентификации, реализуемая КСЗ, должна определять атрибуты, которыми характеризуется пользователь, и услуги, для использования которых необходимы эти атрибуты. Каждый пользователь должен однозначно идентифицироваться КСЗ	4.2.1.2.**4** <=> 4.2.1.1.**1**	4.2.1.3.**7** <=> 4.2.1.1.**1**
4.2.1.1.**2** Прежде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен с использованием защищенного механизма получить от некоторого внешнего источника аутентифицированный идентификатор этого пользователя	4.2.1.2.**5** Прежде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен аутентифицировать этого пользователя с использованием защищенного механизма	4.2.1.3.**8** Прежде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен аутентифицировать этого пользователя с использованием защищенных механизмов двух или более типов
4.2.1.1.**3** не проектируется	4.2.1.2.**6** КСЗ должен обеспечивать защиту данных аутентификации от несанкционированного доступа, модификации или разрушения	4.2.1.3.**9** <=> 4.2.1.2.**6**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НК-1**	

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **2.2** «Достоверный канал»

НК-1. Однонаправленный достоверный канал	**НК-2. Двунаправленный достоверный канал**
(код элемента 4.2.2.1)	(код элемента 4.2.2.2)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ	
4.2.2.1.**1** Политика достоверного канала, реализуемая КСЗ, должна определять механизмы установления достоверной связи между пользователем и КСЗ	4.2.2.2.**4** <=> 4.2.2.1.**1**
4.2.2.1.**2** Достоверный канал должен использоваться для начальной идентификации и аутентификации. Связь с использованием данного канала должна инициироваться исключительно пользователем.	4.2.2.2.**5** Достоверный канал должен использоваться для начальной идентификации и аутентификации и в других случаях, когда необходима прямая связь пользователь / КСЗ или КСЗ / пользователь. Связь с использованием данного канала должна инициироваться пользователем или КСЗ.
4.2.2.1.**3** не проектируется	4.2.2.2.**6** Обмен с использованием достоверного канала, инициируемый КСЗ, должен быть однозначно идентифицируем как таковой и должен происходить только после положительного подтверждения готовности к обмену со стороны пользователя
НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**	

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **3.1** «Разграничение обязанностей»

НО-1. Выделение администратора	**НО-2. Разграничение обязанностей администратора**	**НО-3. Разграничение обязанностей на основании привилегий**
(код элемента 4.3.1.3)	(код элемента 4.3.1.3)	(код элемента 4.3.1.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
4.3.1.1.**1** Политика разграничения обязанностей, реализуемая КСЗ, должна определять роли администратора и обычного пользователя и присущие им функции	4.3.1.2.**5** <=> 4.3.1.1.**1**	4.3.1.3.**9** <=> 4.3.1.1.**1**
4.3.1.1.**2** не проектируется	4.3.1.2.**6** Политика разграничения обязанностей должна определять минимум две различные административные роли: администратора безопасности и иного администратора. Функции, присущие каждой из ролей, должны быть минимизированы так, чтобы включать только те функции, которые необходимы для выполнения данной роли.	4.3.1.3.**10** <=> 4.3.1.2.**6**
4.3.1.1.**3** не проектируется	4.3.1.2.**7** <=> 4.3.1.1.**3**	4.3. 1.3.**11** Политика разграничения обязанностей должна определять множество различных ролей пользователей
4.3.1.1.**4** Пользователь должен иметь возможность выступать в определенной роли только после того, как он выполнит определенные действия, подтверждающие принятие им этой роли	4.3.1.2.**8** <=> 4.3.1.1.**4**	4.3.1.3.**12** <=> 4.3.1.1.**4**
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**		

Столбец-справочник **4:** «Критерии наблюдаемости»; Строка-справочник **3.2** «Целостность комплекса средств защиты»

НЦ-1. КСЗ с контролем целостности	**НЦ-2. КСЗ с гарантированной целостностью**	**НЦ-3. КСЗ с функциями диспетчера доступа**
(код элемента 4.3.2.1)	(код элемента 4.3.2.2)	(код элемента 4.3.2.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
4.3.2.1.**1** Политика целостности КСЗ должна определять состав КСЗ и механизмы контроля целостности входящих в состав КСЗ компонентов	4.3.2.2.**4** Политика целостности КСЗ должна определять домен КСЗ и другие домены, а также механизмы защиты, используемые для реализации разделения доменов	4.3.2.3.**7** <=> 4.3.2.2.**4**
4.3.2.1.**2** В случае обнаружения нарушения целостности какого-либо из своих компонентов КСЗ должен поставить в известность администратора и либо автоматически восстановить соответствие компонента эталону, либо перевести КС в состояние, из которого вернуть ее к нормальному функционированию может только администратор или пользователи, которым предоставлены соответствующие полномочия	4.3.2.2.**5** КСЗ должен поддерживать домен для своего собственного исполнения с целью защиты от внешних воздействий и несанкционированной модификации и/или потери управления	4.3.2.3.**8** <=> 4.3.2.2.**5**
4.3.2.1.**3** Должны быть описаны ограничения, соблюдение которых позволяет гарантировать, что услуги безопасности доступны только через интерфейс КСЗ и все запросы на доступ к защищенным объектам контролируются КСЗ	4.3.2.2.**6** <=> 4.3.2.1.**3**	4.3.2.3.**9** КСЗ должен гарантировать, что услуги безопасности доступны только через интерфейс КСЗ и все запросы на доступ к защищенным объектам контролируются КСЗ
НЕОБХОДИМЫЕ УСЛОВИЯ: **НР-1,НО-1**	НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**	

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **4.1** «Самотестирование»

НТ-1. Самотестирование по запросу	**НТ-2. Самотестирование при старте**	**НТ-3. Самотестирование в реальном времени**
(код элемента 4.4.1.1)	(код элемента 4.4.1.2)	(код элемента 4.4.1.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
4.6.1.1.**1** Политика самотестирования, реализуемая КСЗ, должна описывать свойства КС и реализованные процедуры, которые могут быть использованы для оценки правильности функционирования КСЗ	4.4.1.2.**3** <=> 4.4.1.1.**1**	4.4.1.3.**5** <=> 4.4.1.1.**1**
4.4.1.1.**2** КСЗ должен быть способен выполнять набор тестов с целью оценки правильности функционирования своих критичных функций. Тесты должны выполняться по запросу имеющего соответствующие полномочия пользователя	4.4.1.2.**4** КСЗ должен быть способен выполнять набор тестов с целью оценки правильности функционирования своих критичных функций. Тесты должны выполняться по запросу имеющего соответствующие полномочия пользователя при инициализации КСЗ	4.4.1.3.**6** КСЗ должен быть способен выполнять набор тестов с целью оценки правильности функционирования своих критичных функций. Тесты должны выполняться по запросу имеющего соответствующие полномочия пользователя при инициализации КСЗ и в процессе штатного функционирования
НЕОБХОДИМЫЕ УСЛОВИЯ: **НО-1**		

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **4.2** «Идентификация и аутентификация при обмене»

НВ-1. Аутентификация узла	**НВ-2. Аутентификация источника данных**	**НВ-3. Аутентификация с подтверждением**
(код элемента 4.4.2.1)	(код элемента 4.4.2.2)	(код элемента 4.4.2.3)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ		
4.4.2.1.**1** Политика идентификации и аутентификация при обмене, реализуемая КСЗ, должна определять множество атрибутов КСЗ и процедуры, которые необходимы для взаимной идентификации при инициализации обмена данными с другим КСЗ. КСЗ, прежде чем начать обмен данными с другим КСЗ, должен идентифицировать и аутентифицировать этот КСЗ с использованием защищенного механизма. Подтверждение идентичности должно выполняться на основании утвержденного протокола аутентификации	4.4.2.2.**4** <=> 4.4.2.1.**1**	4.4.2.3.**7** <=> 4.4.2.1.**1**
4.4.2.1.**2** не проектируется	4.4.2.2.**5** КСЗ должен использовать защищенные механизмы для установления источника каждого экспортируемого и импортируемого объекта	4.4.2.3.**8** <=> 4.4.2.2.5
4.4.2.1.**3** не проектируется	4.4.2.2.**6** <=> 4.4.2.1.**3**	4.4.2.3.**9** Используемый протокол аутентификации должен обеспечивать возможность однозначного подтверждения источника объекта независимой третьей стороной
НЕОБХОДИМЫЕ УСЛОВИЯ: **НЕТ**		

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **5.1** «Аутентификация отправителя»

НА-1. Базовая аутентификация отправителя	**НА-2. Аутентификация отправителя с подтверждением**
(код элемента 4.5.1.1)	(код элемента 4.5.1.1)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ	
4.5.1.1.**1** Политика аутентификация отправителя, реализуемая КСЗ, должна определять множество свойств и атрибутов передаваемого объекта, пользователя-отправителя и интерфейсного процесса, а также процедуры, которые позволяли бы однозначно установить, что данный объект был отправлен (создан) определенным пользователем	4.5.1.2.**5** <=> 4.5.1.1.**1**
4.5.1.1.**2** не проектируется	4.5.1.2.**6** Дополнительно должны быть определены те свойства, атрибуты и процедуры, которые могут использоваться для однозначного подтверждения принадлежности объекта независимой третьей стороной
4.5.1.1.**3** Установление принадлежности должно выполняться на основании утвержденного протокола аутентификации	4.5.1.2.**7** <=> 4.5.1.1.**3**
4.5.1.1.**4** не проектируется	4.5.1.2.**8** Используемый протокол аутентификации должен обеспечивать возможность однозначного подтверждения принадлежности объекта независимой третьей стороной
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**	

Столбец-справочник **4** «Критерии наблюдаемости»; Строка-справочник **5.2** «Аутентификация получателя»

НА-1. Базовая аутентификация получателя	**НА-2. Аутентификация получателя с подтверждением**
(код элемента 4.5.2.1)	(код элемента 4.5.2.2)
Коды списков-строк в технологической карте очередности действий в элементах услуг КСЗ	
4.5.2.1.**1** Политика аутентификация получателя, реализуемая КСЗ, должна определять множество свойств и атрибутов передаваемого объекта, пользователя-получателя и интерфейсного процесса, а также процедуры, которые позволяли бы однозначно установить, что данный объект был получен определенным пользователем	4.5.2.2.**5** <=> 4.5.2.1.**1**
4.5.2.1.**2** не проектируется	4.5.2.2.**6** Дополнительно должны быть определены те свойства, атрибуты и процедуры, которые могут использоваться независимой третьей стороной для однозначного подтверждения факта получения объекта пользователем
4.5.2.1.3 Установление получателя должно выполняться на основании утвержденного протокола аутентификации	4.5.2.2.**7** <=> 4.5.2.1.**3**
4.5.2.1.**4** не проектируется	4.5.2.2.**8** Используемый протокол аутентификации должен обеспечивать возможность однозначного подтверждения независимой третьей стороной факта получения объекта пользователем
НЕОБХОДИМЫЕ УСЛОВИЯ: **НИ-1**	

Спецификация функциональности №4. *Приложение 4*

Набор функциональных услуг стандартных профилей защищенности информации по политике услуг КСЗ в ДИС

№ строки *(в столбце)*	Наименование компонентов и элементов критериев КСЗ	Код критерия (базовый)	*Код критерия (минимум)*	Развитие КСЗ по уровням очередности требований критериев проекта:					*Код критерия (максимум)*
(1.1-5) Справочник - строка 1 «ЗАПРОС» - построчно в колонках столбцов 1, 2 - по уровням кодов критериев 1-5 (подлежат декомпозиции)									
1.1.1	Доверительная конфиденциальность	**КД**	*от КД-1*	*КД-1*	*КД-2*	*КД-3*	*КД-4*	=	*до КД-4*
1.1.2	*Элемент критерия не проектируется*	-	-	-					
2.1.1	Доверительная целостность	**ЦД**	*от ЦД-1*	*ЦД-1*	*ЦД-2*	*ЦД-3*	*ЦД-4*	=	*до ЦД-4*
2.1.2	*Элемент критерия не проектируется*	-	-	-					
3.1.1	Использование ресурсов	**ДР**	*от ДР-1*	*ДР-1*	*ДР-2*	*ДР-3*	=	=	*до ДР-3*
3.1.2	*Элемент критерия не проектируется*	-	-	-					
4.1.1	Регистрация	**НР**	*от НР-1*	*НР-1*	*НР-2*	*НР-3*	*НР-4*	*НР-5*	*до НР-5*
4.1.2	***Отсылка к требованиям критериев гарантий***	***Г***	*от Г - 1*	***Г - 2***	***Г - 3***	***Г - 4***	***Г - 5***	***Г - 6***	*до Г - 7*
(2.1-5) Справочник-строка 2 «ДОСТУП» - построчно в колонках столбцов 1, 2 - по уровням кодов критериев 1-5 (подлежат декомпозиции)									
1.2.1	Административная конфиденциальность	**КА**	*от КА-1*	*КА-1*	*КА-2*	*КА-3*	*КА-4*	=	*до КА-4*
1.2.2	*Элемент критерия не проектируется*	-	-	-					
2.2.1	Административная целостность	**ЦА**	*от ЦА-1*	*ЦА-1*	*ЦА-2*	*ЦА-3*	*ЦА-4*	=	*до ЦА-4*
2.2.2	*Элемент критерия не проектируется*	-	-	-					
3.2.1	Устойчивость к отказам	**ДС**	*от ДС-1*	*ДС-1*	*ДС-2*	*ДС-3*	=	=	*до ДС-3*
3.2.2	*Элемент критерия не проектируется*	-	-	-					
4.2.1	Идентификация и аутентификация	**НИ**	*от НИ-1*	*НИ-1*	*НИ-2*	*НИ-3*	=	=	*до НИ-3*
4.2.2	Доверительный канал	**НК**	*от НК-1*	*НК-1*	*НК-2*	=	=	=	*до НК-2*
(3.1-5) Справочник–строка 3 «ОБЪЕКТ» - ***построчно в колонках столбцов 1, 2 - по уровням кодов критериев 1-5 (подлежат декомпозиции)***									
1.3.1	Повторное использование объектов	**КО**	*от К0-1*	*К0-1*	=	=	=	=	*до КО-1*
1.3.2	*Элемент критерия не проектируется*	-	-	-					
2.3.1	Откат	**ЦО**	*от ЦО-1*	*ЦО-1*	*ЦО-2*	=	=	=	*до ЦО-2*
2.3.2	*Элемент критерия не проектируется*	-	-	-					
3.3.1	Горячая замена	**ДЗ**	*от ДЗ-1*	*ДЗ-1*	*ДЗ-2*	*ДЗ-3*	=	=	*до ДЗ-3*
3.3.2	*Элемент критерия не проектируется*	-	-	-					
4.3.1	Разграничение обязанностей	**НО**	*от НО-1*	*НО-1*	*НО-2*	*НО-3*	=	=	*до НО-3*
4.3.2	Целостность КСЗ	**НЦ**	*от НЦ-1*	*НЦ-1*	*НЦ-2*	*НЦ-3*	=	=	*до НЦ-3*
(4.1-5) Справочник–строка 4 «НАДЗОР» - ***построчно в колонках столбцов 1, 2 - по уровням кодов критериев 1-5 (подлежат декомпозиции)***									
1.4.1	Анализ скрытых каналов	**КК**	*от КК-1*	*КК-1*	*КК-2*	*КК-3*	=	=	*до КК-3*
1.4.2	*Элемент критерия не проектируется*	-	-	-					
2.4.1	*Элемент критерия не проектируется*	-	-	-	-	-	-	-	отсутствует
2.4.2	*Элемент критерия не проектируется*	-	-	-					
3.4.1	Восстановление после сбоев	**ДВ**	*от ДВ-1*	*ДВ-1*	*ДВ-2*	*ДВ-3*	=	=	*до ДВ-3*
3.4.2	*Элемент критерия не проектируется*	-	-	-					
4.4.1	Самотестирование	**НТ**	*от НТ-1*	*НТ-1*	*НТ-2*	*НТ-3*	=	=	*до НТ-3*
4.4.2	Идентификация и аутентификация при обмене	**НВ**	*от НВ-1*	*НВ-1*	*НВ-2*	*НВ-3*	=	=	*до НВ-3*
(5.1-5) Справочник–строка 5 «СВЯЗЬ» - ***построчно в колонках столбцов 1, 2 - по уровням кодов критериев 1-5 (подлежат декомпозиции)***									
1.5.1	Конфиденциальность при обмене	**КВ**	*от КВ-1*	*КВ-1*	*КВ-2*	*КВ-3*	*КВ-4*	=	*до КВ-4*
1.5.2	*Элемент критерия не проектируется*	-	-	-					
2.5.1	Целостность при обмене	**ЦВ**	*от ЦВ-1*	*ЦВ-1*	*ЦВ-2*	*ЦВ-3*	=	=	*до ЦВ-3*
2.5.2	*Элемент критерия не проектируется*	-	-	-					
3.5.1	*Элемент критерия не проектируется*								
3.5.2	*Элемент критерия не проектируется*	-	-	-					
4.5.1	Аутентификация отправителя	**НА**	*от НА-1*	*НА-1*	*НА-2*	=	=	=	*до НА-2*
4.5.2	Аутентификация получателя	**НП**	*от НП-1*	*НП-1*	*НП-2*	=	=	=	*до НП-2*

Спецификация функциональности №5. Конструктор технологических режимов по реализации услуг безопасности КСЗ ДИС *Приложение 5*

№ строки *(в столбце)*	Базовые коды	Элементы критериев по иерархии строк справочников-колонок	**Требования к критериям 1-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ЗАПРОС**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **1** (из 1,2,3,4,5); Уровень базового кода **1** (из 1,2,3,4,5); Требование (очередность)			
1.1.1 *1.1.2 не проектируется*	*КД-1*	Минимальная доверительная конфиденциальность	**1.1.1.1.1**Политика **доверительной конфиденциальности**, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится. **1.1.1.1.2**КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта. **1.1.1.1.3** Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ на основании атрибутов доступа пользователя, инициирующего запрос, и объекта. **1.1.1.1.4** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретные процессы и/или группы процессов, которые имеют право получать информацию от объекта. **1.1.1.1.5***не проектируется* **1.1.1.1.6** Права доступа к каждому защищенному объекту должны устанавливаться в момент его создания или инициализации. Как часть политики доверительной конфиденциальности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте. *1.1.1.2.7 - 1.1.1.2.12 реализуются по КД-2, где:* 1.1.1.2.7 <=>1.1.1.1.1; 1.1.1.2.9 <=>1.1.1.1.3; 1.1.1.2.12<=>1.1.1.1.6; *1.1.1.3.13 - 1.1.1.3.18 реализуются по КД-3, где:* 1.1.1.3.14<=>1.1.1.2.8; 1.1.1.3.15<=>1.1.1.1.3; 1.1.1.3.18<=>1.1.1.1.6; *1.1.1.4.19 - 1.1.1.4.24 реализуются по КД-4, где;* 1.1.1.4.19<=>1.1.1.3.13; 1.1.1.4.21<=>1.1.1.1.3; 1.1.1.4.23<=>1.1.1.3.17; 1.1.1.4.24 <=> 1.1.1.1.6;
2.1.1 *2.1.2 не проектируется*	*ЦД-1*	Минимальная доверительная целостность	**2.1.1.1.1** Политика **доверительной целостности**, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится. **2.1.1.1.2** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя и защищенного объекта. **2.1.1.1.3** Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ на основании атрибутов доступа пользователя, инициирующего запрос, и объекта. **2.1.1.1.4** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право модифицировать объект. **2.1.1.1.5** *не проектируется* **2.1.1.1.6** Права доступа к каждому защищенному объекту должны устанавливать в момент его создания или инициализации. Как часть политики доверительной целостности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте. *2.1.1.2.7 - 2.1.1.2.12 реализуются по ЦД-2, где:* 2.1.1.2.7 <=> 2.1.1.1.1; 2.1.1.1.29 <=>2.1.1.1.3; 2.1.1.2.12<=>2.1.1.1.6; *2.1.1.3.13 - 2.1.1.3.18 реализуются по ЦД-3, где:* 2.1.1.3.14<=> 2.1.1.2.8; 2.1.1.3.15 <=>2.1.1.1.3; 2.1.1.3.18<=>2.1.1.1.6; *2.1.1.4.19 - 2.11..4.24 реализуются по ЦД-4, где;* 2.1.1.4.19 <=>2.1.1.3.13; 2.1.1.4.21<=> 2.1.1.1.3; 2.1.1.4.23<=>2.1.1.3.17; 2.1.1.4.24 <=> 2.1.1.1.6;
3.1.1 *3.1.2 не проектируется*	*ДР-1*	Квоты	**3.1.1.1.1** Политика **использования ресурсов**, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится. **3.1.1.1.2** Политика использования ресурсов должна определять ограничения, которые можно накладывать, на количество данных объектов (объем ресурсов), выделяемых отдельному пользователю. **3.1.1.1.3** Запросы на изменение установленных ограничений должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или от пользователей, которым предоставлены соответствующих полномочия. **3.1.1.1.4** *не проектируется* *3.1.1.2.5 - 3.1.1.2.8 реализуются по ДР-2, где:* 3.1.1.2.6 <=>3.1.1.1.2; 3.1.1.2.7 <=> 3.1.1.1.3; *3.1.1.3.9 - 3.1.1.3.12 реализуются по ДР-3, где:* 3.1.1.3.9 <=>3.1.1.2.5; 3.1.1.3.11<=> 3.1.1.1.3;
4.1.1	*НР-1*	Внешний анализ	**4.1.1.1.1** Политика **регистрации**, реализуемая КСЗ, должна определять перечень регистрируемых событий. **4.1.1.1.2** КСЗ должен быть способен осуществлять регистрацию событий, имеющих непосредственное отношение к безопасности. **4.1.1.1.3** Журнал регистрации должен содержать информацию о дате, времени, месте, типе и успешности или неуспешности каждого зарегистрированного события, информацию, достаточную для установления пользователя, процесса и/или объекта, имевших отношение к каждому зарегистрированному событию. **4.1.1.1.4** КСЗ должен быть способен передавать журнал регистрации в другие системы с использованием определенных механизмов защиты. **4.1.1.1.5** *не проектируется* **4.1.1.1.6** *не проектируется* *4.1.1.2.7 - 4.1.1.2.12 реализуются по НР-2, где:* 4.1.1.2.7 <=> 4.1.1.1.1; 4.1.1.2.8 <=> 4.1.1.1.2; 4.1.1.1.29<=> 4.1.1.1.3; 4.1.1.2.11<=> 4.1.1.1.5; 4.1.1.2.12 <=>4.1.1.1.6 *4.1.1.3.13 - 4.1.1.3.18 реализуются по НР-3, где:* 4.1.1.3.13<=>4.1.1.1.1; 4.1.1.3.14<=>4.1.1.1.2; 4.1.1.3.15 <=>4.1.1.1.3; 4.1.1.3.16<=>4.1.1..2.10; 4.1.1.3.18 <=> 4.1.1.1.6 *4.1.1.4.19 - 4.1.1.4.24 реализуются по НР-4, где:* 4.1.1.4.19<=>4.1.1.1.1; 4.1.1.4.21 <=>4.1.1.1.3; 4.1.1.4.22 <=> 4.1.2.10; 4.1.1.4.23<=> 4.1.1.3.17; 4.1.1.4.24 <=> 4.1.1.1.6 *4.1.1.5.25 - 4.1.1.5.30 реализуются по НР-5, где:* 4.1.1.5.25<=>4.1.1.1.1; 4.1.1.5.26<=>4.1.1.1.20; 4.1.1.5.27<=>4.1.1.1.3; 4.1.1.5.28 <=> 4.1.1.2.10; 4.1.1.5.29 <=> 4.1.1.3.17
4.1.2 Отсылки	*до Г-2*	*Требования критериев гарантий Г-1, Г-2.*	1. Архитектура. 2. Среда разработки: *2.1 Процесс разработки; 2.2 Управление конфигурацией.* 3. Последовательность разработки: 3.*1 Политика безопасности;. 3.2 Модель политики безопасности; 3.3 Проект архитектуры; 3.4 Детальный проект; 3.5 Реализация.* 4. Среда функционирования. 5. Документация. 6. Испытания комплекса средств защиты.

Продолжение Приложение 5

№ строки *(в столбце)*	Базовые коды	Элементы критериев по иерархии строк справочников-колонок	Требования к критериям 1-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ
*Набор кода требований по уровням базовых критериев «**ДОСТУП**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **2** (из 1,2,3,4,5); Уровень базового кода **1** (из 1,2,3,4,5); Требование (очередность)			
1.2.1 *1.2.2 не проектируется*	*КА-1*	Минимальная административная конфиденциальность	**1.2.1.1.1** Политика **административной конфиденциальности**, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится. **1.2.1.1.2**КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта. **1.2.1.1.3** Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или от пользователей, которым предоставлены соответствующие полномочия. **1.2.1.1.4** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретные процессы и/или группы процессов, которые имеют право получать информацию от объекта. **1.2.1.1.5** *не проектируется* **1.2.1.1.6** Права доступа к каждому защищенному объекту должны устанавливаться в момент его создания или инициализации. Как часть политики административной конфиденциальности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте. *1.2.1.2.7 - 1.2.1.2.12 реализуются по КА-2, где:* 1.2.1.2.7 <=> 1.2.1.1.1; 1.2.1.2.9 <=> 1.2.1.1.3; 1.2.1.2.12 <=>1.2.1.1.6; *1.2.1.3.13 - 1.2.1.3.18 реализуются по КА-3, где:* 1.2.1.3.14<=>1.2.1.2.8; 1.2.1.3.15<=> 1.2.1.1.3; 1.2.1.3.18 <=>1.2.1.1.6; *1.2.1.4.19 - 1.2.1.4.24 реализуются по КА-4, где;* 1.2.1.4.19<=>1.2.1.3.13; 1.2.1.4.21<=> 1.2.1.1.3; 1.2.1.4.23 <=>1.2.1.3.17; 1.2.1.4.24<=>1.2.1.1.6;
2.2.1 *2.2.2 не проектируется*	*ЦА-1*	Минимальная административная целостность	**2.2.1.1.1** Политика **административной целостности**, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится. **2.2.1.1.2** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя и защищенного объекта. **2.2.1.1.3** Запросы на изменение прав доступа должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или от пользователей, которым предоставлены соответствующих полномочия. **2.2.1.1.4** КСЗ должен давать возможность от администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежности пользователей, процессов и объектов к соответствующим домена определить конкретных пользователей и/или группы пользователей, которые имеют право модифицировать объект. **2.2.1.1.5** *не проектируется* **2.2.1.1.6** Права доступа к каждому защищенному объекту должны устанавливать в момент его создания или инициализации. Как часть политики доверительной целостности должны быть представлены правила сохранения атрибутов доступа объектов при их экспорте и импорте. *2.2.1.2.7 - 2.2.1.2.12 реализуются по ЦА-2, где:* 2.2.1.2.7 <=> 2.2.1.1.1; 2.2.1.2.9 <=> 2.2.1.1.3; 2.2.2.12 <=> 2.2.1.1.6; *2.2.1.3.13 - 2.2.1.3.18 реализуются по ЦА-3, где:* 2.2.1.3.14<=> 2.2.1.2.8; 2.2.1.3.15<=> 2.2.1.1.3; 2.2.3.18 <=> 2.2.1.1.6; *2.2.1.4.19 - 2.2.1.4.24 реализуются по ЦА-4, где:* 2.2.1.4.19 <=>2.2.1.3.13; 2.2.1.4.21<=> 2.2.1.1.3; 2.2.4.23 <=> 2.2.1.3.17; 2.2.1.4.24 <=> 2.2.1.1.6;
3.2.1 *3.2.2 не проектируется*	*ДС-1*	Устойчивость при ограниченных отказах	**3.2.1.1.1** Полтика **устойчивости отказов** требует от Разработчика провести анализ отказов компонентов КС. **3.2.1.1.2** Политика устойчивости к отказам, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится, и типы их отказов, после которых КС в состоянии продолжать функционирование. **3.2.1.1.3** Должны быть четко указаны уровни отказов, при превышении которых отказы приводят к снижению характеристик обслуживания или недоступности услуги. **3.2.1.1.4** Отказ одного защищенного компонента не должен приводить к недоступности всех услуг, а должен в худшем случае проявляться в снижении характеристик обслуживания. **3.2.1.1.5** КСЗ должен быть способен ставить в известность администратора об отказе любого защищенного компонента. *3.2.1.2.6 - 3.2.1.2.10 реализуются по ДС-2, где:* 3.2.1.2.6 <=> 3.2.1.1.1; 3.2.2.8 <=>3.2.1.1.3; 3.2.1.2.9<=> 3.2.1.1.4; 3.2.2.10<=> 3.2.1.1.5; *3.2.1.3.11 - 3.2.1.3.15 реализуются по ДС-3, где:* 3.2.1.3.11<=>3.2.1.1.1; 3.2.3.12<=>2.2.1.1.7; 3.2.1.3.13<=>3.2.1.1.3; 3.2.3.15<=> 3.2.1.1.5;
4.2.1	*НИ-1*	Внешняя идентификация и аутентификация	**4.2.1.1.1** Политика **идентификации и аутентификации**, реализуемая должна определить атрибуты, которыми характеризуется пользователь, и услуги, для использования которых необходимы эти атрибуты. Каждый пользователь должен однозначно идентифицироваться КСЗ. **4.2.1.1.2** Прежде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен с использованием защищенного механизма получить от некоторого внешнего источника аутентифицированный идентификатор этого пользователя. **4.2.1.1.3** *не проектируется* *4.2.1.2.4 - 4.2.1.2.6 реализуются по НИ-2, где:* 4.2.2.4 <=> 4.2.1.1; *4.2.1.3.7 - 4.2.1.3.9 реализуются по НИ-3, где:* 4.2.3.7 <=> 4.2.1.1; 4.2.3.9 <=> 4.2.2.6;
4.2.2	*НК-1*	Однонаправленный достоверный канал	**4.2.2.1.1** Политика **достоверного канала**, реализуемая КСЗ, должна определить механизмы установления достоверной связи между пользователями КСЗ. **4.2.2.1.2** Достоверный канал должен использоваться для начальной идентификации и аутентификации. Связь с использованием данного канала должна инициироваться исключительно пользователем. **4.2.2.1.3** *не проектируется* *4.2.2.1.4 - 4.2.2.1.6 реализуются поНК-2, где:* 4.2.2.1.4 <=> 4.2.2.1.1

Продолжение Приложение 5

№ строки *(в столбце)*	Базовые коды	Элементы критериев по иерархии строк справочников-колонок	Требования к критериям 1-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ
*Набор кода требований по уровням базовых критериев «**ОБЪЕКТЫ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **3** (из 1,2,3,4,5); Уровень базового кода **1** (из 1,2,3,4,5); Требование (очередность)			
1.3.1 / *1.3.2 не проектируется*	*К0-1*	Повторное использование объектов	**1.3.1.1.1** Политика **повторного использования объектов**, реализуемая КСЗ, должна относиться ко всем объектам КС. Прежде чем пользователь или процесс сможет получить в свое распоряжение освобожденный другим пользователем или процессом объект, установленные для предыдущего пользователя или процесса права доступа к данному объекту должны быть отменены. Прежде чем пользователь или процесс сможет получить в свое распоряжение освобожденный другим пользователем или процессом объект, вся содержащаяся в данном объекте информация должна стать недоступной.
2.3.1 / *2.3.2 не проектируется*	*ЦО-1*	Ограниченный откат	**2.3.1.1.1** Политика **отката**, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится. **2.3.1.1.2** Должны существовать автоматизированные средства, которые позволяют автоматизированному пользователю или процессу откатить или отменить определенный набор (множество) операций, проведенных над защищенным объектом за определенный промежуток времени. *2.3.1.2.3 - 2.3.1.2.4 реализуются по ЦО-2, где:* 2.3.1.2.3 <=> 2.3.1.1.1
3.3.1 / *3.3.2 не проектируется*	*ДЗ-1*	Модернизация	**3.3.1.1.1** Политика **горячей замены**, реализуемая КСЗ, должна определять политику проведения модернизации КС. **3.3.1.1.2** Администратор или пользователи, которым предоставлены соответствующие полномочия, должны имеbть возможность провести (upgrade) модернизацию КС. Модернизация КС не должна приводить к необходимости заново производить инсталляцию КС или к прерыванию выполнения КСЗ функций защиты. *3.3.1.2.3 - 3.3.1.2.4 реализуются по ДЗ-2* *3.3.1.3.5 - 3.3.1.3.6 реализуются по ДЗ-3, где:* 3.3.1.3.6 <=> 3.3.1.2.4
4.3.1	*НО-1*	Выделение администратора	**4.3.1.1.1** Политика **разграничения обязанностей**, реализуемая КСЗ, должна определять роли администратора и обычного пользователя и присущие им функции. **4.3.1.1.2** *не проектируется* **4.3.1.1.3** *не проектируется* **4.3.1.1.4** Пользователь должен иметь возможность выступать в определенной роли только после того, как он выполнит определенные действия, подтверждающие принятие им этой роли. *4.3.1.2.5 - 4.3.1.2.8 реализуются по НО-2,где:* 4.3.1.2.5 <=> 4.3.1.1.1; 4.3.1.2.7 <=> 4.3.1.1.3*;* 4.3.1.2.8 <=> 4.3.1.1.4*;* *4.4.1.3.9 - 4.4.1.3.12 реализуются по НО-3, где:* 4.4.1.3.9 <=> 4.4.1.1.1; 4.4.1.3.10 <=> 4.4.1.2.6*;* 4.4.1.3.12 <=> 4.4.1.1.4*;*
4.3.2	*НЦ-1*	КСЗ с контролем целостности	**4.3.2.1.1** Политика **целостности КСЗ** должна определять состав КСЗ и механизмы контроля целостности входящих в состав КСЗ компонентов. **4.3.2.1.2** В случае обнаружения нарушения целостности какого-либо из своих компонентов КСЗ должен поставить в известность администратора и либо автоматически восстановить соответствие компонента эталону, либо перевести КС в состояние, из которого вернуть ее к нормальному функционированию может только администратор или пользователи, которым предоставлены соответствующие полномочия. **4.3.2.1.3** Должны быть описаны ограничения, соблюдение которых позволяет гарантировать, что услуги безопасности доступны только через интерфейс КСЗ и все запросы на доступ к защищенным объектам контролируются КСЗ. *4.3.2.2.4 - 4.3.2.2.6 реализуются по НЦ-2,где:* 4.3.2.2.6 <=> 4.3.1.1.3; *4.3.2.3.7 - 4.3.2.3.9 реализуются по НЦ-3, где:* 4.3.2.3.7 <=> 4.3.2.2.4; 4.3.2.3.8 <=> 4.3.2.2.5*;*

Продолжение Приложение 5

№ строки *(в столбце)*	Базовые коды	Элементы критериев по иерархии строк справочников-колонок	Требования к критериям 1-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ
*Набор кода требований по уровням базовых критериев «**НАДЗОР**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **4** (из 1,2,3,4,5); Уровень базового кода **1** (из 1,2,3,4,5); Требование (очередность)			
1.4.1 / *1.4.2 не проектируется*	*КК-1*	Выявление скрытых каналов	**1.4.1.1.1**Политика безопасности, реализуемая КСЗ, должна обеспечивать выполнение **анализа скрытых каналов.** **1.4.1.1.2** Все скрытые каналы, существующие в аппаратном и программном обеспечении, а также в программах ПЗУ, должны быть документированы. Должна быть документирована максимальная пропускная способность каждого обнаруженного скрытого канала, полученная на основании теоретической оценки или измерений. Для скрытых каналов, которые могут использоваться совместно, должна быть документирована совокупная пропускная способность. **1.4.1.1.3** *не проектируется* *1.4.1.2.4 - 1.4.1.2.6 реализуются по КК-2, где:* 1.4.1.2.4 <=> 1.4.1.1.1; 1.4.1.2.5 <=> 1.4.1.1.2; *1.4.1.3.7 - 1.4.1.3.9 реализуются по КК-3, где:* 1.4.1.3.7 <=> 1.4.1.1.1
2.4.1 / *2.4.2 не проектируется*	*ЦВ-1*	Минимальная целостность при обмене	**2.4.1.1.1** Политика **целостности при обмене** реализуемая КСЗ, должна определять множество объектов КС и интерфейсных процессов, к которым она относится, степень защищенности, обеспечиваемую используемыми механизмами, и способность пользователей и/или процессов управлять степенью защищенности. **2.4.1.1.2** КСЗ должен обеспечивать возможность обнаружения нарушения целостности информации, содержащейся в передаваемом объекте **2.4.1.1.3** *не проектируется* **2.4.1.1.4** *не проектируется* **2.4.1.1.5** *не проектируется* **2.4.1.1.6** *не проектируется* *2.4.1.2.7 - 2.4.1.2.12 реализуются по факту ЦВ-2,где:* 2.4.1.2.7 <=> 2.4.1.1.1; 2.4.1.2.12 <=> 2.4.1.1.6; *2.4.1.3.13 - 2.4.1.3.18 реализуются по факту ЦВ-3,где:* 2.4.1.3.13<=> 2.4.1.1.1; 2.4.1.3.14 <=> 2.4.1.2.8; 2.4.1.3.17 <=> 2.4.1.2.11;
3.4.1 / *3.4.2 не проектируется*	*ДВ-1*	Ручное восстановление	**3.4.1.1.1** Политика **восстановления после сбоев**, реализуемая КСЗ, должна определять множество типов отказов КС и прерываний обслуживания, после которых возможен возврат в известное защищенное состояние без нарушения политики безопасности. Должны быть четко указаны уровни отказов, при превышении которых необходима повторная инсталляция КС. **3.4.1.1.2** После отказа КС или прерывания обслуживания, КСЗ должен перевести КС в состояние, из которого вернуть ее к нормальному функционированию может только администратор или пользователи, которым предоставлены соответствующие полномочия. **3.4.1.1.3** *не проектируется* **3.4.1.1.4** Должны существовать ручные процедуры, с помощью которых можно безопасным образом вернуть КС к нормальному функционированию. *3.4.1.2.5 - 3.4.1.2.8 реализуются по ДВ-2, где:* 3.4.1.2.5 <=> 3.4.1.1.1; 3.4.1.2.8 <=> 3.4.1.1.4; *3.4.1.3.9 - 3.4.1.3.12 реализуются по ДВ-3, где:* 3.4.1.3.9 <=> 3.4.1.1.1; 3.4.1.3.11 <=> 3.4.1.2.7;
4.4.1	*НТ-1*	Самотестирование по запросу	**4.4.1.1.1** Политика **самотестирования**, реализуемая КСЗ, должна описывать свойства КС и реализованные процедуры, которые могут быть использованы для оценки правильности функционирования КСЗ. **4.4.1.1.2** *не проектируется* *4.4.1.2.3 - 4.4.1..2.4 реализуются по факту НТ-2, где:* 4.4.1.2.3 <=> 4.4.1.1.1 *4.6.3.5 - 4.6.3.6 реализуются по факту НТ-3, где:* 4.4.1.3.5 <=> 4.4.1.1.1
4.4.2	*НВ-1*	Аутентификация узла	**4.4.2.1.1** Политика **идентификации и аутентификации при обмене**, реализуемая КСЗ, должна определять множество атрибутов КСЗ и процедуры, которые необходимы для взаимной идентификации при инициализации обмена данными с другим КСЗ. КСЗ, прежде чем начать обмен данными с другим КСЗ, должен идентифицировать и аутентифицировать этот КСЗ с использованием защищенного механизма. Подтверждение идентичности должно выполняться на основании утвержденного протокола аутентификации. **4.4.2.1.2** *не проектируется* **4.4.2.1.3** *не проектируется* *4.4.2.2.4 - 4.4.2.2.6 реализуются по НТ-2, где:* 4.4.2.2.4 <=> 4.4.2.1.1; 4.4.2.2.6 <=> 4.4.2.1.3; *4.7.4.2.7 - 4.4.2.3.9 реализуются по НТ-3, где:* 4.4.2.3.7 <=> 4.4.2.1.1; 4.4.2.3.8 <=> 4.4.2.2.5;

Продолжение Приложение 5

Номер строки *(в столбце)*	Базовые коды	Элементы критериев по иерархии строк справочников-колонок	Требования к критериям 1-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ
*Набор кода требований по уровням базовых критериев «**СВЯЗЬ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **5** (из 1,2,3,4,5); Уровень базового кода **1** (из 1,2,3,4,5); Требование (очередность)			
1.5.1 *1.5.2 не проектируется*	*КВ-1*	Минимальная конфиденциальность при обмене	**1.5.1.1.1**Политика **конфиденциальности при обмене**, реализуемая КСЗ, должна определять множество объектов и интерфейсных процессов, к которым она относится **1.5.1.1.2** Политика конфиденциальности при обмене, реализуемая КСЗ, должна определять уровень защищенности, который обеспечивается используемыми механизмами, и способность пользователей и/или процессов управлять уровнем защищенности. **1.5.1.1.3**КСЗ должен обеспечивать защиту от непосредственного ознакомления с информацией, содержащейся в передаваемом объекте. **1.5.1.1.4** *не проектируется* **1.5.1.1.5** *не проектируется* **1.5.1.1.6** *не проектируется* **1.5.1.1.7** *не проектируется* **1.5.1.1.8** *не проектируется* *1.5.1.2.9 - 1.5.1.2.16 реализуются по КВ-2,где:* 1.5.1.2.9 <=> 1.5.1.1.1; 1.5.1.2.10 <=>1.5.1.1.2; 1.5.1.2.11<=> 1.5.1.1.3; 1.5.1.2.15 <=>1.5.1.1.7; 1.5.1.2.16 <=>1.5.1.1.8 *1.5.1.3.17- 1.5.1.3.24 реализуются по КВ-3,где:* 1.5.1.3.18 <=>1.5.1.1.2; 1.5.1.3.19 <=>1.5.1.1.3; 1.5.1.3.20 <=>1.5.1.2.12; 1.5.1.3.24 <=>1.5.1.1.8 *1.5.1.4.25 -1.5.1.4.32 реализуются по КВ-4,где:* 1.5.1.4.25<=>1.5.1.3.17; 1.5.1.4.26 <=>1.5.1.1.2; 1.5.1.4.27 <=> 1.5.1.1.3; 1.5.1.4.28 <=>1.5.1.2.12; 1.5.1.4.29<=>1.5.1.3.21; 1.5.1.4.30 <=>1.5.1.3.22; 1.5.1.4.31 <=>1.5.1.3.23;
2.5.1 *2.5.2 не проектируется*	-	*Элемент критерия не проектируется*	-
3.5.1 *3.5.2 не проектируется*	-	*Элемент критерия не проектируется*	-
4.5.1	*НА-1*	Базовая аутентификация отправителя	**4.5.1.1.1** Политика **аутентификация отправителя**, реализуемая КСЗ, должна определять множество свойств и атрибутов передаваемого объекта, пользователя-отправителя и интерфейсного процесса, а также процедуры, которые бы позволяли однозначно установить, что данный объект был отправлен (создан) определенным пользователем. **4.5.1.1.2** *не проектируется* **4.5.1.1.3** Установление принадлежности должно выполняться на основании утвержденного протокола аутентификации. **4.5.1.1.4** *не проектируется* *4.5.1.2.5 - 4.5.1.2.8 реализуются по НА-2, где:* 4.5.1.2.5 <=> 4.5.1.1.1; 4.5.1.2.7 <=> 4.5.1.1.3;
4.5.2	*НП-1*	Базовая аутентификация получателя	**4.5.2.1.1** Политика **аутентификация получателя**, реализуемая КСЗ, должна определять множество свойств и атрибутов передаваемого объекта, пользователя-получателя и интерфейсного процесса, а также процедуры, которые бы позволяли однозначно установить, что данный объект был получен определенным пользователем. **4.5.2.1.2** *не проектируется* **4.5.2.1.3** Установление получателя должно выполняться на основании утвержденного протокола аутентификации. **4.5.2.1.4** *не проектируется* *4.5.2.2.5 - 4.5.2.2.8 реализуются по факту НП-2, где:* 4.5.2.2.5 <=> 4.5.2.1.1; 4.5.2.2.7 <=> 4.5.2.1.3;

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 2-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ЗАПРОС**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **1** (из 1,2,3,4,5); Уровень базового кода **2** (из 1,2,3,4,5); Требование (очередность)			
1.1.1	*КД-2*	Базовая доверительная конфиденциальность	***1.1.1.1.1 - 1.1.1.1.6 реализуются по КД-1*** **1.1.1.2.7** <=>1.1.1.1.1 **1.1.1.2.8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя и защищенного объекта. **1.1.1.2.9** <=>1.1.1.1.3 **1.1.1.2.10** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право получать информацию от объекта. **1.1.1.2.11** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс. **1.1.1.2.12** <=>1.1.1.1.6 *1.1.1.3.13 - 1.1.1.3.18 реализуются поКД-3, где:* 1.1.1.3.14 <=>1.1.1.2.8; 1.1.1.3.15<=>1.1.1.1.3; 1.1.1.1.18 <=>1.1.1.1.6; *1.1.1.4.19 - 1.1.1.4.24 реализуются поКД-4, где;* 1.1.1.4.19 <=>1.1.1.3.13; 1.1.1.4.21<=>1.1.1.1.3; 1.1.1.4.23 <=>1.1.1.3.17; 1.1.1.4.24 <=>1.1.1.1.6;
2.1.1	*ЦД-2*	Базовая доверительная целостность	***2.1.1.1.1 - 2.1.1.1.6 реализуются по ЦД-1*** **2.1.1.2.7** <=>2.1.1.1.1 **2.1.1.2.8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта. **2.1.1.2.9** <=> 2.1.1.1.3 **2.1.1.2.10** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретные процессы и/или группы процессов, которые имеют право модифицировать объект. **2.1.1.2.11** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс. **2.1.1.2.12**<=>2.1.1.1.6 *2.1.1.3.13 - 2.1.1.3.18 реализуются по КД-3, где:* 2.1.1.3.14 <=>2.1.1.1.8; 2.1.1.3.15<=>2.1.1.1.3; 2.1.1.1.18<=>2.1.1.1.6; *2.1.1.4.19 - 2.1.1.4.24 реализуются по КД-4, где;* 2.1.1.4.19 <=>2.1.1.3.13; 2.1.1.4.21<=>2.1.1.1.3; 2.1.1.4.23<=>2.1.1.3.17; 2.1.1.4.24 <=>2.1.1.1.6;
3.1.1	*ДР-2*	Пресечение захвата ресурсов	***3.1.1.1.1 - 3.1.1.1.4 реализуются по ДР-1*** **3.1.1.2.5** Политика использования ресурсов, реализуемая КСЗ, должна относиться ко всем объектам КС **3.1.1.2.6** <=> 3.1.1.1.2; **3.1.1.2.7** <=> 3.1.1.1.3; **3.1.1.2.8** Должна существовать возможность устанавливать ограничения таким образом, чтобы КСЗ имел возможность предотвратить действия, которые могут привести к невозможности доступа других пользователей к функциям. КСЗ или защищенным объектам. КСЗ должен контролировать такие действия, осуществляемые со стороны отдельного пользователя. *3.1.1.3.8 - 3.1.1.3.12 реализуются по КД-3, где:* 3.1.1.3.9 <=> 3.1.1.2.5; 3.1.1.3.11 <=> 3.1.1.1.3;
4.1.1	*НР-2*	Защищенный журнал	***4.1.1.1.1 - 4.1.1.1.6 реализуются по НР-1*** **4.1.1.2.7** <=> 4.1.1.1.1.1; **4.1.1.2.8** <=> 4.1.1.1.1.2; **4.1.1.2.9** <=> 4.1.1.1.1.3; **4.1.1.2.10** КСЗ должен обеспечивать защиту журнала регистрации от несанкционированного доступа, модификации или разрушения. Администраторы и пользователи, которым предоставлены соответствующие полномочия, должны иметь в своем распоряжении средства просмотра и анализа журнала регистрации **4.1.1.2.11** <=> 4.1.1.1.5; **4.1.1.2.12** <=> 4.1.1.1.6; *4.1.1.3.13 - 4.1.1.1.18 реализуются по НР-3, где:* 4.1.1.1.13<=>4.1.1.1.1; 4.1.1.1.14<=> 4.1.1.1.2; 4.1.1.1.15<=> 4.1.1.1.3; 4.1.1.1.16<=>4.1.1.1.10; 4.1.1.1.18<=> 4.1.1.1.6 *4.1.1.1.19 - 4.1.1.1.24 реализуются по НР-4, где:* 4.1.1.1.19<=>4.1.1.1.1; 4.1.1.1.21<=> 4.1.1.1.3; 4.1.1.1.22<=> 4.1.1.1.10; 4.1.1.1.23 <=>4.1.1.1.17; 4.1.1.1.24<=> 4.1.1.1.6 *4.1.1.1.25 - 4.1.1.1.30 реализуются по НР-5, где:* 4.1.1.1.25<=>4.1.1.1.1; 4.1.1.1.26<=>4.1.1.1.20; 4.1.1.1.27 <=> 4.1.1.1.3; 4.1.1.1.28 <=>4.1.1.1.10; 4.1.1.1.30<=> 4.1.1.1.6
4.1.2 ***Отсылка***	*до Г-3*	*Требования критериев гарантий (Г-1, 2, 3)*	1. Архитектура. 2. Среда разработки: *2.1 Процесс разработки; 2.2 Управление конфигурацией.* 3. Последовательность разработки: 3.*1 Политика безопасности;. 3.2 Модель политики безопасности; 3.3 Проект архитектуры; 3.4 Детальный проект; 3.5 Реализация* 4. Среда функционирования. 5. Документация. 6. Испытания комплекса средств защиты.

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 2-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ДОСТУП**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **2** (из 1,2,3,4,5); Уровень базового кода **2** (из 1,2,3,4,5); Требование (очередность)			
1.2.1	*КА-2*	Базовая административная конфиденциальность	***1.2.1.1.1 - 1.2.1.1.6 реализуются по КА-1*** **1.2.1.2.7** <=> 1.2.1.1.1; **1.2.1.2.8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя защищенного объекта **1.2.1.2.9** <=> 1.2.1.1.3 **1.2.1.2.10** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право получать информацию от объекта **1.2.1.2.11** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс **1.2.1.2.12** <=>1.2.1.1.6; *1.2.1.3.13 - 1.2.1.3.18 реализуются по КА-3, где:* 1.2.1.3.14 <=>1.2.1.2.8; 1.2.1.3.15 <=>1.2.1.1.3; 1.2.1.3.18 <=>1.2.1.1.6; *1.2.1.4.19 - 1.2.1.4.24 реализуются по КА-4, где;* 1.2.1.4.19 <=>1.2.1.3.13; 1.2.1.4.21 <=>1.2.1.1.3; 1.2.1.4.23 <=>1.2.1.3.17; 1.2.1.4.24 <=>1.2.1.1.6;
2.2.1	*ЦА-2*	Базовая административная целостность	***2.2.1.1.1 - 2.2.1.1.6 реализуются по ЦА-1*** **2.2.1.2.7** <=> 2.2.1.1.1; **2.2.1.2.8** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса и защищенного объекта **2.2.1.2.9** <=> 2.2.1.1.3 **2.2.1.2.10** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретные процессы и/или группы процессов, которые имеют право модифицировать объект **2.2.1.2.11** КСЗ должен давать администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам, определить конкретных пользователей и/или группы пользователей, которые имеют право инициировать процесс **2.2.1.2.12** <=> 2.2.1.1.6; *2.2.1.3.13 - 2.2.1.3.18 реализуются по ЦА-3, где:* 2.2.1.3.14<=> 2.2.1.2.8; 2.2.1.3.15<=> 2.2.1.1.3; 2.2.1.3.18 <=> 2.2.1.1.6; *2.2.1.4.19 - 2.2.1.4.24 реализуются по ЦА-4,где:* 2.2.1.4.19 <=>2.2.1.3.13; 2.2.1.4.21<=> 2.2.1.1.3; 2.2.1.4.23 <=> 2.2.1.3.17; 2.2.1.4.24 <=> 2.2.1.1.6;
3.2.1	*ДС-2*	Устойчивость с ухудшением характеристик обслуживания	***3.2.1.1.1 - 3.2.1.1.5 реализуются по ДС-1*** **3.2.1.2.6** <=> 3.2.1.1.1; **3.2.1.2.7** Политика устойчивости к отказам, реализуемая КСЗ, должна относиться ко всем компонентам КС **3.2.1.2.8** <=> 3.2.1.1.3; **3.2.1.2.9** <=> 3.2.1.1.4; **3.2.1.2.10** <=> 3.2.1.1.5; *3.2.1.3.11 - 3.2.1.3.15 реализуются по ДС-3, где:* 3.2.1.3.11<=> 3.2.1.1.1; 3.2.1.3.12 <=> 3.2.1.2.7; 3.2.1.3.13 <=> 3.2.1.1.3; 3.2.1.3.15 <=> 3.2.1.1.5;
4.2.1	*НИ-2*	Одиночная идентификация и аутентификация	***4.2.1.1.1 - 4.2.1.1.3 реализуются по НИ-1*** **4.2.1.2.4** <=> 4.2.1.1.1; **4.2.1.2.5** Прежде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен аутентифицировать этого пользователя с использованием защищенного механизма **4.2.1.2.6** КСЗ должен обеспечивать защиту данных аутентификации от несанкционированного доступа, модификации или разрушения *4.2.1.3.7 - 4.2.1.3.9 реализуются по НИ-3, где:* 4.2.1.3.7 <=> 4.2.1.1.1; 4.2.1.3.9 <=> 4.2.1.2.6;
4.2.2	*НК-2*	Двунаправленный достоверный канал	***4.3.1.1.1 - 4.3.1.1.3 реализуются по НК-1*** **4.3.1.2.4** <=> *4.3.1.1.1* **4.3.1.2.5** Достоверный канал должен использоваться для начальной идентификации и аутентификации и в других случаях, когда необходима прямая связь пользователь / КСЗ или КСЗ / пользователь. Связь с использованием данного канала должна инициироваться пользователем или КСЗ. **4.3.1.2.6** Обмен с использованием достоверного канала, инициируемый КСЗ, должен быть однозначно идентифицируем как таковой и должен происходить только после положительного подтверждения готовности к обмену со стороны пользователя

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 2-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ОБЪЕКТЫ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **3** (из 1,2,3,4,5); Уровень базового кода **2** (из 1,2,3,4,5); Требование (очередность)			
1.3.1	*К0-1*	Повторное использование объектов	***1.3.1.1.1 реализуются по КО-1***
2.3.1	*ЦО-2*	Полный откат	***2.3.1.1.1 - 2.3.1.1.2 реализуются по ЦО-1*** **2.3.1.2.3** <=> 2.3.1.1.1 **2.3.1.2.4** Должны существовать автоматизированные средства, которые позволяют авторизованному пользователю или процессу откатить или отменить все операции, проведенные над защищенным объектом за определенный промежуток времени
3.3.1	*ДЗ-2*	Ограниченная горячая замена	***3.3.1.1.1 - 3.3.1.1.2 реализуются по ДЗ-1*** **3.3.1.2.3** Политика горячей замены, реализуемая КСЗ, должна определять множество компонентов КС, которые могут быть заменены без прерывания обслуживания **3.3.1.2.4** Администратор или пользователи, которым предоставлены соответствующие полномочия, должны иметь возможность заменить любой защищенный компонент *3.3.1.3.5 - 3.3.1.3.6 реализуются по ДЗ-3, где:* 3.3.1.3.6 <=> 3.3.1.2.4
4.3.1	*НО-2*	Разграничение обязанностей администратора	***4.3.1.1.1 - 4.4.1.1.4 реализуются по НО-1*** **4.3.1.2.5** <=> 4.4.1.1.1; **4.3.1.2.6** Политика разграничения обязанностей должна определять минимум две различные административные роли: администратора безопасности и иного администратора. Функции, присущие каждой из ролей, должны быть минимизированы так, чтобы включать только те функции, которые необходимы для выполнения данной роли. **4.3.1.2.7** <=> 4.3.1.1.3*;* **4.3.1.2.8** <=> 4.3.1.1.4*;* *4.3.1.3.9 - 4.3.1.3.12 реализуются по НО-3, где:* 4.3.1.3.9 <=> 4.3.1.1.1; 4.3.3.10 <=> 4.3.1.2.6*;* 4.3.3.12 <=> 4.3.1.1.4;
4.3.2	*НЦ-2*	КСЗ с гарантируемой целостностью	***4.3.2.1.1 - 4.3.2.1.3 реализуются по НЦ-1*** **4.3.2.2.4** Политика целостности КСЗ должна определять домен КСЗ и другие домены, а также механизмы защиты, используемые для реализации разделения доменов **4.3.2.2.5** КСЗ должен поддерживать домен для своего собственного исполнения с целью защиты от внешних воздействий и несанкционированной модификации и/или потери управления **4.3.2.2.6** <=> 4.3.2.1.3; *4.3.2.3.7 - 4.3.2.3.9 реализуются по НЦ-3, где:* 4.3.2.3.7 <=> 4.3.2.2.4; 4.3.2.3.8 <=> 4.3.2.2.5*;*

Продолжение Приложение 5

Номер строки ***(в столбце)***	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 2-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**НАДЗОР**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **4** (из 1,2,3,4,5); Уровень базового кода **2** (из 1,2,3,4,5); Требование (очередность)			
1.4.1	*КК-2*	Контроль скрытых каналов	***1.4.1.1.1 - 1.4.1.1.3 реализуются по КК-1*** **1.4.1.2.4** <=> 1.4.1.1.1; **1.4.1.2.5** <=> 1.4.1.1.2; **1.4.1.2.6** КСЗ должен обеспечивать регистрацию использования утвержденного подмножества обнаруженных скрытых каналов *1.4.1.3.7 - 1.4.1.3.9 реализуются по КК-3, где:* 1.4.3.7 <=> 1.4.1.1
2.4.1	*ЦВ-2*	Базовая целостность при обмене	***2.4.1.1.1 - 2.4.1.1.6 реализуются по ЦВ-1*** **2.4.1.2.7** <=> 2.4.1.1.1; **2.4.1.2.8** КСЗ должен обеспечивать возможность обнаружения нарушения целостности информации, содержащейся в передаваемом объекте, а также фактов его удаления или дублирования **2.4.1.2.9** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса **2.4.1.2.10** Запросы на экспорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса **2.4.1.2.11** Запросы на присвоение или изменение уровня защищенности должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или пользователей, которым предоставлены соответствующие полномочия **2.4.1.2.12** <=> 2.4.1.1.6; *2.4.1.3.13 - 2.4.3.18 реализуются по ЦВ-3,где:* 2.4.1.3.13 <=> 2.4.1.1.1; 2.4.1.3.14 <=> 2.4.1.2.8; 2.4.1.3.17 <=> 2.4.1.2.11;
3.4.1	*ДВ-2*	Автоматизированное восстановление	***3.4.1.1.1 - 3.4.1.1.4 реализуются по ДВ-1*** **3.4.1.2.5** <=> 3.4.1.1.1; **3.4.1.2.6** После отказа КС или прерывания обслуживания КСЗ должен быть способен определить, могут ли быть использованы автоматизированные процедуры для возврата КС к нормальному функционированию безопасным образом. Если такие процедуры могут быть использованы, то КСЗ должен быть способен выполнить их и вернуть КС к нормальному функционированию **3.4.1.2.7** Если автоматизированные процедуры не могут быть использованы, то КСЗ должен перевести КС в состояние, из которого вернуть ее к нормальному функционированию может только администратор или пользователи, которым предоставлены соответствующие полномочия **3.4.1.2.8** <=> 3.4.1.1.4; *3.4.1.3.9 - 3.4.1.3.12 реализуются по ДВ-3, где:* 3.4.1.3.9 <=> 3.4.1.1.1; 3.4.1.3.11 <=> 3.4.1.2.7;
4.4.1	*НТ-2*	Самотестирование при старте	***4.4.1.1.1 - 4.4.1.1.2 реализуются по НТ-1*** **4.4.1.2.3** <=> 4.4.1.1.1 **4.4.1.2.4** КСЗ должен быть способен выполнять набор тестов с целью оценки правильности функционирования своих критичных функций. Тесты должны выполняться по запросу имеющего соответствующие полномочия пользователя при инициализации КСЗ *4.4.1.3.5 - 4.4.1.3.6 реализуются по НТ-3, где:* 4.6.1.3.5 <=> 4.6.1.1.1
4.4.2	*НВ-2*	Аутентификация источника данных	***4.4.2.1.1 - 4.4.2.1.3 реализуются по НВ-1, где:*** **4.4.2.2.4** <=> 4.4.2.1.1; **4.4.2.2.5** КСЗ должен использовать защищенные механизмы для установления источника каждого экспортируемого и импортируемого объекта 4.4.2.2.6 <=> 4.4.2.1.3; *4.4.2.3.7 - 4.4.2.3.9 реализуются по НТ-3, где:* 4.4.2.3.7 <=> 4.4.2.1.1; 4.4.2.3.8 <=> 4.4.2.2.5;

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 2-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**СВЯЗЬ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка 5 (из 1,2,3,4,5); Уровень базового кода 2 (из 1,2,3,4,5); Требование (очередность)			
1.5.1	*КВ-2*	Базовая конфиденциальность при обмене	***1.5.1.1.1 - 1.5.1.1.8 реализуются по КВ-1*** **1.5.1.2.9** <=> 1.5.1.1.1; **1.5.1.2.10** <=>1.5.1.1.2; **1.5.1.2.11** <=>1.5.1.1.3; **1.5.1.2.12** Запросы на присвоение или изменение уровня защищенности должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или пользователей, которым предоставлены соответствующие полномочия **1.5.1.2.13** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса **1.5.1.2.14** Запросы на импорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса **1.5.1.2.15** <=>1.5.1.1.7; **1.5.1.2.16** <=>1.5.1.1.8; *1.5.1.3.17 - 1.5.1.3.24 реализуются по КВ-3,где:* 1.5.1.3.18 <=>1.5.1.1.2; 1.5.1.3.19 <=>1.5.1.1.3; 1.5.1.3.20 <=>1.5.1.2.12; 1.5.1.3.24 <=>1.5.1.1.8 *1.5.1.4.25 - 1.5.1.4.32 реализуются по КВ-4,где:* 1.5.1.4.25 <=>1.5.1.3.17; 1.5.1.4.26 <=>1.5.1.1.2; 1.5.1.4.27 <=>1.5.1.1.3; 1.5.1.4.28 <=>1.5.1.2.12; 1.5.1.4.29 <=>1.5.1.3.21; 1.5.1.4.30 <=>1.5.1.3.22; 1.5.1.4.31 <=>1.5.1.3.23;
2.5.1	-	*Элемент критерия не проектируется*	
3.5.1	-	*Элемент критерия не проектируется*	
4.5.1	*НА-2*	Аутентификация отправителя с подтверждением	***4.5.1.1.1 - 4.5.1.1.4 реализуются по НА-1*** **4.5.1.2.5** <=> 4.5.1.1.1; **4.5.1.2.6** Дополнительно должны быть определены те свойства, атрибуты и процедуры, которые могут использоваться для однозначного подтверждения принадлежности объекта независимой третьей стороной **4.5.1.2.7** <=> 4.5.1.1.3; **4.5.1.2.8** Используемый протокол аутентификации должен обеспечивать возможность однозначного подтверждения принадлежности объекта независимой третьей стороной
4.5.2	*НП-2*	Аутентификация получателя с подтверждением	***4.5.2.1.1 - 4.5.2.1.4 реализуются по НП-1*** **4.5.2.2.5** <=> 4.5.2.1.1; **4.5.2.2.6** Дополнительно должны быть определены те свойства, атрибуты и процедуры, которые могут использоваться независимой третьей стороной для однозначного подтверждения факта получения объекта пользователем **4.5.2.2.7** <=> 4.5.2.1.3; **4.5.2.2.8** Используемый протокол аутентификации должен обеспечивать возможность однозначного подтверждения независимой третьей стороной факта получения объекта пользователем

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 3-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ЗАПРОС**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **1** (из 1,2,3,4,5); Уровень базового кода **3** (из 1,2,3,4,5); Требование (очередность)			
1.1.1	*КД-3*	Полная доверительная конфиденциальность	***1.1.1.1.1 - 1.1.1.1.6 реализуются по КД-1*** ***1.1.1.2.7 - 1.1.1.2.12 реализуются по КД-2*** **1.1.1.3.13** Политика доверительной конфиденциальности, реализуемая КСЗ, должна относиться ко всем объектам КС **1.1.1.3.14** <=>1.1.1.2.8; **1.1.1.3.15** <=>1.1.1.1.3; **1.1.1.3.16** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права получать информацию от объекта **1.1.1.3.17** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс **1.1.1.3.18** <=>1.1.1.1.6; *1.1.1.4.19 - 1.1.1.4.24 реализуются по КД-4, где;* 1.1.1.4.19 <=>1.1.1.3.13; 1.1.1.4.21<=>1.1.1.1.3; 1.1.1.4.23 <=>1.1.1.3.17; 1.1.1.4.24 <=>1.1.1.1.6;
2.1.1	*ЦД-3*	Полная доверительная целостность	***2.1.1.1.1 - 2.1.1.1.6 реализуются по КД-1*** ***2.1.1.2.7 - 2.1.2.12 реализуются по КД-2*** **2.1.1.3.13** Политика доверительной целостности, реализуемая КСЗ, должна относиться ко всем объектам КС **2.1.1.3.14** <=>2.1.1.1.8; **2.1.1.3.15** <=>2.1.1.1.3; **2.1.1.3.16** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретные процессы (и группы процессов), которые имеют, а также тех, которые не имеют права модифицировать объект **2.1.1.3.17** КСЗ должен давать пользователю возможность для каждого процесса, принадлежащего его домену, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс **2.1.1.3.18** <=>2.1.1.1.6; *2.1.1.4.19 - 2.1.1.4.24 реализуются по КД-4, где;* 2.1.1.4.19 <=>2.1.1.3.13; 2.1.1.4.21<=>2.1.1.1.3; 2.1.1.4.23<=>2.1.1.3.17; 2.1.1.4.24 <=>2.1.1.1.6;
3.1.1	*ДР-3*	Приоритетность использования ресурсов	***3.1.1.1.1 - 3.1.1.1.4 реализуются по ДР-1*** ***3.1.1.2.5 - 3.1.1.2.8 реализуются по ДР-2*** **3.1.1.3.9** <=> 3.1.1.2.5; **3.1.1.3.10** Политика использования ресурсов должна определять ограничения, которые можно накладывать, на количество данных объектов (объем ресурсов), выделяемых отдельному пользователю и произвольным группам пользователей **3.1.1.3.11** <=> 3.1.1.1.3; **3.1.1.3.12** Должна существовать возможность устанавливать ограничения таким образом, чтобы КСЗ имел возможность предотвратить действия, которые могут привести к невозможности доступа других пользователей к функциям КСЗ или защищенным объектам. КСЗ должен контролировать такие действия, осуществляемые со стороны отдельного пользователя и произвольных групп пользователей
4.1.1	*НР-3*	Сигнализация об опасности	***4.1.1.1.1 - 4.1.1.1.6 реализуются по НР-1*** ***4.1.1.2.7 - 4.1.1.2.12 реализуются по НР-2*** **4.1.1.3.13** <=> 4.1.1.1.1; **4.1.1.3.14** <=> 4.1.1.1.2; **4.1.1.3.15** <=> 4.1.1.1.3; **4.1.1.3.16** <=> 4.1.1.2.10; **4.1.1.3.17** КСЗ должен быть способен контролировать единичные или повторяющиеся регистрируемые события, которые могут свидетельствовать о прямых (существенных) нарушениях политики безопасности КС. КСЗ должен быть способен немедленно информировать администратора о превышении порогов безопасности и, если регистрируемые опасные события повторяются, осуществить неразрушающие действия по пресечению повторения этих событий **4.1.3.18** <=> 4.1.1.1.6 *4.1.4.19 - 4.1.1.1.24 реализуются по НР-4, где:* 4.1.1.4.19<=>4.1.1.1.1; 4.1.1.4.21<=>4.1.1.1.3; 4.1.1.4.22 <=> 4.1.1.1.10; 4.1.1.4.23 <=> 4.1.1.3.17; 4.1.1.4.24<=>4.1.1.1.6 *4.1.5.25 - 4.1.1.5.30 реализуются по НР-5, где:* 4.1.1.5.25<=>4.1.1.1.1; 4.1.1.5.26<=>4.1.1.1.20; 4.1.1.5.27 <=> 4.1.1.1.3; 4.1.1.5.28 <=> 4.1.1.2.10; 4.1.1.5.29<=>4.1.1.3.17
4.1.2 **Отсылка**	*до Г-4*	*Требования критериев гарантий (Г-1,2,3,4)*	1. Архитектура. 2. Среда разработки: *2.1 Процесс разработки; 2.2 Управление конфигурацией.* 3. Последовательность разработки: *3.1 Политика безопасности;. 3.2 Модель политики безопасности; 3.3 Проект архитектуры; 3.4 Детальный проект; 3.5 Реализация.* 4. Среда функционирования. 5. Документация. 6. Испытания комплекса средств защиты.

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 3-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ДОСТУП**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **2** (из 1,2,3,4,5); Уровень базового кода **3** (из 1,2,3,4,5); Требование (очередность)			
1.2.1	*КА-3*	Базовая административная конфиденциальность	***1.2.1.1.1 - 1.2.1.1.1.6 реализуются по КА-1*** ***1.2.1.2.7 - 1.2.1.2.12 реализуются по КА-2*** **1.2.1.3.13** Политика административной конфиденциальности, реализуемая КСЗ, должна относиться ко всем объектам КС **1.2.1.3.14** <=> 1.2.1.2.8; **1.2.1.3.15** <=> 1.2.1.1.3; **1.2.1.3.16** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права получать информацию от объекта **1.2.1.3.17** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс **1.2.1.3.18** <=>1.2.1.1.6; *1.2.1.4.19 - 1.2.1.4.24 реализуются по КА-4, где;* 1.2.1.4.19 <=>1.2.1.3.13; 1.2.1.4.21 <=> 1.2.1.1.3; 1.2.1.4.23 <=>1.2.1.3.17; 1.2.1.4.24 <=>1.2.1.1.6;
2.2.1	*ЦА-3*	Базовая административная целостность	***2.2.1.1.1 - 2.2.1.1.6 реализуются по ЦА-1*** ***2.2.1.2.7 - 2.2.1.2.12 реализуются по ЦА-2*** **2.2.1.3.13** Политика административной целостности, реализуемая КСЗ, должна относиться ко всем объектам КС **2.2.1.3.14** <=> 2.2.1.2.8; **2.2.1.3.15** <=> 2.2.1.1.3; **2.2.1.3.16** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретные процессы (и группы процессов), которые имеют, а также тех, которые не имеют права модифицировать объект **2.2.1.3.17** КСЗ должен давать администратору или имеющему соответствующие полномочия пользователю для каждого процесса путем управления принадлежностью пользователей и процессов к соответствующим доменам, определить конкретных пользователей (и группы пользователей), которые имеют, а также тех, которые не имеют права инициировать процесс **2.2.1.3.18** <=> 2.2.1.1.6; *2.2.1.4.19 - 2.2.1.4.24 реализуются по ЦА-4,где:* 2.2.1.4.19 <=>2.2.1.3.13; 2.2.1.4.21 <=> 2.2.1.1.3; 2.2.1.4.23 <=>2.2.1.3.17; 2.2.1.4.24 <=> 2.2.1.1.6;
3.2.1	*ДС-3*	Устойчивость с ухудшением характеристик обслуживания	***3.2.1.1.1 - 3.2.1.5 реализуются по ДС-1*** ***3.2.1.2.6 - 3.2.2.10 реализуются по ДС-2*** **3.2.1.3.11** <=> 3.2.1.1.1; **3.2.1.3.12** <=> 3.2.1.2.7; **3.2.1.3.13** <=> 3.2.1.1.3; **3.2.1.3.14** Отказ одного защищенного компонента не должен приводить к недоступности всех услуг или к снижению характеристик обслуживания **3.2.1.3.15** <=> 3.2.1.1.5;
4.2.1	*НИ-3*	Множественная идентификация и аутентификация	***4.2.1.1.1 - 4.2.1.1.3 реализуются по факту НИ-1*** ***4.2.1.2.4 - 4.2.1.2.6 реализуются по факту НИ-2*** **4.2.1.3.7** <=> 4.2.1.1.1; **4.2.1.3.8 П**режде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен аутентифицировать этого пользователя с использованием защищенных механизмов двух или более **4.2.1.3.9** <=> 4.2.1.1.6;
4.2.2	<=> *НК-2*	Двунаправленный достоверный канал	***4.2.2.1.1 - 4.2.2.1.3 реализуются по НК-1*** ***4.2.2.2.4 - 4.2.2.2.6 реализуются по НК-2***

Продолжение Приложение 5

Номер строки ***(в столбце)***	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 3-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ОБЪЕКТЫ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **3** (из 1,2,3,4,5); Уровень базового кода **3** (из 1,2,3,4,5); Требование (очередность)			
1.3.1	<=> *К0-1*	Повторное использование объектов	***1.3.1.3.1 реализуются по КО-1***
2.3.1	<=> *ЦО-2*	Полный откат	***2.3.1.1.1 - 2.3.1.1.2 реализуются по ЦО-1*** ***2.3.1.2.3 - 2.3.1.2.4 реализуются по ЦО-2***
3.3.1	*ДЗ-3*	Горячая замена любого компонента	***3.3.1.1.1 - 3.3.1.1.2 реализуются по ДЗ-1*** ***3.3.1.2.3 - 3.3.1.2.4 реализуются по ДЗ-2*** **3.3.1.3.5** Политика горячей замены, реализуемая КСЗ, должна обеспечивать возможность замены любого компонента без прерывания обслуживания **3.3.1.3.6** <=> 3.3.1.2.4
4.3.1	*НО-3*	Разграничение обязанностей на основании привилегий	***4.3.1.1.1 - 4.3.1.1.4 реализуются по НО-1*** ***4.3.1.2.5 - 4.3.1.2.8 реализуются по НО-2*** **4.3.1.3.9** <=> 4.3.1.1.1; **4.3.1.3.10** <=> 4.3.1.2.6; **4.3.1.3.11** Политика разграничения обязанностей должна определять множество различных ролей пользователей **4.3.1.3.12** <=> 4.3.1.1.4;
4.3.2	*НЦ-3*	КСЗ с функциями диспетчера доступа	***4.3.2.1.1 - 4.3.2.1.3 реализуются по НЦ-1*** ***4.3.2.2.4 - 4.3.2.2.6 реализуются по НЦ-2*** **4.3.2.3.7** <=> 4.3.2.2.4; **4.3.2.3.8** <=> 4.3.2.2.5; **4.3.2.3.9** КСЗ должен гарантировать, что услуги безопасности доступны только через интерфейс КСЗ и все запросы на доступ к защищенным объектам контролируются КСЗ

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 3-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**НАДЗОР**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **4** (из 1,2,3,4,5); Уровень базового кода **3** (из 1,2,3,4,5); Требование (очередность)			
1.4.1	*КК-3*	Перекрытие скрытых каналов	***1.4.1.1.1 - 1.4.1.1.3 реализуются по КК-1*** ***1.4.1.2.4 - 1.4.1.2.6 реализуются по КК-2*** **1.4.1.3.7** <=> 1.4.1.1.1 **1.4.1.3.8** Все (утвержденное подмножество) обнаруженные при анализе скрытые каналы должны быть устранены
2.4.1	*ЦВ-3*	Полная целостность при обмене	***2.4.1.1.1 - 2.4.1.1.6 реализуются по ЦВ-1*** ***2.4.1.2.7 - 2.4.1.2.12 реализуются по ЦВ-2*** **2.4.1.3.13** <=> 2.4.1.1.1 **2.4.1.3.14** <=> 2.4.1.2.8 **2.4.1.3.15** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса и приемника объекта **2.4.1.3.16** Запросы на экспорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса и источника объекта **2.4.1.3.17** <=> 2.4.1.2.11 **2.4.1.3.18** Представление защищенного объекта должно быть функцией атрибутов доступа интерфейсного процесса, самого объекта, а также его источника и приемника
3.4.1	*ДВ-3*	Избирательное восстановление	***3.4.1.1.1 - 3.4.1.1.4 реализуются по ДВ-1*** ***3.4.1.2.5 - 3.4.1.2.8 реализуются по ДВ-2*** **3.4.1.3.9** <=> 3.4.1.1.1; **3.4.1.3.10** После любого отказа КС или прерывания обслуживания, не приводящих к необходимости заново инсталлировать КС, КСЗ должен быть способен выполнить необходимые процедуры и безопасным образом вернуть КС к нормальному функционированию или, в худшем случае, функционированию в режиме с ухудшенными характеристиками обслуживания **3.4.1.3.11** <=> 3.4.1.2.7; **3.4.1.3.12** Должны существовать ручные процедуры, с помощью которых можно безопасным образом вернуть КС из режима с ухудшенными характеристиками обслуживания в режим нормального функционирования
4.4.1	*НТ-3*	Самотестирование в реальном времени	***4.4.1.1.1 - 4.4.1.1.2 реализуются по НТ-1*** ***4.4.1.2.3 - 4.4.1.2.4 реализуются по НТ-2*** **4.4.1.3.5** <=> 4.4.1.1.1 **4.4.1.3.6** КСЗ должен быть способен выполнять набор тестов с целью оценки правильности функционирования своих критичных функций. Тесты должны выполняться по запросу имеющего соответствующие полномочия пользователя при инициализации КСЗ и в процессе штатного функционирования
4.4.2	*НВ-3*	Аутентификация с подтверждением	***4.4.2.1.1 - 4.4.2.1.3 реализуются по НВ-1*** ***4.4.2.2.4 - 4.4.2.2.5 реализуются по НВ-2*** **4.4.2.3.7** <=> 4.4.2..1.1; **4.4.2.3.8** <=> 4.4.2..2.5; **4.4.2.3.9** Используемый протокол аутентификации должен обеспечивать возможность однозначного подтверждения источника объекта независимой третьей стороной

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 3-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**СВЯЗЬ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **5** (из 1,2,3,4,5); Уровень базового кода **3** (из 1,2,3,4,5); Требование (очередность)			
1.5.1	*КВ-3*	Полная конфиденциальность при обмене	***1.5.1.1.1 - 1.5.1.8 реализуются по КВ-1*** ***1.5.1.2.9 - 1.5.2.16 реализуются по КВ-2*** **1.5.1.3.17** Политика конфиденциальности при обмене, реализуемая КСЗ, должна относиться ко всем объектам и существующим интерфейсным процессам **1.5.1.3.18** <=>1.5.1.1.2; **1.5.1.3.19** <=>1.5.1.1.3; **1.5.1.3.20** <=>1.5.1.2.12; **1.5.1.3.21** Запросы на экспорт защищенного объекта должны обрабатываться передающим КСЗ на основании атрибутов доступа интерфейсного процесса и приемника объекта **1.5.1.3.22** Запросы на импорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса и источника объекта **1.5.1.3.23** Представление защищенного объекта должно быть функцией атрибутов доступа интерфейсного процесса, самого объекта, а также его источника и приемника **1.5.1.3.24** <=>1.5.1.1.8 *1.5.1.4.25 - 1.5.1.4.32 реализуются по КВ-4,где:* 1.5.1.4.25 <=>1.5.1.3.17; 1.5.1.4.26 <=>1.5.1.1.2; 1.5.1.4.27 <=> 1.5.1.1.3; 1.5.1.4.28 <=>1.5.1.2.12; 1.5.1.4.29 <=>1.5.1.3.21; 1.5.1.4.30 <=>1.5.1.3.22; 1.5.1.4.31 <=>1.5.1.3.23;
2.5.1	-	*Элемент критерия не проектируется*	-
3.5.1	-	*Элемент критерия не проектируется*	-
4.5.1	<=> *НА-2*	Аутентификация отправителя с подтверждением	***4.5.1.1.1 - 4.5.1.1.4 реализуются поНА-1*** ***4.5.1.2.5 - 4.5.1.2.8 реализуются поНА-2***
4.5.2	<=> *НП-2*	Аутентификация получателя с подтверждением	***4.5.2.1.1 - 4.5.2.1.4 реализуются по НП-1*** ***4.5.2.2.5 - 4.5.2.2.8 реализуются по НП-2***

Продолжение Приложение 5

Номер строки *(в столб-це)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 4-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ЗАПРОС**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **1** (из 1,2,3,4,5); Уровень базового кода **4** (из 1,2,3,4,5); Требование (очередность)			
1.1.1	КД-4	Абсолютная доверительная конфиденциальность	***1.1.1.1.1 - 1.1.1.1.6 реализуются по КД-1*** ***1.1.1.2.7 - 1.1.1.2.12 реализуются по КД-2*** ***1.1.1.3.13 - 1.1.1.3.18 реализуются по КД-3*** **1.1.1.4.19** <=>1.1.3.13; **1.1.1.4.20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя, процесса и защищенного объекта **1.1.1.4.21** <=>1.1.1.1.3; **1.1.1.4.22** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права получать информацию от объекта **1.1.1.4.23** <=> 1.1.1.3.17; **1.1.1.4.24** <=> 1.1.1.1.6
2.1.1	ЦД-4	Абсолютная доверительная целостность	***2.1.1.1.1 - 2.1.1.1.6 реализуются по КД-1*** ***2.1.1.2.7 - 2.1.1.2.12 реализуются по КД-2*** ***2.1.1.3.13 - 2.1.1.3.18 реализуются по КД-3*** **2.1.1.4.19** <=> 2.1.1.3.13; **2.1.1.4.20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса, пользователя и защищенного объекта **2.1.1.4.21** <=> 2.1.1.1.3; **2.1.1.4.22** КСЗ должен давать пользователю возможность для каждого защищенного объекта, принадлежащего его домену, определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права модифицировать объект **2.1.1.4.23** <=> 2.1.1.3.17; **2.1.1.4.24** <=> 2.1.1.1.6;
3.1.1	*ДР-3*	Приоритетность использования ресурсов	***3.1.1.1.1 - 3.1.1.1.4 реализуются по ДР-1*** ***3.1.1.2.5 - 3.1.1.2.8 реализуются по ДР-2*** ***3.1.1.3.9 - 3.1.1.3.12 реализуются по ДР-3***
4.1.1	НР-4	Детальная регистрация	***4.1.1.1.1 - 4.1.1.1.6 реализуются по НР-1*** ***4.1.1.2.7 - 4.1.1.2.12 реализуются по НР-2*** ***4.1.1.3.13 - 4.1.1.3.18 реализуются по НР-3*** **4.1.1.4.19** <=> 4.1.1.1.1; **4.1.1.4.20** КСЗ должен быть способен осуществлять регистрацию событий, имеющих непосредственное или косвенное отношение к безопасности **4.1.1.4.21** <=> 4.1.1.1.3; **4.1.1.4.22** <=> 4.1.1.1.10; **4.1.1.4.23** <=> 4.1.1.3.17; **4.1.1.4.24** <=> 4.1.1.1.6 *4.1.1.5.25 - 4.1.1.5.30 реализуются по НР-5, где:* 4.1.1.5.25<=>4.1.1.1.1; 4.1.1.5.26<=>4.1.1.1.20; 4.1.1.5.27<=> 4.1.1.1.3; 4.1.1.5.28 <=> 4.1.1.2.10; 4.1.1.5.29 <=> 4.1.1.3.17
4.1.2 Отсылка	*до Г-5*	*Требования критериев гарантий (Г-1,2,3,4,5)*	1. Архитектура. 2. Среда разработки: *2.1 Процесс разработки; 2.2 Управление конфигурацией.* 3. Последовательность разработки: 3.*1 Политика безопасности;. 3.2 Модель политики безопасности; 3.3 Проект архитектуры; 3.4 Детальный проект; 3.5 Реализация.* 4. Среда функционирования. 5. Документация. 6. Испытания комплекса средств защиты.

Продолжение Приложение 5

Номер строки *(в столб-це)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 4-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ДОСТУП**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **2** (из 1,2,3,4,5); Уровень базового кода **4** (из 1,2,3,4,5); Требование (очередность)			
1.2.1	КА-4	Абсолютная административная конфиденциальность	***1.2.1.1.1 - 1.2.1.1.6 реализуются по КА-1*** ***1.2.1.2.7 - 1.2.1.2.12 реализуются по КА-2*** ***1.2.1.3.13 - 1.2.1.3.18 реализуются по КА-3*** **1.2.1.4.19** <=> 1.2.1.3.13 **1.2.1.4.20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя, процесса и защищенного объекта **1.2.1.4.21** <=> 1.2.1.1.3 **1.2.1.4.22** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права получать информацию от объекта **1.2.1.4.23** <=> 1.2.1.3.17 **1.2.1.4.24** <=> 1.2.1.1.6
2.2.1	ЦА-4	Абсолютная административная целостность	***2.2.1.1.1 - 2.2.1.1.6 реализуются по ЦА-1*** ***2.2.1.2.7 - 2.2.1.2.12 реализуются по ЦА-2*** ***2.2.1.3.13 - 2.2.1.3.18 реализуются по ЦА-3*** **2.2.1.4.19** <=> 2.2.1.3.13 **2.2.1.4.20** КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса, пользователя и защищенного объекта **2.2.1.4.21** <=> 2.2.1.1.3 **2.2.1.4.22** КСЗ должен давать возможность администратору или имеющему соответствующие полномочия пользователю для каждого защищенного объекта путем управления принадлежностью пользователей, процессов и объектов к соответствующим доменам определить конкретных пользователей и процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права модифицировать объект **2.2.1.4.23** <=> 2.2.1.3.17 **2.2.1.4.24** <=> 2.2.1.1.6
3.2.1	<=> *ДС-3*	Устойчивость с ухудшением характеристик обслуживания	***3.2.1.1.1 - 3.2.1.1.5 реализуются по ДС-1*** ***3.2.1.2.6 - 3.2.1.2.10 реализуются по ДС-2*** ***3.2.1.3.11 - 3.2.1.3.15 реализуются по ДС-3***
4.2.1	<=> *НИ-3*	Множественная идентификация и аутентификация	***4.2.1.1.1 - 4.2.1.1.3 реализуются по НИ-1*** ***4.2.1.2.4 - 4.2.1.2.6 реализуются по НИ-2*** ***4.2.1.3.7 - 4.2.1.3.9 реализуются по НИ-3***
4.2.2	<=> *НК-2*	Двунаправленный достоверный канал	***4.2.2.1.1 - 4.2.2.1.3 реализуются по НК-1*** ***4.2.2.2.4 - 4.2.2.2.6 реализуются по НК-2***

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 4-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ОБЪЕКТЫ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **3** (из 1,2,3,4,5); Уровень базового кода **4** (из 1,2,3,4,5); Требование (очередность)			
1.3.1	<=> *К0-1*	Повторное использование объектов	***1.3.1.1.1 реализуются по КО-1***
2.3.1	<=> *ЦО-2*	Полный откат	***2.3.1.1.1 - 2.3.1.1.2 реализуются по ЦО-1*** **2.3.1.2.3 - 2.3.1.2.4** ***реализуются по ЦО-2***
3.3.1	<=> *ДЗ-3*	Горячая замена любого компонента	***3.3.1.1.1 - 3.3.1.1.2 реализуются по ДЗ-1*** **3.3.1.2.3 - 3.3.1.2.4** ***реализуются по ДЗ-2*** **3.3.1.3.5 - 3.3.1.3.6** ***реализуются по ДЗ-3***
4.3.1	<=> *НО-3*	Разграничение обязанностей на основании привилегий	***4.3.1.1.1 - 4.3.1.1.4 реализуются по НО-1*** ***4.3.1.2.5 - 4.3.1.2.8 реализуются по НО-2*** ***4.3.1.3.9 - 4.3.1.3.12 реализуются по НО-3***
4.3.2	<=> *НЦ-3*	КСЗ с функциями диспетчера доступа	***4.3.2.1.1 - 4.3.2.1.3 реализуются по НЦ-1*** ***4.3.2.2.4 - 4.3.2.2.6 реализуются по НЦ-2*** ***4.3.2.3.7 - 4.3.2.3.9 реализуются по НЦ-3***

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 4-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**НАДЗОР**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **4** (из 1,2,3,4,5); Уровень базового кода **4** (из 1,2,3,4,5); Требование (очередность)			
1.4.1	<=> *КК-3*	Перекрытие скрытых каналов	***1.4.1.1.1 - 1.4.1.1.3 реализуются по КК-1*** ***1.4.1.2.4 - 1.4.1.2.6 реализуются по КК-2*** ***1.4.1.3.7 - 1.4.1.3.8 реализуются по КК-3***
2.4.1	<=> *ЦВ-3*	Полная целостность при обмене	***2.4.1.1.1 - 2.4.1.1.6 реализуются по ЦВ-1*** ***2.4.1.2.7 - 2.4.1.2.12 реализуются по ЦВ-2*** ***2.4.1.3.13 - 2.4.1.3.18 реализуются по ЦВ-3***
3.4.1	<=> *ДВ-3*	Избирательное восстановление	***3.4.1.1.1 - 3.4.1.1.4 реализуются по ДВ-1*** ***3.4.1.2.5 - 3.4.1.2.8 реализуются по ДВ-2*** ***3.4.1.3.9 - 3.4.1.3.12 реализуются по ДВ-3***
4.4.1	<=> *НТ-3*	Самотестирование в реальном времени	***4.4.1.1.1 - 4.4.1.1.2 реализуются по НТ-1*** ***4.4.1.2.3 - 4.4.1.2.4 реализуются по НТ-2*** **4.4.1.3.5 - 4.4.1.3.6** ***реализуются по НТ-3***
4.4.2	<=> *НВ-3*	Аутентификация с подтверждением	***4.4.2.1.1 - 4.4.2.1.3 реализуются по НВ-1*** ***4.4.2.2.4 - 4.4.2.2.5 реализуются по НВ-2*** ***4.4.2.3.7 - 4.4.2.3.9 реализуются по НВ-3***

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 4-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**СВЯЗЬ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **5** (из 1,2,3,4,5); Уровень базового кода **4** (из 1,2,3,4,5); Требование (очередность)			
1.5.1	КВ-4	Абсолютная конфиденциальность при обмене	***1.5.1.1.1 - 1.5.1.1.8 реализуются по КВ-1*** ***1.5.1.2.9 - 1.5.1.2.16 реализуются по КВ-2*** ***1.5.1.3.17 - 1.5.1.3.24 реализуются по КВ-3*** **1.5.1.4.25** <=> 1.5.1.3.17; **1.5.1.4.26** <=> 1.5.1.1.2; **1.5.1.4.27** <=> 1.5.1.1.3; **1.5.1.4.28** <=> 1.5.1.2.12; **1.5.1.4.29** <=> 1.5.1.3.21; **1.5.1.4.30** <=> 1.5.1.3.22; **1.5.1.4.31** <=> 1.5.1.3.23; **1.5.1.4.32** Политика конфиденциальности при обмене должна включать описание информации, которую можно получить путем совместного анализа ряда полученных объектов. Должен быть выполнен анализ скрытых каналов обмена. Все обнаруженные скрытые каналы обмена и максимальная пропускная способность каждого из них должны быть документированы. Должна быть обеспечена регистрация использования утвержденного подмножества обнаруженных скрытых каналов, их частичное перекрытие или исключение
2.5.1	-	*Элемент критерия не проектируется*	-
3.5.1	-	*Элемент критерия не проектируется*	-
4.5.1	<=> *НА-2*	Аутентификация отправителя с подтверждением	***4.5.1.1.1 - 4.5.1.1.4 реализуются по НА-1*** ***4.5.1.2.5 - 4.5.1.2.8 реализуются по НА-2***
4.5.2	<=> *НП-2*	Аутентификация получателя с подтверждением	***4.5.2.1.1 - 4.5.2.1.4 реализуются по НП-1*** ***4.5.2.2.5 - 4.5.2.2.8 реализуются по НП-2***

Продолжение Приложение 5

Номер строки ***(в столб-це)***	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 5-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ЗАПРОС**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **1** (из 1,2,3,4,5); Уровень базового кода **5** (из 1,2,3,4,5); Требование (очередность)			
1.1.1	<=> *КД-4*	Абсолютная доверительная конфиденциальность	***1.1.1.1.1 - 1.1.1.1.6 реализуются по КД-1*** ***1.1.1.2.7 - 1.1.1.2.12 реализуются по КД-2*** ***1.1.1.3.13 - 1.1.1.3.18 реализуются по КД-3*** ***1.1.1.4.19 - 1.1.1.4.24 реализуются по КД-4***
2.1.1	<=> *ЦД-4*	Абсолютная доверительная целостность	***2.1.1.1.1 - 2.1.1.1.6 реализуются по КД-1*** ***2.1.1.2.7 - 2.1.1.2.12 реализуются по КД-2*** ***2.1.1.3.13 - 2.1.1.3.18 реализуются по КД-3*** **2.1.1.4.19 - 2.1.1.4.24** ***реализуются по КД-4***
3.1.1	<=> *ДР-3*	Приоритетность использования ресурсов	***3.1.1.1.1 - 3.1.1.1.4 реализуются по ДР-1*** ***3.1.1.2.5 - 3.1.1.2.8 реализуются по ДР-2*** ***3.1.1.3.9 - 3.1.1.3.12 реализуются по ДР-3***
4.1.1	НР-5	Анализ в реальном времени	***4.1.1.1.1 - 4.1.1.1.6 реализуются по НР-1*** ***4.1.1.2.7 - 4.1.1.2.12 реализуются по НР-2*** ***4.1.1.3.13 - 4.1.1.3.18 реализуются по НР-3*** ***4.1.1.4.19 - 4.1.1.4.24 реализуются по НР-4*** **4.1.1.5.25** <=> 4.1.1.1.1 **4.1.1.5.26** <=> 4.1.1.1.20 **4.1.1.5.27** <=> 4.1.1.1.3; **4.1.1.5.28** <=> 4.1.1.2.10; **4.1.1.5.29** <=> 4.1.1.3.17 **4.1.1.5.30** КСЗ должен быть способен выявлять и анализировать несанкционированные действия в реальном времени
4.2.2 Отсылка	*до Г-7*	*Требования критериев гарантий (Г-1,2,3,4,5,6,7)*	1. Архитектура. 2. Среда разработки: *2.1 Процесс разработки; 2.2 Управление конфигурацией.* 3. Последовательность разработки: 3.*1 Политика безопасности. 3.2 Модель политики безопасности 3.3 Проект архитектуры 3.4 Детальный проект 3.5 Реализация* 4. Среда функционирования. 5. Документация. 6. Испытания комплекса средств защиты.

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 5-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ДОСТУП**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **2** (из 1,2,3,4,5); Уровень базового кода **5** (из 1,2,3,4,5); Требование (очередность)			
1.2.1	<=> КА-4	Абсолютная административная конфиденциальность	***1.2.1.1.1 - 1.2.1.6 реализуются по КА-1*** ***1.2.1.2.7 - 1.2.2.12 реализуются по КА-2*** ***1.2.1.3.13 - 1.2.3.18 реализуются по КА-3*** ***1.2.1.4.19 - 1.2.4.24 реализуются по КА-4***
2.2.1	<=> ЦА-4	Абсолютная административная целостность	***2.2.1.1.1 - 2.2.1.1.6 реализуются по ЦА-1*** ***2.2.1.2.7 - 2.2.2.12 реализуются по ЦА-2*** ***2.2.1.3.13 - 2.2.3.18 реализуются по ЦА-3*** ***2.2.1.4.19 - 2.2.4.24 реализуются по ЦА-4***
3.2.1	<=> *ДС-3*	Устойчивость с ухудшением характеристик обслуживания	***3.2.1.1.1 - 3.2.1.1.5 реализуются по ДС-1*** ***3.2.1.2.6 - 3.2.1.2.10 реализуются по ДС-2*** ***3.2.1.3.11 - 3.2.1.3.15 реализуются по ДС-3***
4.2.1	<=> *НИ-3*	Множественная идентификация и аутентификация	***4.2.1.1.1 - 4.2.1.1.3 реализуются по НИ-1*** ***4.2.1.2.4 - 4.2.1.2.6 реализуются по НИ-2*** ***4.2.1.3.7 - 4.2.1.3.9 реализуются по НИ-3***
4.2.2	<=> *НК-2*	Двунаправленный достоверный канал	***4.2.2.1.1 - 4.2.2.1.3 реализуются по НК-1*** ***4.2.2.2.4 - 4.2.2.2.6 реализуются по НК-2***

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 5-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**ОБЪЕКТЫ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **3** (из 1,2,3,4,5); Уровень базового кода **5** (из 1,2,3,4,5); Требование (очередность)			
1.3.1	<=> *К0-1*	Повторное использование объектов	***1.3.1.1.1 реализуются по КО-1***
2.3.1	<=> *ЦО-2*	Полный откат	***2.3.1.1.1 - 2.3.1.1.2 реализуются по ЦО-1*** **2.3.1.2.3 - 2.3.1.2.4** ***реализуются по ЦО-2***
3.3.1	<=> *ДЗ-3*	Горячая замена любого компонента	***3.3.1.1.1 - 3.3.1.1.2 реализуются по ДЗ-1*** **3.3.1.2.3 - 3.3.1.2.4** ***реализуются по ДЗ-2*** **3.3.1.3.5 - 3.3.1.3.6** ***реализуются по ДЗ-3***
4.3.1	<=> *НО-3*	Разграничение обязанностей на основании привилегий	***4.3.1.1.1 - 4.3.1.1.4 реализуются по НО-1*** ***4.3.1.2.5 - 4.3.1.2.8 реализуются по НО-2*** ***4.3.1.3.9 - 4.3.1.3.12 реализуются по НО-3***
4.3.2	<=> *НЦ-3*	КСЗ с функциями диспетчера доступа	***4.3.2.1.1 - 4.3.2.1.3 реализуются по НЦ-1*** ***4.3.2.2.4 - 4.3.2.2.6 реализуются по НЦ-2*** ***4.3.2.3.7 - 4.3.2.3.9 реализуются по НЦ-3***

Продолжение Приложение 5

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 5-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**НАДЗОР**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **4** (из 1,2,3,4,5); Уровень базового кода **5** (из 1,2,3,4,5); Требование (очередность)			
1.4.1	<=> *КК-3*	Перекрытие скрытых каналов	***1.4.1.1.1 - 1.4.1.1.3 реализуются по КК-1*** ***1.4.1.2.4 - 1.4.1.2.6 реализуются по КК-2*** ***1.4.1.3.7 - 1.4.1.3.8 реализуются по КК-3***
2.4.1	<=> *ЦВ-3*	Полная целостность при обмене	***2.4.1.1.1 - 2.4.1.1.6 реализуются по ЦВ-1*** ***2.4.1.2.7 - 2.4.1.2.12 реализуются по ЦВ-2*** ***2.4.1.3.13 - 2.4.1.3.18 реализуются по ЦВ-3***
3.4.1	<=> *ДВ-3*	Избирательное восстановление	***3.4.1.1.1 - 3.4.1.1.4 реализуются по ДВ-1*** ***3.4.1.2.5 - 3.4.1.2.8 реализуются по ДВ-2*** ***3.4.1.3.9 - 3.4.1.3.12 реализуются по ДВ-3***
4.4.1	<=> *НТ-3*	Самотестирование в реальном времени	***4.4.1.1.1 - 4.4.1.1.2 реализуются по НТ-1*** ***4.4.1.2.3 - 4.4.1.2.4 реализуются по НТ-2*** **4.4.1.3.5 - 4.4.1.3.6** ***реализуются по НТ-3***
4.4.2	<=> *НВ-3*	Аутентификация с подтверждением	***4.4.2.1.1 - 4.4.2.1.3 реализуются по НВ-1*** ***4.4.2.2.4 - 4.4.2.2.5 реализуются по НВ-2*** ***4.4.2.3.7 - 4.4.2.3.9 реализуются по НВ-3***

Номер строки *(в столбце)*	**Базовые коды**	**Элементы критериев по иерархии строк справочников-колонок**	**Требования к критериям 5-го уровня базового кода в иерархии списков-строк из справочников-строк по справочникам-колонкам о компонентах и элементам КСЗ**
*Набор кода требований по уровням базовых критериев «**СВЯЗЬ**»*: Справочники-столбцы (**1,2,3,4**); Справочник-строка **5** (из 1,2,3,4,5); Уровень базового кода **5** (из 1,2,3,4,5); Требование (очередность)			
1.5.1	<=> КВ-4	Абсолютная конфиденциальность при обмене	***1.5.1.1.1 - 1.5.1.1.8 реализуются по КВ-1*** ***1.5.1.2.9 - 1.5.1.2.16 реализуются по КВ-2*** ***1.5.1.3.17 - 1.5.1.3.24 реализуются по КВ-3*** ***1.5.1.4.25 - 1.5.1.4.32 реализуются по КВ-4***
2.5.1	-	*Элемент критерия не проектируется*	-
3.5.1	-	*Элемент критерия не проектируется*	-
4.5.1	<=> *НА-2*	Аутентификация отправителя с подтверждением	***4.5.1.1.1 - 4.5.1.1.4 реализуются по НА-1*** ***4.5.1.2.5 - 4.5.1.2.5 реализуются по НА-2***
4.5.2	<=> *НП-2*	Аутентификация получателя с подтверждением	***4.5.2.1.1 - 4.5.2.1.4 реализуются по НП-1*** ***4.5.2.2.5 - 4.5.2.2.8 реализуются по НП-2***

Спецификация функциональности № 6. Структура требований к критериям гарантий безопасности КСЗ ДИС **Приложение 6**

Наименование разделов (по коду Г-7)	Код в Г-7	*Код исходный*	Уровни гарантий							*Код проекта*
			Г-1	*Г-2*	*Г-3*	*Г-4*	*Г-5*	*Г-6*	*Г-7*	
Столбец 1. Архитектура										
Архитектура	**Г-5**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Столбец 2. Среда разработки										
Процесс разработки	**Г-4**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Управление конфигурацией	**Г-6**	*от Г-1*	**+**	**=**	**=**	**+***	**=**	**=**	**=**	***до Г-7***
Столбец 3. Последовательность разработки										
Функциональные спецификации (Политика безопасности)	**Г-1**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Функциональные спецификации (Модель политики безопасности)	**Г-1**	*от Г-2*	**-**	**+**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Проект архитектуры	**Г-6**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Детальный проект	**Г-7**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Реализация	**Г-7**	*от Г-3*	**-**	**-**	**+**	**=**	**=**	**=**	**=**	***до Г-7***
Столбец 4. Среда функционирования										
Перечень всех возможных параметров конфигурации	**Г-6**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Гарантии соответствия эталонной копии (контроль Заказчика)	**Г-6**	*от Г-3*	**-**	**-**	**+**	**=**	**=**	**=**	**=**	***до Г-7***
Столбец 5. Документация										
Требования к документации - общие для всех уровней гарантий	**Г-7**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Столбец 6. Испытания комплекса средств защиты										
Тесты по преодолению механизмов защиты КСЗ	**Г-7**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Программа и методику испытаний КСЗ	**Г-7**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***
Процедуры испытаний всех механизмов КСЗ	**Г-7**	*от Г-1*	**+**	**=**	**=**	**=**	**=**	**=**	**=**	***до Г-7***

« - » - требование отсутствует; « + » - требование появляется»; « = » - требование сохраняется;
« * » - базирование на автоматизированных системах

Спецификация функциональности № 7. Матрица иерархии технологических режимов разработки по уровням гарантий безопасности КСЗ ДИС **Приложение 7**

Наименование разделов (по Г-7)	Уровень гарантии Г-1
1. Архитектура	
1.1. Архитектура	1.1.1 КСЗ должен реализовывать политику безопасности. Все его компоненты должны быть четко определены.
2. Среда разработки	
2.1. Процесс разработки	2.1.1 Разработчик должен определить все стадии жизненного цикла, разработать внедрить и поддерживать в рабочем состоянии документально оформленные методики своей деятельности на каждой стадии. Должны быть документированы все этапы каждой стадии жизненного цикла и их граничные требования.
2.2 Управление конфигурацией	2.2.1 Разработчик должен разработать, внедрить и поддерживать в рабочем состоянии документированные методики по управлению конфигурацией КС на всех стадиях ее жизненного цикла. Система управления конфигурацией должна обеспечивать управление внесением изменений в аппаратное обеспечение, программы ПЗУ, исходные тексты, объектные коды, тестовое покрытие и документацию. Система управления конфигурацией должна гарантировать постоянное соответствие между всей документацией и реализацией
3. Последовательность разработки	
3.1. Функциональные спецификации (Политика безопасности)	3.1.1 На стадии разработки технического задания Разработчик должен разработать функциональные спецификации КС. Представленные функциональные спецификации должны включать неформализованное описание политики безопасности, реализуемой КСЗ. Политика безопасности должна содержать перечень и описание услуг безопасности, предоставляемых КСЗ.
3.2. Функциональные спецификации (Модель политики безопасности)	3.2.1 Соответствие политике безопасности. Требования отсутствуют. Функциональные спецификациям должны включать модель политики безопасности: Требования отсутствуют. Стиль спецификации: Требования отсутствуют
3.3 Проект архитектуры	3.3.1 Соответствие модели политики безопасности. Требования отсутствуют. На стадии разработки эскизного проекта Разработчик должен разработать проект архитектуры КСЗ. Представленный проект должен содержать перечень и описание компонентов КСЗ и реализуемых ими функций. Должны быть описаны любые используемые внешние услуги безопасности. Внешние интерфейсы КСЗ должны быть описаны в терминах исключений, сообщений об ошибках и кодов возврата. Стиль спецификации: Неформализованная.
3.4 Детальный проект	3.4.1 Соответствие проекту архитектуры. Требования отсутствуют. На стадиях разработки технического проекта или рабочего проекта Разработчик должен разработать детальный проект КСЗ. Представленный детальный проект должен содержать перечень всех компонентов КСЗ и точное описание функционирования каждого механизма. Должны быть описаны назначение и параметры интерфейсов компонентов КСЗ. Стиль спецификации: Неформализованная.
3.5 Реализация	3.5.1 Соответствие детальному проекту. Требования отсутствуют Разработчик должен представить исходный код. Требования отсутствуют.
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	4.1.1 Разработчик должен предоставить средства инсталляции, генерации и запуска КС, которые гарантируют, что эксплуатация КС начинается из безопасного состояния. Разработчик должен предоставить перечень всех возможных параметров конфигурации, которые могут использоваться в процессе инсталляции, генерации и запуска.
4.2 Гарантии соответствия эталонной копии	4.2.1 Требования отсутствуют
5. Документация	
5.1 Требования к документации	5.1.1 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	6.1.1 Разработчик должен предоставить для проверки программу и методику испытаний, процедуры испытаний всех механизмов, реализующих услуги безопасности. Должны быть представлены аргументы для подтверждения достаточности тестового покрытия. Разработчик должен представить доказательства тестирования в виде детального перечня результатов тестов и соответствующих процедур тестирования, с тем, чтобы полученные результаты могли быть проверены путем повторного тестирования.

Продолжение Приложение 7

Наименование разделов (по Г-7)	**Уровень гарантии Г-2** ***(при условии предварительного выполнения требований по уровню гарантии Г-1)***
1. Архитектура	
1.1 Архитектура	1.1.2 Сохраняются требования Г-1.
2. Среда разработки	
2.1 Процесс разработки	2.1.2 Сохраняются требования Г-1.
2.2 Управление конфигурацией	2.2.2 Сохраняются требования Г-1.
3. Последовательность разработки	
3.1 Функциональные спецификации (Политика безопасности)	3.1. 2 Сохраняются требования Г-1.
3.2 Функциональные спецификации (Модель политики безопасности)	3.2.2 Соответствие политике безопасности. Показ. Функциональные спецификации должны включать модель политики безопасности. Стиль спецификации: Неформализованная.
3.3 Проект архитектуры	3.3.2 Соответствие модели политики безопасности. Показ Сохраняются требования Г-1. Стиль спецификации: Неформализованная.
3.4 Детальный проект	3.4.2 Соответствие проекту архитектуры. Показ. На стадиях разработки технического проекта или рабочего проекта Разработчик должен разработать детальный проект КСЗ. Представленный детальный проект должен содержать перечень всех компонентов КСЗ и точное описание функционирования каждого механизма. Должны быть описаны назначение и параметры интерфейсов компонентов КСЗ. Стиль спецификации: Неформализованная. Для уровня гарантии Г-2 требуется детальный проект всех компонентов КСЗ.
3.5 Реализация	3.5.2 Соответствие детальному проекту. Требования отсутствуют Разработчик должен представить исходный код: Требования отсутствуют
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	4.1.2 Сохраняются требования Г-1.
4.2 Гарантии соответствия эталонной копии	4.2.2 Требования отсутствуют
5. Документация	
5.1 Требования к документации	5.1.2 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	*Сохраняются требования Г-1.* 6.1.2 Разработчик должен устранить или нейтрализовать все обнаруженные «бреши» и выполнить повторное тестирование КСЗ для подтверждения того, что обнаруженные недостатки были устранены и не появились новые «бреши».

Продолжение Приложение 7

Наименование разделов (по Г-7)	**Уровень гарантии Г-3** *(при условии предварительного выполнения требований по уровням гарантий Г-1, Г-2)*
1. Архитектура	
1.1 Архитектура	*Сохраняются требования Г-2 (Г-1).* 1.1.3 КСЗ должен состоять из хорошо определенных и максимально независимых компонентов. Каждый из компонентов должен быть спроектирован в соответствии с принципом минимума полномочий.
2. Среда разработки	
2.1 Процесс разработки	*Сохраняются требования Г-2 (Г-1).* 2.1.3 Разработчик должен описать стандарты кодирования, которым необходимо следовать в процессе реализации, и должен гарантировать, что все исходные коды компилируются в соответствии с этими стандартами. Любой из используемых при реализации языков программирования должен быть хорошо определен. Все зависящие от реализации параметры языков программирования или компиляторов должны быть документированы.
2.2 Управление конфигурацией	2.2.3 Сохраняются требования Г-2 (Г-1).
3. Последовательность разработки	
3.1 Функциональные спецификации (Политика безопасности)	3.1.3 Сохраняются требования Г-2 (Г-1).
3.2 Функциональные спецификации (Модель политики безопасности)	3.2.3 Соответствие политике безопасности. Показ. Функциональные спецификации должны включать модель политики безопасности. Стиль спецификации: Частично формализованная.
3.3 Проект архитектуры	3.3.3 Соответствие модели политики безопасности. Показ Сохраняются требования Г-2 (Г-1). Стиль спецификации: Частично формализованная.
3.4 Детальный проект	3.4.3 Соответствие проекту архитектуры. Показ. Сохраняются требования Г-2 (Г-1). Стиль спецификации: Неформализованная. Для уровня гарантий Г-3 требуется детальный проект всех компонентов КСЗ.
3.5 Реализация	3.5.3 Соответствие детальному проекту. Показ. Разработчик должен представить исходный код части КСЗ.
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	*Сохраняются требования Г-2 (Г-1).* 4.1.3 Должна существовать система технических, организационных и физических мер безопасности, гарантирующее, что программное и программно-аппаратное обеспечения КСЗ, поставляемое Заказчику, в точности соответствует эталонной копии.
4.2 Гарантии соответствия эталонной копии	4.2.3 Должна существовать эталонная копия.
5. Документация	
5.1 Требования к документации	*Сохраняются требования Г-2 (Г-1).* 5.1.3 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	6.1.3 Сохраняются требования Г-2 и Г-1.

Продолжение Приложение 7

Наименование разделов (по Г-7)	**Уровень гарантии Г-4** ***(при условии предварительного выполнения требований по уровням гарантий Г-1, Г-2, Г-3)***
1. Архитектура	
1.1 Архитектура	*Сохраняются требования Г-3 (Г-2, Г-1).* 1.1. 4.1 Критичные для безопасности компоненты КСЗ должны быть защищены от не критичных для безопасности за счет использования механизмов защиты, предоставляемых программно-аппаратными средствами более низкого уровня.
2. Среда разработки	
2.1 Процесс разработки	*Сохраняются требования Г-3 (Г-2, Г-1).* 2.1.4.1 Разработчик должен разработать, внедрить и поддерживать в рабочем состоянии документально оформленные методики обеспечения физической, технической, организационной и кадровой безопасности
2.2 Управление конфигурацией	*Сохраняются требования Г-3 (Г-2, Г-1).* 2.2.4.1 Начиная с уровня Г-4, система управления конфигурацией (Г-3, Г-2, Г-1) должна базироваться на автоматизированных средствах.
3. Последовательность разработки	
3.1 Функциональные спецификации (Политика безопасности)	3.1.4.1 Сохраняются требования Г-3 (Г-2, Г-1).
3.2 Функциональные спецификации (Модель политики безопасности)	3.2.4.1 Соответствие политике безопасности. Демонстрация. Функциональные спецификации должны включать модель политики безопасности. Стиль спецификации: Формализованная.
3.3 Проект архитектуры	3.3.4.1 Соответствие модели политики безопасности. Демонстрация. Сохраняются требования Г-3 (Г-2, Г-1). Стиль спецификации: Частично формализованная.
3.4 Детальный проект	3.4.4.1 Соответствие проекту архитектуры. Показ. Сохраняются требования Г-3 (Г-2, Г-1). Стиль спецификации: Частично формализованная.
3.5 Реализация	3.5.4.1 Соответствие детальному проекту. Показ. Разработчик должен представить исходный код части КСЗ.
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	*Сохраняются требования Г-3 (Г-2, Г-1).* 4.1.4.1 Должна существовать система технических, организационных и физических мер безопасности, гарантирующее, что программное и программно-аппаратное обеспечения КСЗ, поставляемое Заказчику, в точности соответствует эталонной копии.
4.2 Гарантии соответствия эталонной копии	*Сохраняются требования Г-3 (Г-2, Г-1).* 4.2.4.1 Должна существовать эталонная копия.
5. Документация	
5.1 Требования к документации	5.1.4.1 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	6.1.4.1 Сохраняются требования Г-3, Г-2, Г-1

Продолжение Приложение 7

Наименование разделов (по Г-7)	**Уровень гарантии Г-5** ***(при условии предварительного выполнения требований по уровням гарантий Г-1, Г-2, Г-3, Г-4)***
1. Архитектура	
1.1 Архитектура	*Сохраняются требования Г-4 (Г-3, Г-2, Г-1).* 1.1. 5.1 Со стороны Разработчика должны быть предприняты усилия, направленные на исключение из КСЗ компонентов, которые не являются критичными для безопасности. Должны быть представлены основания для включения в КСЗ любого, не имеющего отношения к защите, элемента. 1.1.5.2 Разработка ПО во многом должна быть направлена на минимизацию сложности КСЗ. КСЗ должен быть сконструирован так, чтобы использовать полный и концептуально простой механизм защиты с точно определенной семантикой. Этот механизм должен играть центральную роль в реализации внутренней структуры КСЗ. При разработке КСЗ в значительной степени должны быть задействованы такие подходы как модульность построения и скрытие (локализация видимости) данных.
2. Среда разработки	
2.1 Процесс разработки	*Сохраняются требования Г-4 (Г-3, Г-2, Г-1).* 2.1.5.1 Разработчик должен разработать, внедрить и поддерживать в рабочем состоянии документально оформленные методики обеспечения физической, технической, организационной и кадровой безопасности.
2.2 Управление конфигурацией	2.2.5.1 Сохраняются требования критерия Г-4 (Г-3, Г-2, Г-1).
3. Последовательность разработки	
3.1 Функциональные спецификации (Политика безопасности)	3.1.5.1 Сохраняются требования Г-4 (Г-3, Г-2, Г-1).
3.2 Функциональные спецификации (Модель политики безопасности)	3.2.5.1 Соответствие политике безопасности. Демонстрация. Функциональные спецификации должны включать модель политики безопасности. Стиль спецификации: Формализованная.
3.3 Проект архитектуры	3.3.5.1 Соответствие модели политики безопасности. Демонстрация. Сохраняются требования Г-4 (Г-3, Г-2, Г-1). Стиль спецификации: Частично формализованная.
3.4 Детальный проект	3.4.5.1 Соответствие проекту архитектуры. Показ. Сохраняются требования Г-4 (Г-3, Г-2, Г-1). Стиль спецификации: Частично формализованная.
3.5 Реализация	3.5.5.1 Соответствие детальному проекту. Показ. Разработчик должен представить исходный код всего КСЗ.
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	*Сохраняются требования Г-4 (Г-3, Г-2, Г-1).* 4.1.5.1 Должна существовать система технических, организационных и физических мер безопасности, гарантирующее, что программное и программно-аппаратное обеспечения КСЗ, поставляемое Заказчику, в точности соответствует эталонной копии.
4.2 Гарантии соответствия эталонной копии	*Сохраняются требования Г-4 (Г-3, Г-2, Г-1).* 4.2.5.1 Должна существовать эталонная копия.
5. Документация	
5.1 Требования к документации	5.1.5.1 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	6.1.5.1 Сохраняются требования Г-4 (Г-3, Г-2, Г-1)

Продолжение Приложение 7

Наименование разделов (по Г-7)	**Уровень гарантии Г-6** ***(при условии предварительного выполнения требований по уровням гарантий Г-1, Г-2, Г-3, Г-4, Г-5)***
1. Архитектура	
1.1 Архитектура	1.1.6.1 Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).
2. Среда разработки	
2.1 Процесс разработки	2.1.6.1 Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).
2.2 Управление конфигурацией	2.1.6.2 Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).
3. Последовательность разработки	
3.1 Функциональные спецификации (Политика безопасности)	3.1.6.1 Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).
3.2 Функциональные спецификации (Модель политики безопасности)	3.2.6.1 Соответствие политике безопасности. Демонстрация. Функциональные спецификации должны включать модель политики безопасности. Стиль спецификации: Формализованная.
3.3 Проект архитектуры	3.3.6.1 Соответствие модели политики безопасности. Доказательство. Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1). Стиль спецификации: Формализованная.
3.4 Детальный проект	3.4.5.1 Соответствие проекту архитектуры. Демонстрация. Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1). Стиль спецификации: Частично формализованная.
3.5 Реализация	3.5.5.1 Соответствие детальному проекту. Показ. Разработчик должен представить исходный код всего КСЗ.
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	*Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).* 4.1.6.1 Для поддержания соответствия между КСЗ, поставляемой Заказчику, и эталонной копией должна существовать система управления распространением защищенной КС.
4.2 Гарантии соответствия эталонной копии	*Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).* 4.2.6.1 Должна существовать эталонная копия.
5. Документация	
5.1 Требования к документации	5.1.5.1 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	6.1.6.1 Сохраняются требования Г-5 (Г-4, Г-3, Г-2, Г-1).

Продолжение Приложение 7

Наименование разделов (по Г-7)	**Уровень гарантии Г-7** ***(при условии предварительного выполнения требований по уровням гарантий Г-1, Г-2, Г-3, Г-4, Г-5)***
1. Архитектура	
1.1 Архитектура	1.1.6.1 Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).
2. Среда разработки	
2.1 Процесс разработки	2.1.6.1 Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).
2.2 Управление конфигурацией	2.1.6.2 Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).
3. Последовательность разработки	
3.1 Функциональные спецификации (Политика безопасности)	3.1.6.1 Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).
3.2 Функциональные спецификации (Модель политики безопасности)	3.2.6.1 Соответствие политике безопасности. Демонстрация. Функциональные спецификации должны включать модель политики безопасности. Стиль спецификации: Формализованная.
3.3 Проект архитектуры	3.3.6.1 Соответствие модели политики безопасности. Доказательство. Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1). Стиль спецификации: Формализованная.
3.4 Детальный проект	3.4.5.1 Соответствие проекту архитектуры. Доказательство. Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1). Стиль спецификации: Формализованная.
3.5 Реализация	3.5.5.1 Соответствие детальному проекту. Демонстрация Разработчик должен представить исходный код всех библиотек времени выполнения.
4. Среда функционирования	
4.1 Перечень всех возможных параметров конфигурации	*Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).* 4.1.6.1 Для поддержания соответствия между КСЗ, поставляемой Заказчику, и эталонной копией должна существовать система управления распространением защищенной КС.
4.2 Гарантии соответствия эталонной копии	*Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).* 4.2.6.1 Должна существовать эталонная копия.
5. Документация	
5.1 Требования к документации	5.1.5.1 Требования к документации общие для всех уровней гарантий. В виде отдельных документов или разделов (подразделов) других документов Разработчик должен предоставить описание услуг безопасности, реализуемых КСЗ, руководство администратора по услугам безопасности, руководство пользователя по услугам безопасности.
6. Испытания комплекса средств защиты	
6.1 Требования	6.1.6.1 Сохраняются требования Г-6 (Г-5, Г-4, Г-3, Г-2, Г-1).