**ОПИСАНИЕ ТЕХНОЛОГИЧЕСКИХ ВОЗМОЖНОСТЕЙ *(под НД ТЗИ 2.05-005-99)***
диалоговой информационной системы (ДИС) «НООСФЕРА» с парадигмой требований уровня технической защиты информации к автоматизированной системе класса 3*(АС-3)* с наивысшим стандартным функциональным профилем защищенности 7.3.7 (3.КЦД.5)

# I. КРИТЕРИИ КОНФИДЕНЦИАЛЬНОСТИ

Для того, чтобы КС могла быть оценена на предмет соответствия критериями конфиденциальности, КСЗ оцениваемой КС должен предоставлять услуги по защите объектов от несанкционированного ознакомления с их содержанием (компрометации). Конфиденциальность обеспечивается через такие услуги: доверительная конфиденциальность, административная конфиденциальность, повторное использование объектов, анализ скрытых каналов, конфиденциальность при обмене (в данном случае понятие КСЗ представляет комплекс средств защиты программными средствами «как технологической защиты»).

## *1. Доверительная конфиденциальность*

Данная услуга позволяет пользователю управлять потоками информации от защищенных объектов, принадлежащих его домену, к другим пользователям. Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления (от КД-1 до КД-4).

**КД-4 Абсолютно доверительная конфиденциальность**

1. Политика доверительной конфиденциальности, реализуемая КСЗ, должна относиться ко всем объектам КС.
2. КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя, процесса и защищенного объекта.
3. Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ на основании атрибутов доступа пользователя, инициирующего запрос, и объекта
4. 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.
5. 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.
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.
7. НЕОБХОДИМЫЕ УСЛОВИЯ: КО-1, НИ-1

## *2. Административная конфиденциальность*

Данная услуга позволяет администратору или специально авторизованному пользователю управлять потоками информации от защищенных объектов к пользователям. Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления (от КА-1 до КА-4).

**КА-4 Абсолютная административная конфиденциальность**

1. Политика административной конфиденциальности, реализуемая КСЗ, должна относиться ко всем объектам КС.
2. КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа пользователя, процесса и защищенного объекта
3. Запросы на изменение прав доступа должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или пользователей, которым представлены соответствующие полномочия.
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 процессы (и группы пользователей и процессов), которые имеют, а также тех, которые не имеют права получать информацию от объекта.

5. 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.
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.
7. НЕОБХОДИМЫЕ УСЛОВИЯ: КО-1, НО-1, НИ-1

### *3. Повторное использование объектов*

Данная услуга позволяет обеспечить корректность повторного использования разделяемых объектов, гарантируя, что в случае, если разделяемый объект выделяется новому пользователю или процессу, то он не содержит информации, оставшейся от предыдущего пользователя или процесса (КО-1).

**КО-1 Повторное использование объектов**

1. Данная услуга позволяет обеспечить корректность повторного использования разделяемых объектов, гарантируя, что в случае, если разделяемый объект выделяется новому пользователю или процессу, то он содержит информации, оставшейся от предыдущего пользователя или процесса.
2. Политика повторного использования объектов, реализуемая КСЗ, должна относиться ко всем объектам КС.
3. 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.
4. 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.
5. НЕОБХОДИМЫЕ УСЛОВИЯ: НЕТ.

### *4. Анализ скрытых каналов*

Анализ скрытых каналов выполняется с целью выявления и исключения потоков информации, которые существуют, но не контролируются другими услугами. Уровни данной услуги ранжируются на основании того, выполняется ли только выявление, контроль или перекрытие скрытых каналов (от КК-1 до КК-3)

**КК-2 Контроль скрытых каналов**

1. Должен быть выполнен анализ скрытых каналов.
2. Все скрытые каналы, существующие в аппаратном и программном обеспечении, а также в программах ПЗУ, должны быть документированы.
3. Должна быть документирована максимальная пропускная способность каждого обнаруженного скрытого канала, полученная на основании теоретической оценки или измерений.
4. Для скрытых каналов, которые могут использоваться совместно, должна быть документирована совокупная пропускная способность.
5. КСЗ должен обеспечивать регистрацию использования утвержденного подмножества обнаруженных скрытных каналов.
6. НЕОБХОДИМЫЕ УСЛОВИЯ: КО-1, НР-1, Г-3

### *5. Конфиденциальность при обмене*

Данная услуга позволяет обеспечить защиту объектов от несанкционированного ознакомления с содержащейся в них информацией при их экспорте/импорте через незащищенную среду . Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления (от КВ-1 до КВ-4).

**КВ-4 Абсолютная конфиденциальность при обмене**

1. Политика конфиденциальности при обмене, реализуемая КСЗ, должна относиться ко всем объектам и существующим интерфейсным процессам.

2. Политика конфиденциальности при обмене, реализуемая КСЗ, должна определять уровень защищенности, который обеспечивается используемыми механизмами, и способность пользователей и/или процессов управлять уровнем защищенности.
3. КСЗ должен обеспечивать защиту от непосредственного ознакомления с информацией, содержащейся в передаваемом объекте.
4. 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.
5. Запросы на экспорт защищенного объекта должны обрабатываться «передающим» КСЗ на основании атрибутов доступа интерфейсного процесса и источника информации.
6. Запросы на импорт защищенного объекта должны обрабатываться «принимающим» КСЗ на основании атрибутов доступа интерфейсного процесса и источника информации.
7. Представление защищенного объекта должно быть функцией атрибутов доступа интерфейсного процесса, самого объекта, а также его источника и приемника.
8. 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.
9. НЕОБХОДИМЫЕ УСЛОВИЯ: НО-1, НВ-1, НР-1, Г-3.

## II. КРИТЕРИИ ЦЕЛОСТНОСТИ

Для того, чтобы КС могла быть оценена на предмет соответствия критериям целостности, КСЗ оцениваемой КС должен предоставлять услуги по защите обрабатываемой информации от несанкционированной модификации. Целостность обеспечивается через такие услуги: административная целостность, откат, целостность при обмене.

### *1. Доверительная целостность*

Данная услуга позволяет управлять потоками информации от других пользователей к защищенным объектам, принадлежащим его домену. Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления (от ЦД-1 до ЦД-4).

**ЦД-4 Абсолютная доверительная целостность**

1. Политика доверительной целостности, реализуемая КСЗ, должна относиться ко всем объектам КС.
2. КСЗ должен осуществлять разграничение на основании атрибутов доступа процесса, пользователя и защищенного объекта.
3. Запросы на изменение прав доступа к объекту должны обрабатываться КСЗ на основании атрибутов доступа пользователя, инициирующего запрос, и объекта.
4. 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 права модифицировать объект.
5. 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.
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 объекта при их экспорте и импорте.
7. НЕОБХОДИМЫЕ УСЛОВИЯ: КО-1, НИ-1

### *2. Административная целостность.*

Данная услуга позволяет администратору или специально авторизованному пользователю управлять потоками информации от пользователей к защищенным объектам. Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления (от ЦА-1 до ЦА-4).

**ЦА-4 Абсолютная административная целостность**

1. Политика административной целостности, реализуемая КСЗ, должна относиться ко всем объектам КС.
2. КСЗ должен осуществлять разграничение доступа на основании атрибутов доступа процесса, пользователя и защищенного объекта.
3. Запросы на изменение прав доступа должны обрабатываться КСЗ только в том случае, если они поступают от администраторов или от пользователей, которым представлены соответствующие полномочия.
4. КСЗ должен давать возможность администратору или имеющие 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.
5. 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.
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 объекта при их экспорте и импорте.
7. НЕОБХОДИМЫЕ УСЛОВИЯ: КО-1, НО-1, НИ-1

### *3. Откат*

Данная услуга обеспечивает возможность отменить операцию или последовательность операций и вернуть (откатить) защищенный объект в предыдущее состояние. Уровни данной услуги ранжируются на основании множества операций, для которых обеспечивается откат (от ЦО-1 до ЦО-2).

**ЦО-2 Полный откат**

1. Политика отката, реализуемая КСЗ, должна определять множество объектов КС, к которым она относится.
2. Должны существовать автоматизированные средства, которые позволяют авторизованному пользователю или процессу откатить или отменить все операции, проведенные над защищенным объектом за определенный промежуток времени.
3. НЕОБХОДИМЫЕ УСЛОВИЯ: НИ-1

### *4. Целостность при обмене*

Данная услуга позволяет обеспечить защиту объектов от несанкционированной модификации содержащейся в ней информации при их экспорте/импорте через незащищенную среду. Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления (от ЦВ-1 до ЦВ-3).

**ЦВ-3 Полная целостность при обмене**

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. КСЗ должен обеспечивать возможность обнаружения нарушения целостности информации, содержащейся в передаваемом объекте, а также фактов его удаления или дублирования.
3. Запросы на экспорт защищенного объекта должны обрабатываться «передающим» КСЗ на основании атрибутов доступа интерфейсного процесса и приемника объекта.

4. Запросы на импорт защищенного объекта должны обрабатываться принимающим КСЗ на основании атрибутов доступа интерфейсного процесса и источника объекта.
5. 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.
6. Предоставление защищенного объекта должно быть функцией атрибутов доступа интерфейсного процесса, самого объекта, а также его источника и приемника.
7. НЕОБХОДИМЫЕ УСЛОВИЯ: НО-1, НВ-1

## III. КРИТЕРИИ ДОСТУПНОСТИ

Для того, чтобы КС могла быть оценена на соответствие критериям доступности, КСЗ оцениваемой КС должен предоставлять услуги по обеспечению возможности использования КС в целом, отдельных функций или обрабатываемой информации на определенном промежутке времени и гарантировать способность КС функционировать в случае отказа ее компонентов. Доступность может обеспечиваться в КС через такие услуги: использование ресурсов, устойчивость к отказам, горячая замена, восстановление после сбоев.

### *1. Использование ресурсов*

Данная услуга позволяет пользователям управлять использованием услуг и ресурсов. Уровни данной услуги ранжируются на основании полноты защиты и избирательности управления доступностью услуг КС (от ДР-1 до ДР-3).

**ДР-3 Приоритетность использования ресурсов**

1. Политика использования ресурсов, реализуемая КСЗ, должна относиться ко всем объектам КС.
2. Политика использования ресурсов должна определять ограничения, которые можно накладывать, на количество данных объектов (объем ресурсов), выделяемых отдельному пользователю и произвольным группам пользователей.
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.
4. 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.
5. НЕОБХОДИМЫЕ УСЛОВИЯ: НО-1

### *2. Устойчивость к отказам*

Устойчивость к отказам гарантирует доступность КС (возможность использования информации, отдельных функций или КС в целом) после отказа ее компонента. Уровни данной услуги ранжируются на основании способности КСЗ обеспечить возможность функционирования КС в зависимости от количества отказов и услуг, доступных после отказа (от ДС-1 до ДС-3).

**ДС-3 Устойчивость без ухудшения характеристик обслуживания**

1. Разработчик должен провести анализ отказов компонентов КС.
2. Политика устойчивости к отказам, реализуемая КСЗ, должна относиться ко всем компонентам КС.
3. Должны быть четко указаны уровни отказов, при превышении которых отказы приводят к снижению характеристик обслуживания или недоступности услуги.
4. Отказ одного защищенного компонента не должен приводить к недоступности всех услуг или к снижению характеристик обслуживания.
5. КСЗ должен быть способен ставить в известность администратора об отказе любого защищенного компонента.
6. НЕОБХОДИМЫЕ УСЛОВИЯ: НО-1

### *3. Горячая замена*

Данная услуга позволяет гарантировать доступность КС (возможность использования информации, отдельных функций или КС в целом) в процессе замены отдельных компонентов. Уровни данной услуги ранжируются на основании полноты реализации (от ДЗ-1 до ДЗ-3).

**ДЗ-3 Горячая замена любого компонента**

1. Политика горячей замены, реализуемая КСЗ, должна обеспечивать возможность замены любого компонента без прерывания обслуживания.
2. Администратор или пользователи, которым предоставлены соответствующие полномочия, должны иметь возможность заменить любой защищенный компонент.
3. НЕОБХОДИМЫЕ УСЛОВИЯ: НО-1, ДС-1

### *4. Восстановление после сбоев*

Данная услуга обеспечивает возврат КС в известное защищенное состояние после отказа или прерывания обслуживания. Уровни данной услуги ранжируются на основании степени автоматизации процесса восстановления (от ДВ-1 до ДВ-3).

**ДВ-3 Избирательное восстановление**

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.
2. 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, к функционированию в режиме с ухудшенными характеристиками обслуживания.
3. 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.
4. Должны существовать ручные процедуры, с помощью которых можно безопасным образом вернуть КС из режима с ухудшенными характеристиками обслуживания в режим нормального функционирования.
5. НЕОБДХОДИМЫЕ УСЛОВИЯ: НО-1

## IV. КРИТЕРИИ НАБЛЮДАЕМОСТИ

Для того, чтобы КС могла быть оценена на предмет соответствия критериям наблюдаемости, КСЗ оцениваемой КС должен предоставлять услуги по обеспечению ответственности пользователя за свои действия и по поддержанию способности КСЗ выполнять свои функции. Наблюдаемость обеспечивается КС через такие услуги: регистрация (аудит), идентификация и аутентификация, достоверный канал, разграничение обязанностей, целостность КСЗ, самотестирование, идентификация и аутентификация при обмене, аутентификация отправителя, аутентификация получателя.

### *1. Регистрация*

Регистрация позволяет контролировать опасные для КС действия. Уровни данной услуги ранжируются в зависимости от полноты и избирательности контроля, сложности средств анализа данных журналов регистрации и способности выявления потенциальных нарушений (от НР-1 до НР-5).

**НР-5 Анализ в реальном времени**

1. Политика регистрации, реализуемая КСЗ, должна определять перечень регистрируемых событий.
2. КСЗ должен быть способен осуществлять регистрацию событий, имеющих непосредственное или косвенное отношение к безопасности.
3. Журнал регистрации должен содержать информацию о дате, времени, месте, типе и успешности или отсутствия успешности каждого зарегистрированного события.

   Журнал регистрации должен содержать информацию, достаточную для установления пользователя, процессе и/или объекта, имеющих отношение к каждому зарегистрированному событию.

4. 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.
5. 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. КСЗ должен быть способен выявить и анализировать несанкционированные действия в реальном времени.
5. НЕОБХОДИМЫЕ УСЛОВИЯ: НИ-1, НО-1

### *2. Идентификация и аутентификация*

Идентификация и аутентификация позволяют КСЗ определить и проверить личность пользователя, пытающегося получить доступ к КС. Уровни данной услуги ранжируются в зависимости от числа задействованных механизмов аутентификации (от НИ-1 до НИ-3)

**НИ-2 Одиночная идентификация и аутентификация**

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.
2. Прежде чем разрешить любому пользователю выполнять любые другие, контролируемые КСЗ действия, КСЗ должен аутентифицировать этого пользователя с использование защищенного механизма.
3. КСЗ должен обеспечивать защиту данных аутентификации от несанкционированного доступа, модификации или разрушения.
4. НЕОБХОДИМЫЕ УСЛОВИЯ: НК-1

### *3. Достоверный канал*

Данная услуга позволяет гарантировать пользователю возможность непосредственного взаимодействия с КСЗ. Уровни данной услуги ранжируются в зависимости от гибкости предоставления возможности КСЗ или пользователю инициировать защищенный обмен (от НК-1 до НК-2).

**НК-2 Двунаправленный достоверный канал**

1. Политика достоверного канала, реализуемая КСЗ, должна определять механизмы установления достоверной связи между пользователем и КСЗ
2. 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.
3. Обмен с использованием достоверного канала, инициируемый КСЗ, должен быть однозначно идентифицируемый как таковой и должен происходить только после положительного подтверждения готовности к обмену со стороны пользователя.
4. НЕОБХОДИМЫЕ УСЛОВИЯ: НЕТ

### *4. Разграничение обязанностей*

Данная услуга позволяет уменьшить потенциальный ущерб от умышленных или ошибочных действий пользователя и ограничить авторитарность управления. Уровни данной услуги ранжируются на основании избирательности управления возможностями пользователей и администраторов (от НО-1 до НО-3)

**НО-3 Разграничение обязанностей на основании привилегий**

1. Политика разграничения обязанностей, реализуемая КСЗ, должна определять роли администратора и обычного пользователя и присущие им функции.

2. 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 необходимые для выполнения данной роли.
3. Политика разграничения обязанностей должна определять множество различных ролей пользователей.
4. Пользователь должен иметь возможность выступать в определенной роли только после того, как он выполнит определенные действия, подтверждающие принятие этой роли.
5. НЕОБХОДИМЫЕ УСЛОВИЯ: НИ-1

### *5. Целостность комплекса средств защиты*

Данная услуга определяет меру способности КСЗ защищать себя и гарантировать свою способность управлять защищенными объектами (от НЦ-1 до НЦ-3)

**НЦ-3 КСЗ с функциями диспетчера доступа**

1. Политика целостности КСЗ должна определять домен КСЗ и другие домены, а также механизмы защиты, используемые для реализации разделения доменов.
2. КСЗ должен поддерживать домен для своего собственного исполнения с целью защиты от внешних воздействий и несанкционированной модификации и/или потери управления.
3. КСЗ должен гарантировать, что услуги безопасности доступны только через интерфейс КСЗ и все запросы на доступ к защищенным объектам контролируются КСЗ.
4. НЕОБХОДИМЫЕ УСЛОВИЯ: НЕТ

### *6. Самотестирование*

Самотестирование позволяет КСЗ проверить и на основании этого гарантировать правильность функционирования и целостность определенного множества функций КС. Уровни данной услуги ранжируются на основании возможности выполнения тестов в процессе запуска или штатной работы (от НТ-1 до НТ-3).

**НТ-2 Самотестирование при старте**

1. Политика самотестирования, реализуемая КСЗ, должна описывать свойства КС и реализованные процедуры, которые могут быть использованы для оценки правильности функционирования КСЗ.
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 при инициализации КСЗ.
3. НЕОБХОДИМЫЕ УСЛОВИЯ: НО-1

### *7. Идентификация и аутентификация при обмене*

Данная услуга позволяет одному КСЗ идентифицировать другой КСЗ (установить и проверить его идентичность) и обеспечить другому КСЗ возможность идентифицировать первый, прежде чем начать взаимодействие. Уровни данной услуги ранжируются на основании полноты реализации (от НВ-1 до НВ-3)

**НВ-2 Аутентификация источника данных**

1. Политика идентификации и аутентификации при обмене, реализуемая КСЗ, должна определять множество атрибутов КСЗ и процедуры, которые необходимы для взаимной идентификации и 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.
2. КСЗ должен использовать защищенные механизмы для установления источника каждого экспортируемого и импортируемого объекта.
3. НЕОБХОДИМЫЕ УСЛОВИЯ: НЕТ

### *8. Аутентификация отправителя*

Даная услуга позволяет обеспечить защиту от отказа от авторства и однозначно установить принадлежность определенного объекта определенному пользователю, т.е. тот факт, что объект был создан или отправлен данным пользователем. Уровни данной услуги ранжируются на основании возможности подтверждения результатов проверки независимой третьей стороной (от НА-1 до НА-2)

**НА-1 Базовая аутентификация отправителя**

1. Политика аутентификации 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.
2. Установление принадлежности должно выполняться на основании утвержденного протокола аутентификации.
3. НЕОБХОДИМЫЕ УСЛОВИЯ: НИ-1

### *9. Аутентификация получателя*

Даная услуга позволяет обеспечить защиту от отказа от получения и позволяет однозначно установить факт получения определенного объекта определенным пользователем. Уровни данной услуги ранжируются на основании возможности подтверждения результатов проверки независимой третьей стороной (от НП-1 до НП-2)

**НП-1 Базовая аутентификация получателя**

1. Политика аутентификации 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.
2. Установление получателя должно выполняться на основании утвержденного протокола аутентификации.
3. НЕОБХОДИМЫЕ УСЛОВИЯ: НИ-1

## V. КРИТЕРИИ ГАРАНТИЙ

Критерии гарантий включают требования к архитектуре, среде разработки, последовательности разработки, среде функционирования, документации и испытаниям КСЗ. В данных критериях вводится семь уровней гарантий, которые являются иерархическими. Требования излагаются по разделам. Для того, чтобы КС получила определенный уровень гарантий (если она не может получить более высокий), должны быть удовлетворены все требования, определенные для данного уровня в каждом из разделов.

### *1. Архитектура*

Требования к архитектуре обеспечивают гарантию того , что КСЗ в состоянии полностью реализовать политику безопасности (от Г-1 до Г-7)

**Г-5 (Г-7) Требования**

Разработка ПО во многом должна быть направлена на минимизацию сложности КСЗ. КСЗ должен быть спроектирован 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.

*При этом требования должны предусматривать наличие их иерархии от Г-1 до Г-4:*

- КСЗ должен реализовывать политику безопасности. Все его компоненты должны быть четко определены.
- КСЗ должен состоять из хорошо определенных и максимально независимых компонентов. Каждый из компонентов должен быть спроектирован в соответствии с принципом минимума полномочий.
- Критичные для безопасности компоненты должны быть защищены от не критичных для безопасности за счет использования механизмов защиты, предоставляемых программно-аппаратными средствами более низкого уровня.

- 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.

## *2. Среда разработки*

Требования к среде разработки обеспечивают гарантии того, что процессы разработки и сопровождения оцениваемой КС являются полностью управляемыми со стороны Разработчика (от Г-1 до Г-7)

### 2.1. Процесс разработки

**Г-4 (Г-7) Требования**

Разработчик должен разработать, внедрить и поддерживать в рабочем состоянии документально оформленные методики обеспечения физической, технической, организационной и кадровой безопасности.

*При этом требования должны предусматривать наличие их иерархии от Г-1 до Г-3:*

- Разработчик должен определить все стадии жизненного цикла КС, 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.
- 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

**Г-6 (Г-7) Требования**

Должна использоваться система мер технической, физической, организационной и кадровой безопасности, направленных на защиту всех средств и материалов, используемых для генерации КСЗ, от несанкционированной модификации или разрушения.

*При этом требования должны предусматривать наличие их иерархии от Г-1 до Г-5:*

- 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 и базироваться на автоматизированных средствах.
- Система управления конфигурацией также должна использоваться для генерации КСЗ из исходного кода и учета всех изменений с появлением новых версий.
- Система управления конфигурацией должна быть способна выдавать отчеты о состоянии элементов конфигурации.

## *3. Последовательность разработки*

Требования к процессу проектирования (последовательности разработки) обеспечивают гарантии того, что на каждой стадии разработки (проектирования) существует точное описание КС и реализация КС в точности соответствует исходным требованиям (политике безопасности).

### 3.1. Функциональные спецификации (политика безопасности)

**Г-1 (Г-7) Требования**

На стадии разработки технического задания Разработчик должен разработать функциональные спецификации КС. Представленные специальные 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)**
**Г-4 (Г-7) Требования**

Стиль спецификации - формализованная
Соответствие политике безопасности - демонстрация

*При этом требования должны предусматривать наличие их иерархии от Г-2 до Г-3 (Г-1 нет):*

- Соответствие политике безопасности - показ
- Функциональные спецификации должны включать модель политики безопасности
- Стиль спецификации - неформализованный
  - частично формализованная.

**3.3. Проект архитектуры**
**Г-6 (Г-7) Требования**

Стиль спецификации - формализованный
Соответствие модели политике безопасности - доказательство

*При этом требования должны предусматривать наличие их иерархии от Г-1 до Г-5:*

- Соответствие модели политики безопасности – Г-2 – Г-4 – показ; Г-5 – демонстрация.
- 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 - Г-1 - Г-2 - неформализованный
  - Г-3 - Г-5 - частично формализованная.

**3.4. Детальный проект**
**Г-7 Требования**

Стиль спецификации - формализованный
Соответствие проекту архитектуры - доказательство

*При этом требования должны предусматривать наличие их иерархии от Г-1 до Г-6:*

- Соответствие проекту архитектуры - Г-2 - Г-5 – показ; Г-6 – демонстрация.
- На стадии разработки технического проекта или рабочего проекта Разработчик должен разработать детальный проект КСЗ. Представленный детальный проект должен содержать перечень всех компонентов КСЗ и точное описание функционирование каждого механизма. Должны быть описаны назначение и параметры интерфейсов компонентов КСЗ.
- Стиль спецификации - для уровня Г-1 требуется детальный проект компонентов КСЗ, непосредственно имеющих отношение к безопасности.
  - Г-2 – Г-3 - неформализованная - весь КСЗ.
  - Г-4 - Г-6 - частично формализованная - весь КСЗ.

**3.5. Реализация**
**Г-7 Требования**

Соответствие детальному проекту - демонстрация
Исходный код, представленный Разработчиком - всех библиотек
времени выполнения

*При этом требования должны предусматривать наличие их иерархии:*

- Соответствие детальному проекту - Г-3 - Г-6 – показ (Г-1–Г-2 – нет)
- Исходный код, представленный Разработчиком - Г-3 - Г-6 - части КСЗ
  Г-5 - Г-6 - всего КСЗ

## *4. Среда функционирования*

Требования к среде функционирования обеспечивают гарантии того, что КС поставляется Заказчику без несанкционированных модификаций, а также инсталлируется и инициализируется Заказчиком так, как это предлагается Разработчиком.

**Г-6 (Г-7) Требования**

Для поддержания соответствия между КСЗ, поставляемой Заказчику, и эталонной копией должна существовать система управления распространением защищенной КС.

*При этом требования должны предусматривать наличие их иерархии*
*от Г-1 до Г-7:*

- 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.

*от Г-3 до Г-7:*

- Должна существовать система технических, организационных и физических мер безопасности, гарантирующих, что программное и программно-аппаратное обеспечение КСЗ, поставляемое Заказчику, в точности соответствует эталонной копии.

## *5. Документация*

Требования к документации являются общими 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.

В описании функций безопасности должны быть изложены основные, необходимые правильного использования услуг безопасности, принципы политики безопасности, реализуемой КСЗ , оцениваемой КС, а также сами услуги.

Руководство администратора по услугам безопасности должно содержать описание средств инсталляции , генерации и запуска КС, описание всех возможных параметров конфигурации, которые могут использоваться в процессе инсталляции, генерации и запуска КС, описание свойств КС, которые могут быть использованы для периодической оценки правильности функционирования КСЗ, а также инструкции по использованию администратором услуг безопасности для поддержания политики безопасности, принятой в организации, эксплуатирующей КС.

Руководство пользователя по услугам безопасности должно содержать инструкции по использованию функций безопасности обычным пользователем (не администратором).

Название документов (разделов) не регламентируется. Описание услуг безопасности может быть различным для пользователя и администратора. Руководство пользователя и руководство администратора могут быть объединены в руководство по установке и эксплуатации.

## *6. Испытания комплекса средств защиты*

**Г-4 (Г-7) Требования**

Разработчик должен выполнить тесты по преодолению механизмов защиты и доказать, что КСЗ относительно или абсолютно устойчив к такому характеру атак со стороны Разработчика.

*При этом требования должны предусматривать наличие их иерархии от Г-1 до Г-7:*

- 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.
- 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».

**Разработчик ДИС «Ноосфера»: ООО «Крымское аэрокосмическое агентство» (Лицензия Администрации государственной службы специальной связи и защиты информации Украины: серия АГ, № 500756 от 03.10.2011 г.)**