6. СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стандарты и спецификации бывают двух разных видов:

- *оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;*
- *технических спецификаций, регламентирующих различные аспекты реализации средств защиты.*

6.1 **Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт**

6.1.1 Основные понятия

Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем». Данный труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 года. «Оранжевая книга» поясняет понятие безопасной системы, которая «управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию».

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Оценивается лишь степень доверия, которое можно оказать той или иной системе.

Степень доверия оценивается по двум основным критериям.

- ***Политика безопасности*** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности.
- ***Уровень гарантированности*** - мера доверия, которая может быть оказана архитектуре и реализации ИС. Это пассивный аспект защиты. Уровень гарантированности показывает, насколько

корректны механизмы, отвечающие за реализацию политики безопасности.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности.

***Доверенная вычислительная база** - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.*

***Основное назначение доверенной вычислительной базы** - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями).*

Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

- ***Изолированность.*** Необходимо предупредить возможность отслеживания работы монитора.
- ***Полнота.*** Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
- ***Верифицируемость.*** Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

*Реализация монитора обращений называется **ядром безопасности**. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.*

*Границу доверенной вычислительной базы называют **периметром безопасности**. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию «периметр безопасности» все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.*

6.1.2 Механизмы безопасности

Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом (называемое иногда дискреционным) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов - важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Для реализации **принудительного управления доступом** с субъектами и объектами ассоциируются **метки безопасности**. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Согласно «Оранжевой книге», метки безопасности состоят из двух частей:

- уровня секретности;
- списка категорий.

Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, «конфиденциальный» субъект может записывать данные в секретные файлы,

но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется **принудительным**, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Если понимать политику безопасности узко, как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Обычный способ идентификации - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Переходя к пассивным аспектам защиты, укажем, что в «Оранжевой книге» рассматривается два вида гарантированности:

1. *Операционная гарантированность относится к архитектурным и реализационным аспектам системы.* Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности. Операционная гарантированность включает в себя проверку следующих элементов:
 - архитектура системы;
 - целостность системы;
 - проверка тайных каналов передачи информации;
 - доверенное администрирование;
 - доверенное восстановление после сбоев.
2. *технологическая гарантированность - к методам построения и сопровождения.* Технологическая гарантированность охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия

должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные «закладки».

6.1.3 Классы безопасности

В «Оранжевой книге» определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Классификацию, введенную в «Оранжевой книге» можно сформулировать так:

- уровень C - произвольное управление доступом;
- уровень B - принудительное управление доступом;
- уровень A - верифицируемая безопасность.

6.2 Информационная безопасность распределенных систем. Рекомендации X.800

6.2.1 Сетевые сервисы безопасности

Переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее «Оранжевой книги», но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем. Рекомендации X.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли.

***Аутентификация.** Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает:*

- односторонней (обычно клиент доказывает свою подлинность серверу),
- двусторонней (взаимной).

***Управление доступом.** Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.*

***Конфиденциальность данных.** Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем **конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).*

***Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением*

соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказать от совершенных действий) обеспечивает два вида услуг:

- неотказуемость с подтверждением подлинности источника данных
- неотказуемость с подтверждением доставки.

В таблице 5.1 указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Таблица 5.1 - Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	Уровень						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

6.2.2 Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- **шифрование;**
- **электронная цифровая подпись;**
- **механизмы управления доступом.** Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- **механизмы контроля целостности данных.** В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации.

- **механизмы аутентификации.** Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, криптографических методов, устройств измерения и анализа биометрических характеристик;
- **механизмы дополнения трафика;**
- **механизмы управления маршрутизацией.** Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
- **механизмы нотаризации.** Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В таблице 5.2 сведены сервисы (функции) и механизмы безопасности. Таблица 5.2 показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Таблица 5.2. Взаимосвязь функций и механизмов безопасности

Функции	Механизмы		
	1	2	3
Аутентификация партнеров	-	+	-
Аутентификация источника	-	-	-
Управление доступом	-	-	-
Конфиденциальность	-	-	-
Избирательная конфиденциальность	-	-	-
Конфиденциальность трафика	-	-	+
Целостность соединения	+	-	-
Целостность вне соединения	+	-	-
Неотказуемость	+	-	-

«+» механизм пригоден для реализации данной функции безопасности;

«-» механизм не предназначен для реализации данной функции безопасности.

+	+	-
+	+	-
-	-	+
+	-	+
+	-	-
+	-	-

+	-	-
+	+	-
-	+	-

-	-
-	-
-	-
+	-

-	-
+	-
-	-

-	-
-	+

6.2.3 Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из конечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администрирование средств безопасности должны распределяться по трем направлениям:

- **администрирование информационной системы в целом;** обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, **реагирование** на происходящие события, **аудит и безопасное восстановление.**
- **администрирование сервисов безопасности;** включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.
- **администрирование механизмов безопасности;** определяются перечнем задействованных механизмов:
 - **управление ключами (генерация и распределение);**
 - **управление шифрованием;**
 - **администрирование управления доступом** (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);
 - **управление аутентификацией** (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.);
 - **управление маршрутизацией** (выделение доверенных путей);
 - **управление нотаризацией** (распространение информации о нотариальных службах, администрирование этих служб).

6.3 Стандарт ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий»

6.3.1 Основные понятия

Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. По

историческим причинам данный стандарт часто называют «Общими критериями» (или даже ОК). Мы также будем использовать это сокращение.

«Общие критерии» на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от «Оранжевой книги», «Общие критерии» не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения «Общие критерии» можно считать набором библиотек, помогающих писать содержательные «программы» - задания по безопасности, типовые профили защиты и т.п.

Как и «Оранжевая книга», «Общие критерии» содержат два основных вида требований безопасности:

- **функциональные**, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия**, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Очень важно, что **безопасность в «Общих критериях» рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:**

- *определение назначения, условий применения, целей и требований безопасности;*
- *проектирование и разработка;*
- *испытания, оценка и сертификация;*
- *внедрение и эксплуатация.*

В «Общих критериях» объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

1. *источник угрозы;*
2. *метод воздействия;*
3. *уязвимые места, которые могут быть использованы;*
4. *ресурсы (активы), которые могут пострадать.*

С точки зрения технологии программирования в «Общих критериях» использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в «Общих критериях» введена иерархия **класс-семейство-компонент-элемент**.

Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов:

- **Профиль защиты (ПЗ)** представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).
- **Задание по безопасности** содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В «Общих критериях» нет готовых классов защиты. Сформировать классификацию в терминах «Общих критериев» - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям.

Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

6.3.2 Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в «Оранжевой книге».

Перечислим классы функциональных требований «Общих критериев»:

1. **идентификация и аутентификация;**
2. **защита данных пользователя;**
3. **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
4. **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);

5. **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
6. **доступ к объекту оценки**;
7. **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
8. **использование ресурсов** (требования к доступности информации);
9. **криптографическая поддержка** (управление ключами);
10. **связь** (аутентификация сторон, участвующих в обмене данными);
11. **доверенный маршрут/канал** (для связи с сервисами безопасности).

6.3.3 Требования доверия безопасности

Установление доверия безопасности, согласно «Общим критериям», основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия **разработчиков**;
- представление и содержание **свидетельств**;
- действия **оценщиков**.

Всего в «Общих критериях» 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Применительно к требованиям доверия в «Общих критериях» введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

1. **Оценочный уровень доверия 1 (начальный)** предусматривает анализ **функциональной спецификации**, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.
2. **Оценочный уровень доверия 2**, в дополнение к первому уровню, предусматривает наличие **проекта верхнего уровня** объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.
3. На **3 уровне** ведется контроль среды разработки и управление конфигурацией объекта оценки.
4. На **уровне 4** добавляются полная спецификация интерфейсов, **проекты нижнего уровня**, анализ подмножества реализации, применение неформальной **модели** политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого

можно достичь при существующей технологии программирования и приемлемых затратах.

5. **Уровень 5**, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полужформальных функциональной спецификации и проекта верхнего уровня с **демонстрацией соответствия** между ними.
6. На **уровне 6** реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.
7. Оценочный **уровень 7** (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

6.4 Руководящие документы Гостехкомиссии России

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на «Общие критерии», что можно только приветствовать.

Рассмотрим два важных, хотя и не новых, руководящих документа:

1. **Классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД)**
2. **Классификацию межсетевых экранов (МЭ).**

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Требования ко всем девяти классам защищенности АС сведены в таблицу 5.3.

Переходя к рассмотрению второго РД Гостехкомиссии России - Классификации межсетевых экранов. Данный РД важен не столько содержанием, сколько самим фактом своего существования.

*Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется **фильтрация информации**. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.*

Таблица 5.3 - Требования к защищенности автоматизированных систем

Подсистемы и требования	Классы								
	ЗБ	ЗА	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;									
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-		+	+	+
к программам;	-	-	-	+	-		+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-		+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-		+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);									
выдачи печатных (графических) выходных документов;	-	+	-	+	-		+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-		+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+

Таблица 5.3 - Требования к защищенности автоматизированных систем
(продолжение)

Подсистемы и требования

3. Криптографическая подсистема

3.1. Шифрование конфиденциальной информации.

3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.

3.3. Использование аттестованных (сертифицированных) криптографических средств.

4. Подсистема обеспечения целостности

4.1. Обеспечение целостности программных средств и обрабатываемой информации.

4.2. Физическая охрана средств вычислительной техники и носителей информации.

4.3. Наличие администратора (службы защиты) информации в АС.

4.4. Периодическое тестирование СЗИ НСД.

4.5. Наличие средств восстановления СЗИ НСД.

4.6. Использование сертифицированных средств защиты.

«-» нет требований к данному классу;

«+» есть требования к данному классу;

«СЗИ НСД» система защиты информации от несанкционированного доступа

Классы									
3Б 3А 2Б 2А 1Д 1Г 1В 1Б 1А									
-	-	-	+	-	-	-	+	+	
-	-	-	-	-	-	-	-	+	
-	-	-	+	-	-	-	+	+	
	+	+	+	+	+	+	+	+	
	+	+	+	+	+	+	+	+	
-	-	-	+	-	-		+	+	+
+	+	+	+	+	+	+	+	+	
+	+	+	+	+	+	+	+	+	
-	+	-	+	-	-	+	+	+	