35

O‘z DSt 2814:2014

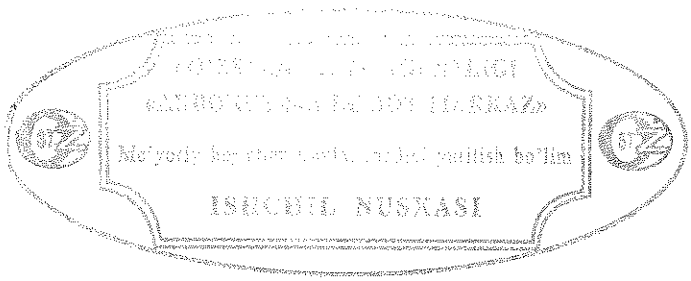
ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ

Классификация по уровню защищенности от несанкционированного доступа к информации

Издание официальное



Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘z DSt 27:2014

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН Службой национальной безопасности Республики Узбекистан

2 УТВЕРЖДЕН и ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») 18.03.2014 № 05-530

3 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Республики Узбекистан публикуются в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агенством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Общие положения 2
5 Требования к классу защищенности 3Б 7
6 Требования к классу защищенности 3А 8
7 Требования к классу защищенности 2Б 9
8 Требования к классу защищенности 2А 10
9 Требования к классу защищенности 1Д 13
10 Требования к классу защищенности 1Г 14
11 Требования к классу защищенности 1В 17
12 Требования к классу защищенности 1Б 20
13 Требования к классу защищенности 1А 24
14 Определение класса АС 28

O‘zbekiston Respublikasi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
АВТОМАТЛАШТИРИЛГАН ТИЗИМЛАР
Ахборотдан рухсатсиз фойдалана олишдан муҳофазаланганлик даражалари буйича таснифлаш

Информационная технология
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ
Классификация по уровню защищенности от несанкционированного доступа к информации

Information technology
Automated systems
Classification by level of protection from unauthorized access to information

Дата введения 31.03.2015

1 Область применения

Настоящий стандарт устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в автоматизированных системах различных классов.

Стандарт может использоваться заказчиками и разработчиками автоматизированных систем при формулировании и реализации требований по обеспечению информационной безопасности.

Классификация распространяется на все действующие и проектируемые автоматизированные системы учреждений, организаций и предприятий, обрабатывающие информацию ограниченного доступа.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt 1106:2009 Информационная технология. Криптографическая защита информации. Функция хэширования

O‘z DSt 1109:2013 Информационная технология. Криптографическая защита информации. Термины и определения

O'ZSTANDART AGENTLIGI
5758 son bilan
«18» 03 2015 yilda
Davlat ro'yxatiga olindi

O‘z DSt 2815:2014 Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации

O‘z DSt 2816:2014 Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей

O‘z DSt 2817:2014 Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации

3 Термины и определения

В настоящем стандарте применены термины по O‘z DSt 1109, а также следующие термины с соответствующими определениями:

3.1 **автоматизированная система**; АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

3.2 **контролируемая зона**; КЗ: Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

3.3 **несанкционированный доступ;** НСД**:** Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

3.4 **система защиты информации от несанкционированного доступа;** СЗИ НСД: Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в системах.

4 Общие положения

4.1 Защита информации от НСД является составной частью общей проблемы обеспечения информационной безопасности. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники (СВТ) - электронно-вычислительных машин (ЭВМ), средств и систем связи.

4.2 Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

4.3 Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количествен-

O‘zbekiston Agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BO‘LIMI

ному и качественному составу пользователей и обслуживающего персонала.

4.4 Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

4.5 Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и требуемый уровень защиты;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

4.6 Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

4.7 К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации ограниченного доступа;
- уровень полномочий субъектов доступа АС на доступ к информации ограниченного доступа;
- режим обработки данных в АС - коллективный или индивидуальный.

4.8 Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности информации и, следовательно, иерархия классов защищенности АС.

4.9 Третья группа включает АС (отдельно стоящие, не подключенные к другим АС), в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

...VLIGHTIRISH, DAVLAT ...MUVOFIQLASHTIRISH VA ...ASIY TEXNOLOGIYALARNI JORIY ETISH BOSHQARMASI

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

4.10 Комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках СЗИ НСД, условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

4.11 Каждая подсистема характеризуется совокупностью требований. Каждый класс АС содержит совокупность требований по подсистемам. Требования, характеризующие каждый класс по подсистемам, приведены в таблице 1 и подробно сформулированы в разделах 5-13.

Таблица 1

Наименование требования	Классы								
	3Б	3А	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) систему(ы) (узел сети)	+	+	+	+	+	+	+	+	+
- выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
- запуска (завершения) программ и процессов (заданий, задач)	-	-	-	+	-	+	+	+	+

Продолжение таблицы 1

Наименование требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-	-	+	-	+	+	+	+
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	-	+	+	+	+
- изменение полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
- создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
- формирование отчетности статистических сведений*	-	-	-	+	-	+	+	+	+
2.2 Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3 Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4 Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+
3 Криптографическая подсистема**									
3.1 Шифрование информации ограниченного доступа записываемой на носители данных	-	-	-	+	-	-	-	+	+
3.2 Шифрование информации при передаче её по каналам связи, выходящим за пределы КЗ	+	+	+	+	+	+	+	+	+

MAXSUS TEXNOLOGIYALAR
JORIY ETISH BOSHQARMASI

Окончание таблицы 1

Наименование требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
3.3 Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	-	-	-	-	+
3.4 Использование сертифицированных средств криптографической защиты информации	+	+	+	+	+	+	+	+	+
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 информации	-	+	-	+	-	-	+	+	+

*- Данное требование для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах неинтегрированных с государственными информационными ресурсами, носит рекомендательный характер.

** - Для защиты информации отнесенной к государственным секретам должны использоваться аппаратные или аппаратно-программные средства криптографической защиты информации (СКЗИ), имеющие сертификаты соответствия по требованиям безопасности информации. Для защиты конфиденциальной информации допускается использование сертифицированных программных СКЗИ.

Примечание - «+» - есть требования к данному классу, «-» - нет требований к данному классу.

5 Требования к классу защищенности 3Б

5.1 В подсистеме управления доступом должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее восьми буквенно-цифровых символов.

5.2 Подсистема регистрации и учета:

- должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются: дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

5.3 Криптографическая подсистема:

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;
- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;
- должны использоваться сертифицированные средства криптографической защиты информации.

5.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
   - целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
   - целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;
2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
3) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
4) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности.

MAZKUR HUJJAT O‘ZBEKISTON RESPUBLIKASI ADLIYA VAZIRLIGI AXBOROT TEXNOLOGIYALARI JORIY ETISH BOSHQARMASI

6 Требования к классу защищенности 3А

6.1 В подсистеме управления доступом должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов.

6.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);

2) регистрация выдачи документов должна осуществляться в печатном (графическом) виде. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

3) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

4) должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;

5) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

6.3 Криптографическая подсистема:

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;
- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;
- должны использоваться сертифицированные средства криптографической защиты информации.

6.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

2) должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специального оборудования помещений АС;

3) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

4) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

5) должны использоваться сертифицированные средства защиты информации.

7 Требования к классу защищенности 2Б

7.1 В подсистеме управления доступом должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых, а также специальных символов.

7.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);

2) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

7.3 Криптографическая подсистема:

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;

- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

- должны использоваться сертифицированные средства криптографической защиты информации.

7.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации.

2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

3) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

4) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности.

8 Требования к классу защищенности 2А

8.1 Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых, а также специальных символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

8.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализа-

ции операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная (при НСД);
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

2) должна осуществляться регистрация выдачи документов в печатном (графическом) виде. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства], краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;

3) должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный);

4) должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная,
- идентификатор субъекта доступа;
- спецификация защищаемого файла;

5) должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, каналам (линиям) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;

STANDARTLASHTIRISH, DAVLAT
AXBOROT TEXNOLOGIYALARI

- спецификация защищаемого объекта [логическое имя (номер)];

6) должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

7) должна формироваться отчетность статистических сведений подсистемы регистрации и учета, предназначенных для создания и формирования отчетов в виде удобном для отображения, в том числе для вывода на печатающие устройства по формам регламентированной отчетности, настройкам планового формирования и предоставления статистических отчетов в различных форматах (включая графические). Также должна быть предусмотрена защита от модификации. Круг субъектов доступа к данной системе должен быть ограничен.

8) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

9) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

10) должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

11) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

8.3 Криптографическая подсистема:

- должно осуществляться шифрование всей информации ограниченного доступа, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные носители данных (дискеты, компакт-диски, флеш-накопители, и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;

- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

- должны использоваться сертифицированные средства криптографической защиты информации.

8.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

O‘zSTANDART
STANDARTLASHTI
MAZMUNINI MUVOF
AXBOROT TEX
JORIY ET

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

2) должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специального оборудования помещений АС;

3) должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;

4) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

5) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности;

6) должны использоваться сертифицированные средства защиты информации.

9 Требования к классу защищенности 1Д

9.1 Подсистема управления доступом: должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых, а также специальных символов.

9.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

2) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);

3) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

9.3 Криптографическая подсистема:

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;

- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

- должны использоваться сертифицированные средства криптографической защиты информации.

9.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

3) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест – программ, имитирующих попытки НСД;

4) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности.

10 Требования к классу защищенности 1Г

10.1 Подсистема управления доступом:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее восьми буквенно-цифровых, а также специальных символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

10.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке;

2) должна осуществляться регистрация выдачи документов в печатном (графическом) виде. В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;

3) должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный);

4) должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;

5) должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, каналам (линиям) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQAR ASI

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];

6) должна формироваться отчетность статистических сведений подсистемы регистрации и учета, предназначенных для создания и формирования отчетов в виде удобном для отображения, в том числе для вывода на печатающие устройства по формам регламентированной отчетности, настройкам планового формирования и предоставления статистических отчетов в различных форматах (включая графические). Также должна быть предусмотрена защита от модификации. Круг субъектов доступа к данной системе должен быть ограничен;

7) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

8) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

9) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

10.3 Криптографическая подсистема:

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;
- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;
- должны использоваться сертифицированные средства криптографической защиты информации.

10.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

O'ZBEKISTON RESPUBLIKASI STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI

3) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

4) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности.

11 Требования к классу защищенности 1В

11.1 Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых, а также специальных символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и (или) адресам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

11.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная - несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке;

2) должна осуществляться регистрация выдачи документов в печатном (графическом) виде. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:

O‘zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQAR ASI

- дата и время выдачи (обращение к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

3) должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный - несанкционированный);

4) должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

5) должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, каналам (линиям) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.).

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

6) должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения;

7) должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

8) должна формироваться отчетность статистических сведений подсистемы регистрации и учета, предназначенных для создания и формирования отчетов в виде удобном для отображения, в том числе для вывода на печатающие устройства по формам регламентированной отчетности, настройкам планового формирования и предоставления статистических отчетов в различных форматах (включая графические). Также должна быть предусмотрена защита от модификации. Круг субъектов доступа к данной системе должен быть ограничен;

9) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку);

10) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

11) должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

12) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

13) должна осуществляться сигнализация попыток нарушения защиты.

11.3 Криптографическая подсистема:

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;
- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;
- должны использоваться сертифицированные средства криптографической защиты информации.

11.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

O‘ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;

2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специального оборудования помещений АС;

3) должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

4) должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;

5) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности;

6) должны использоваться сертифицированные средства защиты информации.

12 Требования к классу защищенности 1Б

12.1 Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

12.2 Подсистема регистрации и учета:

O‘ZBEKISTON ARXITEKTURA STANDARTLASHTIRISH, DAVLAT NAZORATINI MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешный или неуспешный - несанкционированный;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке;

2) должна осуществляться регистрация выдачи документов в печатном (графическом) виде. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный;

3) должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный);

4) должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

O‘zbekiston Agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
-идентификатор субъекта доступа;
-спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

5) должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, каналам (линиям) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

6) должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения;
- идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.);
- спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);

7) должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

8) должна формироваться отчетность статистических сведений подсистемы регистрации и учета, предназначенных для создания и формирования отчетов в виде удобном для отображения, в том числе для вывода на печатающие устройства по формам регламентированной отчетности, настройкам планового формирования и предоставления статистических

STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

отчетов в различных форматах (включая графические). Также должна быть предусмотрена защита от модификации. Круг субъектов доступа к данной системе должен быть ограничен;

9) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки;

10) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

11) должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

12) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;

13) должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

12.3 Криптографическая подсистема:

- должно осуществляться шифрование всей информации ограниченного доступа, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные портативные носители данных (дискеты, компакт-диски, флеш-накопители, и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;

- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

- должны использоваться сертифицированные средства криптографической защиты информации.

12.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС;

- целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;

2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

средств охраны и специального персонала, использование строгого пропускного режима, специального оборудования помещений АС;

3) должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

4) должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

5) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;

6) должны использоваться сертифицированные средства защиты информации.

13 Требования к классу защищенности 1А

13.1 Подсистема управления доступом:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;

- должна осуществляться аппаратурная идентификация и проверка подлинности терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по уникальным встроенным устройствам;

- должна осуществляться идентификация и проверка подлинности программ, томов, каталогов, файлов, записей, полей записей по именам и контрольным суммам (паролям, ключам);

- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

13.2 Подсистема регистрации и учета:

1) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

O'zbekiston Davlat
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
DAVLAT ETISH BOSHQARMASI

- результат попытки входа: успешная или неуспешная - несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке;

2) должна осуществляться регистрация выдачи документов в печатном (графическом) виде. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:

- дата и время выдачи (обращения к подсистеме вывода);
- спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

3) должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный);
- полная спецификация соответствующего файла «образа» программы (процесса, задания) - устройство (том, каталог), имя файла (расширение);

4) должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;

O‘zstandart agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

5) должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, каналам (линиям) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

6) должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:

- дата и время изменения полномочий и статуса;
- идентификатор субъекта доступа (администратора), осуществившего изменения;
- идентификатор субъекта доступа, у которого изменены полномочия и вид изменений (пароль, код, профиль и т.п.);
- спецификация объекта, у которого изменен статус защиты, и вид изменения (код защиты, уровень конфиденциальности);

7) должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

8) должна формироваться отчетность статистических сведений подсистемы регистрации и учета, предназначенных для создания и формирования отчетов в виде удобном для отображения, в том числе для вывода на печатающие устройства по формам регламентированной отчетности, настройкам планового формирования и предоставления статистических отчетов в различных форматах (включая графические). Также должна быть предусмотрена защита от модификации. Круг субъектов доступа к данной системе должен быть ограничен;

9) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

MAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

10) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

11) должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

12) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация;

13) должна осуществляться надежная сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

13.3 Криптографическая подсистема:

- должно осуществляться шифрование всей информации ограниченного доступа, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на любые съемные носители данных (дискеты, компакт-диски, флеш-накопители, и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- должно осуществляться шифрование информации ограниченного доступа передаваемой по каналам связи, выходящим за пределы КЗ;

- должны использоваться разные криптографические ключи для шифрования информации, принадлежащей различным субъектам доступа (группам субъектов);

- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;

- должны использоваться сертифицированные средства криптографической защиты информации.

13.4 Подсистема обеспечения целостности:

1) должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется по имитовставкам (хэш значениям, по контрольным суммам), в соответствии с O‘z DSt 1106 или алгоритмами рекомендованными Уполномоченным органом, всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;

- целостность программной среды обеспечивается качеством приемки любых программных средств в АС;

2) должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических

O‘zbekiston Agentligi
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI

средств охраны и специального персонала, использование строгого пропускного режима, специального оборудования помещений АС;

3) должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

4) должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;

5) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности, а также автоматическое оперативное восстановление функций СЗИ НСД при сбоях;

6) должны использоваться сертифицированные средства защиты информации.

14 Определение класса АС

14.1 Организационные мероприятия в рамках СЗИ НСД в АС, обрабатывающих или хранящих информацию, отнесенную к государственным секретам, должны отвечать требованиям по обеспечению режима секретности проводимых работ.

14.2 При обработке или хранении в АС информации, не отнесенной к государственным секретам, в рамках СЗИ НСД организациям и предприятиям с различной формой собственностью, а также частным лицам рекомендуются следующие организационные мероприятия:

- выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;
- ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или суще-

MAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARI VA
JORIY ETISH BO'LIMI

ственно затрудняющими хищение СВТ, информационных носителей, а также НСД к СВТ и линиям связи;

- выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

- организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

- разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

- осуществление приемки СЗИ НСД в составе АС.

14.3 При разработке АС, предназначенной для обработки или хранения информации, отнесенной к государственным секретам и конфиденциальной информации, необходимо учитывая требования O‘z DSt 2815, O‘z DSt 2816 и O‘z DSt 2817 определить классы защищенности АС следующим образом:

- АС 1 группы, обрабатывающие информацию, отнесенную к государственным секретам с грифом «С», должны быть отнесены по уровню защищенности к классам не ниже 1В. В них должны использоваться СВТ не ниже 4 класса, имеющие сертификат соответствия по требованиям безопасности информации, межсетевые экраны по уровню защищенности от НСД 2 класса, программное обеспечение по 2 уровню контроля отсутствия в нем недекларированных возможностей;

- АС 1 группы, обрабатывающие информацию, отнесенную к государственным секретам с грифом «СС», должны быть отнесены по уровню защищенности к классам не ниже 1Б. В них должны использоваться СВТ не ниже 3 класса, имеющие сертификат соответствия по требованиям безопасности информации, межсетевые экраны по уровню защищенности от НСД 1 класса, программное обеспечение по 1 уровню контроля отсутствия в нем недекларированных возможностей;

- АС 2 и 3 групп обрабатывающие информацию, отнесенную к государственным секретам с грифом «СС» и «С» должны быть отнесены по уровню защищенности к классам не ниже 2А и 3А. В них должны использоваться СВТ не ниже 3 и 4 класса, соответственно, имеющие сертификаты соответствия по требованиям безопасности информации, межсетевые экраны по уровню защищенности от НСД 1 и 2 класса, программное обеспечение по 1 и 2 уровню контроля отсутствия в нем недекларированных возможностей соответственно;

- АС, обрабатывающие конфиденциальную информацию, составляющую служебные сведения, должны быть отнесены по уровню защищен-

O‘zbekiston standartlashtirish, davlat standartlashtirish, davlat nazoratini muvofiqlashtirish va axborot texnologiyalarini joriy etish boshqarmasi

ности к классам 3Б, 2Б и не ниже 1Г. В них должны использоваться СВТ не ниже 5 класса, межсетевые экраны по уровню защищенности от НСД 3 класса, программное обеспечение по 3 уровню контроля отсутствия в нем недекларированных возможностей;

- АС, обрабатывающие конфиденциальную информацию, составляющую персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д. В них должны использоваться СВТ не ниже 5 класса, межсетевые экраны по уровню защищенности от НСД 3 класса, программное обеспечение по 3 уровню контроля отсутствия в нем недекларированных возможностей;

- АС, обрабатывающие остальные виды сведений конфиденциального характера, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д, если по решению руководителя организации не предъявляются более высокие требования. В них должны использоваться СВТ не ниже 5 класса, межсетевые экраны по уровню защищенности от НСД 3 класса, программное обеспечение по 3 уровню контроля отсутствия в нем недекларированных возможностей.

14.4 Ранжирование по классам представлено на рисунке 1.

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Автоматизированные системы									
Третья группа			Вторая группа			Первая группа			
Однопользовательские			Многопользовательские						
			с равными полномочиями			с разными полномочиями			
Уровень конфиденциальности информации									
К	С	СС	К	С	СС	К	С	СС	
Классы защищенности									
3Б	3А		2Б	2А		1Д	1Г	1В	1Б	1А
Использовать сертифицированные СВТ не ниже класса									
5	4	3	5	4	3	5	4	3	2
Межсетевые экраны по уровню защищенности от НСД класса									
3	2	1	3	2	1	3	2	1	1
Программное обеспечение по уровню контроля отсутствия в нем недекларированных возможностей									
3	2	1	3	2	1	3	2	1	1

К - конфиденциальная информация
С - информация с грифом «Секретно»
СС - информация с грифом «Совершенно секретно»

Рисунок 1

УДК 004.056.53 ОКС 35.040 П 89

Ключевые слова: автоматизированная система, конфиденциальная информация, класс защищенности, подсистема, система защиты, информация, несанкционированный доступ

O‘ZBEKISTON AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Сотрудник Службы
национальной безопасности
Республики Узбекистан — Д. Мажидов
12.03.2014

Нормоконтроль — Л. Шаймарданова
11.03.2014

СОГЛАСОВАНО

Государственный комитет
связи, информатизации и
телекоммуникационных
технологий Республики
Узбекистан

письмо от 26.02.2014
№ 14-8/1125

O'zSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI