Соответствие требований класса 1Г РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»
функциональным требованиям из Задания по Безопасности Microsoft® Windows® XP Professional Service Pack 3.

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
1.	Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов	*FIA_ATD.1* Определение атрибутов пользователя **FIA_ATD.1.1** ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности: а) **идентификатор пользователя**;* б) принадлежность к группе; в) **аутентификационные данные**; г) имеющие отношение к безопасности роли; д) привилегии и права входа *FIA_SOS.1* Верификация секретов **FIA_SOS.1.1** ФБО должны предоставить механизм для верификации того, что секреты отвечают следующему: а) для каждой попытки использования механизма аутентификации **вероятность случайного доступа должна быть меньше, чем $2{,}5x10^{-14}$**; б) при неоднократных попытках использования механизма аутентификации в течение одной минуты **вероятность случайного доступа должна быть меньше, чем $2{,}5x10^{-14}$**; в) обратная связь при использовании механизма аутентификации не должна приводить к повышению вероятностей вышеупомянутых метрик. *FIA_UAU.2* Аутентификация до любых действий пользователя **FIA_UAU.2.1** ФБО должны требовать, чтобы **каждый пользователь был успешно аутентифицирован до разрешения любого действия**, выполняемого при посредничестве ФБО от имени этого пользователя. FIA_UID.1 Выбор момента идентификации FIA_UID.2 Идентификация до любых действий пользователя FIA_UID.2.1 ФБО должны требовать, чтобы **каждый пользователь был успешно идентифицирован до разрешения любого действия**, выполняемого при посредничестве ФБО от имени этого пользователя.	Требования РД являются подмножеством множества требований ЗБ
2.	Должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам	FDP_IFF.1.1 ФБО должны осуществлять [политику фильтрации информации], основанную на следующих типах атрибутов безопасности субъекта и информации: [а) атрибуты безопасности программы, функционирующей в среде ОО:	Должно быть реализовано в АС применением иных средств (типа персонального межсетевого экрана), либо с использованием организационных мероприятий.

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		имя программы; б) атрибуты безопасности внешней по отношению к ОО сущности ИТ: предполагаемый адрес; в) атрибуты безопасности информационного потока: предполагаемый адрес субъекта источника; протокол; номер порта].	
3.	Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам	FDP_ACC.1 Ограниченное управление доступом FDP_ACC.1.1 ФБО должны осуществлять политику дискреционного управления доступом для а) субъектов – процессов, действующих от имени пользователей; б) **именованных объектов** – рабочий стол (Desktop), событие (Event), пара событий (Event pair), порт завершение I/O) I/O Completion Port, задание (Job), ключ реестра (Key), мьютекс (Mutant), почтовый ящик (Mailslot), именованный канал (Named pipe), **каталог NTFS** (NTFS directory), **файл NTFS** (NTFS file), каталог объектов (Object Directory), порт LPC (LPC Port), принтер (Printer), **процесс** (Process), секция (Section), семафор (Semaphore), символьная ссылка (Symbolic Link), поток (Thread), таймер (Timer), маркеры (Tokens), **том** (Volume), объект «Window Station», и **объект службы каталогов** (Active Directory objects); в) всех операций между субъектами и объектами Зависимости: FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности (описание см. п.4)	Требования РД являются подмножеством множества требований ЗБ
4.	Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа	FDP_ACC.1 Ограниченное управление доступом FDP_ACC.1.1 ФБО должны осуществлять **политику дискреционного управления доступом** для а) **субъектов** – процессов, действующих от имени пользователей; б) **именованных объектов** – рабочий стол (Desktop), событие (Event), пара событий (Event pair), порт завершение I/O) I/O Completion Port, задание (Job), ключ реестра (Key), мьютекс (Mutant), почтовый ящик (Mailslot), именованный канал (Named pipe), каталог NTFS) NTFS directory, файл NTFS (NTFS file), каталог объектов (Object Directory), порт LPC (LPC Port), принтер (Printer), процесс (Process), секция (Section), семафор (Semaphore), символьная ссылка (Symbolic Link), поток (Thread), таймер (Timer), маркеры (Tokens), том (Volume), объект «Window Station», и объект службы каталогов (Active Directory objects); в) всех операций между субъектами и объектами. Зависимости: FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности FDP_ACF.1.1 ФБО должны осуществлять **политику**	Требования РД являются подмножеством множества требований ЗБ

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		дискреционного управления доступом к объектам, **основываясь на следующем**: а) ассоциированные с субъектом **идентификатор пользователя, принадлежность к группе (группам) и привилегии субъекта**; б) следующие, ассоциированные с объектом, **атрибуты управления доступом** • **владелец объекта**; • **список дискреционного управления доступом** (DACL), который может отсутствовать, быть пустым, либо содержать одну или более записей; каждая запись в DACL содержит: тип (разрешение или запрет); идентификатор пользователя или группы; право доступа к объекту; установлены следующие правила доступа по умолчанию: если DACL отсутствует, то к объекту разрешаются все виды доступа; если DACL в наличии, но не содержит записей, то к объекту запрещаются все виды доступа FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: **доступ к объекту разрешен, если, по крайней мере, выполняется одно из следующих условий**: а) **запись, содержащаяся в DACL, явно разрешает доступ пользователю, и доступ не был запрещен предыдущей записью, содержащейся в DACL;** **б) запись, содержащаяся в DACL, явно разрешает доступ группе, членом которой является субъект, и доступ не был запрещен предыдущей записью, содержащейся в DACL;** **в) список DACL отсутствует;** **г) субъект является владельцем объекта и может просматривать или модифицировать список DACL или субъект является владельцем и может создавать объект** FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: а) для следующих операций уполномоченный администратор может обойти правила, перечисленные в FDP_ACF.1.2: • запрос на смену владельца объекта; б) для следующих операций только уполномоченному администратору может быть предоставлен доступ и правила, определенные FDP_ACF.1.2, не применяются: • запрос на смену или модификацию аудита попыток доступа к объекту. FDP_ACF.1.4 ФБО должны явно отказывать в доступе	

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		субъектов к объектам, основываясь на следующих дополнительных правилах: **в доступе к объекту явно отказано, если выполняется, по крайней мере, одно из следующих условий:** **а) запись в списке DACL явно запрещает доступ для пользователя, и доступ не был разрешен предыдущей записью в DACL;** **б) запись в списке DACL явно запрещает доступ группе, членом которой является пользователь, и доступ не был предоставлен предыдущей записью в DACL** Зависимости: FDP_ACC.1 Ограниченное управление доступом (описание см. п.3) FMT_MSA.3 Инициализация статических атрибутов (описание см. п.5.1.4 ЗБ)	
5.	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	FAU_GEN.1 Генерация данных аудита FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту: а) запуск и завершение выполнения функций аудита; б) следующих типов событий, потенциально подвергаемых аудиту: чтение информации из записей аудита; неуспешные попытки чтения информации из записей аудита; предпринимаемые действия при сбое хранения журнала аудита; все запросы на выполнение операций с объектом, на который распространяется ПФБ; **блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему**; **отклонение или принятие ФБО любого проверенного секрета**; **все случаи использования механизма аутентификации**; **все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя**; успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта); все модификации политики аудита; все модификации значений атрибутов безопасности; модификации настройки по умолчанию разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности; все модификации значений данных ФБО; попытка использовать привилегию уполномоченного администратора для изменения представления времени для ФБО; все модификации ограничений данных ФБО. Все модификации действий, предпринимаемых при нарушениях ограничений;	Требования РД являются подмножеством множества требований ЗБ

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		все попытки отменить атрибуты безопасности; модификация группы пользователей – исполнителей роли. Каждое использование прав, предоставляемых ролью; выполнение тестирования базовой машины и результаты тестирования; изменения внутреннего представления времени; выполнение и результаты самотестирования ФБО; все попытки разблокирования интерактивного сеанса; все попытки открытия сеанса пользователя; **попытки аутентификации и разблокирования**; FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию: а) **дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный)**. Зависимости: FPT_STM.1 Надежные метки времени FAU_GEN.2 Ассоциация идентификатора пользователя FAU_GEN.2.1 **ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события**. Зависимости: FAU_GEN.1 Генерация данных аудита FIA_UID.1 Выбор момента идентификации	
6.	Должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. 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	Функции безопасности ОО «Аудит безопасности» удовлетворяют следующим функциональным требованиям безопасности: – FAU_GEN.1 – ОО обеспечивает генерацию данных аудита для всех категорий событий, представленных в таблице 6.4 (см. п.6.1.1.1 ЗБ) Для каждого события аудита ФБО регистрируют **дату, время, идентификатор пользователя или его имя, идентификатор события, источник, тип и категорию события**; – FAU_GEN.2 – все записи аудита включают идентификатор безопасности пользователя, уникально идентифицирующий пользователя; – FAU_SAR.1 – инструментальные средства просмотра событий предоставляют администратору ОО возможность просмотра данных аудита в удобочитаемом формате; – FAU_SAR.2 и FMT_MTD.1(1) – **только администратору ОО предоставлены все виды доступа к журналу аудита**; – FAU_SAR.3 – ОО обеспечивает возможность выбора для заданной категории типа событий, подвергаемых аудиту («Аудит успехов» или «Аудит отказов»). Для	Может быть реализовано в АС применением иных средств, либо с использованием организационных мероприятий.

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		категории событий доступа к объекту критерием выбора может являться идентификатор пользователя. ФБО определяют перечень подвергаемых аудиту событий на основе текущей конфигурации политики аудита и параметров, определяемых через списки назначений аудита. Инструментальные средство просмотра событий аудита предоставляют возможность выполнения поиска и фильтрации данных аудита по дате, времени, идентификатору безопасности и имени пользователя, имени компьютера, коду, источнику, типу и категории события; – FAU_SEL.1 – ФБО предоставляют возможность включать события, потенциально подвергаемые аудиту, в совокупность событий, подвергающихся аудиту.	
7.	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)	FAU_GEN.1 Генерация данных аудита FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту: а) запуск и завершение выполнения функций аудита; б) следующих типов событий, потенциально подвергаемых аудиту: – чтение информации из записей аудита; – неуспешные попытки чтения информации из записей аудита; – предпринимаемые действия при сбое хранения журнала аудита; – все запросы на выполнение операций с объектом, на который распространяется ПФБ; – блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему; – отклонение или принятие ФБО любого проверенного секрета; – все случаи использования механизма аутентификации; – все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя; – успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта); – все модификации политики аудита; – все модификации значений атрибутов безопасности; – модификации настройки по умолчанию разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности; – все модификации значений данных ФБО;	Требования РД являются подмножеством множества требований ЗБ

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.ЗБ	Примечание
		– попытка использовать привилегию уполномоченного администратора для изменения представления времени для ФБО; – все модификации ограничений данных ФБО. Все модификации действий, предпринимаемых при нарушениях ограничений; – все попытки отменить атрибуты безопасности; – модификация группы пользователей – исполнителей роли. Каждое использование прав, предоставляемых ролью; – выполнение тестирования базовой машины и результаты тестирования; – изменения внутреннего представления времени; – выполнение и результаты самотестирования ФБО; – все попытки разблокирования интерактивного сеанса; – все попытки открытия сеанса пользователя; – попытки аутентификации и разблокирования; FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию: а) **дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный**). Зависимости: FPT_STM.1 Надежные метки времени FAU_GEN.2 Ассоциация идентификатора пользователя FAU_GEN.2.1 **ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события**. Зависимости: FAU_GEN.1 Генерация данных аудита FIA_UID.1 Выбор момента идентификации	
8.	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	FAU_GEN.1 Генерация данных аудита FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту: а) запуск и завершение выполнения функций аудита; б) следующих типов событий, потенциально подвергаемых аудиту: – чтение информации из записей аудита; – неуспешные попытки чтения информации из записей аудита; – предпринимаемые действия при сбое хранения журнала аудита; – **все запросы на выполнение операций с объектом, на который распространяется ПФБ;** – блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему; – отклонение или принятие ФБО любого проверенного	Требования РД являются подмножеством множества требований ЗБ

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		секрета; – все случаи использования механизма аутентификации; – все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя; – успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта); – все модификации политики аудита; – все модификации значений атрибутов безопасности; – модификации настройки по умолчанию разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности; – все модификации значений данных ФБО; – попытка использовать привилегию уполномоченного администратора для изменения представления времени для ФБО; – все модификации ограничений данных ФБО. Все модификации действий, предпринимаемых при нарушениях ограничений; – все попытки отменить атрибуты безопасности; – модификация группы пользователей – исполнителей роли. Каждое использование прав, предоставляемых ролью; – выполнение тестирования базовой машины и результаты тестирования; – изменения внутреннего представления времени; – выполнение и результаты самотестирования ФБО; – все попытки разблокирования интерактивного сеанса; – все попытки открытия сеанса пользователя; – попытки аутентификации и разблокирования; FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию: а) **дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный**). Зависимости: FPT_STM.1 Надежные метки времени FAU_GEN.2 Ассоциация идентификатора пользователя FAU_GEN.2.1 **ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события**. Зависимости: FAU_GEN.1 Генерация данных аудита FIA_UID.1 Выбор момента идентификации	
9.	Должна осуществляться регистрация попыток доступа программных средств к следующим	FAU_GEN.1 Генерация данных аудита FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально	Требования РД являются подмножеством множества требований ЗБ

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
	дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) 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)]	подвергаемых аудиту: а) запуск и завершение выполнения функций аудита; б) следующих типов событий, потенциально подвергаемых аудиту: – чтение информации из записей аудита; – неуспешные попытки чтения информации из записей аудита; – предпринимаемые действия при сбое хранения журнала аудита; – **все запросы на выполнение операций с объектом, на который распространяется ПФБ;** – блокирование учетной записи в результате превышения максимального числа неуспешных попыток входа в систему; – отклонение или принятие ФБО любого проверенного секрета; – все случаи использования механизма аутентификации; – все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя; – успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта); – все модификации политики аудита; – все модификации значений атрибутов безопасности; – модификации настройки по умолчанию разрешающих или ограничительных правил. Все модификации начальных значений атрибутов безопасности; – все модификации значений данных ФБО; – попытка использовать привилегию уполномоченного администратора для изменения представления времени для ФБО; – все модификации ограничений данных ФБО. Все модификации действий, предпринимаемых при нарушениях ограничений; – все попытки отменить атрибуты безопасности; – модификация группы пользователей – исполнителей роли. Каждое использование прав, предоставляемых ролью; – выполнение тестирования базовой машины и результаты тестирования; – изменения внутреннего представления времени; – выполнение и результаты самотестирования ФБО; – все попытки разблокирования интерактивного сеанса; – все попытки открытия сеанса пользователя; – попытки аутентификации и разблокирования;	

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию: а) **дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный**). Зависимости: FPT_STM.1 Надежные метки времени FAU_GEN.2 Ассоциация идентификатора пользователя FAU_GEN.2.1 **ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события**. Зависимости: FAU_GEN.1 Генерация данных аудита FIA_UID.1 Выбор момента идентификации	
10.	Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку)		Должно быть реализовано в АС применением иных средств, либо с использованием организационных мероприятий.
11.	Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема)		Должно быть реализовано в АС применением иных средств, либо с использованием организационных мероприятий.
12.	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)	FDP_RIP.2 Полная защита остаточной информации FDP_RIP.2.1 **ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при распределении ресурсов для всех объектов**. Зависимости: отсутствуют. Замечание по применению: В случае, когда субъект является предметом операций (например, при установлении связи между процессами), над субъектом производятся действия аналогичные как над объектом, т.е. обеспечение недоступности информационного содержания при распределении, и процессы в таком случае выступают в роли объектов.	Требования РД являются подмножеством множества требований ЗБ
13.	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	FPT_TST.1 Тестирование ФБО FPT_TST.1.1 **ФБО должны выполнять пакет программ самотестирования при запуске и периодически в процессе нормального функционирования для демонстрации правильного выполнения ФБО.** FPT_TST.1.2 **ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО**.	Требования РД являются подмножеством множества требований ЗБ

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
	трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации	FPT_TST.1.3 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность хранимого выполняемого кода ФБО. Зависимости: FPT_AMT.1 Тестирование абстрактной машины	
14.	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	В ЗБ предъявляются требования к среде функционирования объекта оценки. (подробнее см. п.3.1.2 ЗБ) В частности: **A.Locate** Для предотвращения несанкционированного физического доступа вычислительные ресурсы, используемые ОО, должны располагаться в контролируемой зоне. **A.Protect** Критичное с точки зрения обеспечения безопасности аппаратное обеспечение, на базе которого функционирует ОО, и программное обеспечение ОО должно быть защищено от несанкционированной физической модификации.	Требования РД являются подмножеством множества требований ЗБ
15.	Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД	FPT_TST.1 Тестирование ФБО FPT_TST.1.1 **ФБО должны выполнять пакет программ самотестирования при запуске и периодически в процессе нормального функционирования для демонстрации правильного выполнения ФБО.** FPT_TST.1.2 **ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО**. FPT_TST.1.3 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность хранимого выполняемого кода ФБО. Зависимости: FPT_AMT.1 Тестирование абстрактной машины FPT_AMT.1 Тестирование абстрактной машины FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ при первоначальном запуске, периодически во время нормального функционирования, по запросу уполномоченного пользователя для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая является базовой для ФБО. Зависимости: отсутствуют.	Дополнительно в ЗБ предъявляются требования к среде функционирования объекта оценки (ОО). В частности: **A.Coop** Уполномоченные для доступа к ОО пользователи должны пройти проверку на благонадежность, их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей. **A.Manage** Управление безопасным функционированием ОО должны осуществлять лица, прошедшие проверку на компетентность. **A.No_Evil_Adm** Персонал, ответственный за выполнение администрирования ОО, должен пройти проверку на благонадежность и в своей деятельности должен

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
			руководствоваться соответствующей документацией.
16.	Должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности	Среди основных функциональных возможностей обеспечения функционирования приведённых в ЗБ приведены следующие: **Теневое копирование тома** Управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей. **Откат драйверов** Данная возможность способствует обеспечению устойчивости системы. При обновлении драйвера копия предыдущего пакета драйверов автоматически сохраняется в специальном подкаталоге системных файлов (для каждого архивируемого драйвера добавляется новое значение к ключам архивации, размещенным в соответствующем разделе реестра). Если новый драйвер будет работать неудовлетворительно, пользователь может восстановить предыдущую версию драйвера, перейдя в «Диспетчере устройств» на вкладку Driver (Драйвер) для соответствующего устройства и нажав кнопку Roll Back Driver (Откатить). Откат драйвера разрешается производить для одного уровня отката, поскольку только одна версия предыдущего драйвера может сохраняться при выполнении обновления. Данная возможность доступна для всех классов устройств, за исключением принтеров. **Восстановление системы** Функциональная возможность восстановления системы позволяет возвращать компьютер в то состояние, в котором он находился до возникновения проблемы. При этом не происходит потери личных файлов данных, которые могут содержать, например, документы, изображения или сообщения электронной почты. При использовании данной возможности осуществляется активный мониторинг изменений системных характеристик и некоторых файлов приложений, а также автоматическое создание легко идентифицируемых контрольных точек восстановления. В Microsoft® Windows® XP Professional Service Pack 3 создание контрольных	Так же может быть реализовано в АС применением иных средств, либо с использованием организационных мероприятий.

№	Требования класса 1Г РД «АС. Защита от НСД к информации. Классификация АС и требования по ЗИ»	Функциональные требования из Задания по Безопасности MS.WIN_XP_SP3.3Б	Примечание
		точек восстановления производится по умолчанию каждый день, а также при значительных изменениях характеристик системы, таких, например, как установка приложения или драйвера. Пользователь также имеет возможность в любое время самостоятельно создать собственные контрольные точки восстановления. При использовании функции восстановления системы мониторинг изменений и восстановление файлов с личными данными не производится. **Аварийное восстановление системы** Функция аварийного восстановления системы (ASR – Automated System Recovery) позволяет сохранять и восстанавливать приложения. Эта функция обеспечивает реализацию механизма технологии Plug and Play, который используется для архивации соответствующих разделов реестра и восстановления данной информации в реестре. Применение этой функциональной возможности целесообразно в различных сценариях восстановления системы после возникновения аварийной ситуации; например, в случае сбоя жесткого диска и потери всех конфигурационных параметров и информации функция ASR может быть использована для восстановления архивированных серверных данных.	

***-**жирным шрифтом выделены функциональные требования из Задания безопасности , которые непосредственно относятся к соответствующим требованиям РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
Обычным шрифтом набраны требования из Задания безопасности, которые в РД не предъявляются, тем не менее проверявшиеся в процессе сертификационных испытаний.