СРАВНЕНИЕ СЕРТИФИЦИРОВАННЫХ СЗИ ОТ НСД ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. Основания для сравнительного анализа

Сравнению подлежат: КСЗИ «Панцирь+», СЗИ от НСД, сертифицированная по 5 классу СВТ, СЗИ от НСД, сертифицированная по 3 классу СВТ, МЭ, сертифицированный по 3 классу (поскольку в состав КСЗИ «Панцирь+» входит МЭ, сертифицированный по 4 классу, функции которого существенно расширены соответствующими возможностями, в отношении которых проведены сертификационные испытания).

Легитимными механизмами защиты в сертифицированных СЗИ от НСД, которые могут учитываться и легитимно использоваться при реализации защиты информационных систем, поскольку корректность их реализации проверена при проведении испытаний, в частности систем защиты ПДн, являются исключительно сертифицированные (проверенные при сертификации СЗИ от НСД) механизмы защиты из состава СЗИ от НСД.

Сертификация СЗИ от НСД ФСТЭК России может быть проведена на соответствие требованиям следующих документов (по отдельности, либо по их какой-либо совокупности):

- руководящие документы Гостехкомиссии России по защите от несанкционированного доступа к информации (прежде всего, это СВТ или МЭ),
- руководящий документ Гостехкомиссии России по контролю отсутствия недекларированных возможностей,
- техническое условие - ТУ,
- задание по безопасности – ЗБ (по требованиям ГОСТ ИСО/МЭК 15408-2002).

В данных документах однозначно определен (определяется для ТУ и ЗБ) набор сертифицируемых механизмов защиты и требования к ним, выполнение которых проверяется при сертификации СЗИ от НСД, что делает их легитимным для последующего использования. **Набор легитимных для использования механизмов защиты** из состава СЗИ от НСД **и реализуемые ими функции защиты однозначно определяется сертификатом**, выданным на систему защиты ФСТЭК России, **в котором указывается на соответствие требованиям каких документов проведены сертификационные испытания**, требования же к механизмам защиты (те требования, выполнение которых проверяется при испытаниях) определены в данных документах.

Так как руководящие документы регламентируют решение далеко не всех актуальных сегодня задач защиты информации, на практике для сертификации механизмов защиты, требования к которым не определены в соответствующих руководящих документах ФСТЭК России, либо в СЗИ от НСД реализуются дополнительные требования к этим механизмам защиты, дополнительно разрабатываются ТУ или ЗБ, в которых определяется набор реализуемых в СЗИ от НСД механизмов защиты информации и требования к их реализации. В случае, если данные **механизмы защиты проверены на соответствие ТУ или ЗБ** при сертификационных испытаниях, что делает их легитимными для последующего использования при реализации защиты информационных систем, **в сертификате на СЗИ от НСД это указывается в явном виде**.

КСЗИ «Панцирь+». Сертификат № 3473 от 17.12.2015 г. - сертифицирована ФСТЭК России на соответствие 4 уровню контроля отсутствия НДВ, 5 классу защищенности по РД для СВТ, 4 классу защищенности по РД для МЭ, на соответствие требованиям технических условий ТУ 50 14107-021-53262993-2014.

Замечание. МЭ входит в состав КСЗИ «Панцирь+» (сертифицирован в составе КСЗИ «Панцирь+»).

Замечание. Все механизмы защиты из состава КСЗИ «Панцирь+» прошли проверку – сертифицированы, большая часть на соответствие ТУ.

Методика сравнения. Сравнение не предполагает оценку эффективности реализации того или иного механизма защиты в той или иной СЗИ от НСД – сравнение осуществляется исключительно по формальному признаку, если требование к механизму защиты и к его реализации в документах, на соответствие которым проведена сертификация СЗИ от НСД, присутствует, считается что он реализован в СЗИ от НСД, причем именно в соответствии с требованиями к этому механизму защиты, сформулированными в документе, используемом при проведении сертификационных испытаний. Если механизм защиты реализован в СЗИ от НСД, но в отношении него не проведены сертификационные испытания, данный механизм защиты считается отсутствующим в СЗИ от НСД.

2. Сводная таблица сертифицированных механизмов защиты в составе сравниваемых СЗИ от НСД

Сертифицированный механизм защиты	**СЗИ от НСД, сертифицированная по 5 классу СВТ**	**СЗИ от НСД, сертифицированная по 3 классу МЭ**	**КСЗИ «Панцирь+»**	**СЗИ от НСД, сертифицированная по 3 классу СВТ**
Механизмы защиты, сертифицированные на соответствие РД СВТ 5 класса				
Идентификация и аутентификация пользователя при входе в систему	+	-	+	+
Дискреционный контроль доступа пользователей к файловым объектам	+	-	+	+
Очистка памяти. При первоначальном назначении или при перераспределении внешней памяти средство защиты должно предотвращать доступ субъекту к остаточной информации.	+	-	+	+
Целостность СЗИ от НСД. Должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части средства защиты	+	-	+	+

Регистрация событий безопасности. Средство защиты должно быть в состоянии осуществлять регистрацию следующих событий: - использование идентификационного и аутентификационного механизма; - использование механизма дискреционного контроля доступа пользователей к файловым объектам: запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.), создание и уничтожение объекта, действия по изменению ПРД.	+	-	+	+
Механизмы защиты, сертифицированные на соответствие РД СВТ 3 класса в дополнение к СВТ 5 класса				
Мандатный контроль доступа пользователей к файловым объектам	-	-	-	+
Очистка памяти. В дополнение к требованиям к СВТ 5 класса защищенности средство защиты должно осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей	-	-	-	+

информации в память при ее освобождении (перераспределении).				
Маркировка документов. При выводе защищаемой информации на документ в начале и конце проставляют штамп N 1 и заполняют его реквизиты в соответствии с Инструкцией N 0126-87 (п. 577).	-	-	-	+
Защита ввода и вывода на отчуждаемый физический носитель информации. Средство защиты должно различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (вывода на "помеченное" устройство) должно обеспечиваться соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с "помеченным"	-	-	-	+

каналом связи.				
Сопоставление пользователя с устройством. Средство защиты должно обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).	-	-	-	+
Целостность СЗИ от НСД. В дополнение к требованиям к СВТ 5 класса защищенности средство защиты должно осуществлять периодический контроль за целостностью СЗИ от НСД.	-	-	-	+
В дополнение к требованиям к СВТ 5 класса защищенности должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).	-	-	-	+
Механизмы защиты, сертифицированные на соответствие РД МЭ 4 класса				
Управление доступом. МЭ должен обеспечивать фильтрацию на сетевом уровне. Решение по	-	+	+	-

фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. МЭ должен обеспечивать: - фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств; - фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов; - фильтрацию с учетом любых значимых полей сетевых пакетов.				
Администрирование: идентификация и аутентификация. МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного	-	+	+	-

действия.				
Администрирование: регистрация. МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ.	-	+	+	-
Целостность. МЭ должен содержать средства контроля за целостностью своей программной и информационной части.	-	+	+	-
Восстановление. МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.	-	+	+	-
Регистрация. МЭ должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.	-	+	+	-

Механизмы защиты, сертифицированные на соответствие РД МЭ 3 класса в дополнение к МЭ 4 класса				
Управление доступом. В дополнение к требованиям к МЭ 4 класса МЭ должен обеспечивать: - фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя; - фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя; - фильтрацию с учетом даты/времени.	-	+	-	-
Администрирование: идентификация и аутентификация. В дополнение к требованиям к МЭ 4 класса должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась. При удаленных запросах администратора	-	+	-	-

МЭ на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.				
Администрирование: регистрация. В дополнение к требованиям к МЭ 4 класса МЭ должен обеспечивать регистрацию действия администратора МЭ по изменению правил фильтрации.	-	+	-	-
Администрирование: простота использования. Многокомпонентный МЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.	-	+	-	-
Целостность. В дополнение к требованиям к МЭ 4 класса МЭ должен обеспечиваться контроль целостности программной и	-	+	-	-

информационной части МЭ по контрольным суммам.				
Регистрация. В дополнение к требованиям к МЭ 4 класса МЭ должен обеспечивать: - регистрацию и учет запросов на установление виртуальных соединений; - локальную сигнализацию попыток нарушения правил фильтрации.	-	+	-	-

Механизмы защиты, дополнительно сертифицированные в КСЗИ «Панцирь+» по ТУ (дословно из текста ТУ 50 14107-021-53262993-2014).

Требования к КСЗИ в ТУ сформулированы в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17, Приказом ФСТЭК России от 18 февраля 2013 г. № 21 и Методическим документом «Меры защиты информации в государственных информационных системах» (Утвержден ФСТЭК России 11 февраля 2014 г.).

1.Идентификация и аутентификация субъектов и объектов доступа

1. В КСЗИ должна быть реализована идентификация и аутентификация пользователя при запросах на доступ к системе (на вход в систему) при удаленном входе в систему (по RDP и в терминальном режиме). В КСЗИ, как при локальном, так и при удаленном входе в систему должна быть реализована как консольная идентификация и аутентификация пользователя, так и аутентификация пользователя с использованием устройств хранения и ввода паролей (ruToken, Aladdin eToken – в форматах ключа и смарт-карты). [ИАФ.1 в части доступа в информационную систему, Усиление ИАФ.1 – 1б, 2б, 3, 4, 5, 6]
2. В КСЗИ объекты доступа (наименованные и создаваемые объекты) при задании ПРД должны идентифицироваться их именами (идентификаторами) и масками, внешние накопители - идентификаторами устройств, включая серийные номера для конкретных устройств. [ИАФ.7, ИАФ.2]
3. В КСЗИ должно быть реализовано управление идентификаторами, в том числе создание, присвоение, уничтожение и блокирование через заданный администратором период времени идентификаторов пользователей (учетных записей) и устройств. [ИАФ.3]
4. В КСЗИ должны быть реализованы следующие возможности задания ограничений на параметры пароля: длина пароля; наличие букв в разных регистрах; наличие цифр; наличие символов, не являющихся буквами и цифрами; отсутствие цепочек символов, вводимых с клавиатуры. В КСЗИ должно быть реализовано ограничение максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки; блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на заданный промежуток времени. В КСЗИ должна быть реализована возможность автоматического генерирования пароля КСЗИ с заданием следующих ограничений: длина генерируемого пароля; алфавит генератора паролей. [ИАФ.4, Усиление ИАФ.4 – 1 (а-г)]
5. В КСЗИ должна быть реализована защита обратной связи «система - субъект

доступа» в процессе аутентификации. Вводимые символы пароля должны отображаться условным знаком «●». [ИАФ.5]

6. КСЗИ должна разрешать или запрещать вход пользователя в безопасном режиме.

7. В КСЗИ должна быть реализована идентификация и аутентификация пользователя при запросах на доступ к разделяемым ресурсам (к наименованным разделяемым в сети объектам удаленной системы). При этом должна быть реализована как консольная идентификация и аутентификация пользователя, так и аутентификация пользователя с использованием устройств хранения и ввода паролей.

8. При консольной аутентификации КСЗИ должна предоставляться возможность назначения пароля, как администратором, так и непосредственно пользователем.

2.Управление доступом субъектов доступа к объектам доступа

2.1. Контроль доступа наименованных субъектов к наименованным объектам

1. В КСЗИ в качестве наименованного субъекта доступа должна использоваться сущность «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)», где сущность «Полнопутевое имя процесса» должна использоваться для возможности задания различных ПРД для различных процессов (приложений), запускаемых одним и тем же пользователем.

В КСЗИ в качестве наименованных объектов доступа должны выступать:

- локальные и разделенные в сети файловые объекты – файлы, каталоги, подкаталоги, логические диски;
- внешние накопители и файловые объекты – файлы, каталоги, подкаталоги на внешних накопителях;
- объекты реестра ОС – ключи и ветви реестра;
- локальные и разделенные в сети принтеры;
- сетевые адаптеры и исходящие из них/поступающие на них фильтруемые локальным сетевым экраном в соответствии с заданными правилами сетевые пакеты;
- любые иные устройства, в том числе, как системные, так и внешние по отношению к системе.

КСЗИ должна обеспечивать назначение прав пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами.

В КСЗИ для предотвращения загрузки исполняемых объектов, включая исполняемые файлы программ, апплетов и скриптов, должен обеспечиваться контроль доступа по расширениям файлов, позволяющий предотвращать создание, удаление, переименование «из», переименование «в» файлы с заданными расширениями.

В КСЗИ для наименованного субъекта доступа «Процесс» должна контролироваться смена исходного идентификатора пользователя (идентификатора, которым запущен этот процесс) на эффективный идентификатор пользователя (идентификатор пользователя, от лица которого запрашивается доступ к объекту этим процессом при запросах доступа).

ПРД должны задавать разрешенные/запрещенные права процессов на смену идентификатора пользователя при запросах доступа. [УПД.2 в части реализации иных методов, Усиление УПД.2 – 1, 3, 4, УПД.5]

2. КСЗИ должна обеспечивать разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями). [УПД.4]

3. КСЗИ должна обеспечивать удаление пользователя через заданный период времени (создание временной учетной записи). [УПД.1, Усиление УПД.1 – 2]

4. КСЗИ должна осуществлять ограничение неуспешных попыток входа и блокировку

учетной записи пользователя при превышении пользователем ограничения заданного количества неуспешных попыток входа в информационную систему, как при консольной аутентификации, так и при аутентификации по электронному ключу. [УПД.6, Усиление УПД.6 – 1]

5. Должна обеспечиваться возможность блокирования доступа в систему при удалении из системы устройства ввода пароля или по запросу пользователя при консольной идентификации и аутентификации. [УПД.10]

6. В КСЗИ должен быть реализован контроль смены идентификатора пользователя при доступе к наименованным объектам в соответствии с заданными правилами.

2.2. Контроль доступа наименованных субъектов к не наименованным объектам

1. В КСЗИ для контроля и предотвращения доступа к данным на жестком диске и на внешних накопителях, как к не наименованным объектам (не как к объектам файловой системы) должен быть реализован контроль прямого доступа наименованных субъектов к дискам (к жесткому диску и к внешним накопителям) с возможностью задания правил разграничения прямого доступа к дискам. В качестве наименованного субъекта доступа должна использоваться сущность «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)». [УПД.2 в части реализации иных методов]

2.3. Контроль доступа наименованных субъектов к создаваемым объектам

1. КСЗИ должна позволять разграничивать права доступа наименованных субъектов к создаваемым в процессе функционирования системы файлам (файлам, используемым для хранения обрабатываемых данных) в NTFS на жестком диске на основе матрицы доступа, при этом объект доступа должен быть исключен из ПРД – правилами должно задаваться, какой субъект доступа, какие права доступа имеет к файлам, созданным иным субъектом доступа (все ПРД должны задаваться исключительно между субъектами доступа) – должны быть реализованы принципы контроля доступа не наименованных субъектов к наименованным файловым объектам, а между наименованными субъектами к создаваемым ими файловым объектам. [УПД.2 в части реализации иных методов, УПД.3]

2. КСЗИ должна позволять разграничивать права доступа на основе матрицы доступа наименованных субъектов к создаваемым файлам для предотвращения возможности их исполнения, как системными, так и интерактивными пользователями, что необходимо для защиты от запуска не санкционированных программ. [УПД.2 в части реализации иных методов]

3. КСЗИ должна позволять разграничивать права доступа на основе матрицы доступа наименованных субъектов к создаваемым в процессе функционирования системы данным в буфере обмена, при этом объект доступа должен быть исключен из ПРД – правилами должно задаваться, какой субъект доступа, какие права доступа имеет к данным, созданным в буфере обмена иным субъектом доступа (все ПРД должны задаваться исключительно между субъектами доступа). [УПД.2 в части реализации иных методов, УПД.3]

4. В КСЗИ должна быть реализована возможность разграничивать права доступа пользователей, определяемых при задании ПРД назначаемыми им метками безопасности, к создаваемым в процессе функционирования системы файлам (файлам, используемым для хранения обрабатываемой информации) в NTFS на жестком диске – правилами должно задаваться, какой субъект доступа, какие права доступа имеет к файлам, созданным иным субъектом доступа (все ПРД должны задаваться исключительно между субъектами доступа). В КСЗИ в случае контроля доступа на основе меток безопасности ПРД должны назначаться на основе арифметического сравнения меток безопасности, назначаемых пользователям (метки безопасности вручную администратором не назначаются). При этом метки безопасности автоматически наследуются от пользователей объектами доступа, создаваемыми в процессе работы пользователя. [УПД.2 в части реализации иных методов, УПД.3, Усиление УПД.3 – 1, УПД.12]

5. КСЗИ должна обеспечивать возможность одновременной непротиворечивой работы (по соответствующим настроенным ПРД) на основе матрицы доступа и на основе меток безопасности к создаваемым файлам. При этом запрошенный доступ субъекта к объекту должен КСЗИ разрешаться только в том случае, если он не противоречит ни ПРД с использованием меток безопасности, ни ПРД на основе матрицы доступа к создаваемым файлам. [УПД.2 в части реализации иных методов]

2.4. Контроль доступа в межсетевом экранировании

1. КСЗИ должна обеспечивать фильтрацию сетевых пакетов на транспортном уровне. При этом фильтрация должна осуществляться для транспортных протоколов TCP и UDP и должны учитываться транспортные адреса (номера TCP и UDP портов) отправителя и получателя. КСЗИ должна обеспечивать невозможность использования иных транспортных протоколов. [УПД.3]
2. КСЗИ должна обеспечивать фильтрацию сетевых пакетов на прикладном уровне - использование прикладных сервисов (протоколы HTTP, FTP, NETBT-SSN, SSL, POP3, IMAP4, SMTP). [УПД.3]
3. КСЗИ должна обеспечивать фильтрацию сетевых пакетов с учетом даты/времени.
4. Решение о возможности выдачи сетевого пакета из компьютера с соответствующего сетевого адаптера в сеть, соответственно, получения на компьютер в соответствующий сетевой адаптер пакета из сети должно приниматься КСЗИ на основании анализа соответствия запроса доступа наименованного субъекта «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)» заданным ПРД к сетевым объектам (сетевой адаптер, IP адрес или символьное имя, локальный и/или удалённый порт, служба).

3. Ограничение программной среды

1. КСЗИ должна обеспечивать управление запуском компонентов программного обеспечения, в том числе определение запускаемых компонентов, контроль за запуском компонентов программного обеспечения. В КСЗИ для ограничения программной среды заданием ПРД должен обеспечиваться контроль за запуском исполняемых файлов и обеспечиваться возможность исполнения файлов только из заданных каталогов (папок), с предотвращением возможности их несанкционированного удаления и/или модификации не администратором. [ОПС.1, Усиление ОПС.1 – 1, 2, 3, 5, 6]
2. КСЗИ должна обеспечивать управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов. В КСЗИ для возможности задания ПРД для каждой пары (субъект-объект) должна быть реализована возможность перенаправления запросов доступа к объектам файловой системы, используемая для разделения между наименованными субъектами не разделяемых системой и приложениями наименованных файловых объектов, в частности, каталогов временного хранения файлов. [ОПС.4]

4. Защита машинных носителей информации

1. КСЗИ должна обеспечивать управление доступом к машинным носителям информации. [ЗНИ.2]
2. КСЗИ должна обеспечивать контроль использования интерфейсов ввода (вывода). [ЗНИ.5]
3. КСЗИ должна обеспечивать контроль ввода (вывода) информации на машинные носители информации. [ЗНИ.6]
4. КСЗИ должна обеспечивать управление подключением (монтированием) к системе устройств (любых устройств, в том числе, как системных, так и внешних по отношению к системе), конкретных устройств - по их серийным номерам, по пользователям. [ЗНИ.7, Усиление ЗНИ.7 – 1, 2; Усиление УПД.2 – 2]
5. КСЗИ должна обеспечивать возможность задания правил монтирования к системе устройств по пользователям, в которых должно задаваться, при работе каких пользователей в системе (в том числе, одновременной работе каких пользователей), какие

устройства могут быть подключены (подключаться) к системе. При нарушении заданных правил монтирования устройств к системе, в результате смены (регистрации нового) пользователя, КСЗИ должна обеспечивать в качестве реакции автоматическое отключение (отмонтирование) от системы несанкционированных устройств.

5. Регистрация событий безопасности

1. В КСЗИ должна обеспечиваться регистрация всех событий (вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы; подключение машинных носителей информации и вывод информации на носители информации; запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации; попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, подключенным к АРМ; внешним устройствам; программам; томам; каталогам; файлам) и иным объектам доступа; попытки удаленного доступа), связанных с реализацией возможностей защиты, требования к которым описаны в п.2.2.3-2.2.6.

Для каждого из этих событий, по крайней мере, должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- удачно ли осуществилось событие (в частности, обслужен ли запрос на доступ или нет). [РСБ.1, РСБ.2, РСБ.3, Усиление РСБ.1 – 2, Усиление АНЗ.5 – 1, Усиление ЗНИ.5 – 1]

2. В КСЗИ должны быть реализованы два режима регистрации событий – оперативный и реального времени, для них правила регистрации должны настраиваться отдельно. Режим оперативной регистрации событий предполагает формирование журнала аудита на клиентской части КСЗИ с возможностью его получения администратором по запросу с серверной части КСЗИ (сервер безопасности). Режим регистрации событий в реальном времени предполагает немедленную (в реальном времени) передачу зарегистрированных событий (в том числе инцидентов) клиентской частью КСЗИ на сервер аудита с соответствующим отображением на нем в реальном времени зарегистрированных событий. Число серверов аудита, подключаемых к клиентской части КСЗИ не должно ограничиваться. [РСБ.1, РСБ.2, ИНЦ.3 в части информирования о возникновении инцидентов]

3. КСЗИ должна обеспечивать возможность удаленного просмотра и фильтрации журналов (в том числе по пользователям) регистрации событий с сервера безопасности, связанных с правилами разграничения доступа. [Усиление РСБ.2 – 2; Усиление РСБ.3 – 1, 2, 3; РСБ.8, Усиление РСБ.8 – 1]

4. КСЗИ должна обеспечивать ограничение максимального размера и количества копий журналов аудита. [РСБ.4 в части защиты от переполнения объема памяти]

5. КСЗИ должна обеспечивать защиту информации о событиях безопасности. При этом доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам. [РСБ.7]

6. КСЗИ должна обеспечивать возможность удаленного просмотра и фильтрации журналов регистрации событий с сервера безопасности, связанных с фильтрацией пакетов.

7. КСЗИ должна обеспечивать сохранение истории настроек КСЗИ. [УКФ.4]

6. Обеспечение целостности информационной системы и информации

1. В КСЗИ должен быть реализован синхронный (периодический) контроль целостности по расписанию файлов (в том числе, системных файлов, исполняемых файлов КСЗИ и файлов ее настройки, файлов, используемых для хранения обрабатываемой информации) и объектов реестра ОС, с возможностью автоматического восстановления из

предварительно созданных резервных копий их эталонных значений при несанкционированной модификации. [ОЦЛ.1, Усиление ОЦЛ.1 – 1, ОЦЛ.3]

2. В КСЗИ должен обеспечиваться контроль целостности файлов КСЗИ (исполняемых файлов КСЗИ и файлов ее настройки) и объектов реестра ОС, используемых КСЗИ, при загрузке системы, с возможностью автоматического восстановления из резервной копии эталонных значений контролируемых объектов КСЗИ. [ОЦЛ.1, Усиление ОЦЛ.1 – 1, ОЦЛ.3]

3. КСЗИ обеспечивает ограничение прав пользователей по вводу информации в определенные типы объектов доступа (объекты файловой системы, объекты прикладного и специального программного обеспечения) исходя из задач и полномочий, решаемых пользователем в информационной системе. [ОЦЛ.6]

7. Защита информационной системы, её средств и систем связи и передачи данных

1. В КСЗИ должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации. [ЗИС.1]

2. КСЗИ должна обеспечивать запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые подключены к АРМ. [ЗИС.5]

3. КСЗИ должна обеспечивать предотвращение несанкционированного использования технологий передачи речи в информационной системе для компьютера в целом или для отдельных пользователей, посредством реализации следующих возможностей: предотвращение запуска требуемого приложения, предотвращение подключения требуемых устройств, предотвращение взаимодействий через требуемые порты с учетом их номеров. [ЗИС.8]

4. КСЗИ должна обеспечивать предотвращение несанкционированного использования технологий передачи видеоинформации в информационной системе для компьютера в целом или для отдельных пользователей, посредством реализации следующих возможностей: предотвращение запуска требуемого приложения, предотвращение подключения требуемых устройств, предотвращение взаимодействий через требуемые порты с учетом их номеров. [ЗИС.9]

5. КСЗИ должна обеспечивать защиту архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации. [ЗИС.15]

6. КСЗИ должна обеспечивать загрузку и исполнение прикладного программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения. [ЗИС.18]

7. КСЗИ должна обеспечивать исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы. [ЗИС.21]

8. КСЗИ должна обеспечивать защиту периметра (логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями. [ЗИС.23]

9. КСЗИ должна осуществляться завершение сетевых соединений по их завершении или по истечению установленного таймаута неактивных соединений. [ЗИС.24]

8. Требования для очистки памяти.

8.1. Для очистки внешней памяти при удалении наименованных файловых объектов

1. В КСЗИ должно обеспечиваться гарантированное удаление наименованных объектов - файлов с возможностью задания шаблонов и числа проходов очистки различных для различных наименованных файловых объектов (файлов, каталогов). [ЗНИ.8, Усиление ЗНИ.8 – 3, 5г]

8.2. Для очистки внешней памяти при удалении создаваемых файловых объектов

1. КСЗИ должна предоставлять возможность гарантированного удаления создаваемых объектов – файлов с возможностью задания шаблонов и числа проходов очистки, идентифицируемых в правилах гарантированного удаления не именем файла (папки), а именем создавшего его субъекта доступа сущностью «Исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс (полнопутевое имя исполняемого файла процесса)», либо меткой безопасности создавшего его пользователя.

9. Требования к управлению процессами

1. КСЗИ должна обеспечивать синхронный (с заданным периодом) контроль запущенных в системе процессов (включая системные). При обнаружении несанкционированного процесса (не заданного администратором в качестве разрешенного для исполнения), в качестве реакции на обнаруженное событие, КСЗИ должна автоматически завершать неразрешенный для запуска процесс.
2. КСЗИ должна обеспечивать синхронный (с заданным периодом) контроль активности в системе обязательных процессов, назначаемых администратором. При обнаружении отсутствия активности обязательного процесса, в качестве реакции на обнаруженное событие, КСЗИ должна автоматически запускать обязательный процесс, с правами того пользователя, который будет задан администратором, включая права системы.
3. КСЗИ должна обеспечивать контроль запуска процессов (приложений) с временными ограничениями – параметры запуска для процессов (приложений) в формате дата/время, задаются администратором. КСЗИ должна обеспечивать возможность синхронного (с заданным периодом) контроля запущенных в системе процессов, для которых установлены ограничения по запуску в формате дата/время, в качестве реакции на обнаруженное несанкционированное событие (для процесса нарушены ограничения по запуску в формате дата/время), КСЗИ должна автоматически завершать неразрешенный для запуска процесс в соответствии с заданными правилами.

10. Требования к удаленному администрированию

1. КСЗИ должна обеспечивать удаленное администрирование - настройку всех механизмов защиты и сетевого экранирования клиентской части КСЗИ с серверной части КСЗИ (с сервера безопасности). Число серверов безопасности, подключаемых к клиентской части КСЗИ не должно ограничиваться, должны синхронизироваться настройки клиентской части, назначенные на серверных частях или локально.
2. Для запуска интерфейса сервера безопасности должна быть реализована парольная защита, предполагающая использование пароля условно-постоянного действия.
3. КСЗИ должна обеспечивать аудит реального времени заданных администратором контролируемых событий всех механизмов защиты и сетевого экранирования клиентской части КСЗИ на сервере аудита КСЗИ. Число серверов аудита, подключаемых к клиентской части КСЗИ не должно ограничиваться.
4. Для запуска интерфейса сервера аудита должна быть реализована парольная защита, предполагающая использование пароля условно-постоянного действия.