ИССЛЕДОВАНИЕ
«ПРИНЦИПИАЛЬНЫЕ ОТЛИЧИЯ КСЗИ «ПАНЦИРЬ+» ДЛЯ ОС MICROSOFTWINDOWS ОТ СЗИ НСД ИНЫХ ПРОИЗВОДИТЕЛЕЙ»

- В исследовании приводятся лишь ключевые отличия, определяющие область эффективного использования системы защиты информации КСЗИ «Панцирь+»;
- В исследовании приводится не сравнение с какой-либо конкретной СЗИ НСД, которые также, хоть и не сильно (по крайней мере, не принципиально), но различаются между собою в некоторых подходах к реализации, а общие отличия КСЗИ «Панцирь+»от остальных систем защиты информации;
- В исследовании приводятся только те механизмы защиты из состава КСЗИ «Панцирь+», реализация которых принципиально отличается от иных СЗИ НСД, при этом системы защиты информации не сравниваются набором реализованных в них механизмов защиты информации;
- В исследовании приводятся отличия КСЗИ «Панцирь+» от иных СЗИ НСД - не преимущества, а именно отличия. Насколько эти отличия являются преимуществами или недостатками КСЗИ «Панцирь+» для конкретного потребителя, зависит от решаемых им задач защиты информации.

Характеристика	Отличия КСЗИ «Панцирь+»	Примечания
Сертификация по требованиям информационной безопасности	Сертифицированы все механизмы защиты, включенные в состав КСЗИ.	Подавляющая часть реализованных в КСЗИ механизмов защиты сертифицирована на соответствие Техническим условиям, поскольку ими реализуются инновационные (в том числе, запатентованные) технические решения, требования к которым отсутствуют в современных Руководящих документах.
Функциональное назначение	КСЗИ предназначена для реализации ролевой или/и сессионной и процессной моделей контроля доступа. Реализация ролевой модели контроля доступа служит для формирования и разделения между собой режимов обработки информации пользователями в рамках выполнения ими функциональных обязанностей в информационной системе. Реализация сессионной модели контроля доступа служит для формирования и разделения между собой режимов обработки пользователями информации различных уровней конфиденциальности. Реализация процессной модели контроля доступа служит для формирования и разделения между собой режимов обработки информации процессами, запускаемыми с правами одного и того же пользователя, с целью защиты от актуальных угроз атак, направленных на наделение системных процессов и приложений вредоносными свойствами. Задачу защиты от актуальных угроз атак в данной постановке и реализованном подходе к решению, можно рассматривать и в качестве задачи защиты от вторжений в информационную	Под каждую роль (сессию) в КСЗИ создается свой режим обработки информации, что предполагает возможность разделения прав доступа между ролями (сессиями) к используемым в них ресурсам (требование к достаточности набора механизмов защиты). Роли и сессии в КСЗИ идентифицируются в разграничительной политики доступа учетными записями, поскольку это единственный корректный способ разделения между ними режимов обработки

	систему, по средством наделения системных процессов и приложений вредоносными свойствами, в том числе, за счет эксплуатации выявленных в них ошибок реализации (программирования).	информации. Ролевая модель расширена возможностью задания прав доступа для субъекта: пользователь, процесс (какой пользователь, каким процессом обращается к ресурсу) – субъект доступа в ролевой модели идентифицируется сущностью «профиль» (пользователь, процесс).
Концептуальные отличия в реализации механизмов защиты в составе КСЗИ	1. Права доступа в разграничительной политике назначаются субъектам доступа, а не присваиваются в качестве атрибутов объектам.	Это обусловливается собственно назначением КСЗИ – не реализация защиты отдельных объектов (в этом случае к ним разграничиваются права доступа), а реализация и разделение режимов обработки информации субъектами – при этом права доступа назначаются субъектам, а не к объектам. Это позволяет использовать маски и переменные среды окружения, как при задании субъектов (пользователь, процесс), так и при задании объектов доступа, что принципиально упрощает настройку механизмов защиты и позволяет реализовать ряд дополнительных важных задач защиты информации, например, полноценное разграничение прав доступа по типам файлов.
	2.Субъект доступа во всех механизмах защиты, используемых, как для реализации ролевой, так и для реализации процессной модели контроля доступа, идентифицируется единым образом – пользователь процесс, при этом при использовании соответствующих масок, можно разграничивать права доступа и только для пользователей, и только для процессов.	Ряд механизмов защиты, в зависимости от их настройки, могут использоваться для реализации и ролевой, и процессной моделей контроля доступа.
	3. Объекты доступа в КСЗИ разделены на статичные, присутствующие в системе на момент задания разграничительной политики доступа, и на создаваемые. К создаваемым относятся создаваемые пользователями файлы (включая конфигурационные) и данные, сохраняемые процессами в буфере обмена.Для них реализованы собственные механизмы защиты.	Механизмы контроля доступа к создаваемым объектам - это ключевые механизмы защиты для разделения режимов обработки информации в рамках реализации, как ролевой (сессионной), так и процессной моделей контроля доступа.
	4. Непривилегированный пользователь полностью исключен из реализации каких-либо функций защиты информации, все действия им могут осуществляться только в рамках реализованной администратором разграничительной политики доступа. Пользователь не может назначать права доступа к создаваемым им файлам, изменять права доступа любым образом к любому объекту, самостоятельно управлять гарантированным удалением файлов и т.д.	По результатам многих исследований именно легальный пользователь несет в себе в настоящее время доминирующую угрозу несанкционированного доступа к обрабатываемой информации.
Отличия в реализации отдельных механизмов защиты изсостава КСЗИ «Панцирь+»		
Управление монтированием устройств	1. Реализуется управление динамическим монтированием/отмонтированием устройств (включая для идентификации их серийные номера) по пользователям– по ролям	Это ключевой механизм защиты при реализации ролевой (сессионной) модели

	(по меткам безопасности при реализации сессионного контроля доступа). Позволяет формировать для каждой учетной записи – роли (сессии) разрешенный для ее работы набор устройств, в том числе тех устройств, права доступа к которым определяются одним правилом – разрешено, либо нет использование, например, сканеры. Реализуется самостоятельным механизмом защиты.	контроля доступа, позволяющий локализовать набор устройств (к которым уже в случае необходимости должны разграничиваться права доступа) для соответствующих режимов обработки информации – ролей (сессий).
	2.Реализуется управление монтированиемсистемных устройств.	Важность данной задачи защиты обусловливается наличием в современных компьютерах крайне критичных, с точки зрения безопасности, системных устройств, таких как микрофоны, видеокамеры и т.д., которые не допустимы к использованию в отдельных режимах (сессиях) обработки информации
Дискреционный контроль доступа к статичным файловым объектам	1. Контроль доступа к статичным (присутствующим в системе на момент задания администратором правил доступа)– локальным и к разделенным в сети файловым объектам, к файловым объектам на внешних накопителях. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту, при создании и субъектов, и объектов доступа в разграничительной политике могут использоваться маски и переменные среды окружения. Объектами, к которым разграничиваются права доступа, в соответствии с приоритетом обработки правил доступа, являются: файл, маска файла, каталог, маска каталога, маска. В интерфейсе механизма защиты в одном окне отображаются все правила доступа, заданные администратором для субъекта доступа. Существенно расширяется возможность реализации замкнутости программной среды, т.к. для любого процесса, включая системный, можно разрешить фиксированный набор запускаемых им процессов. Реализуется самостоятельным механизмом защиты.	Данное реализованное в КСЗИ техническое решение запатентовано. Патенты на изобретения №2534599, №2534488. Второй патент на изобретение предполагает расширение субъекта доступа «пользователь» двумя сущностями – исходный (от лица которого запущен процесс) и эффективный (от лица которого процесс обращается к ресурсу) пользователи. Это, реализованное в КСЗИ техническое решение, позволяет контролировать (поводить аутентификацию) смены процессом учетной записи пользователя при доступе к ресурсам. Данные патенты распространяются на все технические решения, реализующие в КСЗИ дискреционный контроль доступа к разнородным статичным объектам, они реализованы единым образом.
	2. Контроль доступа к неразделяемым системой и приложениями файловым объектам. Реализуется созданием для каждого субъекта копии неразделяемого объекта, с последующим перенаправлением запроса от субъекта к созданной для него копии объекта. Данный механизм защиты обеспечивает корректность реализации разграничительной политики доступа к файловым объектам. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту. Реализуется самостоятельным механизмом защиты.	Данное реализованное в КСЗИ техническое решение запатентовано. Патент на изобретение№2538918.
Дискреционный контроль доступа к типам файлов	Типы файлов, к которым контролируется доступ субъектов, идентифицируютсяв КСЗИ их расширениями. Данный механизм защиты реализуется механизмом дискреционного контроля	Механизм защиты реализуется корректно (может решать соответствующие

	доступа к статичным файловым объектам при задании объекта доступа маской «*.расширение». Может использоваться для разграничений того, какие типы файлов, какими субъектами и в каких объектах (в том числе, на внешних накопителях) могут создаваться, какими типами файлов какие субъекты могут обмениваться и т.д. Может использоваться для предотвращения занесения на защищаемый компьютер вредоносных исполняемых и командных файлов, в частности, для предотвращения наделения вредоносными свойствами командных интерпретаторов, например, web-приложений. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту.	задачи защиты информации) при предотвращении не только переименований расширений контролируемых типов в иные, но и, наоборот, любых иных расширений в контролируемые разграничительной политикой доступа расширения файлов. Данное реализованное в КСЗИ техническое решение запатентовано. Патент на изобретение№2572385.
Дискреционный контроль доступа к создаваемым файлам	Разграничиваются не права доступа субъектов к объектам – файлам, а права доступа субъектов к файлам, создаваемым иными субъектами, какие бы (включая конфигурационные) и где бы, эти файлы не создавались на жестком диске. Данный механизм защиты при минимальной трудоемкости его настройки имеет множество практических приложений, например, запрет доступа (включая системных пользователей) к исполнению создаваемых в процессе работы вредоносных файлов (вредоносных программ, в том числе, эксплоитов, направленных на эксплуатацию выявленных ошибок реализации программных средств), изолирование обрабатываемых данных между различными субъектами доступа и т.д. Это основной механизм защиты для реализации разделения режимов обработки информации при реализации, как ролевой, так и процессной моделей контроля доступа. Субъектом доступа является сущность пользователь, процесс (профиль, здесь не используется, поскольку данный механизм защиты в равной мере может использоваться при реализации и ролевой, и процессной (где в качестве субъекта доступа выступает только процесс) моделей контроля доступа), права доступа назначаются субъекту. Реализуется самостоятельным механизмом защиты.	Реализация механизма защиты предполагает наследование создаваемым файлом учетных данных создающего его субъекта доступа (пользователь, процесс). Права доступа разграничиваются между субъектом доступа, создавшим файл, и впоследствии обращающимся к файлу субъектом. Контроль доступа реализуется анализом на соответствие заданным правилам доступа, по средством сравнения учетных данных субъекта, создавшего файл (унаследован этим файлом) и субъекта доступа, запрашивающего доступ к файлу. Данное реализованное в КСЗИ техническое решение запатентовано. Патенты на изобретения №2524566, №2543556 (второй патент на изобретение предполагает, как автоматическую разметку создаваемого файла при его создании/модификации, так и ручную разметку администратором статичного файла для использования этого механизма для контроля доступа к статичным файлам).
Мандатный контроль доступа к создаваемым файлам	Данный механизм защиты является основой реализации сессионной модели контроля доступа. Разграничиваются не права доступа субъектов к объектам– файлам (на основе присвоенных им мандатов – меток безопасности), а права доступа субъектов к файлам, создаваемым иными субъектами, какие бы (включая конфигурационные) и где бы, эти файлы не создавались на жестком диске, на основе присваиваемых субъектам доступа меток безопасности. Данный механизм защиты при минимальной трудоемкости его настройки (необходимо присваивать метки безопасности исключительно субъектам доступа) наиболее подходит для реализации и разделения режимов обработки конфиденциальной информации на основе меток безопасности (мандатов) по двум причинам, во-первых, при решении данной задачи защиты требуется контроль доступа к обрабатываемым данным, т.е. именно к создаваемым файлам, во-вторых, он позволяет реализовать корректную разграничительную политику	Реализация механизма защиты предполагает наследование создаваемым файлом метки безопасности (мандата) создающего его субъекта доступа (пользователь). Метки безопасности присваиваются администратором исключительно субъектам доступа.Права доступа разграничиваются между субъектом доступа, создавшим файл, и впоследствии обращающимся к файлу. Контроль доступа

	доступа в общем случае, т.к. размечаются непосредственно файлы, причем все файлы, создаваемые контролируемыми субъектами доступа. При настройке разграничительной политики доступа можно задать различные правила сравнения иерархических меток безопасности. Субъектом доступа является учетная запись (пользователь), которому присваивается метка безопасности. Реализуется самостоятельным механизмом защиты.	реализуется сравнением на соответствие заданному правилу мандатного доступа, метки безопасности субъекта, создавшего файл (унаследована этим файлом) и субъекта доступа, запрашивающего доступ к файлу. Данное реализованное в КСЗИ техническое решение запатентовано. Патенты на изобретения №2524566, №2543556 (второй патент на изобретение предполагает, как автоматическую разметку создаваемого файла при его создании, так и ручную разметку администратором статичного файла для использования этого механизма для мандатного контроля доступа к статичным файлам).
Дискреционный контроль доступа к внешним файловым накопителям	Реализуется механизмом дискреционного контроля доступа к статичным файловым объектам по полной аналогии с реализацией контроля доступа к файловым объектам. Внешние файловые накопители (монтируемые устройства) в разграничительной политике доступа идентифицируются серийными номерами устройств, прошиваемых аппаратно в устройстве их изготовителем. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту.	В общем случае возможны три способа идентификации внешнего файлового накопителя (монтируемого к системе устройства), определяемых тем, что за серийный номер используется для его идентификации (естественно, идентификацию устройства по букве диска, присваиваемой ему системой, не рассматриваем). Это идентификатор, создаваемый ОС и хранимый в реестре для последующего подключения одного и того же устройства к одной и той же букве диска, это уникальный номер тома, создаваемого на устройстве при его форматировании, и это серийный номер устройства, прошиваемый аппаратно в устройстве изготовителем. Естественно, что самый надежный и безопасный способ идентификации устройства – по серийным номерам устройства, прошиваемым аппаратно в устройстве изготовителем (поскольку поменять серийный номер может только изготовитель). Именно такое решение реализовано в КСЗИ. Эффективность же широко используемого на практике метода идентификации устройства по номеру тома, создаваемого на накопителе

		при его форматировании, определяется криптостойкостью используемого метода его преобразования, по сути, шифрования. Данное реализованное в КСЗИ техническое решение подпадает под патенты на изобретения №2534599, №2534488.
Дискреционный контроль прямого доступа к дискам	Реализуется по полной аналогии с реализацией дискреционного контроля доступа к статичным файловым объектам, позволяет разграничивать права доступа субъектов в части прямого, не как к файловым объектам, доступа к данным на жестком диске и на внешних файловых накопителях (монтируемых устройствах). Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту. Реализуется самостоятельным механизмом защиты.	Прямой доступ к диску крайне критичная возможность обхода разграничительной политики доступа к файловым объектам, позволяет обращаться к данным, записанным на жестком диске и на накопителях напрямую, не как к файловым объектам. Данной возможностью обладают не только специальные программы, но и ряд текстовых редакторов, при использовании в них соответствующих плагинов. Данное реализованное в КСЗИ техническое решение подпадает под патенты на изобретения №2534599, №2534488.
Дискреционный контроль доступа к сервисам олицетворения	Разграничиваются права доступа субъектов к сервисам олицетворения – к штатной возможности современных ОС, позволяющей процессу запросить у системы и получить от нее права иного пользователя, после чего осуществить доступ к ресурсам под другой учетной записью с нарушением разграничительной политики доступа. В том числе, предотвращается возможность получение процессом, запущенным с правами интерактивного пользователя, системных прав, а также прав привилегированных пользователей. Субъектом доступа является сущность процесс, права доступа назначаются субъекту – определяются правила для процесса (могут использоваться маски), с правами какого пользователя, он себя может олицетворить, с учетом того, с правами какого пользователя он запущен, при обращении к какому накопителю. Реализуется самостоятельным механизмом защиты.	Использование сервисов олицетворения - крайне критичная возможность обхода разграничительной политики доступа ко всем объектам, включая файловые. Данный механизм защиты позволяет реализовать множество дополнительных функций защиты при разграничении доступа к сервисам олицетворения для системных процессов. Например, если для процесса winlogon разрешить олицетворение из системного пользователя только с одним интерактивным пользователем (включая доменных), то только этот пользователь сможет войти в систему, соответствующим образом можно контролировать запуск программ с правами иного пользователя с использованием утилиты runas, и многое другое.
Дискреционный контроль доступа к буферу обмена	Разграничиваются не права доступа субъектов к объекту – к буферу обмена, а права доступа субъектов к данным, сохраняемым иными субъектами в буфере обмена. Данный	Данное реализованное в КСЗИ техническое решение подпадает под патент на

	механизм защиты предназначен для изолирования обрабатываемых данных между различными субъектами доступа, в первую очередь, между процессами. Наряду с дискреционным контролем доступа к создаваемым файлам, это основной механизм защиты для реализации разделения режимов обработки информации при реализации, как ролевой, так и процессной моделей контроля доступа. Субъектом доступа является сущность пользователь, процесс (профиль, здесь не используется, поскольку данный механизм защиты в равной мере может использоваться при реализации и ролевой, и процессной (где в качестве субъекта доступа выступает только процесс) моделей контроля доступа), права доступа назначаются субъекту. Реализуется самостоятельным механизмом защиты.	изобретения №2524566.
Дискреционный контроль доступа к объектам реестра ОС	Реализуется по полной аналогии с реализацией дискреционного контроля доступа к статичным файловым объектам, с поправкой на особенности объекта доступа (ключи и ветви реестра ОС) и назначаемых к ним прав доступа субъектов – чтение, запись. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту, могут использоваться маски для задания и субъектов, и объектов доступа. Реализуется самостоятельным механизмом защиты.	Это один из ключевых механизмов защиты информации от актуальных угроз атак, поскольку в объектах реестра ОС хранятся основные настройки ОС, приложений, системы защиты информации. Без разграничений доступа к объектам реестра ОС, особенно для критичных процессов - критичных, в части возможности наделения их вредоносными свойствами, о какой-либо эффективности защиты говорить не имеет смысла. Данное реализованное в КСЗИ техническое решение подпадает под патенты на изобретения №2534599, №2534488.
Контроль доступа к локальным и к разделенным в сети принтерам	Реализуется по полной аналогии с реализацией дискреционного контроля доступа к статичным файловым объектам, с поправкой на особенности объекта доступа (принтер) и назначаемых к нему прав доступа субъектов – разрешена печать субъекту доступа, либо нет. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с одинаковыми правами доступа к объектам), права доступа назначаются субъекту, при создании и субъектов, и объектов доступа в разграничительной политике могут использоваться маски. При реализации сессионной модели контроля доступа, права доступа к принтерам устанавливаются с учетом меток безопасности (мандатов), присвоенных пользователям. Реализуется самостоятельным механизмом защиты.	Данное реализованное в КСЗИ техническое решение подпадает под патенты на изобретения №2534599, №2534488.
Контроль доступа к сетевым объектам	1. Контроль доступа. Реализуется по полной аналогии с реализацией дискреционного контроля доступа к статичным файловым объектам, с поправкой на особенности объектов доступа (сетевые объекты) и назначаемых к ним прав доступа субъектов. В качестве сетевых объектов, применительно к которым разграничиваются права доступа субъектов, выступают: сетевые адаптеры, определяющие способы взаимодействия с внешней сетью – по проводному каналу, по Wi-Fi, с использованием соответствующих модемов и т.д., сетевые адреса и имена хостов (по исходящим и входящим соединениям), транспортные протоколы – номера портов, включая управление установлением соединений и отправкой/получением сообщений, сетевые службы, команды управляющих протоколов и т.д. Субъектом доступа является сущность пользователь, процесс (профиль, используемый для объединения субъектов с	Данное реализованное в КСЗИ техническое решение,подпадающее под патенты на изобретения №2534599, №2534488, в составе КСЗИ сертифицировано по требованиям информационной безопасности как межсетевой экран.

	одинаковыми правами доступа к объектам), права доступа назначаются субъекту. Реализуется самостоятельным механизмом защиты.	
	2. Фильтрация сетевых пакетов. Все исходящие и входящие сетевые пакеты фильтруются по значимым полям заголовков пакетов, что реализуется на уровне NDIS	
	3. Временное регламентирование прав доступа к сетевым объектам. Каждому субъекту можно задать дни недели, время, продолжительность по времени доступа к соответствующим сетевым объектам, к которым ему разграничиваются права доступа, что позволяет регламентировать работу пользователей с сетевыми объектами в рамках реализации ролевой (сессионной) моделей контроля доступа.	
Гарантированное удаление информации	1. Гарантированное удаление файлов. Реализуется КСЗИ автоматически (также может осуществляться вручную администратором, включая полную гарантированную очистку диска или внешнего накопителя). Задается число «проходов» (циклов) и шаблон очистки - кода перезаписи КСЗИ информации в файл перед его удалением системой. Возможны следующие настройки механизма гарантированного удаления: - Задание объектов (например, каталогов), в которых файлы будут гарантированно удаляться, либо непосредственно файлов; - Задание субъектов (при использовании дискреционного или мандатного методов контроля доступа к создаваемым файлам), файлы созданные которыми, включая конфигурационные, будут гарантированно удаляться. Субъектом доступа является сущность пользователь, процесс, либо метка безопасности. Реализуется самостоятельным механизмом защиты.	Гарантированное удаление данных в КСЗИ реализуется не только при удалении, но и при модификации файла, предполагающей уменьшение его объема. С учетом того, что файлы, объемом менее 1Кб, ОС сохраняются не файловой системе, в КСЗИ реализовано принудительное увеличение объема сохраняемых данных при создании файлов до размера в 1Кб.
	2. Гарантированное удаление остаточной информации в оперативной памяти. Удаление может проводиться на основании следующих правил – вход в систему, либо выход из системы определенного пользователя, запуск, либо завершение определенного процесса. Реализуется самостоятельным механизмом защиты.	При запуске процесса ОС выделяет ему для работы соответствующую область оперативной памяти, которую не зачищает при завершении работы процесса, выделяя ее далее (с соответствующей остаточной информацией) другому запускаемому в системе процессу.
Управление процессами	1. Контроль разрешенных процессов. Реализуется временное регламентирование работы системы и работы пользователей с приложениями в рамках реализации ролевой (сессионной) моделей контроля доступа. Каждому процессу, в том числе, сетевому, можно задать дни недели, время, продолжительность его работы. При нарушении регламента работы процесса, он не сможет быть запущен, а если уже был запущен ранее, то будет (при задании соответствующей реакции на нарушение) принудительно завершен КСЗИ. Реализуется самостоятельным механизмом защиты.	Это универсальное решение в части временного регламентирования работы системы и приложений. Заданием соответствующего временного ограничения для приложения, регламентируется работа с этим приложением. Заданием соответствующего регламента для системного процесса winlogon, определяется регламент работы с защищенным компьютером в целом. Задавая регламенты работы соответствующих системных процессов, можно регламентировать и работу с соответствующими устройствами.
	2. Контроль обязательных процессов. Реализуется защита от несанкционированного завершения в системе процесса, например, процесса какого-либо дополнительно используемого на защищаемом компьютере средства защиты или контроля, по	Несанкционированно завершенный процесс, в зависимости от задаваемых администратором правил,

	средством его принудительного перезапуска КСЗИ. Реализуется самостоятельным механизмом защиты.	может перезапускаться КСЗИ, как с правами интерактивного пользователя, так и с системными правами.
Аудит реального времени	С учетом назначения КСЗИ в части защиты от актуальных угроз атак, в том числе, защиты от вторжений, некоторые регистрируемые КСЗИ события аудита событий безопасности (правила аудита настраиваются администратором) могут удаленно предоставлять администратору в реальном времени на отдельный компонент системы защиты – сервер безопасности. Реализуется самостоятельным механизмом защиты.	В состав КСЗИ входят: клиентская часть, реализующая механизмы защитыи устанавливаемая на защищаемые компьютеры, сервер безопасности, позволяющий осуществлять удаленное администрирование клиентских частей, интерактивный (по запросу администратора) аудит событий, управление работой удаленных защищаемых компьютеров, и сервер аудита. Любая клиентская часть может подключаться к неограниченному числу серверов безопасности, что позволяет решать различные задачи резервирования и разделения нагрузки (в том числе, в части подключения особо важных защищаемых объектов) между серверами. Может быть реализована иерархия серверов безопасности с различными правилами администрирования и синхронизации настроек клиентских частей и серверов безопасности). Любая клиентская часть может подключаться к неограниченному числу серверов аудита. На сервер аудита, в соответствии с заданными администратором правилами, события аудита предоставляются от всех подключенных к нему клиентских частей в реальном времени (не по запросу администратора), где отображаются, либо в едином окне интерфейса, либо по отдельным клиентским частям. Совмещение в компоненте сервера аудита интерактивного аудита событий безопасности и аудита реального времени позволяет использовать сервер аудита в качестве отдельного компонента сетевой защиты информации. В общем случае при организации рабочего места

		(рабочих мест, число которых в одной сети не ограничивается) администратора (администраторов) безопасности, сервер безопасности и сервер аудита могут устанавливаться как на одном, так и на различных компьютерах, решая различные задачи.

Заключение

1. В исследовании представлены далеко не все механизмы защиты, реализованные в КСЗИ «Панцирь+», в частности, не рассмотрены механизм идентификации и аутентификации пользователя при локальном и удаленном входе в систему, механизмы контроля целостности (с возможностью восстановления) файловых объектов и объектов реестра ОС (контроль целостности объектов ОС, в том числе, позволяет контролировать неизменность аппаратной и программной конфигураций защищаемого компьютера) и некоторые другие. Рассмотрены лишь те механизмы защиты из состава КСЗИ, которые принципиально отличаются, как в части решаемых ими задач, так и в части реализуемых ими технологий и методов защиты информации, от соответствующих решений, использованных в иных СНИ НСД.
2. Данное исследование наглядно иллюстрирует то, что КСЗИ «Панцирь+» принципиально отличается от иных представленных сегодня на рынке средств защиты СЗИ НСД, причем не в каких-либо частных вопросах реализации отдельных механизмов защиты, а собственно в своем назначении, как следствие, в реализуемых возможностях защиты информации.
3. Технические решения, реализующие основные механизмы защиты из состава КСЗИ «Панцирь+», запатентованы, что, с одной стороны, подтверждает их новизну, с другой стороны, предполагает невозможность (без нарушения авторских прав) реализации данных решений иными разработчиками средств защиты информации.