РЕАЛИЗАЦИЯ КОНТРОЛЯ И РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К СЕТЕВЫМ ОБЪЕКТАМ

Введение.

На сегодняшний день подавляющее число компьютерных систем, используемых для обработки конфиденциальной информации, нуждающейся в эффективной защите, имеют доступ в сеть. С учетом же того, что основу защиты современных информационных систем составляет реализация разграничительной политики доступа к защищаемым ресурсам, сетевые объекты должны рассматриваться в качестве подобных ресурсов – к ним должны контролироваться и разграничиваться права доступа субъектов. На практике исторически широкое применение нашли межсетевые экраны, в том числе, существуют требования к решаемым ими задачам в различных приложениях данного средства защиты [1]. В последнее время средства контроля и разграничения прав доступа к сетевым объектам, устанавливаемые в компьютерных системах, подключенных к сети, стали называть «локальными межсетевыми (или сетевыми) экранами», а корректность их реализации, в том числе, набор решаемых ими задач, оценивать с использованием документов, формулирующих требования к межсетевым экранам [1]. Однако, это принципиально разные средства защиты даже по своему назначению, принципиально различны решаемые ими задачи, а если говорить о реализации разграничительной политики доступа, то она для рассматриваемых средств вообще имеет мало общего, поскольку для них кардинально различаются субъекты и объекты доступа. В данной статье исследуем вопросы реализации контроля и разграничения прав доступа субъектов компьютерной системы к сетевым объектам, попытаемся определить и обосновать набор решаемых ими задач защиты, и на примере апробированного технического решения «Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows» рассмотрим реализацию подобного технического средства защиты.

1. Решаемые задачи и требования к архитектуре средства защиты.

Реализацию разграничительной политики доступа к сетевым объектам нельзя рассматривать в отрыве от реализации разграничительной политики доступа к иным защищаемым ресурсам компьютерной системы – файловым объектам, объектам реестра ОС, буферу обмена и т.д. Именно такой подход к реализации защиты позволяет обеспечить защиту информации на всех этапах ее обработки – разграничивать потоки информации при ее обработке, в том числе позволяет изолировать обработку информации отдельными приложениями, например, сетевыми, разграничить (в том числе, изолировать) режимы обработки открытой и конфиденциальной информации в компьютерной системе и т.д.

Поскольку на сегодняшний день угрозу несанкционированного доступа к информации несет в себе и пользователь, и процесс (приложение) – эти вопросы нами исследованы в [2,3], субъект доступа в разграничительной политике доступа к сетевым объектам должен определяться, как «пользователь, процесс» (какой пользователь, каким процессом запрашивает доступ к ресурсу, в нашем случае, к сетевому объекту). Для защиты же от обхода разграничительной политики, задавая в разграничительной политике пользователя, целесообразно контролировать возможную смену, например, с использованием сервисов олицетворения, исходной учетной записи (от лица которой запущен процесс) на эффективную (от лица которой запрашивается доступа к защищаемому ресурсу), этот вопрос исследован в [4]. Таким образом, субъект доступа в разграничительной политике доступа к защищаемым ресурсам целесообразно задавать следующим образом «исходный идентификатор пользователя, эффективный идентификатор пользователя, полнопутевое имя процесса», где под полнопутевым именем процесса понимаем полнопутевое имя его исполняемого файла [4]. При задании подобным образом в разграничительной политике субъекта доступа, можно разграничить, какой пользователь, каким процессом, при какой смене исходного идентификатора пользователя будет (или не будет) иметь доступ к сетевому объекту. Естественно, что, говоря о пользователях, мы

подразумеваем, как интерактивных, так и системных пользователей, то же относится и к процессам, поскольку атака на системные процессы несет в себе серьезную угрозу реализации несанкционированного доступа к обрабатываемой в компьютерной системе информации [5].

К слову сказать, подобное задание субъекта возможно именно применительно к реализации разграничительной политики доступа к сетевым объектам, реализуемой в компьютерной системе, но если же говорить о межсетевом экране, то данным средством защиты, как субъект, так и объект доступа идентифицируются исключительно по средством анализа заголовков сетевых пакетов, в которых отсутствует информация о том, каким пользователем, каким процессом (приложением) отправлен этот пакет в сеть, соответственно и для обработки каким пользователем каким процессом предназначены данные, передаваемые по сети.

С субъектом доступа мы разобрались. Теперь о сетевом объекте доступа.

Объект в разграничительной политике доступа к сетевым объектам в общем случае должен задаваться следующими сущностями (с учетом их иерархии):

- Сетевой адаптер;
- IP адрес (или сетевое имя) удаленного компьютера;
- Номер UDP, TCP порта для транспортных протоколов (виртуальный транспортный канал, включающий номера портов участвующих в сетевом взаимодействии компьютеров);
- Служба.

Прокомментируем сказанное.

При использовании в качестве объекта доступа сущности сетевой адаптер, для каждого сетевого адаптера, присутствующего на компьютере (например, для сетевой платы, внешнего модема и т.д.), может быть реализована своя разграничительная политика доступа (в том числе, например, запрещен доступ для сетевого взаимодействия по Wi-Fi с

компьютерами в составе корпоративной сети), в которой для субъектов доступа уже с использованием иных сущностей, идентифицирующих сетевой объект доступа, может быть задано, с какими компьютерами (по адресам или именам), по каким портам, с использованием каких служб и по каким правилам они могут взаимодействовать.

Понятно, что разграничительную политику доступа, применительно к использованию современных сетевых технологий, следует реализовывать в отношении транспортных протоколов TCP/UDP. При этом возможность любого иного вида транспорта, за исключением протокола ARP, который должен разрешаться для обеспечения корректной работы в локальной сети, в общем случае должна быть предотвращена. Если же подобный протокол необходимо использовать, то в отношении него также должна быть реализована соответствующая разграничительная политика.

Особое место в разграничительной политике доступа занимает управляющий протокол ICMP. Обмен по нему должен, либо предотвращаться средством защиты, либо средством защиты должно обеспечиваться разграничение прав доступа на уровне задания разрешенных (запрещенных) управляющих команд.

Разрешение/запрет (разграничение прав) доступа субъектов к определенным службам крайне важен ввиду того, что подключение конкретных служб к конкретным портам лишь регламентируется соответствующей рекомендацией. В общем случае службы могут подключаться к иным портам. Поэтому разграничивать доступ субъектов к службам по номерам портов в общем случае нельзя – служба должна рассматриваться в качестве самостоятельного сетевого объекта доступа.

Использование для идентификации сетевых объектов перечисленных ранее сущностей выдвигает соответствующие требования к архитектуре средства защиты, решающего рассматриваемые задачи, состоящие в следующем. В составе средства защиты для реализации контроля и разграничения прав доступа к сетевым объектам должны присутствовать два

драйвера, функционирующих одновременно на различных уровнях ядра ОС. Первый драйвер, используемый для перехвата запроса доступа, с целью получения и анализа корректности запроса субъекта к сетевым объектам, в частности, для идентификации субъекта доступа, должен работать на уровне драйвера TCP/IP ОС [6]. Однако на этом уровне драйвер средства защиты не имеет возможности анализа заголовков сетевых пакетов (фильтрации сетевых пакетов), они обрабатываются ОС на более низком уровне. А именно из заголовков сетевых пакетов можно корректно идентифицировать некоторые сетевые объекты доступа, необходимые при реализации разграничительной политики доступа, например, протоколы и службы, команды протокола ICMP и др. Как следствие, средство защиты должно иметь в своем составе также и драйвер, работающий на уровне NDIS[6]. На этом уровне уже могут перехватываться сетевые пакеты для анализа их заголовков, но, в свою очередь, на этом уровне невозможно определение субъекта доступа (какой пользователь каким процессом запросил доступ к сетевому объекту).

Назначаемые правила доступа субъектов к объектам должны учитывать разрешение/запрет доступа (использования), в том числе, отдельных команд, применяемых в соответствующих протоколах. Достаточно важным расширением правил доступа является возможность временного регламентирования (по дням недели и времени) доступа субъектов к сетевым объектам.

Теперь, в двух словах, о реализации собственно разграничительной политики доступа. В данном случае, как и при реализации разграничительной политики доступа к иным защищаемым ресурсам, имеет смысл реализация подходов, предложенных и обоснованных, например, в [5], состоящих в следующем. Контроль и разграничение прав доступа к сетевым объектам в рассматриваемом случае (субъект доступа идентифицируется, как пользователем, так и процессом) состоит в реализации дискреционного контроля доступа (на основе матрицы доступа) субъектов к сетевым

объектам с принудительным управлением потоками информации (непривилегированный пользователь должен быть исключен из схемы администрирования – правила доступа могут задаваться/модифицироваться исключительно администратором).

Важнейшим требованием к реализации является то, что правила доступа должны задаваться для субъектов (а не назначаться в качестве атрибутов объектам) доступа. Это позволяет существенно упростить задачу администрирования, в том числе, за счет использования масок при задании сетевых объектов доступа.

При реализации разграничительной политики доступа имеет смыл реализация групповых политик. Поскольку достаточно большое число субъектов будут иметь совпадающие права доступа к ряду сетевых объектов, субъекты следует объединять в группы (профили), с последующим назначением прав доступа к сетевым объектам для профилей.

В отношении, как системы в целом, так и в отношении любого субъекта доступа должна быть реализована разрешительная – «Все, что явно не разрешено, то запрещено», и опционально запретительная – «Все, что явно не запрещено, то разрешено» разграничительные политики доступа к сетевым объектам. Естественно, что разграничения прав доступа должны применяться и в отношении системных пользователей и процессов, при этом при реализации разрешительной разграничительной политики им необходимо назначить соответствующие права доступа для корректной работы компьютерной системы в сети.

Прежде, чем перейти к вопросам практической реализации средства защиты, еще раз акцентируем внимание на следующем крайне важном, на наш взгляд, моменте. В отличие от задачи межсетевого экранирования, задачу реализации контроля и разграничения прав доступа к сетевым объектам следует рассматривать не как самостоятельную задачу защиты информации, а, как отмечали, как часть общей задачи реализации разграничительной политики доступа к защищаемым ресурсам

компьютерной системы, что выдвигает соответствующие требования к построению средства защиты, в том числе, к способу задания субъекта и правил доступа в разграничительной политике.

2. Практическая реализация.

Задание в разграничительной политике субъекта доступа.

Интерфейс «Субъекты доступа», в котором отображаются созданные администратором субъекты, приведен на рис.1, окно, в котором создаются субъекты, на рис.2. Созданные субъекты, которые будут обладать одинаковыми правами доступа к защищаемым ресурсам, в нашем случае – к сетевым объектам, помещаются в один и тот же профиль (для помещения субъекта в профиль, имена соответствующего субъекта и профиля задаются при создании субъекта в окне задания субъекта доступа, см. рис.2). Интерфейс «Профили», в котором отображаются созданные администратором профили и включенные в профили субъекты, приведен на рис.3. Именно профили в качестве субъектов доступа будут использоваться далее в разграничительной политике.

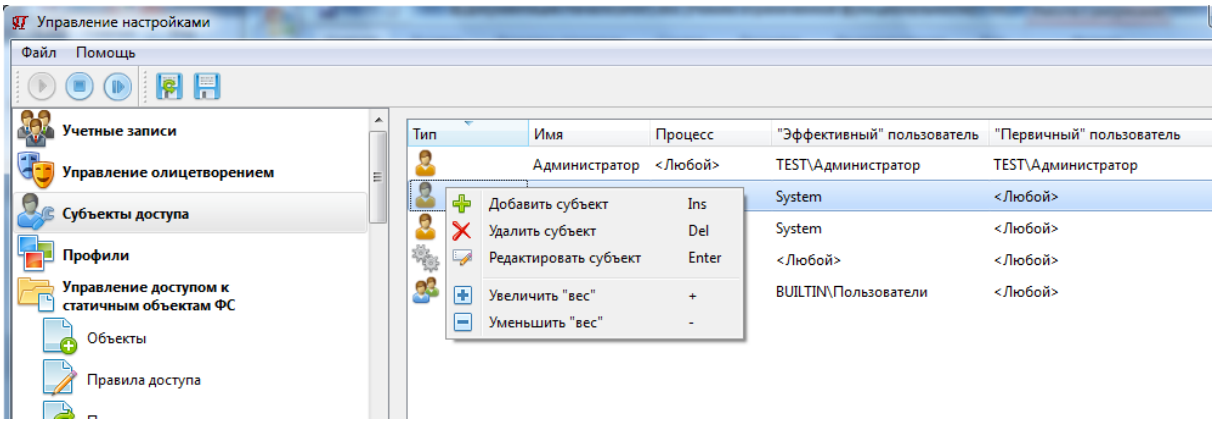

Рис.1. Интерфейс «Субъекты доступа»

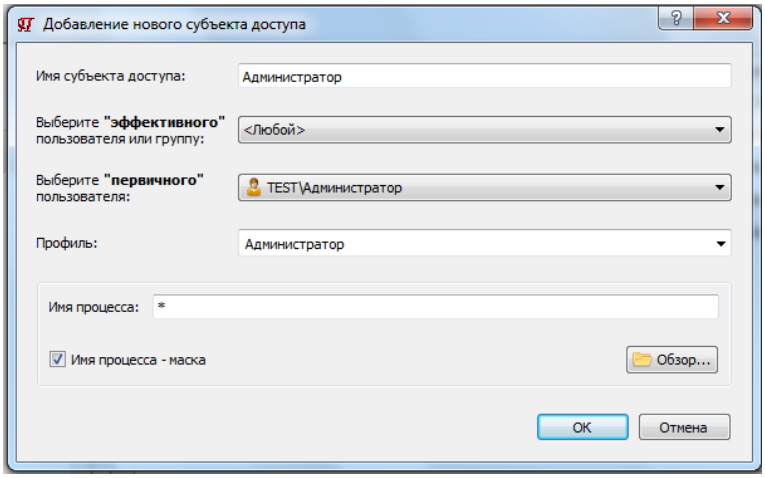

Рис.2. Окно задания субъекта доступа

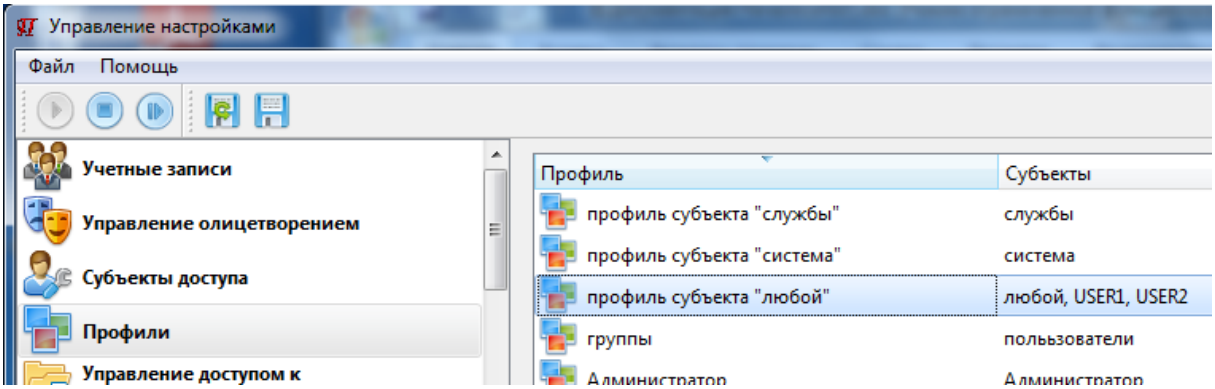

Рис.3. Интерфейс «Профили»

При задании идентификатора пользователя (как первичного, так и эффективного), см. рис.2, может использоваться маска "*" - "Любой", в этом случае заданные правила будут распространяться на всех пользователей – при этом разграничения прав доступа реализуются между процессами (приложениями). Имя процесса, может задаваться либо полнопутевым именем его исполняемого файла, либо маской (возможно также использование переменных среды окружения). Например, маской C:\Program File* (аналогично и при задании %Program File%*) покрываются все исполняемые файлы из соответствующего каталога Program File, маской же "*" - "Любой" в данном случае задается то, что правило будет применимо к любому процессу, т.е. при таком задании процесса в субъекте разграничения прав доступа будут реализовываться между пользователями. Поскольку один и тот же реальный субъект доступа в разграничительной политике может

"покрываться" одновременно несколькими масками, при анализе запроса доступа диспетчером принимаются разграничения по матрице доступа для субъекта, наиболее точно соответствующего своим описателем в разграничительной политике субъекту, запросившему доступ.

Задание в разграничительной политике объектов доступа.

Интерфейс «Объекты доступа», в котором отображаются созданные администратором сетевые объекты доступам, приведен на рис.4. Объекты доступа создаются в соответствии с их иерархией. Сначала из окна задания IP объекта, см. рис.5, для каждого сетевого адаптера компьютерной системы задаются IP адреса удаленных компьютеров, с которыми сможет взаимодействовать компьютерная система, на которой настраивается средство защиты (либо сетевые имена – в этом случае средство защиты само делает преобразование сетевого имени в IP адрес). Адрес может указываться маской – можно задать какой-либо интервал адресов, можно задать «Любой» адрес, в том числе, например, с целью запрета доступа в сеть для какого-либо адаптера.

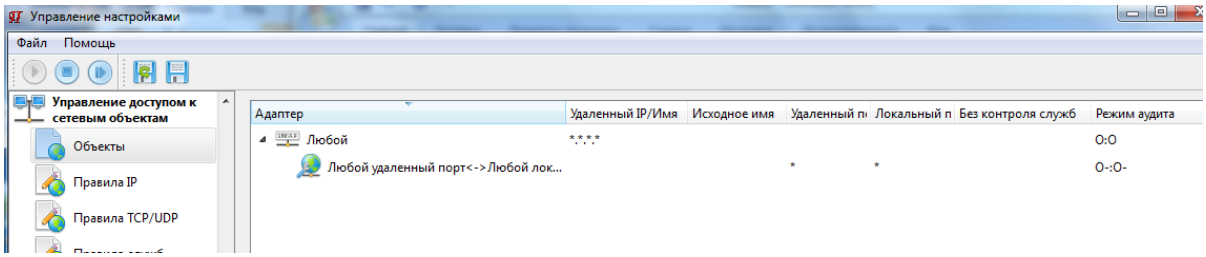

Рис.4. Интерфейс «Объекты доступа»

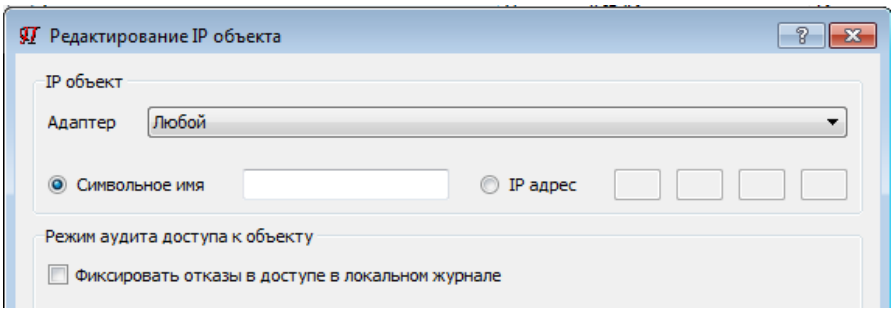

Рис.5. Окно задания IP объекта

Далее из окна задания TCP/UDP объекта, см. рис.6, для каждого заданного IP объекта (соответственно, для сетевого адаптера) задаются TCP/UDP объекты – виртуальные транспортные каналы (локальный и

удаленные номера портов, по которым могут взаимодействовать компьютеры по сети – компьютер, на котором настраивается средство защиты и удаленный компьютер, идентифицируемый как соответствующий IP объект).

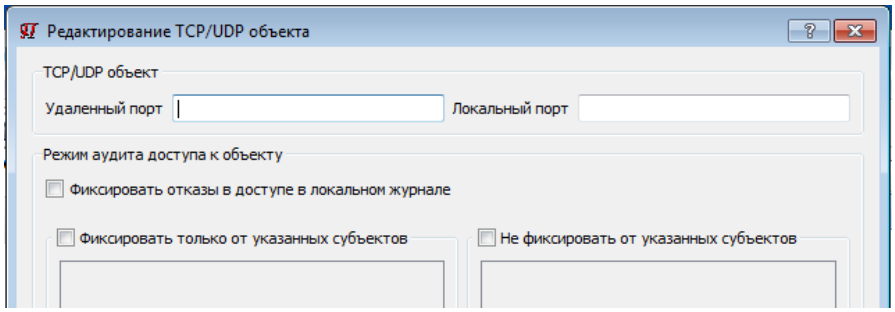

Рис.6. Окно задания TCP/UDP объекта

Из окна задания служб, см. рис.7, для компьютера в целом, либо, если настройки для различных профилей (напомним, что профиль – это субъект доступа) будут различаться, можно задать (выбрать из заданного списка) разрешенные (запрещенные) службы. Уточним, что службы будут разрешаться (запрещаться) в отношении объектов (локального сетевого адаптера, сетевого адреса (или имени) и номеров (локального и удаленного) портов), заведенных ранее, которые могут взаимодействовать по сети. Соответственно для каждого идентифицируемого таким образом объекта может разрешаться/запрещаться служба (службы).

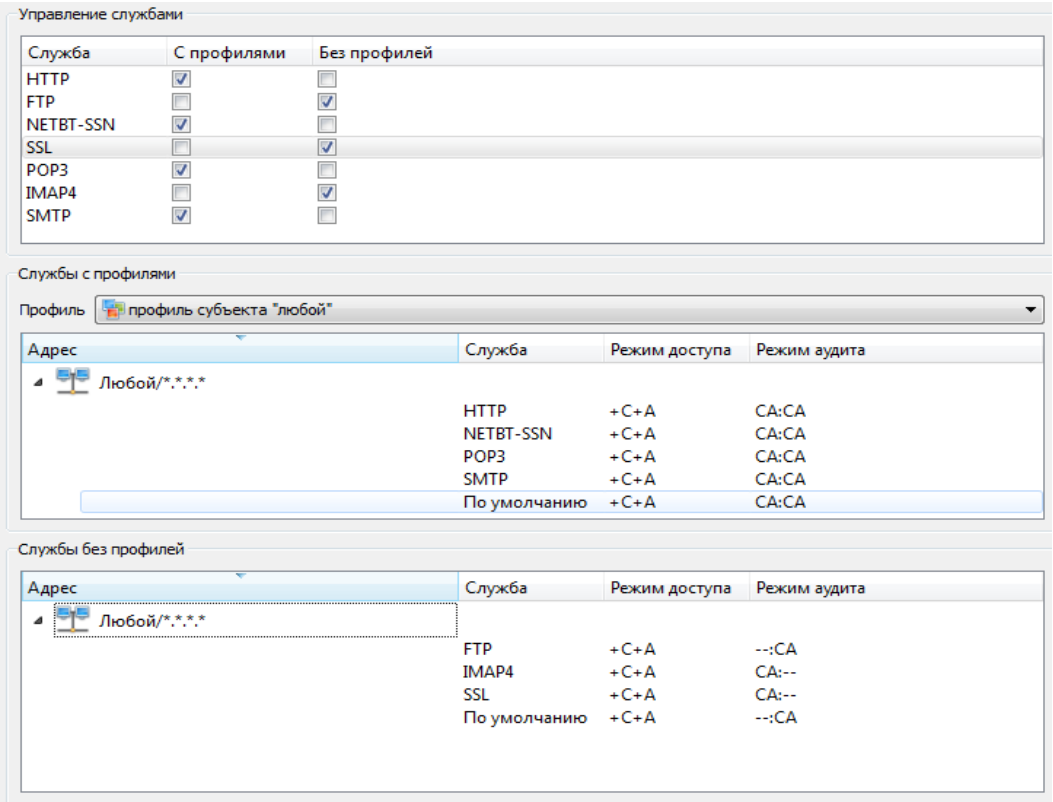

Рис.7. Окно задания объекта служба и интерфейс отображения заданных правил для служб

Задание в разграничительной политике правил доступа.

Правилами доступа для субъектов разрешается/запрещается использование команд, которые могут использоваться в рамках определенных протоколов при доступе к объекту соответствующего уровня иерархии.

Окно задания дополнительно разрешаемых транспортных протоколов (по умолчанию разрешены TCP, UDP, ICMP с собственным транспортом, ARP - служебный протокол, обеспечивающий корректную работу локальной сети) и правил доступа субъектов к объектам при использовании этих протоколов представлено на рис.8. При настройке разграничительной политики доступа необходимо выбрать субъект доступа, для него открыть соответствующее окно, см. рис.8, в котором выбрать объект (последовательно выбирать необходимые объекты), для которого требуется разрешить дополнительные транспортные протоколы и задать соответствующие правила (команды) доступа. В интерфейсе,

представленном на рис.9, для любого субъекта доступа (для просмотра необходимо выбрать субъект) отображаются дополнительно разрешенные транспортные протоколы взаимодействия с любым объектом доступа (для просмотра необходимо выбрать объект).

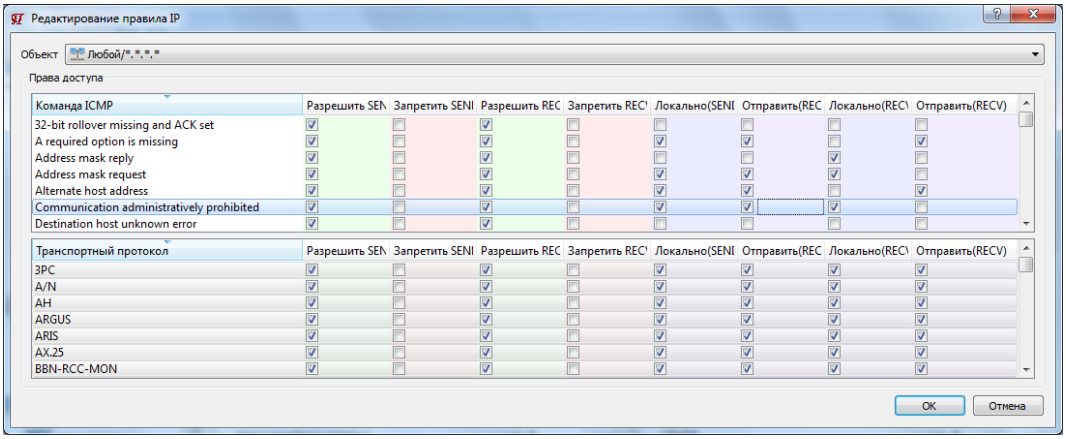

Рис.8. Окно задания дополнительные транспортных протоколов и правил

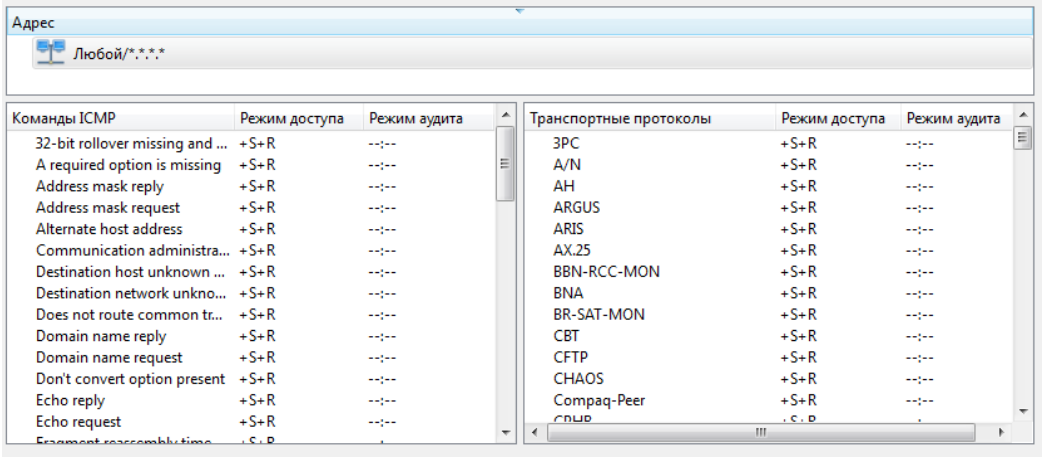

Рис.9. Интерфейс отображения дополнительно разрешенных транспортных протоколов и правил доступа

Из окна интерфейса, приведенного на рис.8, также задаются разрешенные/запрещенные для использования команды протокола ICMP, заданные правила использования команд ICMP отображаются в интерфейсе, представленном на рис.9.

Окно задания правила доступа для выбранного субъекта к TCP/UDP объекту представлено на рис.10, в интерфейсе же, представленном на рис.11, отображаются все заданные администратором правила доступа субъекта к

TCP/UDP объектам, применительно ко всем IP объектам, разрешенным для всех сетевых адаптеров.

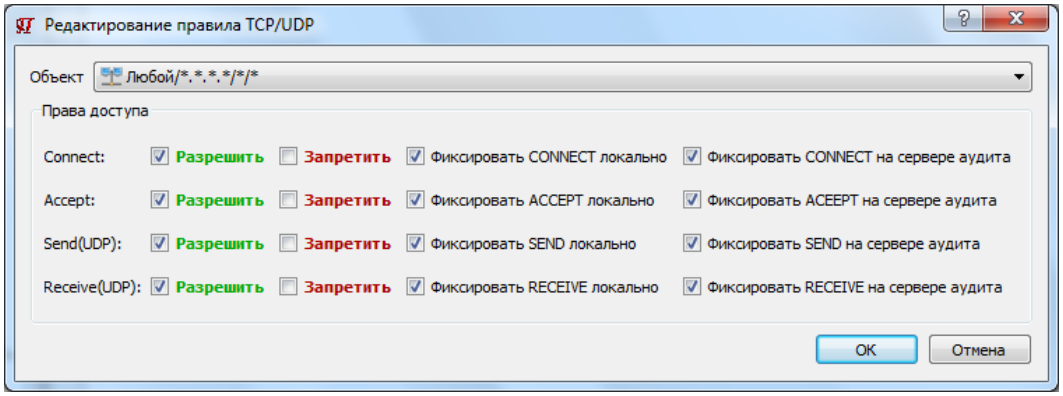

Рис.10. Окно задания правила для TCP/UDP объекта

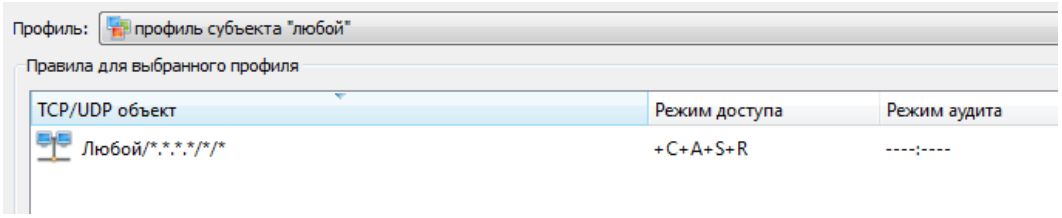

Рис.11. Интерфейс отображения правил доступа субъекта к TCP/UDP объектам

Правила служб, которые могут задаваться, как для всех субъектов одновременно - одинаковыми, в отношении конкретного объекта, так и задаваться различными для различных субъектов, что определяется при задании объекта служба, см. рис.7, задаются из окна, представленного на рис.12 и соответствующим образом отображаются в интерфейсе, представленном на рис.7.

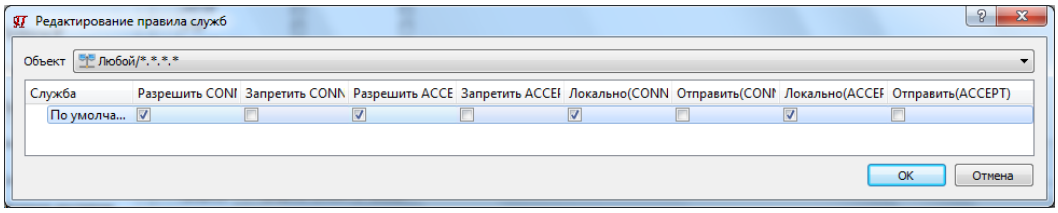

Рис.12. Окно задания правил для служб

Для каждой сущности объекта доступа может быть назначено расписание взаимодействия с ним субъектов (для каждого субъекта может задаваться свое расписание). Т.е. можно назначить, какой пользователь, каким процессом (приложением) к какому сетевому объекту имеет доступ по времени и по дням недели, что позволяет техническими средствами

обеспечить реализацию регламента предприятия по доступу к сетевым объектам. При задании временных режимов доступа соответствующим образом меняются представленные ранее интерфейсы, что проиллюстрировано на интерфейсе, приведенном на рис.13.

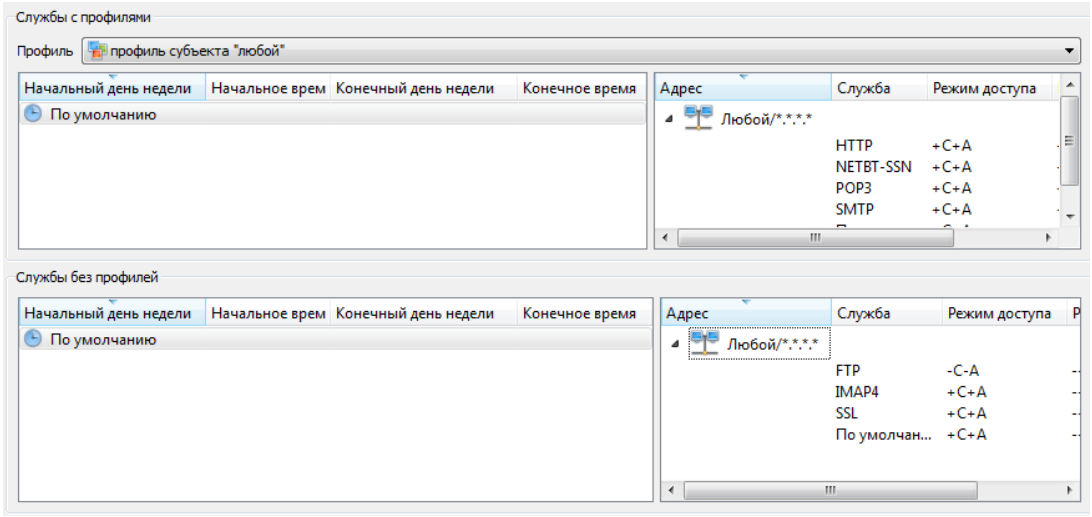

Рис.13. Интерфейс отображения заданных правил для служб по времени

Субъект доступа при назначении разграничительной политики может содержать системных пользователей и системные процессы. Необходимые для корректной работы с сетью правила доступа для системных субъектов, которые можно определить из журнала аудита, см. рис.14, установлены в средстве защиты «по умолчанию».

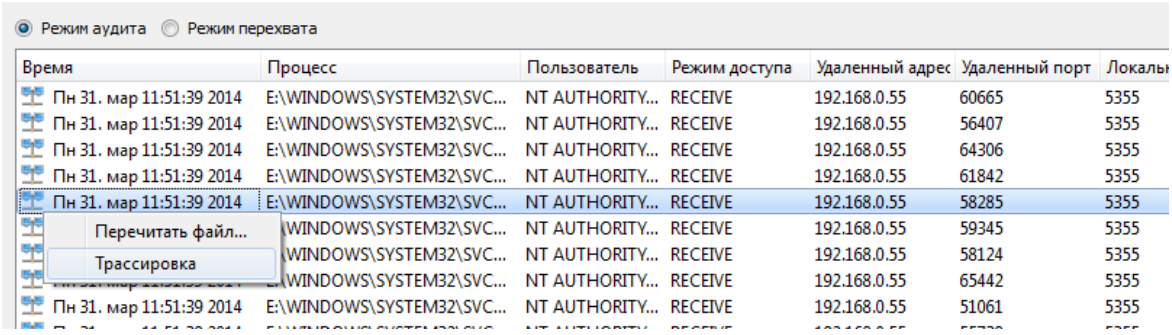

Рис.14. Журнал аудита с отображением запрашиваемого доступа системными субъектами

В «режиме перехвата», см. рис.14, администратор может просмотреть в реальном времени все текущие установленные соединения с защищаемой компьютерной системой.

Заключение.

Сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации. Основу же контроля и разграничения прав доступа к сетевым объектам составляет реализация разграничительной политики доступа к сетевым ресурсам для пользователей и процессов. Фильтрация сетевых пакетов здесь также, безусловно, необходима для корректной идентификации сетевых объектов. Вместе с тем, это абсолютно иной класс средств защиты, предназначенных для решения совершенно иных задач защиты обрабатываемой в компьютерной системе информации от несанкционированного доступа.

Литература.

1. Руководящий документ «Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации» - М.: Гостехкомиссия России, 1997.

2. Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации. - 2013. - Вып. 101. - № 2. - С. 36-43.

3. Щеглов К.А., Щеглов А.Ю. Защита от атак со стороны приложений, наделяемых вредоносными функциями. Модели контроля доступа // Вопросы защиты информации. - 2012. - Вып. 99. - № 4. - С. 31-36.

4. Щеглов К.А., Щеглов А.Ю. Методы идентификации и аутентификации пользователя при доступе к файловым объектам // Вестник компьютерных и информационных технологий. - 2012. - № 10. - С. 47-51.

5. Щеглов К.А., Щеглов А.Ю. Контроль доступа к статичным файловым объектам // Вопросы защиты информации. - 2012. - Вып. 97. - № 2. - С. 12-20.

6. М. Руссинович, Д. Соломон. Внутреннее устройство Microsoft Windows. – СПб.: Питер, 2005.