

**СИСТЕМА VPN «ПАНЦИРЬ»
для ОС Windows
2000/XP/2003/Vista**

2008 г.

1. НАЗНАЧЕНИЕ СЗИ «VPN «ПАНЦИРЬ» ДЛЯ ОС WINDOWS 2000/XP/2003/Vista»

В СЗИ «VPN «Панцирь» для ОС Windows 2000/XP/2003/Vista» предназначена для создания защищенных автоматизированных систем (АС) предприятия и корпоративных локальных и распределенных сетей (Intranet).

Решаемые задачи:

- Реализации разграничительной политики внешнего доступа к ресурсам корпоративной АС, локальной, либо распределенной корпоративной сети;
- Реализации разграничительной политики доступа к ресурсам в корпоративной АС, в локальной, либо в распределенной корпоративной сети;
- Шифрования трафика в корпоративной АС, в локальной, либо в распределенной корпоративной сети.
- Интеграция со средствами защиты иных производителей:
- ключи eToken PRO/32K и eToken PRO/64K (в форм факторе USB ключа и смарт-карты) производства ЗАО «Аладдин Р.Д.» Используются для хранения и ввода пользователем идентификационных данных и ключевой информации;
- Криптопровайдер «КриптоПро CSP» версий 3.0 (и 3.6), сертифицирован по требованиям к шифрованию конфиденциальной информации ФСБ России.

2. ТРЕБОВАНИЯ К КОРПОРАТИВНОЙ VPN (INTRANET), РЕАЛИЗУЕМЫЕ СЗИ «VPN «ПАНЦИРЬ» ДЛЯ ОС WINDOWS 2000/XP/2003/Vista»

Корпоративная VPN (или Intranet) – это «наложенная» (виртуальная) сетевая инфраструктура, ограниченная рамками корпорации. Подобную инфраструктуру в общем случае составляют локальные вычислительные средства (рабочие станции и серверы предприятия), объединяемые каналами связи в корпоративную автоматизированную систему (АС), локальную сеть (ЛВС), корпоративные локальные сети, объединяемые, в большинстве своем, каналами связи общего пользования в единое коммуникационное пространство, к которому, кроме того, могут подключаться удаленные и мобильные корпоративные пользователи.

Для создания сетевой инфраструктуры, ограниченной рамками корпорации (Intranet), используются средства защиты, целью которых является предотвращение несанкционированного раскрытия конфиденциальности и нарушения целостности (в том числе, обеспечение доступности) корпоративной информации. Не смотря на то, что, как известно, данные задачи обеспечения информационной безопасности корпоративной сети являются основными задачами защиты информации от несанкционированного доступа (НСД), решаемыми реализацией соответствующей разграничительной политики доступа к информационным корпоративным ресурсам, построение Intranet невозможно без использования криптографических методов защиты информации, передаваемой по каналам связи.

Задача защиты информации в корпоративной сети (построение Intranet) имеет свои существенные особенности, поэтому далеко не все средства защиты, используемые для построения VPN, могут эффективно применяться в данных приложениях. Принципиальная особенность защиты информации в корпоративной сети, состоит в том, что информация должна защищаться, как от

внешних, так и от внутренних угроз, т.е. в качестве потенциального злоумышленника здесь следует рассматривать не только (а может быть и не столько) некое стороннее по отношению к корпоративным ресурсам лицо, но и санкционированных пользователей, допущенных к ресурсам корпоративной сети в рамках выполнения своих служебных обязанностей (их принято называть инсайдерами). Это обусловливается тем, что пользователь в данных приложениях обрабатывает не личную информацию – не он является ее владельцем, при том, что компьютерная обработка информации проникает во все сферы деятельности корпорации, все более и более приобретая конфиденциальный характер.

Из рассмотренных особенностей корпоративных приложений могут быть сформулированы основополагающие требования к построению корпоративной VPN (именно выполнение этих требований и позволяет позиционировать то или иное средство, как средство защиты для построения Intranet)):

- Все задачи администрирования, как в части задания разграничительной политики доступа к корпоративным ресурсам, так и в части реализации ключевой политики (создания и распространения ключей шифрования виртуальных каналов связи), должны решаться администратором безопасности - пользователь должен быть исключен из схемы администрирования, должен работать в корпоративной сети «под принуждением» - в рамках тех прав, которые ему предоставлены администратором – должен общаться только с теми пользователями (или компьютерами), с которыми ему разрешено, при этом должен обмениваться с ними данными только в том виде (открытыми, либо зашифрованными), в котором разрешено. Как следствие, шифрование виртуальных каналов связи должно осуществляться автоматически «прозрачно» для пользователя, ключ шифрования должен быть недоступен пользователю (а уж тем более, не им создаваться), что предотвращает возможность нарушения санкционированным пользователем конфиденциальности данных, в случае их хищения (инсайдерская атака);
- Должна предоставляться возможность шифрования виртуальных каналов связи, как в составе ЛВС, так и каналов сети общего пользования, объединяющих подсети (либо/и обеспечивающих доступ к корпоративным ресурсам удаленных и мобильных пользователей). Тому есть две причины, во-первых, необходимо обеспечивать защиту от инсайдерских атак (санкционированным пользователям достаточно просто получить доступ к внутренним (в составе ЛВС) каналам связи), во-вторых, только в этом случае (при условии надежной идентификации субъектов и объектов доступа, что также является важнейшим требованием к корпоративной VPN), в корпоративных приложениях могут реализовываться беспроводные внутриофисные (indoor) корпоративные сети (либо беспроводные сегменты ЛВС).
- Реализация этих основополагающих требований к построению корпоративной VPN влечет за собою формирование требований к составу средства защиты, используемому для построения Intranet:
- Поскольку должна предоставляться возможность шифрования виртуальных каналов связи, как в составе ЛВС, так и каналов сети общего пользования, основным компонентом средства защиты для построения корпоративной VPN является клиентская часть, устанавливаемая на компьютеры в составе VPN - реализует автоматическое («под принуждением») «прозрачное» для пользователя шифрование виртуальных каналов связи VPN, как следствие, основной компонент клиентской части средства защиты, используемого для построения корпоративной VPN – это драйвер, обеспечивающий «перехват» и соответствующую обработку всех обращений к/из виртуальным каналам;

- Поскольку все задачи администрирования возлагаются на администратора безопасности (все задачи администрирования и контроля функционирования VPN должны решаться централизованно), в состав VPN, помимо клиентских частей, устанавливаемых на защищаемые компьютеры, должны быть включены сервер VPN, ответственный за генерирование и распределение ключей шифрования, и АРМ администратора безопасности, предоставляющий возможность централизованной настройки и аудита работы VPN с одного рабочего места администратора безопасности;
- Критичность хищения конфиденциальной корпоративной информации обуславливает формирование для этих приложений дополнительных требований к ее защите в виртуальных каналах связи:
- Поскольку высокий уровень криптостойкости обеспечивается не только заданием необходимой длины ключа шифрования, но и высокой интенсивностью смены ключей – процедура генерирования ключей шифрования и их распределения в сети должна осуществляться сервером VPN автоматически с минимально возможным периодом (однако это не должно существенно сказываться на загрузке связного ресурса);
- Поскольку в VPN всегда присутствует угроза компрометации ключа шифрования, должна предусматриваться минимизация ущерба, связанная с его хищением, что достигается использованием своего ключа шифрования (периодически автоматически изменяемого, см. выше) для каждой пары взаимодействующих субъектов/объектов в сети.

Важнейшим вопросом при построении корпоративной VPN является то, какие сущности должны быть определены в качестве субъекта и объекта доступа при реализации разграничительной политики доступа, соответственно, принадлежностью какой сущности «субъект доступа», должен являться ключ шифрования. Традиционно принято, что в VPN в качестве субъекта и объекта доступа выступает компьютер (рабочая станция или сервер) – между компьютерами в сети разграничиваются права доступа, именно принадлежностью компьютера является ключ шифрования (не случайно, что дополнительно при построении VPN на практике часто используется электронная цифровая подпись, позволяющая идентифицировать не компьютер, а уже непосредственно пользователя).

При реализации же разграничительной политики доступа к ресурсам при решении задач защиты информации от НСД, в качестве субъекта доступа, как правило, выступает сущность «пользователь», как конечный «потребитель» информации.

При построении эффективной защиты корпоративной сети в качестве субъекта (в общем случае он же здесь может являться и объектом) доступа целесообразно рассматривать обе сущности – компьютер и пользователь. Например, хранилища данных (файловые серверы, серверы баз данных и т.д.) могут однозначно идентифицироваться тем, на каких компьютерах они располагаются, тогда в качестве объектов доступа (как правило, сервер – это объект доступа – к нему осуществляются обращения) выступают собственно компьютеры. А вот субъект доступа далеко не всегда однозначно может идентифицироваться компьютером (рабочей станцией), например, в том случае, когда один и тот же пользователь может иметь доступ к объектам корпоративной сети с различных рабочих станций, либо, когда одна и та же рабочая станция может использоваться различными пользователями, при этом, каждый пользователь должен иметь свои права доступа к объектам корпоративной сети. При использовании в качестве субъекта доступа сущности «компьютер», в общем случае задача реализации разграничительной политики доступа в корпоративной VPN становится неразрешимой (корректно она в этом случае может быть реализована лишь при следующем ограничении на использование ресурсов: один компьютер (рабочая станция) - один пользователь).

Это обуславливает формирование следующих требований к способу определения сущностей «субъект» и «объект» (в общем случае «субъект/объект») доступа в корпоративной VPN:



Субъекты и объекты (в общем случае субъект/объект) доступа в корпоративной VPN должны определяться как сущностью «пользователь», так и сущностью «компьютер» (средством защиты должны поддерживаться оба эти способа определения субъекта и объекта доступа). Для обеих этих сущностей средством защиты в равной мере должна обеспечиваться возможность реализации разграничительной политики доступа и предоставления ключей шифрования виртуальных каналов связи.

К основным задачам, решаемым при реализации разграничительной политики доступа к ресурсам корпоративной VPN, относятся:

- обеспечение изолированности обработки информации рамками корпорации (в частном случае, рамками одной корпоративной подсистемы – АС). Компьютерам из состава корпоративной VPN, на которые установлены клиентские части средства защиты, должна предоставляться возможность обмениваться информацией с компьютерами из состава корпоративной VPN, т.е. с теми компьютерами, на которые также установлены клиентские части средства защиты. При этом весь трафик между компьютерами из состава корпоративной VPN должен шифроваться (со своим ключом шифрования для каждой пары субъектов/объектов). Таким образом, условием разрешения сетевого (криптографически защищенного) взаимодействия является взаимная идентификация клиентских частей средства защиты в составе VPN;
- обеспечение изолированности обработки информации в рамках различных АС из состава корпоративной сети, реализацией, как разграничительной политики доступа субъектов к объектам, так и использованием в рамках каждой АС собственно ключа шифрования – в пределе (наиболее общий случай) каждая пара субъект/объект в составе VPN должна иметь свой ключ шифрования.

В общем случае ряду субъектов (либо объектов) корпоративной VPN (например, ряду доверенных пользователей) требуется разрешать доступ не только к объектам VPN, но и к объектам внешней сети. Этот случай характеризуется тем, что, во-первых, объекты внешней сети не имеют установленной клиентской части VPN (либо не могут быть идентифицированы в данной корпоративной VPN), во-вторых, подобный внешний трафик не должен шифроваться.

Это обуславливает формирование следующих требований к способу определения сущностей «субъект» и «объект» (в общем случае «субъект/объект») доступа в корпоративной VPN:

- Субъекты и объекты в корпоративной VPN должны подразделяться на корпоративных и доверенных;
- Корпоративные субъекты (к корпоративным объектам) имеют возможность доступа только к объектам (только субъекты) корпоративной сети, на которых установлены клиентские части средства защиты (после их идентификации), весь трафик между ними должен шифроваться;
- Доверенные субъекты (к доверенным объектам) имеют возможность доступа как к объектам (как субъекты) корпоративной сети, на которых установлены клиентские части средства защиты (после их идентификации), весь трафик между ними должен шифроваться, так и к объектам (субъекты) внешней сети, данный трафик криптографически защищаться не должен.

Пример использования сущности «доверенный субъект». Пусть некому пользователю (например, менеджеру) необходимо разрешить, как защищенное взаимодействие в корпоративной сети (в рамках определенных АС), так и доступ к открытым ресурсам сети Интернет. Соответствующий пользователь (либо его компьютер, в зависимости от способа задания субъекта) определяется, как доверенный субъект. Тогда с компьютера корпоративной сети, на котором установлена клиентская часть средства защиты, данный пользователь сможет взаимодействовать с субъектами/объектами АС, к которым ему разрешен доступ разграничительной политикой, весь трафик подобных взаимодействий будет автоматически («прозрачно» для пользователя) шифроваться. Кроме того, пользователь с компьютера корпоративной сети, на который установлена клиентская часть средства защиты, получит возможность выхода во внешнюю сеть, данный трафик шифроваться не будет.

Пример использования сущности «доверенный объект». Пусть требуется организовать корпоративную почту. Если почтовый сервер, на который устанавливается клиентская часть средства защиты, определить (здесь объект – компьютер), как корпоративный объект, то будет организована служба корпоративной почты – почтовыми сообщениями смогут обмениваться только компьютеры из состава корпоративной сети (на которых установлена клиентская часть средства защиты), весь почтовый трафик будет автоматически шифроваться. Достоинством такого решения является то, что можно «забыть» о спаме, как о таковом, минимизируется вероятность сетевых атак и т.д. Недостаток – невозможность обмениваться почтовыми сообщениями через корпоративный почтовый сервер с внешними по отношению к корпоративной сети субъектами. Если же определить почтовый сервер, как доверенный объект, то через него будет проходить, как корпоративная, так и открытая почта. При этом передача корпоративных почтовых сообщений будет осуществляться в шифрованном виде, внешних в открытом виде. При этом опять же доступ во внешнюю (по отношению к корпорации) сеть будет возможен только для доверенных субъектов.

3. ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ, РЕАЛИЗОВАННЫЕ В СЗИ «VPN «ПАНЦИРЬ» ДЛЯ ОС WINDOWS 2000/XP/2003/Vista»

3.1. Состав СЗИ

СЗИ содержит в своем составе следующие компоненты:

- Клиентскую часть. Устанавливается на компьютеры (локальные, удаленные, мобильные) в составе корпоративной сети. Реализует прозрачное для пользователя шифрование трафика на стеке протоколов TCP/IP и разграничительную политику доступа субъектов к объектам;
- Опционально криптопровайдер «КриптоПро CSP» версия 3.0 (версия 3.6 для ОС Windows Vista) - применяется при необходимости использования сертифицированного по требованиям безопасности решения. Устанавливается вместе с клиентской частью на компьютеры (локальные, удаленные, мобильные) в составе корпоративной сети и на серверную часть (основную, резервную);
- Серверную часть (основную). Устанавливается на выделенном компьютере в составе корпоративной сети. Идентифицирует компьютеры в составе корпоративной сети, автоматически генерирует и предоставляет клиентским частям сеансовые ключи шифрования, формирует разграничительную политику доступа к ресурсам, осуществляет аудит идентификации субъектов и объектов доступа в корпоративной сети. ;

- Серверную часть (резервную). Используется (опционально) для повышения отказоустойчивости корпоративной VPN. Устанавливается на выделенном компьютере в составе корпоративной сети. Идентифицирует компьютеры в составе корпоративной сети, автоматически генерирует и предоставляет клиентским частям сеансовые ключи шифрования, формирует разграничительную политику доступа к ресурсам, осуществляет аудит идентификации субъектов и объектов доступа в корпоративной сети. Взаимодействует с клиентскими частями при отказе основного сервера VPN;
- АРМ администратора безопасности. Устанавливается на выделенном компьютере в составе корпоративной сети (в частном случае может устанавливаться на одном компьютере с серверной частью). Предоставляет администратору безопасности интерфейс настройки VPN, инструментальные средства обработки аудита.

3.2. Идентификация субъектов/объектов доступа в VPN

Существует две причины, по которым идентификацию субъектов и объектов доступа в корпоративной VPN не следует осуществлять по адресам компьютеров в составе сети. Во-первых, как отмечалось выше, в зависимости от реализуемой разграничительной политики доступа, субъектом доступа может выступать, как компьютер, так и пользователь, при том, что с одного компьютера доступ в сеть может предоставляться нескольким пользователям (права доступа к ресурсам которых могут быть различными), либо, один и тот же пользователь может получать доступ к сетевым ресурсам с различных компьютеров (и в этом случае его права доступа могут различаться). Во-вторых, идентификация по адресам связана с существенным усложнением, как эксплуатации, так и администрирования корпоративной VPN.

В СЗИ «VPN «Панцирь» для ОС Windows 2000/XP/2003/Vista» для идентификации субъектов и объектов доступа введена отдельная логическая сущность «Идентификатор субъекта/объекта» (ID), которая, в общем случае, никак не связана ни с конкретным компьютером, ни с учетной записью пользователей, заведенных на компьютере.

При создании на сервере VPN субъекта/объекта доступа администратор безопасности создает его идентификатор, и, в соответствии с тем, что эта сущность идентифицирует (пользователя или компьютер) размещает данный идентификатор при установке клиентской части СЗИ в соответствующем ресурсе компьютера (объект реестра или файловый объект) для его последующей идентификации, либо предоставляет данный идентификатор на внешнем носителе пользователю (Flash- устройство, электронный ключ или смарт-карта).

Данная сущность не является секретной информацией, передается по каналам связи в открытом виде, служит для идентификации субъекта/объекта на сервере VPN и взаимной идентификации субъектов/объектов в составе корпоративной VPN.

При назначении идентификатора субъекту/объекту на сервере VPN администратор безопасности относит его либо к корпоративным, либо к доверенным (присваивая идентификатору соответствующую дополнительную логическую сущность «тип субъекта/объекта»). Корпоративные субъекты/объекты смогут взаимодействовать только с корпоративными субъектами/объектами (на которых устанавливаются клиентские части СЗИ), весь трафик между ними будет шифроваться. Доверенные субъекты/объекты смогут взаимодействовать, как с корпоративными субъектами/объектами (на которых устанавливаются клиентские части СЗИ), весь трафик между ними будет шифроваться, так и с внешними по отношению к корпоративной VPN субъектами/объектами по открытым каналам связи.

Сервер VPN (и резервный сервер VPN) идентифицируются своими IP адресом и портом. Данные параметры должны быть заданы администратором безопасности при установке на компьютеры в составе корпоративной сети клиентских частей СЗИ.

3.3. Реализация ключевой политики

Решение по реализации ключевой политики в СЗИ основано на использовании двух типов симметричных ключей шифрования: ключ шифрования трафика между клиентской и серверной частями (технологический ключ) и сеансовые ключи шифрования между парами клиентских частей.

При создании субъекта/объекта доступа на сервере VPN, вместе с назначением идентификатора и его типа (корпоративный или доверенный), администратором безопасности генерируется технологический ключ (для каждого субъекта/объекта генерируется свой технологический ключ). В зависимости от того, что представляет собою сущность субъект/объект (пользователя или компьютер), администратор размещает технологический ключ при установке клиентской части СЗИ в ресурсе компьютера (объект реестра или файловый объект), либо предоставляет технологический ключ на внешнем носителе пользователю (Flash- устройство, электронный ключ или смарт-карта), на этом же носителе должен располагаться идентификатор пользователя

Технологический ключ является секретной информацией, возможность несанкционированного доступа к которой должна предотвращаться, ключ не должен передаваться по каналу связи в открытом виде.

Технологический ключ используется для получения в зашифрованном виде клиентской частью VPN таблицы сеансовых ключей субъекта/объекта для обмена информацией с другими субъектами/объектами из состава VPN (для каждой пары субъектов/объектов свой сеансовый ключ), и при сеансовой идентификации субъекта/объекта на сервере VPN при запросе таблицы сеансовых ключей.

Сеансовая идентификация субъекта/объекта на сервере VPN осуществляется следующим образом. Клиентская часть СЗИ автоматически при включении компьютера, если идентифицируется субъект/объект компьютер, либо по запросу пользователя – при подключении пользователем к компьютеру носителя с идентифицирующей его информацией – ID и технологическим ключом шифрования, если идентифицируется субъект/объект пользователь, обращается к серверу VPN, высылая ему в открытом виде соответствующий идентификатор (ID) и хэш (необратимое шифрование) технологического ключа. Сервер VPN, получив запрос от субъекта/объекта, определяет его ID, определяет корректность соответствия технологического ключа и ID. Если они соответствуют, сеансовая идентификация субъекта/объекта считается успешной (об этом, и в случае некорректной идентификации, на сервере VPN откладывается соответствующая информация в аудите).



Замечание. До проведения сеансовой аутентификации субъекта/объекта на сервере VPN, доступ к сети с соответствующего компьютера невозможен.

После проведения сеансовой идентификации сервер VPN отправляет субъекту/объекту (в зашифрованном технологическим ключом данного субъекта/объекта виде) таблицу сеансовых ключей шифрования, которые далее используются им для шифрования взаимодействий с иными

субъектами/объектами в составе VPN. Данная таблица содержит список ключей шифрования данного субъекта/объекта с другими субъектами/объектами VPN (для каждой пары субъект/объект свой ключ шифрования, при этом субъект/объект однозначно идентифицируется соответствующей логической сущностью ID), которые активны на текущий момент времени. Таблица сеансовых ключей размещается в оперативной памяти компьютера и недоступна пользователю – сеансовые ключи ему не известны.

Сеансовые ключи шифрования генерируются сервером VPN автоматически и распределяются следующим образом. На каждый момент времени на каждом идентифицированном компьютере (либо, соответственно, на компьютере, с которого осуществлена идентификация пользователя) располагается текущая таблица сеансовых ключей - содержит в своем составе сеансовые ключи активных – идентифицированных на данный момент времени сервером VPN субъектов/объектов (в любой момент времени она может быть не полной). При идентификации (после успешной идентификации) каждого субъекта/объекта для него на сервере VPN автоматически генерируются сеансовые ключи шифрования с теми субъектами/объектами, которые идентифицированы и активны на данный момент времени в сети – их активность при этом проверяется сервером VPN, таблица этих ключей отсылается активизировавшемуся идентифицированному субъекту/объекту. Одновременно остальным активным на данный момент времени субъектам/объектам с сервера VPN отсылаются соответствующие текущие таблицы сеансовых ключей шифрования, с включенным для них сеансовым ключом (разным для всех субъектов/объектов) вновь активизировавшегося субъекта/объекта.

Таким образом, в каждый момент времени каждый активный субъект/объект содержит (хранится в оперативной памяти соответствующего компьютера) актуальную на данный момент времени таблицу сеансовых ключей шифрования с активными субъектами/объектами в корпоративной сети. Сеанс же (продолжительность «жизни» ключа шифрования) определяется активностью субъекта/объекта. Для смены сеансового ключа шифрования субъекта/объекта достаточно перезагрузить компьютер, после его активизации в корпоративной сети (идентификации на сервере VPN), сервером для соответствующего субъекта/объекта будет автоматически сгенерирован новый ключ шифрования, после чего представлена таблица сеансовых ключей шифрования этому субъекту/объекту, и актуализированы текущие таблицы ключей шифрования других субъектов/объектов корпоративной сети.

3.4. Реализация разграничительной политики

В СЗИ реализовано три иерархических уровня реализации разграничительной политики доступа к ресурсам корпоративной VPN.

Первый уровень – уровень контроля доступа к сетевым ресурсам. Состоит в полном запрете доступа к сетевым ресурсам не идентифицированных субъектов/объектов. Реализуется следующим образом. Вне зависимости от того, как определен субъект/объект доступа (корпоративный или доверенный), какой-либо иной доступ с компьютера (к компьютеру), на котором установлена клиентская часть СЗИ, кроме, как к серверу VPN, до осуществления его успешной идентификации на сервере VPN (что подтверждается загрузкой с сервера таблицы сеансовых ключей шифрования), невозможен.

Второй уровень – уровень контроля доступа к корпоративным ресурсам. Состоит в реализации различных возможностей доступа к сетевым ресурсам для корпоративных и доверенных субъектов/объектов. Корпоративным субъектам/объектам разрешается взаимодействие только с корпоративными субъектами/объектами, при этом их трафик шифруется

соответствующими сеансовыми ключами (для каждой пары субъект/объект свой сеансовый ключ шифрования). Доверенным субъектам/объектам разрешается взаимодействие, как с корпоративными субъектами/объектами, при этом их трафик шифруется соответствующими сеансовыми ключами (для каждой пары субъект/объект свой сеансовый ключ шифрования), так и с внешними по отношению к корпорации субъектами/объектами, при этом их трафик не шифруется. Это реализуется следующим образом. При сетевом взаимодействии в рамках VPN, взаимодействующие клиентские части взаимно идентифицируют друг друга (обмениваются своими ID). Результатом подобной взаимной идентификации является принятие сторонами решения о возможности взаимодействия, при возможности – выбор способа взаимодействия, при выборе защищенного способа – выбор сеансового ключа шифрования. Так, если к корпоративному субъекту/объекту обращается корпоративный субъект/объект, будет осуществлена взаимная идентификация субъектов/объектов клиентскими частями СЗИ, взаимодействие сторонам будет разрешено, каждой стороной будет однозначно определен сеансовый ключ шифрования (он свой для каждой пары идентифицированных субъектов/объектов). То же произойдет, если к доверенному субъекту/объекту обращается доверенный субъект/объект (их взаимодействие будет разрешено по защищенному сеансовым ключом каналу). В случае если к корпоративному субъекту/объекту обращается некий внешний по отношению к VPN субъект/объект, не будет осуществлена взаимная идентификация субъектов/объектов - взаимодействие будет запрещено. В случае если к доверенному субъекту/объекту обращается некий внешний по отношению к VPN субъект/объект, не будет осуществлена взаимная идентификация субъектов/объектов - взаимодействие будет разрешено по открытому каналу связи. То же произойдет и в случае, если доверенный субъект/объект обращается к некому внешнему по отношению к VPN субъекту/объекту.

Третий уровень – уровень разграничения доступа к корпоративным ресурсам в составе VPN. К корпоративным ресурсам VPN имеют доступ корпоративные и доверенные субъекты/объекты (доступ к ним осуществляется по защищенным сеансовыми ключами каналам связи), каждый из которых идентифицируется своим ID. Реализация разграничений доступа состоит в возможности задания администратором безопасности (разграничительная политика реализуется с сервера VPN) разграничений (разрешений или запретов) по взаимодействию корпоративных и доверенных субъектов/объектов между собою – задается какой ID с каким ID может (либо не может) взаимодействовать. При задании разграничительной политики доступа к корпоративным ресурсам на сервере VPN, после успешной идентификации субъекта/объекта на сервере, с сервера ему будет передана таблица сеансовых ключей шифрования (и идентификаторов субъектов/объектов) только тех субъектов/объектов, с которыми разрешено взаимодействие идентифицированному субъекту/объекту в рамках реализации заданной разграничительной политики доступа к ресурсам VPN. Идентифицировавшийся субъект/объект сможет взаимодействовать только с теми субъектами/объектами VPN, для взаимодействия с которыми им будут получены с сервера VPN сеансовые ключи шифрования.

4. ПРИМЕНЕНИЕ СЗИ «VPN «ПАНЦИРЬ» ДЛЯ ОС WINDOWS 2000/XP/2003/Vista»

4.1. Защита ресурсов локальной АС предприятия

Клиентские части СЗИ устанавливаются только на рабочие станции и серверы защищаемой АС в составе корпоративной ЛВС. В результате этого обработка информации в АС изолируется на общем сетевом пространстве ЛВС – к серверам АС могут обращаться только рабочие станции из состава АС (также они могут взаимодействовать между собой, если это разрешается заданной разграничительной политикой), весь трафик, передаваемый в составе АС шифруется. Если требуется, чтобы с отдельных рабочих станций из состава АС (либо соответствующим пользователям) был возможен доступ к ресурсам иных АС в составе ЛВС, либо во внешнюю сеть, данные рабочие станции определяются, как доверенные субъекты доступа. Это же относится и к серверам, как к объектам доступа.

4.2. Защита ресурсов локальных АС предприятия

Если в составе корпоративной сети требуется одновременно защитить несколько АС, то клиентские части СЗИ устанавливаются на рабочие станции и серверы защищаемых АС в составе корпоративной ЛВС. В результате этого обработка информации в защищаемых АС изолируется на общем сетевом пространстве ЛВС. Изолированность обработки информации в различных АС между собой достигается реализацией соответствующей разграничительной политики, позволяющей задавать какие рабочие станции (или пользователи) с какими серверами могут взаимодействовать. При этом одна и та же рабочая станция (пользователь) или сервер одновременно могут быть включены в несколько АС. Изолированность трафика между различными защищаемыми АС достигается использованием сеансовых ключей шифрования для каждой пары субъект/объект. Если требуется, чтобы с отдельных рабочих станций из состава АС (либо соответствующим пользователям) был возможен доступ к ресурсам иных АС в составе ЛВС, либо во внешнюю сеть, данные рабочие станции определяются, как доверенные субъекты доступа. Это же относится и к серверам, как к объектам доступа.

4.3. Защита ресурсов ЛВС предприятия

Если требуется защищать все ресурсы (АС) в составе корпоративной ЛВС, то клиентские части СЗИ устанавливаются на все рабочие станции и серверы ЛВС. Заданием соответствующей разграничительной политики доступа к ресурсам и шифрованием трафика с сеансовыми ключами для каждой пары субъект/объект реализуется виртуальная сегментация ресурсов ЛВС (рабочих станций или пользователей, а также серверов, виртуальных каналов связи) на отдельные изолированные АС. При этом одна и та же рабочая станция (пользователь) или сервер одновременно могут быть включены в несколько АС. Если требуется, чтобы с отдельных рабочих станций из состава ЛВС (либо соответствующим пользователям) был возможен доступ во внешнюю сеть, данные рабочие станции определяются, как доверенные субъекты доступа. Это же относится и к серверам, как к объектам доступа.

4.4. Защита ресурсов распределенной АС предприятия

Клиентские части СЗИ устанавливаются только на рабочие станции и серверы защищаемой распределенной АС в составе корпоративной сети. В результате этого обработка информации в распределенной АС изолируется на общем сетевом пространстве распределенной корпоративной сети – к серверам АС могут обращаться только рабочие станции из состава АС – локальные, находящиеся в той же ЛВС, что и серверы, либо удаленные по каналам связи сети общего пользования (также они могут взаимодействовать между собой, если это разрешается заданной разграничительной политикой), весь трафик, передаваемый в составе защищаемой распределенной АС шифруется. Если требуется, чтобы с отдельных рабочих станций из состава защищенной распределенной АС (либо соответствующим пользователям) был возможен доступ к иным ресурсам распределенной корпоративной сети, либо во внешнюю сеть, данные рабочие станции определяются, как доверенные субъекты доступа. Это же относится и к серверам, как к объектам доступа.

Примеры реализации.

1. Пусть требуется реализовать защищенную распределенную корпоративную почту. В состав одной из ЛВС включается почтовый сервер, на который устанавливается клиентская часть СЗИ. Если данный компьютер определяется в VPN, как корпоративный субъект/объект, почтовый сервер сможет использоваться только для реализации защищенной корпоративной почтовой службы, если, как доверенный, то он одновременно может использоваться для реализации и защищенной корпоративной почты, и открытой внешней почты. На те рабочие станции (локальные – в одной ЛВС с почтовым сервером, и удаленные), которые подключаются к корпоративной почтовой службе устанавливаются клиентские части СЗИ, которые соответствующим образом (компьютеры, либо работающие за ними пользователи) определяются, как субъекты/объекты доступа в VPN. Если требуется, чтобы с отдельных рабочих станций, подключенных к корпоративной почте (либо соответствующим пользователям) был возможен доступ к иным ресурсам распределенной корпоративной сети, либо во внешнюю сеть, данные рабочие станции (пользователи) определяются, как доверенные субъекты доступа. Для того, чтобы подключить к почте какого-либо удаленного или мобильного клиента, достаточно, установить на его компьютер клиентскую часть СЗИ и определить его (задать на сервере VPN) в качестве субъекта/объекта доступа в VPN – назначить для него ID и задать технологический пароль для связи с сервером VPN (данная информация должна быть введена на подключаемый к корпоративной почте компьютер, либо предоставлена соответствующему пользователю на соответствующем носителе).

2. Пусть требуется реализовать корпоративный Web-сервис. В состав одной из ЛВС включается Web сервер, на который устанавливается клиентская часть СЗИ. Если данный компьютер определяется в VPN, как корпоративный субъект/объект, Web сервер сможет использоваться только для реализации защищенной корпоративной службы, если, как доверенный, то он одновременно может использоваться для реализации и защищенного, и открытого (внешнего доступа) Web-сервиса. Во втором случае корпоративная часть Web должна дополнительно защищаться паролем для корпоративного доступа.

Замечание. При построении защищенной распределенной АС предприятия выдвигается следующее требование по размещению в корпоративной сети сервера VPN. Он должен быть доступен по своему IP-адресу (по заданному порту) со всех компьютеров в составе распределенной АС (то же относится и к резервному серверу VPN). При реализации в ЛВС, в которой устанавливается сервер VPN, демилитаризованной зоны с трансляцией адресов (NAT) возможны следующие варианты размещения сервера VPN:



- В сегменте общедоступных серверов (при реализации демилитаризованной зоны - между межсетевым экраном и NAT);
- В сегменте серверов внутренней сети (при реализации демилитаризованной зоны - за NAT). В этом случае при трансляции адресов должна осуществляться трансляция запросов на сервер VPN либо по соответствующему номеру порта, либо по IP-адресу (т.е. в этом случае VPN должен обладать своим IP-адресом, по которому можно обращаться из внешней сети).

4.5. Защита ресурсов распределенных АС предприятия

Если в составе корпоративной сети требуется одновременно защитить несколько распределенных АС, то клиентские части СЗИ устанавливаются на рабочие станции и серверы защищаемых распределенных АС в составе корпоративной сети. В результате этого обработка информации в защищаемых распределенных АС изолируется на общем сетевом пространстве, в том числе, и внешней сети общего пользования. Изолированность обработки информации в различных АС между собой достигается реализацией соответствующей разграничительной политики, позволяющей задавать какие рабочие станции (или пользователи) с какими серверами могут взаимодействовать. При этом одна и та же рабочая станция (пользователь) или сервер одновременно могут быть включены в несколько АС. Изолированность трафика между различными защищаемыми АС достигается использованием сеансовых ключей шифрования для каждой пары субъект/объект. Если требуется, чтобы с отдельных рабочих станций из состава АС (либо соответствующим пользователям) был возможен доступ к ресурсам иных АС в составе корпоративной сети, либо во внешнюю сеть, данные рабочие станции определяются, как доверенные субъекты доступа. Это же относится и к серверам, как к объектам доступа.

4.6. Защита ресурсов распределенной сети предприятия

Если требуется защищать все ресурсы (АС) в составе корпоративной сети, то клиентские части СЗИ устанавливаются на все рабочие станции и серверы корпоративной сети. Заданием соответствующей разграничительной политики доступа к ресурсам и шифрованием трафика с сеансовыми ключами для каждой пары субъект/объект реализуется виртуальная сегментация ресурсов корпоративной сети (рабочих станций или пользователей, а также серверов, виртуальных каналов связи) на отдельные изолированные распределенные и локальные АС. При этом одна и та же рабочая станция (пользователь) или сервер одновременно могут быть включены в несколько АС. Если требуется, чтобы с отдельных рабочих станций из состава корпоративной сети (либо соответствующим пользователям) был возможен доступ во внешнюю сеть, данные рабочие станции определяются, как доверенные субъекты доступа. Это же относится и к серверам, как к объектам доступа.

5. ИНТЕГРАЦИЯ СЗИ «VPN «ПАНЦИРЬ» ДЛЯ ОС WINDOWS 2000/XP/2003/Vista» С ДРУГИМИ СРЕДСТВАМИ ЗАЩИТЫ СЕМЕЙСТВА «ПАНЦИРЬ»

СЗИ «VPN «Панцирь» для ОС Windows 2000/XP/2003/Vista» - это специализированное средство защиты, позволяющее эффективно решать широкий круг задач защиты, связанных с построением Intranet-сети (сетей), защищенных корпоративных приложений (АС). Задачи же защиты информации и обеспечения компьютерной безопасности на предприятии в общем случае намного шире, что обуславливает целесообразность применения данного средства защиты с иными средствами семейства «Панцирь» (со средствами, предназначенными для решения иных задач защиты информации и обеспечения компьютерной безопасности) в комплексе.

5.1. Интеграция с Системой защиты данных (СЗД) «Панцирь» для ОС Windows 2000/XP/2003/Vista»

Система защиты данных (СЗД) «Панцирь» - это специализированное средство защиты - реализует шифрование данных «на лету» на жестком диске (локальном и разделенном в сети) и на внешних накопителях, автоматическое гарантированное удаление остаточной информации, разграничение прав доступа к защищаемым объектам на основе ключевой информации, скрывание защищаемых объектов файловой системы. СЗД позволяет подключать криптопровайдер «КриптоПро CSP» версий 3.0 и 3.6.

Отличительная особенность СЗД «Панцирь» состоит в том, что защищаемыми объектами являются любые файловые объекты – логические диски, каталоги, подкаталоги, отдельные файлы (для задания объектов может использоваться механизм масок), как на жестком диске, так и на внешних накопителях, как локальные, так и удаленные - разделенные в сети.

СЗД позволяет создавать на одном компьютере неограниченное число групп защищаемых файловых объектов, для каждой из которых может быть назначен свой уникальный ключ шифрования. Доступ пользователя к группе защищаемых объектов возможен только при наличии у него ключа шифрования, позволяет организовывать коллективный доступ пользователей к корпоративным базам и банкам данных (шифруемым при хранении на серверах), т.к. ключи шифрования никоим образом не связаны с паролями пользователей.

СЗД реализует различные политики задания и хранения ключевой информации для шифрования данных. Ключевая информация может храниться с использованием ключей eToken PRO/32K и eToken PRO/64K (в форм факторе USB ключа и смарт-карты) производства ЗАО «Аладдин Р.Д.». СЗД обеспечивает возможность их расшифрования только при наличии нескольких ключей (одновременно несколькими пользователями), только на конкретном компьютере, а также позволяет создавать ключевой сервер в локальной сети.

СЗД «Панцирь» ориентирована на корпоративное применение - позволяет эффективно противодействовать инсайдерским атакам (внутренним ИТ-угрозам), делая невозможным нарушение конфиденциальности данных при хищении носителя (компьютера, жесткого диска или отчуждаемого накопителя, например, Flash-устройства) даже при наличии у злоумышленника (инсайдера) ключа шифрования.

При совместном использовании СЗИ «VPN «Панцирь» для ОС Windows 2000/XP/2003/Vista» и СЗД «Панцирь» для ОС Windows 2000/XP/2003/Vista» реализует комплексная криптографическая защита информации – информация защищается и при передаче по каналам связи, и при хранении, причем, как на жестких дисках, так и на внешних накопителях (например, на Flash-устройствах). Эффективность интеграции данных продуктов семейства «Панцирь» обуславливается не только различием решаемых данными средствами задач защиты информации (которые следует решать в комплексе при защите корпоративной сети), но и единообразием подходов к реализации (разграничительная политика реализуется на основании ID, ключевая информация не связана с идентификаторами и паролями пользователей, предусмотрены меры по противодействию внутренним ИТ-угрозам, используется одна и та же номенклатура криптопровайдеров и внешних устройств для хранения ключевой информации и т.д.).

5.2. Интеграция с Комплексными системами защиты информации (КСЗИ) «Панцирь» для ОС Windows 2000/XP/2003/Vista»

На сегодняшний день линейка продуктов семейства «Панцирь» представлена следующими КСЗИ:

- Комплексная система защиты информации (КСЗИ) «Панцирь-К» собственными средствами (без использования встроенных в ОС механизмов защиты) реализует все требования, предъявляемые к защите конфиденциальной информации от несанкционированного доступа. КСЗИ сертифицирована ФСТЭК России по 5 классу СВТ (сертификат №1144) и может использоваться при построении АС до класса 1Г включительно;
- Комплексная система защиты информации (КСЗИ) «Панцирь-С», разграничительная политика доступа к ресурсам в которой основана на реализации мандатного контроля и управления потоками, сертифицирована ФСТЭК России по 4 классу СВТ и 3 уровню контроля НДВ (сертификат №1595) и может использоваться при построении АС до класса 1В включительно.



Замечание. СЗД «Панцирь» поставляется, как в качестве самостоятельного средства защиты, так и в составе КСЗИ «Панцирь-К» и «Панцирь-С».

К комплексным системам защиты данные КСЗИ могут быть отнесены ввиду того, что они могут эффективно применяться для защиты, как от внешних, так и от внутренних ИТ-угроз, обеспечивая эффективное противодействия атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей). КСЗИ могут использоваться для эффективного противодействия вирусным атакам, эксплойтам, вредоносным, шпионским и любым иным деструктивным программам, атакам на ошибки программирования в системном и прикладном ПО; содержат в своем составе, как механизмы защиты от несанкционированного доступа, так и механизмы криптографической защиты данных на жестком диске и отчуждаемых накопителях (реализуются средствами СЗД «Панцирь»).

В отличие от СЗД, основу которой составляет криптографическая защита данных, КСЗИ, в первую очередь, это средство защиты информации и системных ресурсов от несанкционированного доступа, основанное на реализации разграничительной политики доступа пользователей и процессов к защищаемым информационным и системным ресурсам, и к устройствам.

В КСЗИ внедрены инновационные технологии защиты информации (НОУ-ХАУ компании). На способы и технические решения, реализованные в КСЗИ, получено 11 патентов на изобретения. Реализация практически каждого механизма защиты КСЗИ оригинальна (запатентована), обладает принципиально новыми свойствами защиты, что позволяет принципиально поднять уровень эффективности защиты и расширить ее функциональные возможности.

К инновационным технологиям, реализованным в КСЗИ, могут быть отнесены: включение в основные механизмы контроля доступа к ресурсам (к файловым объектам, к реестру ОС, к сетевым ресурсам и т.д.) субъекта «процесс», как самостоятельного субъекта доступа, контроль сервисов олицетворения – эффективный механизм защиты от атак на повышение привилегий; разделение между пользователями ресурсов, не разделяемых ОС и приложениями, без которого невозможна корректная реализация разграничительной политики доступа к ресурсам, вероятностный контроль доступа к файловым объектам (мандатный принцип контроля доступа несет в себе угрозу заражения макровирусами конфиденциальных данных при обработке открытой информации), контроль подключения (монтирования) устройств, в том числе, по их серийным номерам, защита системного диска от несанкционированной модификации даже с системными правами и многое другое.

КСЗИ предлагают различные, унифицированные с иными средствами семейства «Панцирь», варианты хранения парольной информации, используемой при аутентификации пользователя при входе в систему (в файловом объекте, в реестре ОС, на внешних накопителях, на ключах eToken PRO/32K и eToken PRO/64K (в форм факторе USB ключа и смарт-карты) производства ЗАО «Аладдин Р.Д.». При интеграции средств семейства «Панцирь» на одном и том же внешнем устройстве (накопитель, ключ, карта) может располагаться и пароль пользователя для входа в систему, и технологический ключ шифрования для доступа в VPN, и ключи шифрования для расшифровывания данных, сохраняемых на жестком диске (локальном и разделенном в сети) и внешних накопителях – одно устройство для хранения всей необходимой информации для работы с защищаемыми ресурсами.

Интеграция СЗИ «VPN «Панцирь» для ОС Windows 2000/XP/2003/Vista» с КСЗИ семейства «Панцирь» (в состав которых включена СЗД «Панцирь») позволяет в комплексе обеспечить эффективное решение наиболее актуальных на сегодняшний день задач защиты информации и обеспечения компьютерной безопасности.

6. ИНТЕРФЕЙСЫ. АДМИНИСТРИРОВАНИЕ

Реализованные технологии при разработке СЗИ «VPN «Панцирь» для ОС Windows 2000/XP/2003/Vista» направлены, в том числе, и на снижение трудоемкости администрирования средства защиты при создании и эксплуатации VPN.

Настройка сервера VPN (осуществляется с АРМ, который может быть установлен, как собственно на сервере, так и на удаленной рабочей станции) включает следующие шаги:

- Задаются системные настройки сервера VPN. Это реализуется из интерфейса серверной части, приведенного на рис.1;
- Задается алгоритм шифрования, который будет использован для защиты каналов связи VPN, что реализуется из интерфейса, приведенного на рис.2;
- Создается база субъектов/объектов VPN. Это реализуется из интерфейса серверной части, приведенного на рис.1 (для каждого создаваемого субъекта/объекта могут быть внесены соответствующие произвольные комментарии, см. рис.3). При этом для каждого созданного субъекта/объекта определяется его статус – указывается, доверенный он (тогда ему разрешается взаимодействие с компьютерами, на которых не установлена клиентская часть КСЗИ), либо нет – корпоративный – сможет взаимодействовать только с корпоративными субъектами/объектами;
- При создании субъектов/объектов сервером VPN автоматически генерируются и запоминаются их идентификаторы (ID) и технологические ключи шифрования взаимодействия с сервером VPN (соответствующая информация по каждому субъекту/объекту сохраняется в одном файле на внешнем накопителе), которые необходимо экспортировать (сохранить на внешнем носителе, например, на Flash-устройстве), для последующей настройки клиентской части СЗИ;
- Настраивается разграничительная политика доступа в составе VPN (права доступа субъектов к объектам в составе VPN), что реализуется на сервере из интерфейса, приведенного на рис.3. Для этого в левой части интерфейса следует выбрать субъект/объект, для которого необходимо разграничить доступ (это может быть пользователь, либо компьютер). В качестве субъекта/объекта при задании разграничительной политики доступа может выступать и концентрирующий элемент (папка в «дереве сети»), например, для всех компьютеров (или сотрудников) одного филиала, отдела (в зависимости от того, какие ресурсы объединены в папку). В правой части, где также отображаются субъекты/объекты VPN (соответствующее «дерево сети»), следует выбрать субъекты/объекты (это также могут быть пользователи, либо компьютеры, при задании разграничений здесь также могут использоваться папки в «дереве сети»), к которым следует разрешить, либо запретить (в зависимости от реализуемой разграничительной политики – разрешительная или запретительная) доступ для выбранного субъекта/объекта.

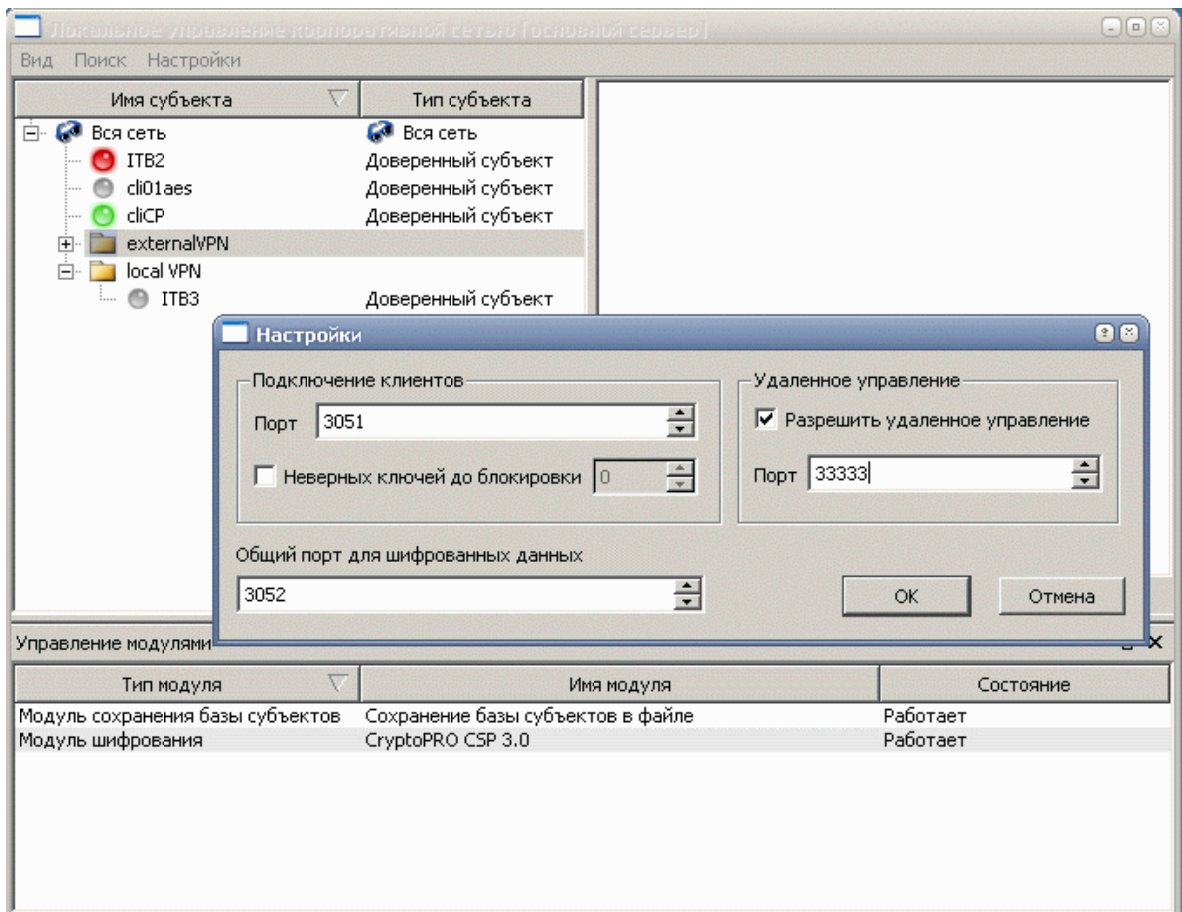


Рис.1. Системные настройки сервера VPN

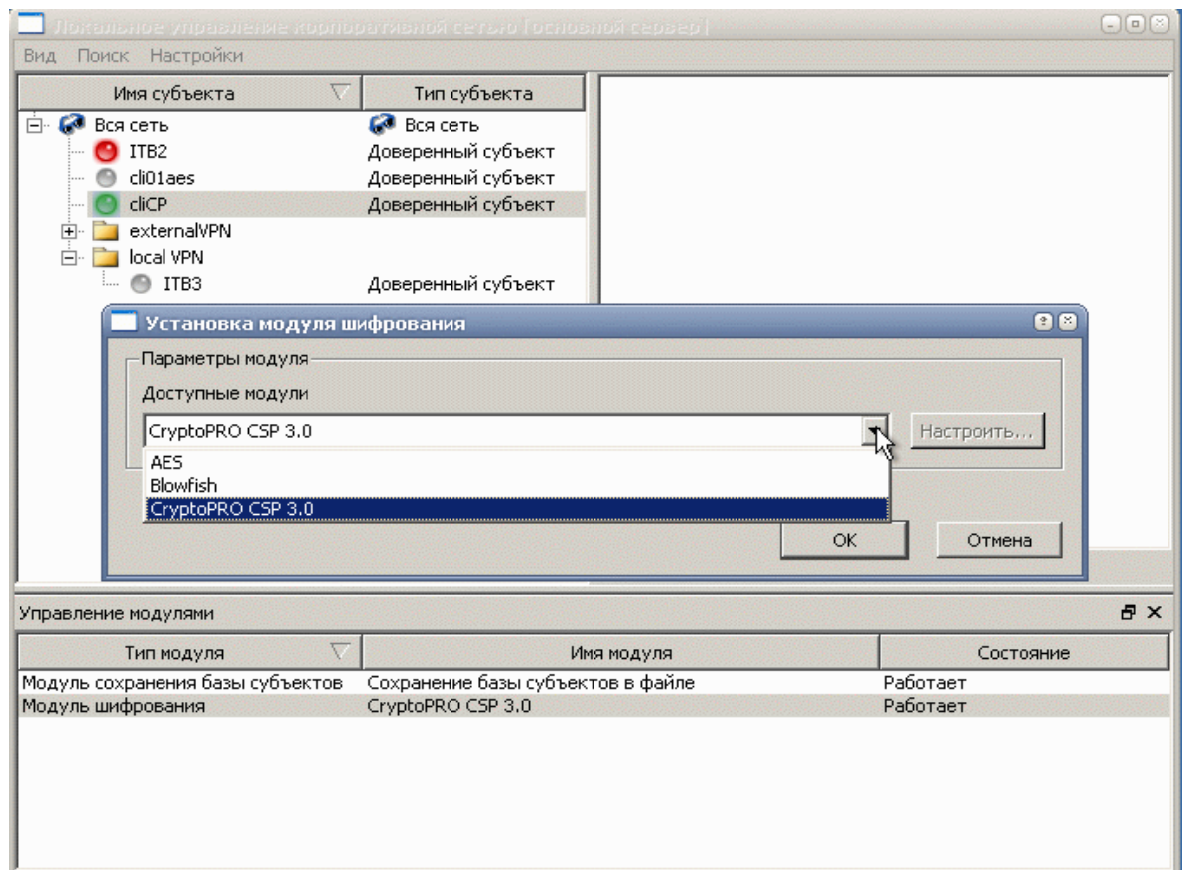


Рис.2. Задание алгоритма шифрования в VPN на сервере

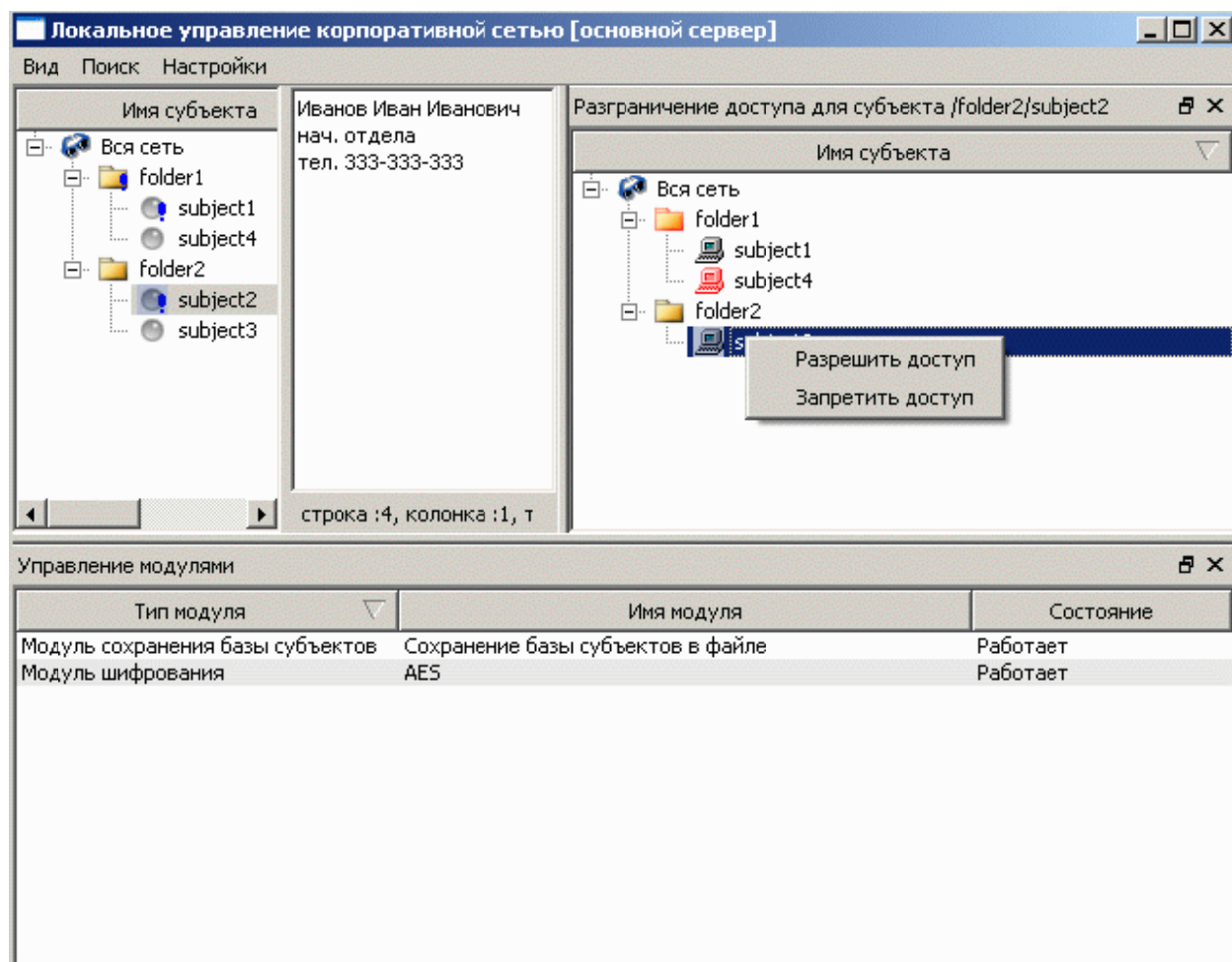


Рис.3. Настройка разграничительной политики доступа в составе VPN

Настройка клиентских частей VPN (осуществляется локально на рабочих станциях и серверах, включенных в состав VPN, при установке на них клиентской части СЗИ), включает следующие шаги:

- Задаются системные настройки взаимодействия с сервером VPN. Это реализуется из интерфейса клиентской части, приведенного на рис.4, и алгоритм шифрования, который будет использован для защиты каналов связи VPN (он должен совпадать с алгоритмом, заданным на сервере VPN);
- Задается способ хранения и ввода идентифицирующих субъект/объект данных и технологического ключа взаимодействия с сервером VPN. Это реализуется из интерфейса клиентской части, приведенного на рис.5. При этом определяется сущность «субъект/объект» - если соответствующая информация будет сохраняться в файле (на жестком диске), либо в реестре ОС, то в качестве субъекта/объекта VPN будет выступать непосредственно компьютер. Если на внешний накопитель (в файле, например на Flash-устройстве), либо на электронный ключ или карту, то пользователь;
- Идентифицирующие субъект/объект данные и технологический ключ взаимодействия с сервером VPN записываются в выбранное место хранения (в файл, в реестр ОС, на внешний накопитель, на электронный ключ, либо магнитную карту);
- В случае сохранения идентифицирующих субъект/объект данных и технологического ключа взаимодействия с сервером VPN на внешний накопитель, на электронный ключ, либо на магнитную карту, данный носитель предоставляется пользователю.

Замечание. Если на компьютере определен способ хранения и ввода идентифицирующих субъект/объект данных и технологического ключа взаимодействия с сервером VPN с электронного ключа, либо с магнитной карты – в качестве субъекта/объекта определен не компьютер, а пользователь, то с этого компьютера может получить доступ к ресурсам VPN любой пользователь (в рамках заданной для него разграничительной политики, определяемой ID), идентифицированный в VPN – являющийся субъектом/объектом (со своим технологическим ключом). При настройке клиентских частей СЗИ на компьютерах, для которых определен способ хранения и ввода идентифицирующих субъект/объект данных и технологического ключа взаимодействия с сервером VPN с электронного ключа, либо с магнитной карты, не требуется записывать соответствующую идентифицирующую информацию на внешний носитель – достаточно задать соответствующий способ хранения идентифицирующих субъект/объект данных и технологического ключа взаимодействия с сервером VPN (из интерфейса, представленного на рис.5). Собственно внешние носители могут быть созданы администратором централизованно – на них должны быть записаны соответствующие идентифицирующие субъект/объект данные и технологический ключ взаимодействия с сервером VPN, после чего, данные носители должны быть розданы администратором пользователям, допущенным к работе в VPN.

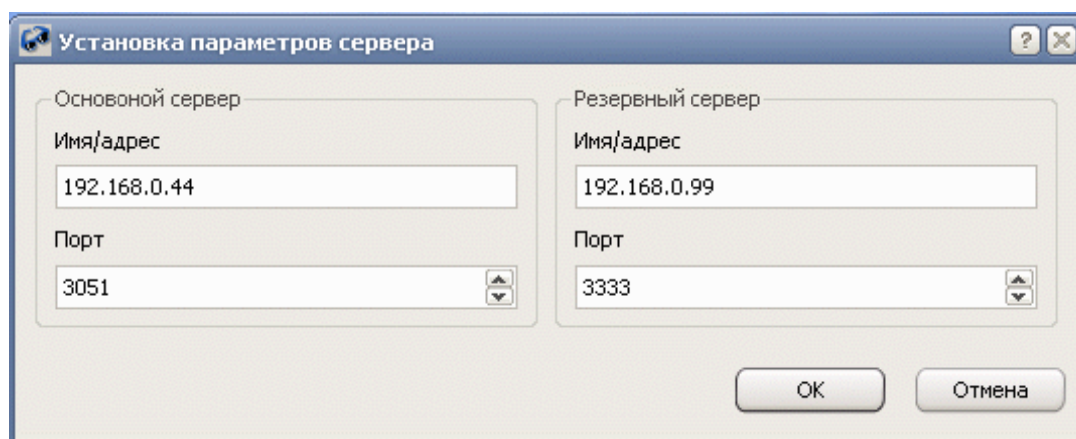


Рис.4. Системные настройки взаимодействия с сервером VPN на клиентской части

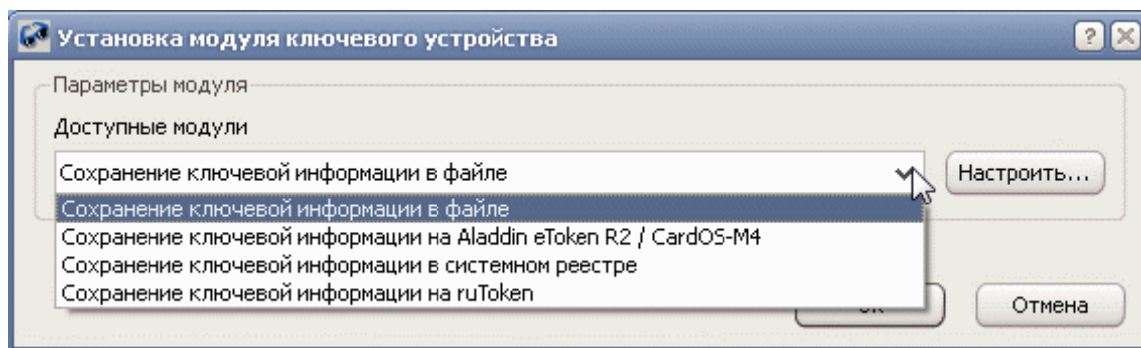


Рис.5. Задание способа хранения и ввода идентифицирующих субъект/объект данных



Настройка VPN завершена.

В процессе функционирования, от пользователя (если он, а не компьютер, является субъектом VPN) требуется лишь подключить электронный ключ (карту) к компьютеру для идентификации, с целью получения доступа к сети (если субъектом/объектом является компьютер, его идентификация проводится автоматически, при включении), от администратора в процессе функционирования VPN не требуется никаких дополнительных действий (все ключи шифрования между каждой парой субъектов/объектов на сервере VPN генерируются автоматически, при каждом подключении компьютера из состава VPN к серверу VPN). Администратору остается только осуществлять функции контроля работы пользователей в VPN с использованием соответствующих средств аудита. Кроме того, он может осуществлять необходимые текущие оперативные действия по управлению VPN, например, создать новый субъект/объект, временно заблокировать идентификатор (субъект/объект) – вывести его из состава корпоративной VPN, изменить статус субъекта/объекта, изменить технологический ключ взаимодействия с сервером VPN и т.д.

7. ТЕКУЩЕЕ СОСТОЯНИЕ РАЗРАБОТКИ СЗИ «VPN «ПАНЦИРЬ» ДЛЯ ОС WINDOWS 2000/XP/2003/Vista»

На данный момент времени завершается тестирование СЗИ, начало ее поставок намечено на октябрь-ноябрь 2008 года.