УТВЕРЖДЕН

ФРКЕ. 00029-04 90 01-ЛУ

Регламент информационной безопасности при использовании программно-аппаратных средств комплекса ViPNet

ФРКЕ. 00029-04 90 01

Москва, 2010 г.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

АП	Абонентский пункт
КД	Ключевая дискета
КН	Ключевой набор
КЦ	Ключевой центр
НСД	Несанкционируемый доступ
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
РНПК	Резервный набор персональных ключей
СКЗИ	Средство криптографической защиты информации
СМ	Сервер-маршрутизатор
СУ	Сетевой узел
ТК	Тип коллектива
ТС	Технические средства
УКЦ	Удостоверяющий и Ключевой центр
УЛ	Уполномоченное лицо
УЦ	Удостоверяющий центр
ЦР	Центр регистрации
ЦУС	Центр управления сетью
ЭЦП	Электронная цифровая подпись

1 ОБЩИЕ ПОЛОЖЕНИЯ

Технология ViPNet – это комплекс программно–технических средств, предоставляющий возможность создать в любой телекоммуникационной инфраструктуре распределенную виртуальную сеть, защищенную от сетевых атак и несанкционированного доступа к информации.

Комплекс ViPNet позволяет создать:

- распределенную структуру межсетевых и персональных сетевых экранов;
- распределенную систему шифрования IP-трафика любых приложений;
- распределенную систему организации доступа к открытым ресурсам;
- систему управления (администрирования) средствами комплекса в защищенной сети;
- систему электронной цифровой подписи и шифрования информации на прикладном уровне;
- систему сертификации ключей подписи;
- систему защищенного обмена оперативными сообщениями;
- систему автоматической доставки файлов любого типа (служба автопроцессинга) с автоматической подписью и проверкой подписи доставляемых файлов.

1.1 ОСНОВНЫЕ ОБЪЕКТЫ СЕТИ VIPNET

Виртуальная сеть ViPNet – сеть, состоящая из компьютеров, на которых установлено ПО ViPNet. Каждая сеть ViPNet имеет свой уникальный номер при поставке сети конкретному заказчику. Каждая сеть должна содержать свой Центр управления сетью (ЦУС) и свой Удостоверяющий и Ключевой центр (УКЦ).

Сеть состоит из сетевых узлов (СУ), каждый из которых является либо сервером-маршрутизатором (СМ) (с установленным ПО ViPNet Координатор), либо абонентским пунктом (АП) (с установленным ПО ViPNet Клиент). Каждый АП привязан к одному серверу. Для размещения ЦУС и УКЦ в сети выделяются один или 2 АП – АП ЦУС и АП УКЦ.

СУ регистрируется в прикладных задачах, которые необходимы пользователям данных СУ для выполнения своих задач.

На каждом СУ регистрируются один или несколько типов коллективов (ТК). С

точки зрения шифрования информации в сети ViPNet основными объектами адресации при шифровании являются коллективы. Коллектив – это совокупность пользователей одного сетевого узла, зарегистрированных в одном и том же ТК. Общий коллектив СУ – это совокупность всех пользователей данного сетевого узла. Матрица связей задается в ЦУС для коллективов, генерация ключей обмена в УКЦ производится только для коллективов в соответствии с заданными связями. Любые два СУ считаются связанными, если задана некоторая связь между любым ТК, зарегистрированном на одном СУ, и любым ТК, зарегистрированным на другом СУ.

Пользователи сети ViPNet регистрируются в ТК. Пользователь может входить в несколько коллективов, зарегистрированных на одном или нескольких СУ, в каждом ТК может быть зарегистрировано 1 или более пользователей. Пользователь считается зарегистрированным на СУ только в том случае, если он зарегистрирован хотя бы в одном ТК, зарегистрированном на данном СУ. При этом любой пользователь, зарегистрированный на СУ, автоматически регистрируется в общем коллективе СУ. Это означает, что все пользователи, зарегистрированные на СУ, имеют равный доступ к ключам общего коллектива. Более подробное описание объектов сети ViPNet приведено в документах [1], [6].

1.2 СОСТАВ ПРОГРАММНЫХ СРЕДСТВ КОМПЛЕКСА VIPNET, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОСТРОЕНИЯ ЗАЩИЩЕННОЙ СЕТИ

1.2.1 ViPNet Администратор

Включает в себя ПО ViPNet Центр управления сетью, ПО ViPNet Удостоверяющий и Ключевой центр. Устанавливается на АРМ Администратор.

Центр управления сетью (ЦУС) – предназначен для создания инфраструктуры виртуальной сети, установления требуемых связей между объектами сети и управления средствами защиты ViPNet, установленных на объектах данной сети.

Удостоверяющий и Ключевой центр (УКЦ) – предназначен для формирования первичной ключевой информации (файлов ключевых дистрибутивов), обновления ключевой информации в процессе эксплуатации в соответствии с заданными связями для объектов сети, оснащенными средствами защиты ViPNet, выдачи пользователям сертификатов ключей подписей (далее–сертификатов) и выполнения всех других функций, необходимых для функционирования служб ЭЦП.

1.2.2 ViPNet Координатор

Многофункциональное средство защиты сети предназначено для обеспечения, в зависимости от настроек, следующих основных функций:

- сервера IP–адресов (регистрация и оповещение объектов сети о способах доступа к ним);
- прокси–сервера, осуществляющего преобразование адресов (NAT), для защищенных соединений;
- сервера–туннеля (шифрование межсетевого трафика);
- межсетевого и персонального экрана;
- сервера почтовых и управляющих сообщений.

1.2.3 ViPNet Клиент (абонентский пункт)

Многофункциональное средство защиты, реализующее на каждом компьютере (рабочей станции, сервере) следующие функции:

- защиту от несанкционированного доступа из внешней и локальной сети с помощью встроенного персонального сетевого экрана, в том числе с защищенных модулями ViPNet рабочих станций внутри защищенных соединений в соответствии с установленными для каждого узла ViPNet правилами фильтрации;
- автоматическое установление виртуальных криптографически защищенных соединений (туннелей) для трафика любых приложений при их взаимодействии с другими объектами виртуальной защищенной сети;
- гарантированную доставку подписанных документов (файлов) по назначению (автопроцессинг, Деловая почта) с возможностью автоматического подтверждения доставки и прочтения документов подписанными извещениями;
- работу защищенных служб Деловой почты и оперативного обмена сообщениями;

1.2.4 ViPNet Центр регистрации

Средство регистрации внешних по отношению к сети ViPNet пользователей ЭЦП. Обеспечивает следующие функции:

- формирование ключей ЭЦП для пользователей, не являющихся

пользователями защищенной сети ViPNet;

- создание запросов на сертификаты ключей ЭЦП для пользователей;
- прием и выдачу изданных УКЦ сертификатов ЭЦП;
- создание запросов на отзыв, приостановление и возобновление сертификатов ЭЦП.

1.3 ТРЕБОВАНИЯ К СОСТАВУ ТЕХНИЧЕСКИХ СРЕДСТВ И ОПЕРАЦИОННЫМ СИСТЕМАМ

ПО ViPNet предназначено для работы на IBM-совместимых компьютерах со следующей рекомендуемой конфигурацией:

процессор:

не ниже Pentium IV,

ОЗУ не менее:

- ViPNet Клиент – 512 Мбайт;
- ViPNet Координатор – в зависимости от количества защищенных компьютеров:

Количество АП	ОЗУ
до 100 шт.	1 Гбайт
до 1000 шт.	2 Гбайт
до 5000 шт.	4 Гбайт

- ViPNet Администратор, ViPNet Центр регистрации – 1 Гбайт,

свободное место на жестком диске:

- ViPNet Клиент – не менее 1 Гбайт;
- ViPNet Координатор, – не менее 10 Гбайт;
- ViPNet Администратор, ViPNet Центр регистрации – не менее 20 Гбайт,

сетевые интерфейсы:

одна или более сетевых плат, WiFi- адаптеры, модем, виртуальные адаптеры и другие интерфейсы, поддерживающие IP-протокол,

дополнительное оборудование:

- устройства типа «Электронный замок» - является обязательным для компьютеров, на которых установлены компоненты ПО ViPNet Администратор. Допускается эксплуатация ПО ViPNet Координатор/Клиент без устройств типа «Электронный замок» в

охраняемых помещениях, обеспечивающих невозможность доступа посторонних лиц к компьютерам;

- устройства бесперебойного питания – рекомендуется для ViPNet Координатор, ViPNet Администратор,

настройки локальной сети:

для работы Координатора для его сетевых интерфейсов, по – возможности, должны быть выделены постоянные IP-адреса,

операционные системы:

Windows: 2000 (SP2)/ XP / Server 2003/, Vista / Server 2008; допускается установка пакетов обновлений Microsoft,

Linux: Linux XP 2008 Server/ Desktop Secure Edition/ RedHat Enterprise Linux 4.0 AS/ Open SuSe Linux 10.0, 11.1/ SuSE Linux Enterprise Server 10 SP1, SP2/ Slackware Linux 10.2, 12.0/ Ubuntu 8.04 LTS Desktop/ Debian Etch 4.0 r1.

дополнительное ПО:

- на клиентах Windows, при необходимости, офисный пакет Microsoft;
- антивирусные программы – обязательно.

Запрещается:

- пользоваться измененными или отладочными версиями ОС, такими, например, как Debug/Checked Build;
- устанавливать средства отладки и трассировки ПО.

2 РАЗГРАНИЧЕНИЕ ПОЛНОМОЧИЙ В СЕТИ VIPNET

Пользователи сети ViPNet в соответствии со своими полномочиями разделяются на 3 группы.

Пользователи сети ViPNet – пользователи, зарегистрированные на одном или нескольких СУ и имеющие доступ к ключевой информации СУ.

Внешние пользователи ЭЦП – пользователи, не зарегистрированные ни на одном СУ ViPNet и имеющие доступ только к ключам ЭЦП. Использование средств ЭЦП данными пользователями допускается на выделенных для этих целей АП сети ViPNet.

Администраторы сети ViPNet – пользователи сети ViPNet, обладающие дополнительными полномочиями. Для обеспечения безопасной эксплуатации сети рекомендуется формировать 3 группы администраторов со следующими полномочиями.

2.1 ГРУППА АДМИНИСТРАТОРОВ БЕЗОПАСНОСТИ

Администратор безопасности выполняет следующие функции:

- осуществляет контроль и несет ответственность за соблюдением правил безопасной эксплуатации сети или группы подчиненных ему СУ;
- осуществляет настройки ОС и прикладного ПО;
- осуществляет контроль за попытками несанкционированного изменения режима безопасности;
- осуществляет контроль за соблюдением правил эксплуатации и соблюдением мер защиты от НСД;
- периодически осуществляет проверку целостности ПО;
- контролирует попытки несанкционированного доступа к ПО, попытки сетевых атак и проявления сетевой активности приложений.

Для обеспечения своих функций администратор безопасности должен:

- быть зарегистрирован как пользователь сети ViPNet;
- обладать максимальным уровнем полномочий в прикладной задаче «Защита трафика»;
- иметь связи со всеми подконтрольными ему СУ сети;
- обладать паролями входа в ОС с правами администратора и паролем администратора СУ сети ViPNet.

При выполнении своих обязанностей администратор безопасности руководствуется данным документом, должностными инструкциями, а также документами [6], [8].

2.2 ГРУППА АДРЕСНОЙ АДМИНИСТРАЦИИ

Данная группа включает в себя администраторов ЦУС и ЦР.

Администратор ЦУС выполняет следующие функции:

- осуществляет регистрацию сетевых узлов и пользователей сети ViPNet;
- регистрирует сетевые узлы в прикладных задачах;
- назначает полномочия пользователей сети ViPNet в прикладных задачах;
- назначает связи между объектами сети;
- формирует и рассылает справочники для всех сетевых узлов и Удостоверяющего и Ключевого центра, а также рассылает обновления ключевой и справочной информации, сформированные в УКЦ;
- обеспечивает плановую смену ключей СУ и смену ключей при компрометации;
- обеспечивает взаимодействие с ЦУС других сетей ViPNet.

Для обеспечения своих функций администратор ЦУС должен:

- быть зарегистрирован как пользователь сети ViPNet на абонентском пункте, на котором зарегистрирована прикладная задача «Центр управления сетью», а также прикладная задача «Защита трафика» с минимальными полномочиями;
- обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей;
- иметь полный доступ к программе ViPNet Администратор [Центр управления сетью] и ее рабочим каталогам.

При выполнении своих обязанностей администратор ЦУС руководствуется данным документом, должностными инструкциями, а также документами [1] и [5].

Администратор ЦР выполняет следующие функции:

- осуществляет регистрацию внешних пользователей;
- создает запросы на издание обновление и отзыв сертификатов внешних пользователей;
- осуществляет, при необходимости проверку сертификатов внешних пользователей.

Для обеспечения своих функций администратор ЦР должен:

- быть зарегистрирован как пользователь сети ViPNet на абонентском пункте, на котором зарегистрирована прикладная задача «Центр регистрации», а также прикладная задача «Защита трафика» с минимальными полномочиями;
- иметь действительный ключ подписи и сертификат для подписи запросов к Удостоверяющему центру;
- обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей;
- иметь полный доступ к программе ViPNet Администратор [Центр регистрации] и ее рабочим каталогам.

При выполнении своих обязанностей администратор ЦР руководствуется данным документом, должностными инструкциями, а также документами [1], [4], [5].

2.3 ГРУППА АДМИНИСТРАТОРОВ УКЦ

Данная группа включает в себя администраторов УКЦ. В соответствии с функциональностью программы УКЦ администраторы данной группы могут разделяться на подгруппы: уполномоченное лицо (УЛ) Удостоверяющего центра, администратор Ключевого центра (КЦ).

- **Администратор УКЦ, как администратор КЦ, выполняет следующие функции:**
  - осуществляет первичную генерацию ключевой информации УКЦ и сетевых узлов;
  - осуществляет формирование симметричных ключей шифрования для сетевых узлов;
  - осуществляет формирование и своевременную смену мастер-ключей своей сети и для межсетевого взаимодействия;
  - обеспечивает своевременную передачу в ЦУС сформированной ключевой и справочной информации.
- **Администратор УКЦ, как уполномоченное лицо УЦ, выполняет следующие функции:**
  - формирует ключ подписи УЛ и издает корневой сертификат УЛ;
  - формирует ключи подписи УЛ и запросы на сертификаты УЛ к вышестоящему УЦ;
  - осуществляет первичную генерацию ключей подписи и издание

сертификатов для пользователей сети;

- издает сертификаты ключей подписей по запросам ЦР и запросам на обновление сертификатов;
- отзывает, приостанавливает и возобновляет сертификаты пользователей по их запросам или по запросам ЦР;
- осуществляет экспорт и отправку в ЦУС справочников сертификатов УЛ, пользователей, списков отозванных сертификатов.

В общие обязанности администраторов УКЦ включаются:

- своевременное создание архивов баз данных и восстановление при сбоях;
- настройка и ведение журналов УКЦ;
- ведение документации УКЦ в соответствии с [5] и должностными инструкциями.

Для обеспечения своих функций администратор УКЦ должен:

- быть зарегистрирован как пользователь сети ViPNet на абонентском пункте, на котором зарегистрирована прикладная задача «Удостоверяющий и Ключевой центр», а также прикладная задача «Защита трафика» с минимальными полномочиями;
- обладать паролями входа в ОС с правами, достаточными для выполнения своих обязанностей;
- иметь полный доступ к программе ViPNet Администратор [Удостоверяющий и Ключевой центр] и ее рабочим каталогам.

При выполнении своих обязанностей администратор ЦР руководствуется данным документом, должностными инструкциями, а также документами [2], [4], [5].

3 РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ И СУ В СЕТИ VIPNET

Регистрацию пользователей и СУ в сети ViPNet осуществляет администратор, входящий в группу адресной администрации с использованием ПО ViPNet Администратор [Центр управления сетью].

При регистрации СУ администратор руководствуется следующими правилами:

- СУ регистрируется только в тех прикладных задачах, которые необходимы пользователям данных СУ для выполнения своих задач;
- связи СУ задаются выборочно, не следует без необходимости использовать опцию «Автоматически связывать новый ТК со всеми ТК»;
- связь с АП, на котором зарегистрирована задача «УКЦ», устанавливается только с АП, на котором зарегистрирована задача «ЦУС» (если эти АП разные);
- связь с АП ЦУС устанавливается только для СУ с зарегистрированной задачей «Пункт Регистрации» и, при необходимости, для АП пользователей, входящих в группу администраторов безопасности.

При регистрации пользователя администратор руководствуется следующими правилами:

- пользователям, не входящим в группу администраторов безопасности, устанавливается минимальный уровень полномочий в задаче «Защита трафика»;
- пользователи, входящие в группу администраторов безопасности, регистрируются со средним или максимальным уровнем полномочий в зависимости от возложенных на них задач;
- пользователи регистрируются только на тех СУ, доступ к которым им необходим для выполнения своих служебных обязанностей;
- право подписи безусловно присваивается пользователям, входящим в группы администраторов ЦР и УКЦ. Остальным пользователям - при необходимости.

4 РЕЖИМЫ БЕЗОПАСНОСТИ В СЕТИ VIPNET

ПО ViPNet Координатор (ViPNet Клиент) может работать в следующих режимах безопасности обработки открытого трафика:

1. **блокировать IP-пакеты всех соединений**;
2. **блокировать все соединения, кроме разрешенных**;
3. пропускать все исходящие соединения, кроме запрещенных (режим Бумеранг);
4. пропускать все соединения;
5. пропускать IP-пакеты без обработки.

Режимы 4 и 5 предназначены исключительно для проведения тестирования и настроек ЛВС, требующих исключения влияния ViPNet на работу сети. Временный перевод ПО в данные режимы может осуществляться только с разрешения и под контролем администраторов группы администраторов безопасности при проведении работ по настройке или восстановлению ЛВС.

Необходимость и возможность использования иных режимов работы определяется администратором безопасности для конкретных групп СУ исходя из структуры ЛВС и политики безопасности. При выборе режимов для СУ, входящих в один сегмент ЛВС с АП ЦУС и УКЦ, администратор обязан руководствоваться требованиями документа [4].

При выборе 2 режима безопасности перечень открытых адресов или пар адресов (для Координатора), направлений соединений, допустимых протоколов и портов в фильтрах открытой сети, регистрируемый для конкретных групп СУ, определяется по согласованию с администратором безопасности.

При необходимости использования 3 режима безопасности администратор безопасности обязан:

- определить, при необходимости, перечень открытых адресов, протоколов и портов, запрещенных к использованию при инициативных соединениях для конкретных групп СУ;
- обеспечить соответствующие настройки фильтров открытой сети, блокирующие открытые инициативные соединения с запрещенными адресами;
- осуществлять периодический контроль IP-трафика СУ.

Контроль трафика осуществляется администратором путем удаленного запроса журналов IP-пакетов. При выявлении установленных соединений с потенциально опасными открытыми сетевыми ресурсами или изменении списка запрещенных адресов и протоколов администратор осуществляет дополнительную настройку фильтров открытый сети или принимает решение об изменении режима безопасности для данного СУ.

5 УСТАНОВКА И ВВОД В ЭКСПЛУАТАЦИЮ СУ В СЕТИ VIPNET

5.1 ТРЕБОВАНИЯ К РАЗМЕЩЕНИЮ ТЕХНИЧЕСКИХ СРЕДСТВ

5.1.1 Общие требования

При размещении технических средств (ТС) ViPNet следует руководствоваться следующими рекомендациями.

1. Размещение, охрана и специальное оборудование помещений, в которых установлены ТС и ведется работа с носителями персональной ключевой информации, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, прослушивания ведущихся там переговоров и просмотра помещений посторонними лицами, а также гарантировать сохранность находящихся в этих помещениях конфиденциальных документов.
2. Порядок охраны и организации режима помещений, в которых установлены ТС, регламентируется разделом IV инструкции [10].
3. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок эвакуации конфиденциальных документов и дальнейшего их хранения.
4. Технические средства ViPNet могут подключаться к общегородской сети электроснабжения с учетом требований инструкций по эксплуатации вычислительных средств и правил техники безопасности.
5. Оборудование помещений средствами вентиляции и кондиционирования воздуха должно соответствовать санитарно-гигиеническими нормам СНиП, устанавливаемым законодательством Российской Федерации.
6. При подключении СКЗИ к каналам передачи данных, выходящих за пределы контролируемой зоны, необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К). При монтаже каналов связи, гальванические цепи которых непосредственно от ПЭВМ (с установленным на нем СКЗИ) выходят за

пределы контролируемой территории, должны использоваться оптоволоконные развязки. При использовании СКЗИ только для выполнения функций генерации/проверки ЭЦП, а также, если подключение к каналам передачи данных, выходящих за пределы контролируемой зоны, осуществляется через активное канальное оборудование (находящееся в пределах контролируемой зоны), то использование оптоволоконной развязки не требуется

5.1.2 Размещение ViPNet Администратор, ViPNet Центр регистрации

1. Помещения, в которых устанавливаются компоненты ViPNet Администратор, ViPNet Центр регистрации, относятся к защищаемым помещениям, обеспечивающим конфиденциальность проводимых работ и исключающим возможность бесконтрольного нахождения в нем посторонних лиц.
2. Входные двери помещений должны быть оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время. Окна (при необходимости) и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.
3. Служебные помещения Удостоверяющего центра и Пункта регистрации, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях, оборудуются средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.
4. В помещение допускаются только сотрудники, имеющие непосредственное отношение к организации эксплуатации ViPNet Администратор, ViPNet Центр регистрации.
5. Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора.
6. Должны быть приняты меры по надежному сохранению в тайне паролей доступа, ключевых дистрибутивов и другой ключевой информации, размещенной на съемных носителях. Для хранения съемных носителей

помещение должно быть оборудовано сейфом.

7. По окончании рабочего дня, помещения закрываются, опечатываются и сдаются под охрану. Порядок сдачи помещений определяется эксплуатирующей организацией.

5.1.3 Размещение ViPNet Координатор

1. ViPNet Координаторы рекомендуется устанавливать в выделенных помещениях серверных узлов.
2. Доступ в помещение серверных узлов должен быть ограничен.
3. Дополнительных специальных требований к помещениям, где установлено ПО ViPNet Координатор, не предъявляется.

5.1.4 Размещение ViPNet Клиент

ViPNet Клиент является персональным средством защиты пользователя ViPNet и размещается на рабочем месте сотрудника эксплуатирующей организации – пользователя ViPNet . Дополнительных специальных требований к помещениям, где установлено ПО ViPNet Клиент, не предъявляется.

5.2 ТРЕБОВАНИЯ К СОСТАВУ И НАСТРОЙКАМ ОС

На компьютере устанавливается только одна ОС. Установленное программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

Примечание: Для ОС Linux при установке ПО ViPNet Координатор требуется наличие средств разработки (сборки модулей ядра). По завершении инсталляции данные средства должны быть удалены.

До установки ПО ViPNet и в дальнейшем в процессе работы должна осуществляться проверка на наличие вирусов.

При осуществлении настроек ОС Windows, учетных записей и прав пользователей следует руководствоваться справочной системой Windows (http://windowshelp.microsoft.com/Windows/ru-RU/Help) и рекомендациями разработчика ОС (http://www.microsoft.com/rus/technet/security).

Установка пакетов обновлений и дополнительного ПО в соответствии с.п. 1.3 производится, как правило, до установки ПО ViPNet. При необходимости установки

дополнительного ПО или пакета обновлений на СУ с уже установленным ПО ViPNet производится проверка настроек ОС в соответствии с данным пунктом и проверка работоспособности ПО ViPNet в соответствии с п. 6.3.

На компьютере, на котором устанавливается программа ViPNet Администратор [Центр управления сетью], должен быть установлен пакет программ ViPNet Клиент. До установки и первичной инициализации программы ViPNet Клиент [Монитор] (на этапе установки и первичного развертывания справочно-ключевой информации) компьютеры, на которых установлено ПО ViPNet Администратор должны быть физически отключены от локальной сети. При установке программ ViPNet Администратор [Центр управления сетью] и ViPNet Администратор [Удостоверяющий и Ключевой центр] на разные компьютеры последний должен быть физически отключен от локальной сети.

До установки ПО ViPNet рекомендуется осуществить следующие настройки ОС:

5.2.1 Общие требования:

- исключить из состава системы все оборудование, которое может создавать угрозу безопасности;
- каждый пользователь должен иметь для входа в ОС свою учетную запись;
- учетные записи пользователей, не входящих в группу администраторов безопасности, не должны входить в группу локальных администраторов данного компьютера;
- длина пароля учетной записи должна быть не менее 6 символов;
- запретить пользователям, не входящим в группу администраторов безопасности, осуществлять установку и модификацию прикладного и системного ПО;
- установить права доступа к каталогам установки ПО и другим каталогам компьютера для каждой учетной записи в соответствии с полномочиями пользователя в объеме, необходимом для выполнения его обязанностей;
- отключить учетную запись для гостевого входа (Guest);
- запретить или ограничить удаленное управление ОС путем отключения всех служб, реализующих данные механизмы, или путем настроек, запрещающих фильтров для протоколов и портов удаленного управления ОС для всех узлов, кроме специально выделенных для этих целей;
- права доступа к используемым общим ресурсам задать в соответствии с

политикой безопасности, принятой в организации;

5.2.2 ОС Windows

- удалить у группы Everyone все привилегии;
- ограничить права пользователей, не входящих в группу администраторов безопасности, на запись в системный реестр, что реализуется при помощи ACL или установкой прав доступа;
- ограничить использование Scheduler;
- устанавливать атрибуты SECURITY_ATTRIBUTES процессов и потоков в соответствии с требованиями безопасности всей системы в целом;
- для предотвращения стороннего анализа остаточной информации желательно использовать дополнительные ограничения по доступу к временным файлам;
- отказаться от использования режима автоматического входа пользователя при ее загрузке, если это специально не предусмотрено руководством пользователя или администратора ПО ViPNet или настоящим документом;
- исключить возможность удаленного редактирования системного реестра, если в модуле ViPNet разрешены открытые соединения с данным компьютером по соответствующим протоколам;
- отключить сервис DCOM, если в модуле ViPNet разрешены открытые соединения с данным компьютером по протоколам, использующим этот сервис;
- запретить вход в ОС через общедоступные каналы передачи данных для всех пользователей, включая группу Administrators, если в модуле ViPNet разрешены открытые соединения с данным компьютером по соответствующим протоколам;
- включать фильтры паролей, устанавливаемые вместе с пакетами обновлений ОС;
- ограничить доступ пользователей в каталог %SystemRoot%;
- установить права доступа к каталогам %Systemroot%\System32\Config, %Systemroot%\System32\SPOOL, %Systemroot%\Repair, %Systemroot%\COOKIES, %Systemroot%\FORMS, %Systemroot%\HISTORY, %Systemroot%\SENDTO, %Systemroot%\PROFILES,

%Systemroot%\OCCACHE, \TEMP, а также файлам boot.ini, autoexec.bat, config.sys, ntdetect.com и ntldr в соответствии с политикой безопасности, принятой в организации;

- после установки операционной системы удалить из каталога %Systemroot%\System32\Config файл sam.sav;
- использовать систему аудита в соответствии с политикой безопасности, принятой в организации;
- если в модуле ViPNet необходимо разрешить открытые соединения с данным компьютером по протоколу SMB, то следует установить в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\ Parameters** параметр EnableSecuritySignature (REG_DWORD) со значением 1 и параметр RequireSecuritySignature (REG_DWORD) со значением 1.

Рекомендуется внести следующие изменения в системном реестре:

- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa** установить параметр **RestrictAnonymous** (REG_DWORD) со значением 1 для исключения доступа анонимного пользователя к списку разделяемых ресурсов, а также для исключения доступа к содержимому системного реестра;
- удалить имя SPOOLSS из ключа **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes** для исключения утечки информации при передаче данных по именованному каналу \\server\PIPE\SPOOLSS;
- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters** установить параметры **AutoShareWks** (для Windows NT Workstation) и **AutoShareServer** (для Windows NT Server), имеющие тип REG_DWORD, со значением 0 для запрета автоматического создания скрытых совместных ресурсов;
- в ключе **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon** установить параметр **CachedLogonsCount** (REG_DWORD) со значением 0 для отключения кэширования паролей последних десяти пользователей, вошедших в систему;
- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog**

<LogName> (LogName – имя журнала, для которого следует ограничить доступ пользователям группы Everyone) установить параметр **RestrictedGuestAccess** (REG_DWORD) со значением 1 для исключения доступа группы Everyone к системному журналу и журналу приложений;

- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\MemoryManagement** установить параметр **ClearPageFileAtShutDown** (REG_DWORD) со значением 1 для включения механизма затирания файла подкачки при перезагрузке;
- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers** установить параметр **winreg** (REG_DWORD) со значением 1 для ограничения удаленного доступа к реестру;
- в ключе **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon** установить параметр **AllocateFloppies** (REG_SZ) со значением 1 для исключения параллельного использования дисковода для гибких дисков;
- в ключе **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon** установить параметр **DontDisplayLastUserName** (REG_SZ) со значением 1 для отключения отображения имени последнего зарегистрированного пользователя;
- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa** установить параметр **AuditBaseObjects** (REG_DWORD) со значением 1 для включения аудита базовых объектов системы;
- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa** установить параметр FullPrivilegeAuditing (REG_BINARY) со значением 1 для включения аудита привилегий;
- в ключе **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters** установить параметр **EnablePlainTextPassword** (REG_DWORD) со значением 0 для исключения передачи пароля пользователей по сети в открытом виде.

При использовании **Windows XP** следует произвести дополнительные настройки:

- запретить использование функции резервного копирования паролей;
- отключить режимы отображения окна всех зарегистрированных на

компьютере пользователей и быстрого переключения пользователей;

5.2.3 ОС Linux:

- на все директории, содержащие системные файлы ОС Linux и каталоги ПО ViPNet, устанавливают права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись;
- виртуальную память в ОС Linux следует организовать в виде отдельного раздела на отдельном жестком диске компьютера и доступ к ней должен иметь только пользователь root. В случае выхода из строя жесткого диска, на котором находится область виртуальной памяти, криптографические ключи считаются скомпрометированными, а жесткий диск неподлежащим ремонту. Этот жесткий диск уничтожается по правилам уничтожения ключевых носителей;
- установить право доступа к файлам конфигурации только пользователю root;
- ограничить (с учетом выбранной в организации политики безопасности) доступ пользователей к файлам и каталогам, находящимся на жестком диске рабочей станции;
- разрешить пользователям только запуск исполняемых файлов необходимых им для работы;
- отключить использование сетевой файловой системы NFS;
- отключить службу RPC удаленного вызова процедур;
- отключить использование почтовой программы sendmail;
- ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команды su – предоставления пользователю административных полномочий;
- ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команд cron и at – запуска команд в указанное время;
- включить протоколирование неудачных попыток регистрации в системе.

5.3 ТРЕБОВАНИЯ К НАСТРОЙКАМ ПО VIPNET

Настройки ПО ViPNet осуществляются администратором безопасности или уполномоченным лицом. Для осуществления настроек необходимо ввести пароль

администратора СУ.

5.3.1 Настройки ПО ViPNet Клиент/Координатор [Монитор]

1. Установить режим работы в соответствии с выбранным для данного СУ1 (см. раздел 4 и руководства пользователя [6], [7] и [8]).
2. При выборе 2 режима осуществить, при необходимости, в фильтрах открытой сети регистрацию открытых адресов, направлений соединений и протоколов, разрешенных для данного СУ.
3. При выборе 3 режима осуществить, при необходимости, настройку фильтров открытой сети для открытых адресов, запрещенных для данного СУ.

Для ViPNet Клиент/Координатор Windows:

1. Включить опцию «Обнаружение атак» (включена по умолчанию).
2. Ограничить интерфейс пользователя (за исключением СУ администраторов безопасности и других СУ, определенных специальным распоряжением).
3. Включить опцию «Обязательный ввод пароля при входе в ОС» (включена по умолчанию).
4. Включить опцию «Перезапускать Монитор при аварийном завершении» (включена по умолчанию).
5. Установить интервал автоматического блокирования компьютера 15 мин.
6. Опция «Разрешить сохранение пароля в реестре» – включение данной опции допустимо для СУ, работающих в необслуживаемом режиме при условии, что в окне "Настройки" включена опция "Блокировать компьютер при старте программы" и при условии обеспечения дополнительных организационных мер, исключающих доступ посторонних лиц к данному СУ. Во всех остальных случаях данная функция должна быть отключена. В этом случае допускается настройка операционной системы с автоматическим логоном при загрузке.
7. Рекомендуется включить опцию «Проводить обновления без предупреждений».

[1] Для ПО ViPNet Координатор данную настройку необходимо произвести для каждого сетевого интерфейса отдельно.

8. Осуществить иные настройки в соответствии с руководствами [6], [8] с учетом назначения СУ.

Для ViPNet Координатор Linux

1. Выполнить настройки системы защиты от сбоев.
2. Осуществить иные необходимые настройки в соответствии с руководством администратора [7].
3. Включить файлы конфигурации ViPNet Координатор Linux в список контроля целостности АПМДЗ («Аккорд» или «Соболь» в зависимости от комплектации)[2]. Перечень файлов конфигурации:

- /etc/failover.ini
- /etc/vipnet/user/iplir.conf
- /etc/vipnet/user/iplir.conf-<имя интерфейса>
- /etc/vipnet/user/upgrade.conf
- /etc/vipnet/user/firewall.conf
- /etc/vipnet/user/monitoring.conf
- /etc/vipnet/user/sga.conf
- /etc/vipnet/user/policy.conf
- /etc/vipnet/user/mftp.conf.

5.3.2 Настройки системы Контроля приложений:

Осуществить настройку списка приложений, которым разрешен доступ к сетевым ресурсам с данного СУ, осуществить другие настройки:

1. автоматически стартовать при входе в Windows – включено;
2. авторизация программ – по контрольному значению файла;
3. при регистрации – автоматически поместить в черный список;
4. при неуспешной авторизации – автоматически поместить в черный список.

5.4 ТРЕБОВАНИЯ ПО НАСТРОЙКАМ ЖУРНАЛОВ АУДИТА

Для журнала регистрации IP-пакетов необходимо установить следующие

[2] В дальнейшем изменение настроек требует прав администратора АПМДЗ для пересчета контрольных сумм файлов конфигурации.

настройки:

- регистрировать весь IP-трафик (по умолчанию);
- интервал регистрации 60 мин. (по умолчанию);
- размер журнала выбрать в зависимости от предполагаемого объема трафика. Рекомендуемые значения 1 Мб для журнала и 10 Мб для архива журналов (по умолчанию).

Для журнала системы контроля приложений:

- регистрировать события для приложений из:
  - белого списка – включит,
  - из черного списка – включить;
- интервал объединения однотипных событий – 60 мин. (по умолчанию);
- размер журнала выбрать в зависимости от предполагаемого объема трафика. Рекомендуемые значения 1 Мб для журнала и 10 Мб для архива журналов (по умолчанию).

6 УСТАНОВКА И ЭКСПЛУАТАЦИЯ СУ В СЕТИ VIPNET

6.1 УСТАНОВКА ПО

Установка ПО ViPNet осуществляется администратором безопасности или другим подготовленным специалистом под его контролем. До установки ПО должны быть осуществлены:

- проверка работоспособности технических средств и их соответствия требованиям (см. п. 1.3);
- проверка ОС на отсутствие вирусов;
- проверка и настройка ОС в соответствии с требованиями п. 5.2;
- проверка состава установленного ПО: должны отсутствовать средства отладки и ПО, не имеющее прямого отношения к назначению СУ.

Установка ПО и первичная инициализация ключевой информации осуществляется в соответствии с документацией на ПО.

По завершении инициализации осуществляются настройки ПО в соответствии с требованиями п. 5.3 и контроль работоспособности ПО (см. п. 6.3).

На каждое рабочее место, оснащенное ПО ViPNet, оформляется акт о вводе в эксплуатацию по типовой форме 1. Акт может храниться у администратора безопасности или у лица, ответственного за эксплуатацию СУ.

6.2 КОНТРОЛЬ ЦЕЛОСТНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПО

ПО ViPNet оснащено встроенными механизмами проверки целостности ПО, справочной, ключевой информации и журналов аудита (для ПО с СКЗИ «Домен-КМ»). Проверка производится при каждом старте ПО. Кроме того, в криптографическое ядро системы встроены механизмы периодического тестирования работоспособности и целостности криптографических библиотек и ключевой информации. Контроль целостности файлов журналов событий осуществляется при обращении к функциям просмотра или настройки журналов событий данного ПО. При наличии установленного на СУ устройства типа «Электронный замок» допускается использование дополнительных механизмов проверки целостности, предусмотренных такими устройствами. При обнаружении ошибок проверки целостности пользователь обязан прекратить эксплуатацию СУ и уведомить администратора безопасности о возникновении ошибок.

Примечание 1: в случае нарушения целостности программных модулей ПО

ViPNet при загрузке операционной системы выводится сообщение о данном факте с указанием имени модуля, после чего ПО ViPNet выгружается и передается управление компонентам операционной системы. В связи с этим в случае возникновения подобной ситуации администратор (пользователь) должен исключить возможность удаленного влияния на незащищенную ОС (отсоединить сетевые кабели) и произвести процедуру восстановления ПО ViPNet согласно документации.

Примечание 2: в случае нарушения целостности файлов журналов событий вход в прикладное ПО, обеспечение и восстановление работоспособности подсистемы аудита возможен после ввода пароля администратора СУ. При возникновении сообщения о наличии искажений пользователь обязан уведомить администратора безопасности и прекратить эксплуатацию прикладного ПО.

Администратор безопасности обязан:

- отключить СУ от ЛВС до устранения неисправностей;
- провести исследование с целью выяснения возможных причин искажения:
  - произвести проверку работоспособности технических средств СУ,
  - произвести проверку ОС и установленного ПО на наличие вирусов,
  - провести анализ журналов аудита с целью выявления попыток несанкционированного доступа в систему и сетевых атак,
  - провести анализ установленного ПО с целью выявления попыток несанкционированной установки дополнительных программ;
- при обнаружении признаков несанкционированного доступа к СУ уведомить администратора ЦУС о возможной компрометации ключевого набора СУ;
- устранить обнаруженные причины возникновения искажений;
- произвести переустановку ПО ViPNet;
- при необходимости произвести обновление ключевой информации СУ.

6.3 КОНТРОЛЬ РАБОТОСПОСОБНОСТИ И СОБЛЮДЕНИЯ ПРАВИЛ ЭКСПЛУАТАЦИИ

Администратор безопасности обязан осуществлять периодический контроль работоспособности и соблюдения правил эксплуатации СУ.

Контроль осуществляется как непосредственно на проверяемом СУ, так и удаленно.

Контрольная проверка на СУ осуществляется в следующих случаях:

- при вводе СУ в эксплуатацию;
- при изменении лица, ответственного за эксплуатацию;
- при изменении состава аппаратных средств СУ;
- при установке пакетов обновлений ОС, изменении версии ОС или состава дополнительного ПО, установленного на СУ;
- периодически.[3]

Результаты проверки оформляются в виде протокола проверки в соответствии с Приложением 2.

Удаленная проверка СУ осуществляется выборочно или полностью для всех СУ после процедуры удаленного обновления ПО ViPNet и периодически в промежутках между контрольными проверками[4]. Результаты проверки оформляются в виде протокола проверки в соответствии с Приложением 3.

При обнаружении фактов сбоев в работе ПО или нарушения правил эксплуатации администратор безопасности обязан принять меры для устранения выявленных нарушений, оценить возможные последствия. При обнаружении событий, которые могли привести к компрометации ключей СУ немедленно прекратить его работу и поставить в известность администратора ЦУС.

6.4 ОБНОВЛЕНИЕ ПО

Обновление ПО ViPNet может осуществляться двумя способами:

- локально, путем запуска штатной процедуры установки на локальном компьютере. Установка обновлений таким способом производится администратором безопасности или с его ведома лицом, имеющим доступ к данному СУ с правами администратора ОС;
- централизовано, путем рассылки обновления ПО из ЦУС (см. [1]).

По завершении обновления ПО рекомендуется произвести проверку настроек и работоспособности ПО.

[3] Периодичность определяется инструкцией администратора безопасности в зависимости от числа подчиненных ему СУ, назначения и загрузки СУ и других факторов. Рекомендуемое значение - 1 раз в месяц.

[4] Рекомендуется 1 раз в 10 дней

6.5 ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ ПРИ СБОЯХ

6.5.1 Восстановление ViPNet Администратор

1. Программное обеспечение ViPNet Центр управления сетью и ViPNet Удостоверяющий и Ключевой центр участвуют в работе комплекса ViPNet эпизодически при необходимости реконфигурации структуры комплекса или выполнения других функций управления, в связи с чем их временный выход из строя не приводит к перерывам в обработке информации. Однако потеря баз данных ViPNet Администратор может привести к серьезным последствиям с точки зрения возможности дальнейшей эксплуатации защищенной сети. В связи с этим необходимо периодически не реже одного-двух раз в неделю производить резервное копирование критически важных данных, формируемых ПО.
2. Для восстановления актуального на момент последнего копирования состояния ПО ViPNet Центр управления сетью достаточно выполнять резервное копирование вновь появившихся архивных файлов из подкаталога ARC каталога установки ПО.

Если работа программы ЦУС длительное время не прерывается (по окончании работы программы архивные файлы создаются автоматически), то необходимо не реже одного раза в сутки средствами данного ПО создавать указанные архивные файлы.

Если программа ЦУС запускается, но необходимо восстановить состояние баз данных на некоторый момент времени, то рекомендуется воспользоваться штатной процедурой восстановления архива, имеющейся в программе.

При установке на новый компьютер следует провести инсталляцию программы заново, положить в рабочий каталог установки ПО регистрационные файлы INFOTECS.REG и INFOTECS.RE, в подкаталог ARC этого каталога - исправный файл архива и штатными средствами программы открыть этот архив.

3. Для восстановления актуального на момент последнего копирования состояния ПО ViPNet Удостоверяющий и Ключевой центр необходимо выполнять резервное копирование вновь появившихся архивных файлов из подкаталога ARCHIEVE каталога установки ПО.

В настройках УКЦ рекомендуется выбрать временной интервал создания архивов, например 24 часа. В этом случае программа будет автоматически

создавать архивы с интервалом 24 часа при наличии изменений.

Для восстановления работоспособности УКЦ достаточно этих файлов.

Если программа УКЦ запускается, но необходимо восстановить состояние баз данных на некоторый момент времени, то рекомендуется воспользоваться штатной процедурой восстановления архива, имеющейся в программе.

При установке на новый компьютер следует:

- провести инсталляцию программы заново, положить в рабочий каталог установки ПО регистрационный файл INFOTECS.RE, в подкаталог ARCHIEVE этого каталога - исправный файл архива и штатными средствами программы открыть этот архив;
- проверить и при необходимости восстановить настройки Ключевого центра.

6.5.2 Восстановление ViPNet Координатор (Клиент)

ViPNet Координатор является программным средством, которое может быть установлено на любой аналогичный компьютер с необходимым числом сетевых интерфейсов в случае выхода из строя основного компьютера с ПО ViPNet Координатор. Для этого необходимо иметь инсталляционный диск и ключевой дистрибутив для данного Координатора, созданный в Ключевом центре.

В процессе работы Координатора после проведения на нем каких-либо настроек рекомендуется делать экспорт настроек с помощью главного меню «Сервис/Экспорт настроек». Программа предложит скопировать настройки по умолчанию в каталог SaveData каталога установки программы. Вы можете изменить путь и имя файла. В этом файле будут сохранены практически все настройки программы за исключением настроек прикладных протоколов, настроек параметров безопасности, настроек транспорта.

Можно также сделать полную резервную копию рабочего каталога программы, тогда будут сохранены и указанные выше настройки, а также журналы Координатора.

В случае выхода из строя компьютера с ПО ViPNet Координатор необходимо.

1. Произвести копирование рабочего каталога на другой компьютер в

каталог с теми же путями, что и на вышедшем из строя компьютере. Если не требуются сохранения всех указанных выше настроек, то данную операцию можно не производить.

2. Произвести установку ПО ViPNet Координатор на этот же компьютер с использованием ключевого дистрибутива.
3. Подсоединить компьютер к сети и в сетевых настройках присвоить новому компьютеру IP-адреса действующего Координатора, настроить необходимые свойства сети (gateway, Routing и др.).
4. Произвести перезагрузку операционной системы.
5. Импортировать с помощью главного меню «Сервис/Импорт настроек» экспортированный ранее файл. По умолчанию откроется каталог SaveData каталога установки программы. Вы можете указать другой путь к файлу.
6. Экспорт настроек фильтров будет успешным для тех интерфейсов, у которых адреса подсетей совпадают с адресами подсетей интерфейсов отказавшего компьютера. Сами IP-адреса могут не совпадать. Импорт можно повторять многократно.
7. Для повышения отказоустойчивости предусмотрена также функция Watchdog обеспечения контроля за состоянием программных средств ПО ViPNet и автоматического восстановления работоспособности ПО после программных, аппаратных или иных сбоев. Функция реализована программно в ПО ViPNet Координатор. Функция позволяет автоматически перезапускать приложения ViPNet или производить перезагрузку операционной системы в случае обнаружения критических сбоев в работе системного ПО или ПО ViPNet.
8. Если на компьютере с ПО ViPNet Coordinator установлена плата АМДЗ «Аккорд», то может быть использован Watchdog-таймер, расположенный на этой плате.

7 КЛЮЧЕВАЯ ИНФОРМАЦИЯ

Состав ключевой информации УКЦ, порядок ее хранения и обработки изложен в документах [4], [5] и в данном документе не рассматривается.

Содержание данного раздела касается ключевой информации СУ.

7.1 СОСТАВ КЛЮЧЕВОЙ ИНФОРМАЦИИ, АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ

В состав ключевой информации СУ входят следующие составляющие:

- личные ключи пользователя (ключевая дискета – КД). КД пользователя содержит ключи защиты пользователя, необходимые для его аутентификации на СУ, и может содержать ключи подписи пользователя;
- ключевой набор (КН) СУ – набор ключей и справочной информации, общий для всех пользователей данного СУ;
- резервный набор персональных ключей пользователя (РНПК), предназначенный для получения дистанционного обновления ключевой информации при изменении исходной ключевой информации в УКЦ.

УКЦ формирует для первичной инициализации СУ дистрибутивы справочно-ключевой информации. Дистрибутивы представляют собой сборники, содержащие КД пользователя, КН и адресные справочники ViPNet. Для каждого пользователя, зарегистрированного на СУ, изготавливается свой дистрибутив.

На СУ предусмотрено 3 типа аутентификации пользователей.

1. Парольная (только пароль). При этом типе аутентификации КД пользователя хранится на жестком диске компьютера или дискете. Для доступа к СУ пользователь вводит пароль в диалоге аутентификации и указывает, если необходимо, место хранения личных ключей.
2. С устройством. При этом типе аутентификации пароль пользователя заносится на некоторое отделяемое устройство (Smart Card, eToken, iKey, iButton и т. д.). Ключевая информация хранится так же, как и при парольной аутентификации, на жестком диске компьютера. При использовании данного типа аутентификации пользователь предъявляет устройство для получения доступа к СУ.
3. Сильная (пароль и устройство). При этом типе аутентификации

персональные ключи защиты пользователя переносятся на устройство. Для получения доступа к СУ пользователь предъявляет устройство и вводит пароль доступа к нему в диалоге аутентификации.

Выбор типа аутентификации осуществляется в УКЦ при изготовлении ключей или на СУ при первичной инициализации ключевой информации. Администратор безопасности при выборе типа аутентификации для конкретного пользователя и СУ должен исходить из имеющихся условий хранения и эксплуатации технических средств СУ.

Рекомендуется использовать 3 тип аутентификации.

При использовании 1 или 2 типа аутентификации для хранения личных ключей должны использоваться только отчуждаемые носители информации (дискеты или флэш-память).

При необходимости использования иных типов аутентификации должны быть обеспечены дополнительные организационные меры по предотвращению доступа посторонних лиц в помещения, где расположены технические средства СУ.

На мобильных ПК 3 тип аутентификации **обязателен** к использованию.

7.2 ТРЕБОВАНИЯ ПО ХРАНЕНИЮ, РАСПРЕДЕЛЕНИЮ И УДАЛЕНИЮ КЛЮЧЕВОЙ ИНФОРМАЦИИ

7.2.1 Дистрибутивы для первичной инициализации

Дистрибутивы для первичной инициализации формируются в УКЦ и передаются пользователям при первой установке ПО ViPNet лично без использования канала связи или по защищенным ПО ViPNet каналам связи с использованием ПО «Деловая почта» через администраторов безопасности с оформлением соответствующей записи в журнале по форме (см. Приложение 4).

Пользователь должен хранить дистрибутив на съемном носителе. Должны быть приняты меры по надежному хранению ключевых дистрибутивов и другой ключевой информации, размещенной на съемных носителях. Для хранения съемных носителей помещение должно быть оборудовано сейфом. При отсутствии условий хранения дистрибутивов на рабочих местах они должны быть уничтожены с соответствующей отметкой в журнале.

Дистрибутив может быть использован в дальнейшем для восстановления работоспособности ПО или при переносе на другой компьютер.

ВНИМАНИЕ! Информация, находящаяся на дистрибутиве при повторном его

использовании может быть неактуальной. При повторном использовании дистрибутива необходимо обратиться к администратору ЦУС и запросить обновление справочников и ключевых наборов для получения актуальной информации о разрешенных связях, справочников сертификатов администраторов и списков отозванных сертификатов.

7.2.2 Резервные наборы персональных ключей

Данные наборы предназначены для получения обновлений при изменении исходной ключевой информации УКЦ или в случае компрометации ключей пользователя. Наборы должны храниться на дискете или других съемных носителях. Помещение для хранения должно быть оборудовано сейфом для хранения ключевых документов и охранной сигнализацией.

Хранение наборов на жестком диске СУ допускается для необслуживаемых СУ (например, Координаторах), находящихся в специально оборудованных помещениях при обеспечении дополнительных организационных и технических мер по защите от несанкционированного доступа к СУ. Жесткий диск такого СУ подлежит учету наравне с ключевыми носителями.

Запрещается хранение наборов на мобильных ПК и на СУ в помещениях, в которые могут иметь доступ посторонние лица.

При отсутствии условий для хранения данных наборов они должны быть уничтожены вместе с дистрибутивами для первичной инициализации и на данные сетевые узлы более не передаются. Обновления для таких сетевых узлов передаются, при необходимости, в виде дистрибутивов для первичной инициализации.

7.2.3 Личные ключи пользователя

Личные ключи пользователя могут передаваться пользователю вместе с дистрибутивом для первичной инициализации или переноситься на ключевой носитель в процессе первичной инициализации СУ. Ответственность за сохранность личных ключей пользователя несет сам пользователь.

Тип ключевого носителя пользователя и состав ключевой информации, сохраняемой на ключевом носителе, определяется типом аутентификации пользователя (см. 7.1).

7.2.4 Удаление ключевой информации

Удаление ключей при обновлениях или деинсталляции ПО производится штатными средствами ПО ViPNet.

При удалении дистрибутивов или невозможности воспользоваться штатными средствами удаление ключевой информации производится администратором безопасности.

Удаление ключевой информации, перенесенной на отделяемые носители, не имеющие файловой системы, производится путем физического уничтожения самого носителя. Удаление ключевой информации на жестких дисках, дискетах или флэш-памяти производится с использованием утилиты CLEAN.exe, входящей в состав поставки ПО ViPNet. В журнале учета выдачи ключевых документов делается отметка об уничтожении ключей.

7.3 ПЛАНОВАЯ СМЕНА И ОБНОВЛЕНИЕ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Обновление ключевой и справочной информации при изменении структуры сети производится дистанционно (по сети) в соответствии с документацией [1], [2], [5]. При дистанционной смене ключей личные ключи защиты пользователей по сети не передаются. Для приема обновлений используются личные ключи пользователя, находящиеся в его распоряжении. Для приема обновлений при изменении исходной информации в УКЦ используются ключи из резервного набора персональных ключей пользователя. В связи с этим для СУ, на которых отсутствует резервный набор персональных ключей (невозможно обеспечить условия надежного хранения набора), обновление производится путем первичной инициализации с новым ключевым дистрибутивом. Отметки о выдаче и последующем уничтожении нового дистрибутива делается в журнале хранения ключевых документов, аналогично п. 7.2.1

7.4 КОМПРОМЕТАЦИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ, СМЕНА КЛЮЧЕЙ ПРИ КОМПРОМЕТАЦИИ

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

В случае, если есть сомнение в неизвестности посторонним лицам пароля доступа к ключам модуля ViPNet, но доступ к компьютеру этих посторонних лиц

невозможен, следует сменить пароль и продолжить работу. Если доступ к компьютеру посторонних лиц возможен, то следует считать ключи скомпрометированными.

Ключи пользователя считаются скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным файл ключевого дистрибутива;
- посторонним лицам мог стать доступным съемный носитель с ключевой информацией;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере при 1 или 2 типе аутентификации, если все ключи хранятся на компьютере;
- на компьютере, подключенном к сети, не установлен модуль ViPNet Клиент [Монитор] или он устанавливался в 4 или 5 режим работы и:
  - в локальной сети считается возможным присутствие посторонних лиц или
  - на границе локальной сети отсутствует (отключен) межсетевой экран;
- уволился пользователь, имевший доступ к паролям и ключам.

7.4.1 Администратор безопасности:

- уведомляет администраторов ЦУС и УКЦ о факте и обстоятельствах компрометации и необходимости отзыва сертификата ключа подписи;
- приостанавливает работу скомпрометированного СУ до получения обновления при компрометации;
- после получения обновления производит обновление при компрометации.

7.4.2 Администратор ЦУС:

- при наличии факта компрометации резервного набора персональных ключей уведомляет администратора УКЦ о необходимости смены мастера персональных ключей;
- объявляет ключи данного пользователя (или СУ) скомпрометированными и уведомляет об этом администратора УКЦ;
- при получении новых ключей от УКЦ осуществляет рассылку обновлений на все СУ, кроме скомпрометированного;
- при наличии на скомпрометированном СУ резервного набора

персональных ключей и отсутствия факта компрометации этого набора высылает новый ключевой набор для данного СУ. В остальных случаях обеспечивает доставку нового ключевого дистрибутива пользователю.

7.4.3 Администратор УКЦ:

- принимает решение о необходимости отзыва сертификата ключа подписи пользователя;
- принимает решение о формировании нового мастер-ключа персональных ключей;
- формирует новые ключевые наборы (дистрибутивы) для скомпрометированного СУ и всех СУ с ним связанных;
- отправляет изготовленные ключи для ЦУС.

7.4.4 Обновление при компрометации:

- если резервный набор персональных ключей пользователя на СУ отсутствует или был скомпрометирован, то осуществляется первичная инициализация;
- если резервный набор доступен для использования, то производится:
  - прием дистанционного обновления при компрометации (см. [8]),
  - смена пароля пользователя.

ПРИЛОЖЕНИЕ 1

Акт

о вводе в эксплуатацию ПК ViPNet Координатор (Клиент)

«___» _____ 20___ г.

Комиссия в составе: председателя комиссии _____, членов комиссии _____ _____и администратора ПК ViPNet Координатор _____ составила акт о том, что ViPNet Координатор установлен в_____

Наименование подразделения

по адресу_____

в помещении №_____.

в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию.

Состав ПК ViPNet Координатор:

Системный блок № _____

Программный комплекс:

ViPNet Координатор версия _____ сборка _____.

Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т. д.) указать

_____

_____

Председатель комиссии	_____ должность	_____ Ф.И.О.	_____ Подпись
Члены комиссии:	_____ должность	_____ Ф.И.О.	_____ Подпись
	_____ должность	_____ Ф.И.О.	_____ Подпись

Подп. и дата | Инв. № | Взам. инв. | Подп. и дата | Подп.

Изм	Лис	№ докум.	Подп.	Дат	ФРКЕ. 00029-04 90 01	Лист 40

ПРИЛОЖЕНИЕ 2

Протокол
контрольной проверки ПК ViPNet Координатор(Клиент)

«___» _____ 20___ г.

ViPNet Координатор установлен

в_____

Наименование подразделения

по адресу_____

в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию.

в помещении №_____.

Акт о вводе в эксплуатацию №_____от _____.

Состав ПК ViPNet Координатор (Клиент):

Системный блок № _____

Программный комплекс:

1. ViPNet Координатор версия _____ сборка _____.
2. Дополнительно установленное оборудование (наименование, назначение, серийный номер и т. д.) указать
3. Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т. д.) указать

_____

_____

1. Состав и результаты проверок и контрольных тестов

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
1.	Загрузка ОС с отказом от ввода пароля ViPNet	Отказ в загрузке ОС		
2.	Загрузка ОС с аутентификацией	Загрузка ОС и старт ПО ViPNet		Указать тип аутентификации

	пользователя			
3.	Проверка установленных режимов безопасности[5]	Режимы безопасности соответствуют назначению СУ		
4.	Проверка настроек ПО	Настройки ПО соответствуют требованиям 5.3.1		
5.	Аутентификация с паролем администратора СУ	Переход ПО в режим работы администратора СУ		
6.	Контроль журнала событий ПО ViPNet Координатор [Монитор]	Отсутствие попыток несанкционированного изменения режимов, настроек фильтров, отсутствие признаков НСД, аварийных завершений ПО.		
7.	Контроль журнала регистрации IP-пакетов	Отсутствие признаков сетевых атак, отсутствие информации о пропуске пакетов на запрещенные режимом (фильтрами) адреса (протоколы)		
8.	Проверка связи с видимыми СУ защищенной сети	Наличие сообщений о доступности СУ		
9.	Проверка связи с видимым СУ защищенной сети, для которого включен	Наличие сообщений о недоступности СУ, информация в журнале о		

[5] Для координаторов на каждом из сетевых интерфейсов

	фильтр блокировки пакетов	блокировании пакетов		
10.	Проверка связи (ping nnn.nnn.nnn.nnn) с открытым не зарегистрированным адресом (во 2 режиме)	Отсутствие ответа от узла. Информация в журнале о блокировке пакетов для данного адреса		
11.	Настройка фильтра, блокирующего отдельный протокол (например, ICMP) для отдельного СУ защищенной сети, проверка соединения с СУ по данному протоколу (например, ping)	Отсутствие ответа от СУ, информация о блокировании пакетов по выбранному протоколу		
12.	Настройка фильтра, запрещающего отдельный протокол (например, UDP) для всех СУ защищенной сети, проверка связи с СУ по данному протоколу (например, проверка соединения)	Наличие сообщений о недоступности СУ. Информация в журнале о блокировании пакетов		
13.	Настройка фильтра, разрешающего отдельный протокол (например, ICMP) для всех узлов открытой сети, проверка связи с любым открытым узлом	Наличие ответа от узла. Информация в журнале о пропуске пакетов для данного адреса		

	по данному протоколу (например, ping)			
14.	Проверка связи по разрешенному протоколу для зарегистрированных открытых адресов[6]	Наличие соединения по данному протоколу		
15.	Проверка связи по запрещенному протоколу для зарегистрированных открытых адресов	Отсутствие соединения по данному протоколу		
16.	Отправка зашифрованного и подписанного письма адресатам ДП[7]	Отправка письма, получение квитанций о доставке (прочтении)		
17.	Контроль журналов автопроцессинга ДП[8]	Отсутствие сбоев в работе правил		

Администратор безопасности	Пользователь
" "_____20___г.	" "_____20___г.

[6] Только для 2 режима безопасности

[7] При наличии установленного ПО ViPNet Клиент [Деловая Почта]

[8] При наличии данного функционала на СУ

ПРИЛОЖЕНИЕ 3

Протокол

удаленной проверки ПК ViPNet Координатор(Клиент)

«___» _____ 20___ г.

Результат проверки соединения с СУ: _____

Пользователь: _____

Компьютер:_____

Версия ПО ViPNet: _____

Версия ОС: № версии_____

Режим безопасности: _____

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
1.	Проверка установленных режимов безопасности[9]	Режимы безопасности соответствуют назначению СУ		
2.	Проверка установленных версий ОС и ПО	Соответствие версий акту о вводе в эксплуатацию, отсутствие несанкционированных изменений		
3.	Удаленный запрос журнала регистрации пакетов	Получение журнала регистрации пакетов		
4.	Контроль журнала регистрации IP-	Отсутствие признаков сетевых атак.		

[9] Для Координаторов на каждом из сетевых интерфейсов

	пакетов	Отсутствие информации о пропуске пакетов на запрещенные режимом (фильтрами) адреса (протоколы)		
5.	Проверка связи с открытого адреса на проверяемый СУ	Отсутствие ответа от узла. Информация в журнале о блокировке пакетов для данного адреса		
6.	Проверка связи по разрешенному протоколу для зарегистрированных открытых адресов	Наличие соединения по данному протоколу		
7.	Проверка связи по запрещенному протоколу для зарегистрированных открытых адресов	Отсутствие соединения по данному протоколу		
8.	Отправка зашифрованного и подписанного письма адресатам ДП[10]	Отправка письма, получение квитанций о доставке (прочтении)		

Администратор безопасности

" "_____20___г.

[10] При наличии установленного ПО ViPNet Клиент [Деловая Почта]

ПРИЛОЖЕНИЕ 4

Журнал учета выдачи ключевых документов

(ведется администратором безопасности)

Номер по порядку	Дата выдачи	Организация, ФИО пользователя	Идентификатор дистрибутива (пользователя)	Тип носителя	Способ передачи (Лично в руки, нарочным, письмо ДП (рег. номер) в адрес…)	Подпись получившего (отправившего по ДП)	Отметка об уничтожении
1							
2							
3							

СПИСОК ДОКУМЕНТОВ

1. «ViPNet [Центр Управления Сетью]. Руководство администратора», ОАО «ИнфоТеКС», ФРКЕ.00006-04 90 01.
2. «ViPNet [Удостоверяющий и Ключевой центр]. Руководство администратора», ОАО «ИнфоТеКС», ФРКЕ.00006-04 90 03.
3. «ViPNet Центр Регистрации. Руководство администратора ЦР», ОАО «ИнфоТеКС», ФРКЕ.00010-04 90 01.
4. Программно-аппаратный комплекс "Удостоверяющий центр корпоративного уровня сети ViPNet. Общее описание, правила пользования, ОАО «ИнфоТеКС», ФРКЕ.00022-04 90 01.
5. Программно-аппаратный комплекс "Удостоверяющий центр корпоративного уровня сети ViPNet. Типовой регламент функционирования, ОАО «ИнфоТеКС», ФРКЕ.00022-04 90 02.
6. «ViPNet Координатор. Руководство администратора», ОАО «ИнфоТеКС», ФРКЕ.00005-04 90 01.
7. «ViPNet Координатор Linux. Руководство администратора», ОАО «ИнфоТеКС», ФРКЕ.000031-04 90 01.
8. «ViPNet Клиент [Монитор]. Руководство пользователя», ОАО «ИнфоТеКС», ФРКЕ.00004-04 90 01.
9. «ViPNet Клиент [Деловая почта]. Руководство пользователя», ОАО «ИнфоТеКС», ФРКЕ.00004-04 90 02.
10. Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа	Подп.	Дата
Изм.	измененных	заменен ных	новых	аннули-рован-ных					

Подп. и дата | Инв. № | Взам. инв. | Подп. и дата | Подл.