УТВЕРЖДЕН

ФРКЕ.00116-03 99 01 ПП-ЛУ

Программный комплекс

ViPNet Client 4

Правила пользования

ФРКЕ.00116-03 99 01 ПП

infotecs

2016

Содержание

1 Общие положения

Программный комплекс ViPNet Client 4 (далее – ПК ViPNet Client) предназначен для обеспечения безопасной (защищенной) передачи данных между сегментами виртуальной сети ViPNet с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сеть связи общего пользования.

ПК ViPNet Client предназначен для использования в составе защищенных виртуальных сетей ViPNet, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну.

ПК ViPNet Client выполняет функции шифрования и имитозащиты IP-пакетов узла в защищенной сети ViPNet, персонального сетевого экрана, клиента для обмена зашифрованными и подписанными сообщениями.

ПК ViPNet Client предназначен для эксплуатации на территории Российской Федерации в приложениях и системах защиты информации, не содержащей сведений, составляющих государственную тайну, и может вывозиться с территории Российской Федерации в соответствии с законодательством Российской Федерации в области экспортного контроля или (и) таможенным законодательством Евразийского экономического союза в составе указанных систем или в качестве самостоятельного изделия.

ПК ViPNet Client обеспечивает совместную работу с программными и программно-аппаратными комплексами ViPNet производства ОАО «ИнфоТеКС».

ПК ViPNet Client предназначен для эксплуатации в составе программного комплекса защиты информации ViPNet 4 согласно формуляру ФРКЕ.00131-01 30 01 ФО.

1.1 Состав программных средств ПК ViPNet Client

В состав специализированного программного обеспечения ПК ViPNet Client входят:

- драйвер сетевой защиты IPLIR, взаимодействующий непосредственно с драйвером сетевого интерфейса компьютера и осуществляющий контроль, и фильтрацию трафика обмена компьютера с внешней сетью;
- сервис управления драйвером сетевой защиты IPLIRCONTROL, обеспечивающий функционирование узла в сети ViPNet, а именно загрузку в драйвер защиты правил фильтрации, справочной информации о структуре сети ViPNet, сведений о сетевых параметрах доступа для узлов сети ViPNet, передачу в ПО ViPNet Монитор результатов обработки IP-пакетов; загрузку в драйвер шифрования ключей шифрования; аудит основных событий;

- драйвер шифрования IP-пакетов ITCSCRPT, осуществляющий шифрование и имитозащиту IP-пакетов;
- приложение ViPNet Client Монитор, осуществляющее аутентификацию пользователя, настройку фильтров, а также установку соответствующих фильтров IP-трафика в дополнение к собственным настроенным правилам фильтрации трафика;
- система обновления, обеспечивающая обновление ключевой и справочной информации, а также ПО ViPNet Client;
- сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя ViPNet Client;
- транспортный модуль ViPNet MFTP, реализующий обмен управляющей, адресной и ключевой информацией с программным обеспечением централизованного управления сетью ViPNet (ПО ViPNet Administrator, ПО ViPNet Policy Manager), отправку, прием и маршрутизацию электронных документов (почтовых конвертов), отправку, прием и маршрутизацию электронных документов (почтовых конвертов);
- служба ViPNet Контроль приложений, осуществляющая контроль сетевой активности приложений и позволяющая реализовывать политики доступа приложений в сеть;
- прикладное ПО ViPNet Деловая почта для обмена зашифрованными и подписанными сообщениями;
- программа KeySetup, осуществляющая первичную установку справочно-ключевой информации (файлы дистрибутивов ключей *.dst), сформированной в Центре управления сетью ViPNet Administrator, на узел сети ViPNet;
- средство криптографической защиты информации (далее – СКЗИ) ViPNet CSP 4.2.

ViPNet Client выполняет следующие основные функции:

- функция персонального сетевого экрана, которая контролирует информацию, проходящую через сетевые интерфейсы компьютера, и обеспечивает защиту информации непосредственно на компьютере посредством ее фильтрации, т.е. ее анализа по совокупности критериев и принятия решения об ее распространении в (из) компьютер(а);
- функция обмена зашифрованными и подписанными сообщениями (электронная почта), а также контроль за прохождением и состоянием сообщений;

- шифрование IP-трафика, файлов и почтовых сообщений;
- создание и проверка электронной подписи (далее – ЭП);
- прием и обновление справочной и ключевой информации, изготавливаемой ViPNet Administrator;
- прием и обновление программного обеспечения, переданное из ПО ViPNet Administrator;
- прием и обновление справочной информации, изготавливаемой ViPNet Policy Manager;
- создание ключей ЭП и ключей проверки ЭП;
- хэширование данных в соответствии с алгоритмами ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- формирование ключей шифрования для алгоритма ГОСТ 28147-89;
- аутентификация, передача данных по протоколу TLS;
- формирование сообщений PKCS #7 (CMS);
- формирование транспортных ключевых контейнеров в формате PKCS #12 (PFX).

1.2 Требования к составу технических средств и операционным системам

Компьютер с ПК ViPNet Client является одним из сетевых узлов (далее − СУ) виртуальной частной сети ViPNet и выполняет функции защищенного рабочего места пользователя сети ViPNet. Для использования ПК ViPNet Client требуется, чтобы в организации существовала сеть ViPNet, управление которой осуществляется с помощью ПК ViPNet Administrator.

ViPNet Client предназначен для использования на компьютерах, поддерживающих архитектуру x86, x86-64 с минимально рекомендуемой производителем операционной системы (далее – ОС) аппаратной конфигурацией, а также в виртуальной среде, поддерживающей эти архитектуры.

ПК ViPNet Client функционирует под управлением ОС MS Windows:

- Microsoft Windows Server 2008 R2 (64-разрядная);
- Microsoft Windows 7 (32/64-разрядная);
- Microsoft Windows 8 (32/64-разрядная);
- Microsoft Windows 8.1 (32/64-разрядная);

- Microsoft Windows 10 (32/64-разрядная);
- Microsoft Windows Server 2012 (64-разрядная);

Примечание. В операционной системе должен быть установлен последний пакет обновления ОС (Service Pack) и все известные критические обновления, опубликованные производителем ОС.

ПК ViPNet Client поддерживает работу в следующих виртуальных средах:

- Microsoft Hyper-V;
- VMWare Workstation;
- VMWare Player;
- VMWare vSphere ESXi.

Примечание. В указанных виртуальных средах ПК ViPNet Client может функционировать только в исполнении 1.

1.3 Дополнительное программное обеспечение

Антивирусная защита ПК ViPNet Client и среды функционирования криптосредства (СФК) обеспечивается путем использования антивирусных средств, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции.

На компьютере, где устанавливается ПК ViPNet Client, не должны быть активированы сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT).

2 Разграничение полномочий в сети ViPNet

Администраторы сети ViPNet – привилегированные пользователи сети ViPNet, обладающие дополнительными полномочиями.

Администраторы сети ViPNet должны назначаться из числа особо доверенных лиц.

Назначение Администраторов сети ViPNet должно осуществляться в соответствии с приказом (распоряжением) руководителя организации (подразделения), ответственного за обеспечение защиты информации. Деятельность Администраторов сети ViPNet должна регламентироваться требованиями инструкций, определяющих порядок и правила выполнения Администраторами своих функциональных обязанностей.

Для обеспечения безопасной эксплуатации сети ViPNet должны быть сформированы три группы Администраторов со следующими полномочиями.

2.1 Группа администраторов безопасности

Администратор безопасности выполняет следующие функции:

- осуществляет развертывание и ввод в эксплуатацию сетевого узла (далее − СУ), установку ключей на СУ и контроль их хранения;
- осуществляет контроль и несет ответственность за соблюдение правил безопасной эксплуатации СУ или группы обслуживаемых им СУ;
- осуществляет настройки ОС и прикладного ПО;
- осуществляет контроль над соблюдением правил эксплуатации и соблюдением мер защиты от несанкционированного доступа (далее − НСД);
- периодически осуществляет проверку целостности ПО;
- проводит мониторинг событий НСД к ПО и попыток сетевых атак.

Для обеспечения своих функций Администратор безопасности должен иметь выделенную учетную запись для входа в ОС с правами администратора.

2.2 Группа администраторов ЦУС

Администратор Центра управления сетью (далее – ЦУС) выполняет следующие функции:

- осуществляет регистрацию сетевых узлов и пользователей сети ViPNet;
- задает роли сетевым узлам;
- задает свойства ролей (например, уровень полномочий пользователя);
- назначает связи между объектами сети ViPNet (сетевыми узлами, пользователями, группами пользователей);

- формирует и рассылает узлам и пользователям сети ViPNet обновления справочников, ключевой информации и программного обеспечения узлов сети ViPNet;
- обеспечивает межсетевое взаимодействие с другими сетями ViPNet.

Для обеспечения своих функций Администратор ЦУС должен:

- быть зарегистрирован на СУ, на котором установлено ПО ViPNet Administrator ЦУС;
- обладать паролем входа в ОС с правами, достаточными для выполнения своих обязанностей;
- обладать паролем для входа в программу ViPNet Administrator ЦУС и иметь доступ к ее рабочим каталогам.

2.3 Группа администраторов УКЦ

Администратор УКЦ выполняет следующие функции:

- осуществляет формирование и обновление симметричной ключевой и первичной парольной информации для узлов и пользователей сети ViPNet;
- осуществляет формирование наборов справочно-ключевой информации для первичной инициализации узлов сети ViPNet;
- осуществляет формирование и своевременную смену мастер-ключей своей сети и мастер-ключей для межсетевого взаимодействия;
- обеспечивает формирование и обновление ключевой информации при компрометациях;
- обеспечивает своевременную передачу в ViPNet Administrator ЦУС сформированной ключевой и справочной информации;
- осуществляет создание ключей ЭП и ключей проверки ЭП как для пользователей сети ViPNet, так и для внешних пользователей.

Для обеспечения своих функций Администратор УКЦ должен:

- быть зарегистрирован на СУ, на котором установлено ПО ViPNet Administrator УКЦ;
- обладать паролем входа в ОС с правами, достаточными для выполнения своих обязанностей;
- обладать паролем для входа в программу ViPNet Administrator УКЦ и иметь доступ к ее рабочим каталогам.

3 Требования к размещению технических средств

При размещении технических средств (компьютеров) с ПК ViPNet Client следует руководствоваться следующими рекомендациями:

1 Размещение ПК ViPNet Client, специальное оборудование, организация режима и охрана места установки, эксплуатации и хранения должны обеспечивать:
   - безопасность информации ограниченного доступа, в том числе ключевой информации, и гарантировать сохранность находящихся в этих помещениях конфиденциальных документов;
   - невозможность доступа лиц, не допущенных к работе с ПК ViPNet Client, к эксплуатационной документации, к наблюдению за работой с СКЗИ;
   - невозможность прослушивания ведущихся там переговоров и просмотра помещений посторонними лицами;
   - исключение возможности умышленного повреждения или кражи ТС с ПК ViPNet Client.

2 Порядок допуска в помещение определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации, эксплуатирующей ПК ViPNet Client.

3 Должны быть приняты меры по исключению несанкционированного доступа (далее – НСД) на объект посторонних лиц. Порядок допуска на объект должен определяться внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования эксплуатирующей организации.

4 Должны быть приняты меры по надежному сохранению в тайне паролей доступа, дистрибутивов ключей и другой ключевой информации. Для хранения ключевых носителей помещение должно быть оборудовано сейфом.

5 На время инициализации дистрибутива ключей ТС должно быть отключено от информационной сети (локальной сети, Wi-Fi и др.).

6 Порядок охраны и организации режима помещений, в которых находятся ТС, регламентируется разделом IV инструкции [3].

7 При эксплуатации ПК ViPNet Client на объектах заказчика (эксплуатирующей организации) должны выполняться действующие в Российской Федерации требования по защите информации от утечки по техническим каналам, в том числе каналу связи (например, СТР-К).

4 Установка и ввод в эксплуатацию ПК ViPNet Client

4.1 Порядок распространения и учета ПК ViPNet Client

ПК ViPNet Client и пакет документов к нему поставляется в электронном виде на носителях, изготовленных производителем (ОАО «ИнфоТеКС»).

ПК ViPNet Client поставляется в двух вариантах – дистрибутив для первичной инсталляции и пакет удаленного обновления для централизованного обновления из ViPNet Центра управления сетью (ViPNet ЦУС).

Передача дистрибутива и пакета документов от производителя в эксплуатирующую организацию осуществляется доверенным способом администратору ЦУС либо администратору безопасности.

В первом случае проверку целостности осуществляет администратор ЦУС путем сравнения контрольных сумм дистрибутива с указанными контрольными суммами в формуляре на изделие. Далее администратор ЦУС отправляет дистрибутив администратору безопасности по защищенному каналу связи при помощи ViPNet Деловая почта. Для такого способа передачи на рабочих местах администраторов должен быть установлен ПК ViPNet Client (в состав которого входит ViPNet Деловая почта), сертифицированный в ФСБ России.

Во втором случае проверка целостности дистрибутива перед его инсталляцией осуществляется администратором безопасности путем сравнения контрольных сумм дистрибутива с указанными контрольными суммами в формуляре на изделие.

Передача пакета удаленного обновления и пакета документов от производителя в эксплуатирующую организацию осуществляется доверенным способом только администратору ЦУС.

Проверка целостности пакета удаленного обновления осуществляется администратором ЦУС перед проведением процедуры удаленного обновления ПО путем сравнения контрольной суммы файла пакета удаленного обновления с указанной контрольной суммой в формуляре. В этом случае доставка обновления ПО осуществляется для уже установленных и введенных в эксплуатацию узлов ViPNet по защищенным каналам и с выполнением проверок целостности ПО средствами ПО ViPNet Client Монитор. Пользователю узла ViPNet не требуется проводить проверку целостности дистрибутива при приеме и обновлении ПО, высланного из ViPNet ЦУС.

Поэкземплярный учет дистрибутивов ПК ViPNet Client осуществляется производителем – ОАО «ИнфоТеКС» в процессе подготовки комплекта изделия.

Далее, в зависимости от способа получения ПК ViPNet Client:

1 В случае получения комплекта изделия на электронном носителе администратору ЦУС или администратору безопасности, ответственному за установку и эксплуатацию ПК, предоставляется экземпляр дистрибутива, формуляр изделия в бумажном виде с указанием регистрационного номера СКЗИ, серийного номера и контрольной суммы дистрибутива.

2 В случае выполнения централизованного обновления посредством отправки обновления из ViPNet Administrator (ЦУС) администратору ЦУС предоставляется экземпляр ПК ViPNet Client в виде пакета удаленного обновления (*.lzh), формуляр изделия в бумажном виде с указанием серийного номера, контрольной суммы файла пакета удаленного обновления и списка регистрационных номеров СКЗИ по количеству обновляемых узлов.

8 Поэкземплярный учёт копий изделия должен осуществляться в эксплуатирующей организации. Для этого:

– Администратор безопасности при установке и вводе в эксплуатацию изделия присваивает устанавливаемой копии СКЗИ учетный номер, который должен включать регистрационный номер СКЗИ, зафиксированный в формуляре, и идентифицирующий копию признак (например, порядковый номер инсталляции или название (номер) ТС, на который установлена копия ViPNet Client). Между регистрационным номером и идентифицирующим признаком должен находиться разделяющий знак (например: «-», «/», «:» и т.п.).

– Администратор безопасности вносит регистрационный номер в журнал поэкземплярного учета.

– Для каждого установленного СКЗИ при необходимости изготавливается копия формуляра (с пометкой «Копия»), в раздел 5 которого вносится разделяющий знак и идентифицирующий копию признак. Полученный номер СКЗИ должен совпасть с приведенным в журнале поэкземплярного учёта.

9 ***Примечания:***

– Установка должна осуществляться в соответствии с разделом 4.2 настоящих правил пользования.

– Для обеспечения контроля целостности должны быть приняты меры по проверке контрольной суммы полученного дистрибутива согласно разделу 4.1.

– Максимально допустимое количество копий ViPNet Client, устанавливаемых на ТС эксплуатирующей организации, ограничивается числом, указанным в лицензионном соглашении.

- Допускается делать необходимое число учтённых копий компакт-диска с дистрибутивом и эксплуатационной документацией.
- Журнал поэкземплярного учёта допускается вести в бумажном или электронном виде. Форма журнала поэкземплярного учёта приведена в [3].

4.2 Установка ПК ViPNet Client

Установка ПК ViPNet Client осуществляется только Администратором безопасности.

До установки ПК ViPNet Client должны быть осуществлены следующие действия:

- проверить работоспособность ТС и их соответствия требованиям по размещению (см. раздел 3);
- проверить, что установленное ПО не содержит средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам;
- проверить, что отсутствуют средства, запоминающие нажатия клавиш и другие действия пользователя (например, Punto Switcher);
- проверить компьютер на отсутствие вирусов;
- отключить учетную запись для гостевого входа (Guest);
- 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;
- проверить целостность файла дистрибутива ПО ViPNet путем сравнения контрольной суммы файла с контрольной суммой, указанной в формуляре.

В BIOS должен быть установлен один вариант загрузки ОС – с жесткого диска, все альтернативные варианты загрузки должны быть отключены, в том числе сетевая загрузка.

Настройки BIOS должны быть защищены паролем, удовлетворяющим условиям подраздела 4.5.

Установка ПК ViPNet Client осуществляется в соответствии с документом [4].

При установке ПК ViPNet Client в исполнении 3 должна быть установлена программа ViPNet SysLocker (модуль защиты СФК).

По завершении установки осуществляются настройки ПО в соответствии с требованиями подраздела 4.4, формирование контрольных сумм в соответствии с подразделом 5.1 и контроль работоспособности ПО в соответствии с подразделом 5.2.

4.3 Ввод в эксплуатацию

Ввод в эксплуатацию ПК ViPNet Client осуществляется Администратором безопасности.

На каждое рабочее место, оснащенное ПК ViPNet Client, оформляется Акт о вводе в эксплуатацию по типовой форме. Акт может храниться у Администратора безопасности или у пользователя, ответственного за эксплуатацию ПК ViPNet Client.

4.4 Требования к настройкам ПК ViPNet Client

Перед вводом ПК ViPNet Client 4 в эксплуатацию Администратор безопасности должен настроить СКЗИ ViPNet CSP 4.2 в соответствии с правилами пользования на данное СКЗИ.

Для осуществления настроек необходимо ввести пароль Администратора СУ, затем:

1 Осуществить настройку ПК ViPNet Client в соответствии с [4].
2 Установить минимально возможное значение допустимой разницы между временем отправки и приема IP-пакета, не превышающее 10 мин.
3 Установить в качестве алгоритма шифрования ГОСТ 28147-89 в настройках параметров безопасности.
4 Включить регистрацию в журнале всех IP-пакетов, настроить параметры размеров журнала и архива журнала и интервала агрегации, исходя из интенсивности трафика, проходящего через СУ.
5 Запретить или ограничить удаленное управление ОС путем настроек, запрещающих фильтров для протоколов и портов удаленного управления ОС для всех узлов, кроме специально выделенных для этих целей.

Дополнительно для исполнения 3 ПК ViPNet Client необходимо:

1 Включить опцию «Обязательный ввод пароля при входе в операционную систему».
2 Выбрать тип аутентификации «Устройство», перенести (при необходимости) ключ защиты пользователя на устройство. Другие типы аутентификации могут использоваться только при условии обеспечения дополнительных организационных мер, исключающих доступ посторонних лиц к данному СУ.
3 Выключить опцию «Разрешить сохранение пароля в реестре» – включение данной опции допустимо для СУ, работающих в необслуживаемом режиме при условии обеспечения дополнительных организационных мер, исключающих доступ посторонних лиц к данному СУ. Во всех остальных случаях данная функция должна быть отключена.

4 Установить интервал автоматического блокирования компьютера при бездействии пользователя в течение 15 минут.

5 Включить опцию блокировки компьютера при отключении устройства аутентификации.

6 Убедиться, что установлена и настроена программа SysLocker, предназначенная для защиты среды функционирования, входящая в состав СКЗИ ViPNet CSP 4.2.

После настройки запретить или ограничить интерфейс пользователя в программе, воспользовавшись правами Администратора СУ либо настройками полномочий пользователя узла в ViPNet Administrator ЦУС.

4.5 Регистрация пользователей и СУ в сети ViPNet

Регистрацию ПК ViPNet Client в сети ViPNet осуществляют Администраторы, входящие в группу Администраторов ЦУС, с использованием ПК ViPNet Administrator Центр управления сетью в соответствии с документом [1].

При регистрации СУ Администратор руководствуется следующими правилами:

– связи сетевым узлам задаются выборочно – не следует без необходимости использовать опцию «Связать все сетевые узлы»;

– СУ должны быть назначены только роли, которые необходимы пользователям данных СУ для выполнения своих задач.

Если для пользователя СУ был установлен способ аутентификации «Пароль на устройстве» (например, данный способ был настроен в ПО ViPNet более ранней версии), то при первой возможности Администратор безопасности должен сменить этот тип аутентификации на другой.

Для СУ должен быть задан пароль Администратора СУ. Пароль задается Администратором УКЦ, с использованием ViPNet УКЦ в соответствии с документом [2].

При назначении пароля пользователю СУ (далее по тексту – пароля) должны выполняться следующие требования:

1 Пароль должен состоять не менее чем из восьми символов.

2 В пароле должны присутствовать символы двух категорий из числа следующих четырех:

– строчные буквы английского алфавита от «a» до «z» (всего 26 символов);

– прописные буквы английского алфавита от «A» до «Z»;

– десятичные цифры от «0» до «9»;

– символы, не принадлежащие к алфавитно-цифровому набору (всего 68 символов).

3 Использование трех и более символов, расположенных подряд на клавиатуре, недопустимо.

4 Использование трех и более символов, идущих подряд в алфавитном порядке, недопустимо.

5 Использование трех и более одинаковых символов, идущих подряд, недопустимо.

6 Задание пароля, совпадающего с одним из трех последних паролей, недопустимо.

Кроме того, должны действовать следующие правила:

1 Смена пароля производится не реже чем 1 раз в 6 месяцев.

2 Пароли должны быть случайны, насколько это возможно, и не связаны каким-либо образом с конкретным пользователем, например, с датой его рождения.

5 Эксплуатация ПК ViPNet Client

Все действия по обслуживанию и настройкам должны производиться Администратором безопасности.

Помимо требований и рекомендаций, изложенных в данном документе, в процессе эксплуатации ПК ViPNet Client должны выполняться требования и рекомендации, приведенные в правилах пользования на СКЗИ ViPNet CSP 4.2.

5.1 Контроль целостности ТС и ПО

До включения ПК ViPNet Client пользователь обязан убедиться в отсутствии:

- внешних признаков вскрытия системного блока (например, повреждение пломб при их наличии);
- подключенного дополнительного оборудования, не предусмотренного Актом о вводе в эксплуатацию.

ПК ViPNet Client оснащен встроенными механизмами проверки целостности ПО ViPNet, справочной и ключевой информации. Проверка производится при каждом старте ПО ViPNet. Кроме того, встроены механизмы периодического тестирования работоспособности базовых криптографических библиотек, а также механизм проверки целостности ключевой информации при попытках доступа к ней.

После установки ПК ViPNet Client необходимо сформировать контрольные суммы для файлов, типовой перечень которых приведен в Приложении 2. Этот перечень соответствует содержимому файла os.prg, расположенного в каталоге C:\ProgramData\Infotecs\ViPNetCSP. Часть файлов из перечня может отсутствовать в некоторых сборках ОС Windows. Чтобы создать перечень исполняемых модулей ОС, под управлением которой работает конкретный компьютер, системному администратору необходимо получить в ОАО «ИнфоТеКС» специальные утилиты и запустить их со следующими параметрами:

- Infotecs.DependencyGenerator.exe depends.exe "C:\Program Files\InfoTeCS\ViPNet CSP" os.prg — для 32-разрядных ОС Windows.
- Infotecs.DependencyGenerator.exe depends.exe "C:\Program Files (x86)\InfoTeCS\ViPNet CSP" os.prg — для 64-разрядных ОС Windows.

В результате будет сформирован файл os.prg, подходящий для конкретной ОС.

Для формирования контрольных сумм необходимо запустить с правами администратора утилиту make_ext_crg из каталога ViPNet CSP (по умолчанию: C:\Program Files\InfoTeCS\ViPNet CSP) со следующими параметрами:

Make_ext_crg.exe –r “C:\ProgramData\Infotecs\ViPNet CSP\os.prg”.

После обновления ОС системному администратору необходимо создать новый файл os.prg с перечнем исполняемых модулей ОС. А затем для вновь сформированного списка файлов пересчитать контрольные суммы. Для этого следует выполнить те же действия, что и при начальном формировании списка.

Перед началом работы должен быть проведен контроль целостности при помощи утилиты check_crg. Контролем целостности должны быть охвачены файлы, перечень которых приведен в приложении 2. Для этого необходимо выполнить команды: check_crg “C:\ProgramData\Infotecs\ViPNet CSP\os.prg”. В результате проверки будет сформирован протокол, который заканчивается обобщенным итогом в следующей форме:

Total:

1 PRG files checked, 1 checks passed, 0 checks failed

6 files checked, 6 checks passed, 0 files corrupted, 0 checks failed;

Он не должен содержать ошибок.

После обновления ОС Windows возможно возникновение ошибки при проверке контрольных сумм системных библиотек, используемых ПК, что будет отражено на консоли при проверке. В этом случае необходимо:

- уведомить разработчика о несоответствии хэш-значений системных библиотек с целью постановки работ по проведению анализа обновленных системных библиотек, используемых ПК установленным порядком;
- на период до получения результатов исследований следовать инструкциям разработчика, полученным им из специализированной организации.

При обнаружении неустранимых ошибок или нарушения контроля целостности ПО программа ViPNet Client Монитор выдает сообщение о невозможности продолжения эксплуатации ПК ViPNet Client. В этом случае Администратор безопасности обязан:

- отключить ПК ViPNet Client от локальной вычислительной сети до устранения неисправностей;
- провести исследование с целью выяснения возможных причин возникновения неисправностей;
- произвести проверку работоспособности ТС, на которых установлен ПК ViPNet Client;
- провести анализ журналов аудита с целью выявления попыток несанкционированного доступа и сетевых атак;
- при обнаружении признаков несанкционированного доступа к ПК ViPNet Client уведомить Администратора УКЦ о возможной компрометации ключей узла;

- устранить обнаруженные причины возникновения неисправностей или искажений;
- при необходимости произвести переустановку ПК ViPNet Client;
- при необходимости произвести обновление ключевой информации СУ.

5.2 Контроль работоспособности и соблюдения правил эксплуатации

Администратор безопасности обязан осуществлять периодический контроль работоспособности и соблюдения правил эксплуатации ПК ViPNet Client. Контроль осуществляется непосредственно на проверяемом СУ. При проведении данной проверки необходимо провести проверку целостности ПО путем анализа журналов и логов ПО на предмет наличия сообщений об ошибках.

Администратор безопасности должен настроить архивирование журнала IP-пакетов и журнала событий, а также обеспечить разграничение доступа к архивам журналов.

Архивирование журнала IP-пакетов производится средствами ViPNet. Администратор безопасности должен убедиться, что архивирование журнала осуществляется: в окне программы ViPNet Монитор в меню **Сервис -> Настройка приложения** -> **Журнал IP-пакетов** в поле **Максимальный размер архива журнала** значение не должно быть равно нулю (по умолчанию – 10 Мбайт).

Архивирование журнала событий и разграничение доступа к архивам журналов обеспечивается средствами ОС. Для этого администратор безопасности должен написать скрипт, который будет запускаться по расписанию с правами администратора, и копировать архив журнала IP-пакетов и журнала событий в отдельную папку. Доступ к этой папке должны иметь только учетные записи Администратора безопасности и Администратора СУ: в свойствах данной папки на вкладке **Безопасность** администратор должен удалить все учетные записи, кроме учетной записи администратора безопасности и администратора СУ.

Примечание.

Для 32-разрядных ОС расположение журналов по умолчанию следующее:

- Журнал событий:
  %ProgramData%\InfoTeCS.Admin\ServicesPrivate\IpLirControlData\databases\admlog.mdb
- Журнал IP-пакетов:
  %ProgramData%\InfoTeCS.Admin\ServicesPrivate\IpLirControlData\databases\IPPacketLog\packet.stg

Контрольная проверка на ПК ViPNet Client осуществляется в следующих случаях:

- при вводе ПК ViPNet Client в эксплуатацию;
- при изменении лица, ответственного за эксплуатацию СУ;
- периодически, периодичность определяется инструкцией Администратора безопасности в зависимости от числа обслуживаемых им СУ, назначения и загрузки СУ и других факторов. Рекомендуемое значение – 1 раз в месяц.

Результаты проверки оформляются в виде протокола проверки в соответствии с Приложением 1.

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 ПК ViPNet Client, немедленно прекратить работу программного комплекса и поставить в известность администратора УКЦ.

5.3 Обновление ПК ViPNet Client

Обновление ПО ПК ViPNet Client осуществляется двумя способами:

- локально, путем запуска штатной процедуры установки на локальном компьютере (осуществляется администратором безопасности);
- дистанционно, путем централизованной отправки обновлений ПО ViPNet Client по сети с помощью ViPNet ЦУС (осуществляется администратором ЦУС).

Для проведения обновления ПО ViPNet Client в исполнении 3 необходимо выполнить следующую последовательность действий:

- администратор безопасности должен убедиться, что он является единственным пользователем, выполнившим вход в сеанс работы ОС, установленной на компьютер с ViPNet Client;
- при наличии других пользователей, работающих в сеансах работы ОС, администратору безопасности необходимо принять меры по прекращению сеансов работы указанных пользователей;
- администратор безопасности должен запретить пользователям возможность удаленного входа в сеансы работы ОС во время проведения обновления ПО ViPNet Client;
- администратор безопасности должен отключить в программе ViPNet SysLocker режим контроля замкнутости СФК;

- должно быть проведено обновление ПО ViPNet Client в соответствии с документом [4]. ViPNet Client 4 не поддерживает совместную работу с ViPNet SafeDisk-V. Если на компьютере установлено ПО ViPNet SafeDisk-V необходимо выполнить рекомендации, приведенные в документе [4], в разделе «Обновление при использовании программы SafeDisk-V».
- администратор безопасности должен включить в программе ViPNet SysLocker режим контроля замкнутости СФК.

После завершения обновления ПК ViPNet Client необходимо произвести проверку настроек и работоспособности ПК ViPNet Client.

5.4 Восстановление работоспособности при сбоях, действия в нештатных ситуациях, связанных с использованием СКЗИ

Все действия в нештатных ситуациях, связанных с использованием СКЗИ, а также по восстановлению работоспособности ПК ViPNet Client производятся только Администратором безопасности.

Для восстановления работы ПК ViPNet Client в случае искажения файлов ПО ПК ViPNet Client или файлов справочно-ключевой информации необходимо иметь инсталляционный диск с экземпляром дистрибутива ПО и дистрибутив ключей.

В случае искажения файлов справочно-ключевой информации необходимо провести первичную инициализацию ключей из дистрибутива ключей.

В случае искажения файлов ПО ПК ViPNet Client необходимо:

1 Произвести установку ПК ViPNet Client в каталог установки с использованием инсталляционного диска с экземпляром дистрибутива СКЗИ.
2 При необходимости провести первичную инициализацию ключевой информации из дистрибутива ключей.
3 Настроить сетевые интерфейсы и подсоединить компьютер к сети.
4 Произвести перезагрузку операционной системы.

В случае выхода из строя компьютера с ПК ViPNet Client программный комплекс может быть установлен на любой аналогичный компьютер с необходимым числом сетевых интерфейсов. Для этого необходимо иметь инсталляционный диск и дистрибутив ключей.

Рекомендуется сделать полную резервную копию рабочего каталога программного комплекса, тогда будут сохранены и указанные выше настройки, а также журналы ПК ViPNet Client.

В случае выхода из строя компьютера с ПК ViPNet Client необходимо:

1 Произвести, по необходимости и при наличии возможности, копирование каталога установки ПК ViPNet Client на другой компьютер в каталог с теми же путями, что и на вышедшем из строя компьютере.
2 Произвести установку ПК ViPNet Client в этот каталог с использованием инсталляционного диска с экземпляром СКЗИ.
3 При необходимости провести первичную инициализацию ключевой информации из имеющегося дистрибутива ключей.
4 Настроить сетевые интерфейсы и подсоединить компьютер к сети.
5 Произвести перезагрузку операционной системы.

6 Организационно-технические и административные мероприятия по защите от несанкционированного доступа при использовании ПК ViPNet Client

6.1 Общие положения

Защита аппаратного и программного обеспечения от НСД при установке и использовании ПК ViPNet Client является составной частью общей задачи обеспечения безопасности информации в сети ViPNet, в состав которой входит ПК ViPNet Client.

Наряду с применением средств защиты от НСД необходимо выполнение ряда мер, включающих в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности использования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

В приведенных ниже разделах содержатся основные требования по выполнению указанных мер защиты.

6.2 Организация работ по защите от НСД

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости Администратором безопасности или пользователем.

При эксплуатации ПК ViPNet Client в организации может быть назначен Администратор безопасности, на которого возлагаются задачи организации работ по использованию ПК ViPNet Client, а также контроль над соблюдением описанных ниже требований.

Правом доступа к ПК ViPNet Client должны обладать только определенные (выделенные для эксплуатации) лица (пользователи), прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, эксплуатирующего ПК ViPNet Client, с документацией на данный программный комплекс, а также с другими нормативными документами, созданными на ее основании.

При организации работ по защите информации от НСД необходимо разработать и применить политику назначения и смены паролей, использовать пароль в соответствии с

правилами, приведенными в п. 4.4. Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

6.3 Требования по защите от НСД при эксплуатации ПК ViPNet Client

Администратор безопасности должен следить за выполнением пользователями принятой политики смены паролей.

Запрещается:

- оставлять без контроля ПК ViPNet Client после прохождения процесса аутентификации на СУ;
- вносить какие-либо изменения в программное обеспечение ПК ViPNet Client;
- осуществлять несанкционированное Администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием ПК ViPNet Client;
- записывать на ключевые носители постороннюю информацию.

Администратор безопасности должен осуществлять периодический контроль в соответствии со следующими требованиями:

- на ТС должна быть установлена только одна операционная система;
- в зависимости от целей использования ПК ViPNet Client настроить необходимый уровень безопасности, создав сетевые фильтры и назначив соответствующий уровень полномочий пользователю;
- всем пользователям, зарегистрированным на данном СУ, необходимо назначить минимально возможные для нормальной работы права.

Необходимо организовать затирание (по окончании сеанса работы) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы ПК ViPNet Client. Затирание следует выполнять путем запуска утилиты clean.exe, входящей в состав ПК ViPNet Client и расположенной в каталоге установки ПК ViPNet Client. Ключи утилиты и их описание можно посмотреть при запуске clean.exe без параметра в консольном окне или файловом процессоре типа FAR.

Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться следующие требования:

- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- в случае подключения ПК ViPNet Client к сетям связи общего доступа необходимо исключить возможность открытия и исполнения файлов и скриптов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов;
- организовать и использовать комплекс мероприятий антивирусной защиты.

Дополнительно, в качестве организационной меры обеспечения эксплуатации СКЗИ, рекомендуется при каждой загрузке операционной системы проверять целостность защищенных системных файлов с помощью утилиты sfc, входящей в состав ОС. Для этого необходимо через командную строку запустить утилиту с правами администратора и проверить файлы с помощью команды /VERIFYONLY.

7 Ключевая информация

Состав ключевой информации УКЦ, порядок ее хранения и обработки изложен в документе [2] и в данном документе не рассматривается.

Содержание данного раздела касается ключевой информации ПК ViPNet Client.

7.1 Состав ключей, аутентификация

В состав справочно-ключевой информации сети ViPNet входят следующие компоненты:

- текущий персональный ключ пользователя, необходимый для аутентификации пользователя на СУ;
- справочники и ключи узла – набор файлов с данными, которые необходимы для взаимодействия между сетевыми узлами ViPNet;
- резервный набор персональных ключей пользователя (далее РНПК), предназначенный для обновления ключей в случае смены мастер-ключа персональных ключей в ViPNet УКЦ или в случае перехода на новый вариант персонального ключа пользователя. При смене варианта персонального ключа пользователя в процессе обновления ключей на узле из РНПК будет использован следующий персональный ключ, а при смене мастера персональных ключей – весь РНПК будет заменен новым;
- ключ ЭП и ключ проверки ЭП.

Администратор УКЦ формирует для первичной инициализации СУ дистрибутивы ключей со справочно-ключевой информацией. Дистрибутивы ключей необходимы для ввода в эксплуатацию СУ в сети ViPNet. При первом формировании дистрибутива ключей для пользователя в его состав помещается РНПК.

На СУ аутентификация может быть выполнена с использованием пароля или устройства:

1 Пароль. Для доступа к СУ необходимо ввести пароль пользователя в диалоговом окне аутентификации.

2 Устройство. При этом типе аутентификации используются устройство аутентификации (подробно о видах устройств аутентификации в [2]) и ПИН-код устройства или пароль пользователя. Для доступа к СУ необходимо подключить устройство аутентификации, на котором сохранен персональный ключ пользователя или сертификат, и ввести ПИН-код (и в некоторых случаях пароль).

Выбор типа аутентификации осуществляется Администратором УКЦ при подготовке дистрибутива ключей. Сменить тип аутентификации может либо Администратор УКЦ с последующей отправкой ключей узла, либо пользователь на узле в режиме Администратора СУ.

7.2 Требования по хранению ключей

7.2.1 Дистрибутивы ключей

Дистрибутивы ключей для первичной инициализации формируются в ViPNet УКЦ и передаются Администраторам безопасности лично, доверенным способом (доверенный канал связи или фельдсвязь) или по защищенным с помощью ПО ViPNet каналам связи с использованием ПО ViPNet Деловая почта с оформлением соответствующей записи в журнале учета выдачи ключевых документов.

При необходимости хранения дистрибутивов ключей должны быть приняты меры по надежному хранению в соответствии с требованиями к хранению ключевой информации. Для хранения отделяемых носителей информации помещение должно быть оборудовано сейфом. При отсутствии условий хранения дистрибутивов на рабочих местах они должны быть уничтожены с соответствующей отметкой в журнале учета выдачи ключевых документов.

Информация, находящаяся в составе дистрибутива ключей, при повторном его использовании может быть неактуальной. Для актуализации справочно-ключевой информации необходимо обратиться с запросом на обновление к Администратору ЦУС.

7.2.2 Персональные ключи пользователей

Персональный ключ передается пользователю в составе дистрибутива ключей, если для пользователя задан тип аутентификации по паролю или на съемном носителе, если пользователю назначена аутентификация с устройства. В дальнейшем персональный ключ пользователя, в случае передачи в составе дистрибутива ключей, может быть перенесен на съемный носитель при смене типа аутентификации в режиме Администратора СУ. Ответственность за сохранность персональных ключей пользователей сети определяется внутренним регламентом эксплуатирующей изделие организации.

7.2.3 Резервные наборы персональных ключей

РНПК предназначены для получения обновлений при смене мастер-ключа персональных ключей или в случае поднятия варианта персонального ключа пользователя. РНПК должны храниться на съемных носителях информации. Помещение для хранения должно быть оборудовано сейфом для хранения отделяемых носителей информации и охранной сигнализацией.

РНПК передаются Администратору безопасности на съемном носителе или в составе дистрибутива ключей. В том случае, если РНПК был передан в составе дистрибутива ключей, Администратор безопасности должен обеспечить его удаление на узле после развертывания дистрибутива ключей и запросить РНПК в отдельном файле у Администратора УКЦ.

7.3 Удаление ключей

При деинсталляции ПО ПК ViPNet Client в случае прекращения эксплуатации СУ на компьютере должна быть удалена вся ключевая информация. Удаление ключевой информации должно производиться с использованием утилиты clean.exe, входящей в состав ПО ViPNet Client. Если ключи при развертывании дистрибутива ключей были установлены не в папку по умолчанию, то при запуске утилиты clean.exe, необходимо указать папку, в которой они находятся. Если персональный ключ пользователя хранится на съемном носителе, то его требуется также удалить, отформатировав съемный носитель. В журнале учета выдачи ключей после удаления ключей должны быть сделана соответствующая отметка.

7.4 Плановая смена и обновление ключей

Обновление ключей узлов при изменении структуры сети производится централизованно (по сети). Плановая смена ключей узлов и пользователей производится также дистанционно (по сети) в соответствии с документацией [1], [2].

Плановая смена ключей осуществляется в ViPNet УКЦ одним из способов:

- путем поднятия варианта ключей узлов и ключей пользователей. Поднятие варианта ключей узла означает увеличение порядкового номера ключей обмена и ключей защиты, которые идут в составе ключей узла. Поднятие варианта ключа пользователя означает увеличение порядкового номера персонального ключа пользователя;
- путем смены мастер-ключа для данного типа ключей.

При централизованной плановой смене ключей пользователя используется РНПК. В случае отсутствия РНПК (невозможно обеспечить условия надежного хранения РНПК, отсутствует к нему доступ по какой-либо причине) централизованная плановая смена ключей возможна только при присутствии Администратора безопасности. Администратор безопасности должен подключить съемный носитель с РНПК этого пользователя для обновления ключей на узле.

Если у пользователя имеется ключ ЭП, инициатива создания которого принадлежит Администратору сети, то плановая смена этого ключа производится Администратором УКЦ

не менее чем раз в 15 месяцев. Контроль соблюдения сроков действия ключевой информации СУ ViPNet и своевременности ее обновления осуществляется группой Администраторов УКЦ.

7.5 Компрометация ключевой информации, смена ключей при компрометации

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

События, квалифицируемые как факт компрометации ключей, определяются регламентом безопасности эксплуатирующей организации, в чьем ведении находятся административные ресурсы сети ViPNet.

7.5.1 Компрометация ключа ЭП пользователя

При компрометации ключа ЭП пользователя Администратору УКЦ требуется провести стандартную процедуру аннулирования сертификата. Пользователю необходимо удалить контейнер с ключом ЭП и ключом проверки ЭП. В случае если ключи хранятся на устройстве, его требуется отформатировать. После этого пользователю нужно обратиться к Администратору УКЦ с запросом на выдачу нового ключа ЭП, ключа проверки ЭП и сертификата.

7.5.2 Компрометация ключей пользователя и ключей узла

Если ключи узла скомпрометированы, то ключи пользователя также считаются скомпрометированными.

При компрометации ключей пользователя и ключей узла необходимо:

1 Удалить в ViPNet ЦУС учетную запись скомпрометированного узла пользователя.
2 Сформировать для пользователя новую учетную запись (в ViPNet ЦУС), новый дистрибутив ключей (в ViPNet УКЦ) и развернуть его на узле.
3 Остальным связанным узлам сети увеличить номер варианта ключей и отправить новые ключи из ViPNet УКЦ на узлы.

8 Список документов

1 ViPNet Центр управления сетью 4. Руководство администратора, ФРКЕ.00109-07 32 01.

2 ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора, ФРКЕ.00109-07 32 02.

3 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.

4 ViPNet Client 4. Руководство пользователя, ФРКЕ.00116-03 34 01.

5 ViPNet CSP 4.2. Руководство пользователя, ФРКЕ.00106-04 34 01.

6 Программный комплекс ViPNet Client 4. Формуляр ФРКЕ.00116-03 30 01 ФО.

9 Сокращения и обозначения

НСД	–	несанкционированный доступ
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
РНПК	–	резервный набор персональных ключей
СУ	–	сетевой узел
ТС	–	техническое средство
УКЦ	–	Удостоверяющий и ключевой центр
ЦУС	–	Центр управления сетью
ЭП	–	электронная подпись

ПРИЛОЖЕНИЕ 1

Протокол

контрольной проверки ViPNet Client

«___» _____ 20___ г.

ViPNet Client 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 и результаты проверок и контрольных тестов:

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Загрузка ОС с проведением аутентификации пользователя ViPNet.	Загрузка ОС и запуск программного обеспечения ViPNet Client.	
Проверка настроек программного обеспечения.	Настройки программного обеспечения соответствуют требованиям.	
Вход в режим администратора сетевого узла.	Переход программного обеспечения в режим работы администратора сетевого узла.	
Проверка журнала событий ViPNet Client/Coordinator.	Отсутствие в журнале событий несанкционированного изменения настроек сетевых фильтров, признаков НСД, аварийных завершений работы программного обеспечения.	
Проверка журнала регистрации IP-пакетов.	Отсутствие в журнале признаков сетевых атак, информации о пропуске IP-пакетов на запрещенные сетевыми фильтрами адреса (протоколы).	
Проверка соединения с видимыми узлами защищенной сети.	Наличие сообщений о доступности сетевых узлов.	
Проверка соединения с видимым узлом защищенной сети, который указан в фильтре, блокирующем прохождение IP- пакетов.	• Наличие сообщений о недоступности сетевого узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых данному узлу.	

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Проверка соединения (ping nnn.nnn.nnn.nnn) с открытым узлом с не зарегистрированным адресом.	• Отсутствие ответа от узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых по данному адресу.	
1. Настройка сетевого фильтра, блокирующего прохождение IP-пакетов в рамках отдельного протокола (например, ICMP) для конкретного узла защищенной сети. 2. Проверка соединения с узлом по данному протоколу (например, ping).	• Отсутствие ответа от узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых в рамках выбранного протокола.	
1. Настройка сетевого фильтра, блокирующего прохождение IP-пакетов в рамках отдельного протокола (например, UDP) для всех узлов защищенной сети. 2. Проверка соединения с одним из узлов защищенной сети по данному протоколу (например, проверка соединения)	• Наличие сообщений о недоступности сетевого узла. • Наличие информации в журнале IP-пакетов о блокировке IP-пакетов, передаваемых данному узлу.	
1. Настройка сетевого фильтра, разрешающего прохождение IP-пакетов в рамках отдельного протокола (например, ICMP) для всех узлов открытой сети. 2. Проверка связи с любым открытым узлом по данному протоколу (например, ping).	• Наличие ответа от узла. • Наличие информации в журнале IP-пакетов о прохождении IP-пакетов, передаваемых по данному адресу.	
Проверка соединения с открытыми узлами с зарегистрированными адресами в рамках разрешенного протокола.	Получение ответа от узлов.	
Проверка соединения с открытыми узлами с зарегистрированными адресами в рамках запрещенного протокола.	Отсутствие ответа от узлов.	

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Отправка зашифрованного и подписанного письма адресатам в программе ViPNet Деловая почта.	• Отправка письма. • Получение квитанций о доставке (прочтении).	
Контроль журналов автопроцессинга в программе ViPNet Деловая почта.	Отсутствие сбоев в работе правил автопроцессинга.	

Администратор безопасности

" "_____20___г.

Пользователь

" "_____20___г.

ПРИЛОЖЕНИЕ 2

Типовой перечень исполняемых модулей ОС Windows и разделов реестра, подлежащих контролю целостности

Перечень исполняемых модулей:

\windows\apppatch\acgenral.dll
\windows\explorer.exe
\windows\system32\activeds.dll
\windows\system32\actxprxy.dll
\windows\system32\adsldpc.dll
\windows\system32\advapi32.dll
\windows\system32\advpack.dll
\windows\system32\alg.exe
\windows\system32\apphelp.dll
\windows\system32\atl.dll
\windows\system32\audiosrv.dll
\windows\system32\authz.dll
\windows\system32\autochk.exe
\windows\system32\basesrv.dll
\windows\system32\batmeter.dll
\windows\system32\bootvid.dll
\windows\system32\browser.dll
\windows\system32\browseui.dll
\windows\system32\cabinet.dll
\windows\system32\certcli.dll
\windows\system32\clbcatq.dll
\windows\system32\clusapi.dll
\windows\system32\cnbjmon.dll
\windows\system32\colbact.dll
\windows\system32\comctl32.dll
\windows\system32\comdlg32.dll
\windows\system32\comres.dll
\windows\system32\comsvcs.dll
\windows\system32\credui.dll
\windows\system32\crypt32.dll
\windows\system32\cryptdll.dll
\windows\system32\cryptsvc.dll
\windows\system32\cryptui.dll
\windows\system32\cscdll.dll
\windows\system32\cscui.dll
\windows\system32\csrsrv.dll
\windows\system32\csrss.exe
\windows\system32\ctfrnon.exe
\windows\system32\davclnt.dll
\windows\system32\dhcpcsvc.dll
\windows\system32\dmserver.dll
\windows\system32\dmusic.dll
\windows\system32\dnsapi.dll

\windows\system32\dnsrslvr.dll
\windows\system32\dpcdll.dll
\windows\system32\drprov.dll
\windows\system32\dssenh.dll
\windows\system32\ersvc.dll
\windows\system32\es.dll
\windows\system32\esent.dll
\windows\system32\eventlog.dll
\windows\system32\framebuf.dll
\windows\system32\gdi32.dll
\windows\system32\hal.dll
\windows\system32\hnetcfg.dll
\windows\system32\icaapi.dll
\windows\system32\icmp.dll
\windows\system32\imagehlp.dll
\windows\system32\imapi.exe
\windows\system32\inetpp.dll
\windows\system32\iphlpapi.dll
\windows\system32\ipnathlp.dll
\windows\system32\kbdru.dll
\windows\system32\kbdus.dll
\windows\system32\kdcom.dll
\windows\system32\kerberos.dll
\windows\system32\kernel32.dll
\windows\system32\Iinkinfo.dll
\windows\system32\lmhsvc.dll
\windows\system32\localspl.dll
\windows\system32\lsasrv.dll
\windows\system32\lsass.exe
\windows\system32\mfc42.dll
\windows\system32\midimap.dll
\windows\system32\mnmdd.dll
\windows\system32\mpr.dll
\windows\system32\mprapi.dll
\windows\system32\msacm32.dll
\windows\system32\msasnI.dll
\windows\system32\msctf.dll
\windows\system32\msgina.dll
\windows\system32\msi.dll
\windows\system32\msidle.dll
\windows\system32\msimg32.dll
\windows\system32\msisip.dll
\windows\system32\mspatcha.dll
\windows\system32\msprivs.dll
\windows\system32\mstask.dll
\windows\system32\mstlsapi.dll
\windows\system32\msutb.dll
\windows\system32\msvl_0.dll
\windows\system32\msvcp60.dll
\windows\system32\msvcrt.dll
\windows\system32\mswsock.dll

\windows\system32\msxml3.dll
\windows\system32\mtxclu.dll
\windows\system32\ncobjapi.dll
\windows\system32\nddeapi.dll
\windows\system32\netapi32.dll
\windows\system32\netcfgx.dll
\windows\system32\netlogon.dll
\windows\system32\netman.dll
\windows\system32\netmsg.dll
\windows\system32\netrap.dll
\windows\system32\netshell.dll
\windows\system32\netui0.dll
\windows\system32\netuil.dll
\windows\system32\ntdll.dll
\windows\system32\ntdsapi.dll
\windows\system32\ntlanman.dll
\windows\system32\ntmarta.dll
\windows\system32\ntoskrnl.exe
\windows\system32\ntshrui.dll
\windows\system32\odbc32.dll
\windows\system32\odbcint.dll
\windows\system32\ole32.dll
\windows\system32\oleacc.dll
\windows\system32\oleaut32.dll
\windows\system32\pautoenr.dll
\windows\system32\pjlmon.dll
\windows\system32\powrprof.dll
\windows\system32\profmap.dll
\windows\system32\psapi.dll
\windows\system32\psbase.dll
\windows\system32\pstorsvc.dll
\windows\system32\rasadlilp.dll
\windows\system32\rasapi32.dll
\windows\system32\raschap.dll
\windows\system32\rasdlg.dll
\windows\system32\rasman.dll
\windows\system32\rastls.dll
\windows\system32\regapi.dll
\windows\system32\regsvc.dll
\windows\system32Vresutils.dll
\windows\system32\riched20.dll
\windows\system32\rpcrt4.dll
\windows\system32\rpcss.dll
\windows\system32\rsaenh.dll
\windows\system32\rtutils.dll
\windows\system32\rundll32.exe
\windows\system32\samlib. dll
\windows\system32\samsrv.dll
\windows\system32\scecli.dll
\windows\system32\scesrv.dll
\windows\system32\schannel.dll

\windows\system32\schedsvc.dll
\windows\system32\seclogon.dll
\windows\system32\secur32.dll
\windows\system32\sens.dll
\windows\system32\services.exe
\windows\system32\setupapi.dll
\windows\system32\sfc.exe
\windows\system32\sfc_os.dll
\windows\system32\sfcfiles.dll
\windows\system32\shdoclc.dll
\windows\system32\shdocvw. dll
\windows\system32\shell32.dll
\windows\system32\shfolder.dll
\windows\system32\shimeng.dll
\windows\system32\shlwapi.dll
\windows\system32\shsvcs.dll
\windows\system32\smss.exe
\windows\system32\spoolss.dll
\windows\system32\spoolsv.exe
\windows\system32\srsvc.dll
\windows\system32\srvsvc.dll
\windows\system32\ssdpapi.dll
\windows\system32\ssdpsrv.dll
\windows\system32\stobject.dll
\windows\system32\svchost.exe
\windows\system32\sxs.dll
\windows\system32\tapi32.dll
\windows\system32\tcpmon.dll
\windows\system32\termsrv.dll
\windows\system32\themeui.dll
\windows\system32\trkwks.dll
\windows\system32\twext.dll
\windows\system32\umpnpmgr.dll
\windows\system32\upnp.dll
\windows\system32\urlmon.dll
\windows\system32\usbmon.dll
\windows\system32\user32.dll
\windows\system32\userenv.dll
\windows\system32\userinit.exe
\windows\system32\uxtheme.dll
\windows\system32\version.dll
\windows\system32\vga.dll
\windows\system32\vga256.dll
\windows\system32\vga64k.dll
\windows\system32\vssapi.dll
\windows\system32\w32time.dll
\windows\system32\watchdog.sys
\windows\system32\wbem\esscli.dll
\windows\system32\wbem\fastprox.dll
\windows\system32\wbem\ncprov.dll
\windows\system32\wbem\repdrvfs.dll

\windows\system32\wbem\wbemcomn.dll
\windows\system32\wbem\wbemcons.dll
\windows\system32wbem\wbemcore.dll
\windows\system32\wbem\wbemess.dll
\windows\system32\wbem\wbemprox.dll
\windows\system32\wbem\wbemsvc.dll
\windows\system32\wbem\wmiprvsd.dll
\windows\system32\wbem\wmisvc.dll
\windows\system32\wbem\wmiutils.dll
\windows\system32\wdigest.dll
\windows\system32\webcheck.dll
\windows\system32\webclnt.dll
\windows\system32\win32k.sys
\windows\system32\wm32spl.dll
\windows\system32\winhttp.dll
\windows\system32\wminet.dll
\windows\system32\winlogon.exe
\windows\system32\winmm.dll
\windows\system32\winrnr.dll
\windows\system32\winscard.dll
\windows\system32\winspool.exe
\windows\system32\winsrv.dll
\windows\system32\winsta.dll
\windows\system32\wintrust.dll
\windows\system32\wkssvc.dll
\windows\system32\wldap32. dll
\windows\system32\wlnotify.dll
\windows\system32\wmi.dll
\windows\system32\ws2_32.dll
\windows\system32\ws2help.dll
\windows\system32\wscsvc.dll
\windows\system32\wshext.dll
\windows\system32\wshnetbs.dll
\windows\system32\wshtcpip.dll
\windows\system32\wsock32.dll
\windows\system32\wtsapi32.dll
\windows\system32\wuauclt.exe
\windows\system32\wuaueng.dll
\windows\system32\wuauserv.dll
\windows\system32\wups.dll
\windows\system32\wzcsapi.dll
\windows\system32\wzcsvc.dll
\windows\system32\xpob2res.dll
\windows\system32\xpsp2res.dll
\ntldr
\ntdetect.com

Перечень разделов реестра:
HKLM\System\CurrentControlSet\Control
HKLM\System\CurrentControlSet\Services
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions

Дополнительно для платформы Win64:

\Windows\SysWOW64

Лист регистрации изменений

№ изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					
1.	6, 20	–	–	–	42	Извещение № 1, ФРКЕ.00116-03.1-2017	–	Тохтуева Н.А.	22.05.2017
2.	2-8, 12-16, 18, 20-23, 31, 41-42	–	1	–	44	Извещение № 2, ФРКЕ.00110.FB.2-2019	–	Тохтуева Н.А.	19.04.2019
3	6, 7, 10, 11, 18, 19, 36-41	–	–	–	41	Извещение № 3, ФРКЕ.00110.FB.3-2019	–	Тохтуева Н.А., Казанцев П.В.	30.01.2019