УТВЕРЖДЕН

ФРКЕ.00109-07 99 01 ПП-ЛУ

Программный комплекс

ViPNet Administrator 4

Правила пользования

ФРКЕ.00109-07 99 01 ПП

2017

Содержание

1 Общие положения

Программный комплекс ViPNet Administrator 4 (далее – ПК ViPNet Administrator) предназначен для формирования и управления сетью ViPNet, а также обеспечения ключевой информацией объектов и пользователей этой сети.

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

ПК ViPNet Administrator предназначен для эксплуатации на территории Российской Федерации, а также для экспортных поставок в качестве самостоятельных изделий или в составе указанных приложений и систем.

ПК ViPNet Administrator обеспечивает совместную работу с программными и программно-аппаратными комплексами ViPNet производства ОАО «ИнфоТеКС». Для обеспечения криптографических функций ПК ViPNet Administrator использует средство криптографической защиты информации (СКЗИ) ViPNet CSP 4.2 [4].

1.1 Состав программных средств ПК ViPNet Administrator

В состав специализированного программного обеспечения ПК ViPNet Administrator входят:

- ViPNet Administrator Центр управления сетью (далее − ViPNet ЦУС);
- ViPNet Administrator Удостоверяющий и Ключевой центр (далее − ViPNet УКЦ);
- средство криптографической защиты информации (далее – СКЗИ) ViPNet CSP 4.2.

1.2 Функции ПК ViPNet Administrator

Функции, реализуемые ViPNet ЦУС:

- аутентификация администраторов ViPNet ЦУС;
- регистрация узлов и пользователей сети ViPNet;
- задание связей между объектами (узлы, пользователи, группы пользователей) сети ViPNet;
- организация межсетевого взаимодействия с другими сетями ViPNet;
- централизованное управление настройками узлов сети ViPNet и политиками доступа пользователей к функциям узлов сети ViPNet;
- управление конфигурациями и справочниками узлов и пользователей сети ViPNet;
- рассылка узлам и пользователям сети ViPNet справочно-ключевой информации и программного обеспечения ViPNet;

- аудит действий администраторов ЦУС сети ViPNet;
- аудит обновления справочно-ключевой информации на узлах ViPNet;
- многопользовательский режим работы администраторов ViPNet ЦУС.

Функции, реализуемые ViPNet УКЦ:

- аутентификация администраторов ViPNet УКЦ;
- формирование и смена мастер-ключей;
- формирование и обновление симметричной ключевой и первичной парольной информации для узлов и пользователей сети ViPNet;
- формирование наборов справочно-ключевой информации для первичной инициализации узлов сети ViPNet, а также управление обновлением ключевой информации для узлов и пользователей сети ViPNet;
- издание сертификатов ключей проверки электронной подписи (далее – ЭП) и шифрования по запросам от пользователей сети ViPNet, от Центров регистрации и по собственной инициативе;
- отзыв, приостановление и возобновление действия сертификатов ключей проверки ЭП;
- ведение реестра сертификатов;
- издание списка аннулированных сертификатов (CRL);
- издание корневых сертификатов и кросс-сертификатов для взаимодействия с удостоверяющими центрами;
- импорт корневых сертификатов внешних удостоверяющих центров (УЦ);
- рассылка корневых сертификатов и CRL через ViPNet ЦУС на узлы сети ViPNet;
- управление обновлением ключевой информации узлов и пользователей при компрометации ключей.

Функции, реализуемые СКЗИ ViPNet CSP 4.2:

- формирование ключей шифрования;
- шифрование информации;
- выработка значения хэш-функции;
- вычисление имитовставки;
- создание ключа ЭП, создание ключа проверки ЭП;
- создание ЭП, проверка ЭП в автоматическом режиме.

1.3 Требования к составу технических средств и операционным системам

ПК ViPNet Administrator 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 Administrator функционирует под управлением ОС MS Windows:

- Microsoft Windows 7 SP1 (32/64-разрядная);
- Microsoft Windows 8.1 (32/64-разрядная);
- Microsoft Windows 10 (32/64-разрядная);
- Microsoft Windows Server 2008 R2 (64-разрядная);
- Microsoft Windows Server 2012 (64-разрядная);
- Microsoft Windows Server 2012 R2 SP1 (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 Administrator поддерживает работу в следующих виртуальных средах:

- Microsoft Hyper-V;
- VMware Workstation;
- VMware Player.

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

1.4 Дополнительное программное обеспечение

Для обеспечения функций распределения ключевой и справочной информации, а также обновления программного обеспечения узлов сети ViPNet совместно с ПК ViPNet Administrator необходимо использовать ПК ViPNet Client 4 (далее – ПК ViPNet Client), имеющее заключение ФСБ России о подтверждении соответствия требованиям ФСБ России и реализующее протокол MFTP. Класс используемого СКЗИ должен быть не ниже соответствующего класса ПК ViPNet Administrator.

Для обеспечения функций защиты от несанкционированного доступа по сетевому соединению при подключении к телекоммуникационной сети совместно с ПК ViPNet Administrator 4 должен использоваться межсетевой экран, сертифицированный ФСБ России по требованиям к устройствам типа межсетевые экраны по четвертому классу защищенности.

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

На компьютер, где установлен ПК ViPNet Administrator, запрещается устанавливать средства отладки и трассировки программного обеспечения (далее − ПО).

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 СУ, установку ключей на СУ и контроль их хранения;
- осуществляет контроль и несет ответственность за соблюдение правил безопасной эксплуатации сетевого узла (далее − СУ) или группы обслуживаемых им СУ;
- осуществляет настройки ОС и прикладного ПО и ПО ViPNet;
- 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;
- назначает список доступного на СУ функционала (задает роли узла);
- задает полномочия пользователей по доступу к функционалу (свойства ролей);
- 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:

- обладать паролем входа в ОС с правами, достаточными для выполнения своих обязанностей;
- обладать паролем для входа в программу ViPNet 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 ЦУС сформированной ключевой 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:

- обладать паролем входа в ОС с правами, достаточными для выполнения своих обязанностей;
- обладать паролем для входа в программу ViPNet УКЦ и иметь доступ к ее рабочим каталогам.

3 Требования к размещению технических средств

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

1 Размещение, охрана и специальное оборудование помещений, в которых установлены технические средства (далее – ТС) и ведется работа с персональной ключевой информацией, 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 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.

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

4 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.

5 ТС с ПК ViPNet Administrator могут подключаться к общегородской сети электроснабжения с учетом требований инструкций по эксплуатации вычислительных средств и правил техники безопасности.

6 Оборудование помещений средствами вентиляции и кондиционирования воздуха должно соответствовать санитарно-гигиеническими нормам СНиП, устанавливаемым законодательством Российской Федерации.

7 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.

8 В помещение допускаются только сотрудники, имеющие непосредственное отношение к организации эксплуатации ПК ViPNet Administrator.

9 Уборка помещения осуществляется назначенным персоналом при выключенных мониторах в присутствии Администратора безопасности.

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

11 При эксплуатации ПК ViPNet Administrator на объектах заказчика должны выполняться действующие в Российской Федерации требования по защите информации, предназначенной для шифрования, от утечки по техническим каналам, в том числе каналам связи[1].

12 Размещение СКЗИ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

[1] Требования по защите информации от утечки по техническим каналам, в том числе по каналу связи приведены, например, в СТР-К.

4 Установка и ввод в эксплуатацию ПК ViPNet Administrator

4.1 Порядок распространения и учета ПК ViPNet Administrator

ПК ViPNet Administrator и пакет документов к нему поставляется в электронном виде в соответствии с эталонным диском, хранящимся в ОАО «ИнфоТеКС». Формуляр поставляется в печатном виде.

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

Проверку целостности администратор осуществляет путем сравнения контрольных сумм дистрибутива с указанными контрольными суммами в формуляре на изделие [6].

Поэкземплярный учет ПК ViPNet Administrator осуществляется производителем – ОАО «ИнфоТеКС» в процессе подготовки комплекта изделия. Далее Администратору ЦУС или Администратору безопасности, ответственному за установку и эксплуатацию ПК Administrator, предоставляется экземпляр дистрибутива, формуляр изделия в бумажном виде с указанием регистрационного номера СКЗИ, серийного номера дистрибутива, контрольной суммы дистрибутива.

4.2 Установка ПК ViPNet Administrator

До установки ПК ViPNet Administrator 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 [6].

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

Средствами BIOS должна быть исключена дальнейшая загрузка ТС с установленным ПК ViPNet Administrator в случае, если во время начальной загрузки не проходят встроенные тесты Power-On-Self-Test.

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

При настройке учетных записей средства типа «электронный замок» также необходимо соблюдать требования к сложности и времени обновления паролей, приведенные в п. 4.5.

До установки ПК ViPNet Administrator компьютер должен быть отключен от локальной сети.

Для того чтобы развернуть ПК ViPNet Administrator, необходимо выполнить следующие действия:

1 Установить и настроить программу ViPNet ЦУС.
2 Создать минимальную (необходимую для начала работы с сетью) структуру сети ViPNet в ViPNet ЦУС.
3 Установить и провести первоначальную инициализацию программы ViPNet УКЦ.
4 Сформировать в ViPNet УКЦ дистрибутивы ключей для узлов, ранее зарегистрированных в ViPNet ЦУС.
5 Установить ПО ViPNet Client на компьютер с ПК ViPNet Administrator. Затем при помощи созданного в ViPNet УКЦ дистрибутива ключей провести первичную инициализацию на данном СУ.

После развертывания ПК ViPNet Administrator необходимо убедиться в выполнении требований по защите от НСД, описанных в разделе 6.3 и документе [4].

Проводить настройку и работу в ViPNet ЦУС и ViPNet УКЦ могут только администраторы ЦУС и администраторы УКЦ, соответственно. Уполномоченный Администратор безопасности имеет права только на установку и настройку ОС и ПО, необходимого для работы ПК ViPNet Administrator.

Установка ПК ViPNet Administrator осуществляется в соответствии с документами [1], [2]. По завершении установки осуществляются настройки ПО в соответствии с требованиями п. 4.4 и контроль работоспособности ПО в соответствии с п.5.2.

4.3 Ввод в эксплуатацию

Ввод в эксплуатацию ПК ViPNet Administrator осуществляется Администратором безопасности.

На каждое рабочее место, оснащенное ПК ViPNet Administrator, оформляется Акт о вводе в эксплуатацию по типовой форме. Акт может храниться у Администратора безопасности или у Администратора ЦУС или УКЦ.

4.4 Требования к настройкам ПК ViPNet Administrator

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

Настройки программ ViPNet ЦУС и ViPNet УКЦ осуществляются Администратором ЦУС и Администратором УКЦ, соответственно. Настройки проводятся в соответствии с документацией [1] и [2].

После установки и настройки ПК ViPNet Administrator необходимо включить ведение журналов событий администратора и криптопровайдера.

Дополнительно для исполнения 3 ПК ViPNet Administrator необходимо:

1 Включить опцию «Обязательный ввод пароля при входе в операционную систему».

2 Убедиться, что установлен и настроен модуль защиты среды функционирования, входящий в состав СКЗИ ViPNet CSP 4.2. Описание настройки данного модуля приведено в документе [5].

Также Администратор безопасности должен настроить архивирование журналов событий ViPNet Administrator, а также обеспечить разграничение доступа к архивам журналов. Архивирование журналов событий и разграничение доступа к архивам журналов обеспечивается средствами ОС.

Для архивирования журналов необходимо при настройке параметров хранения файла журнала событий в ОС выбрать пункт «Архивировать журнал при заполнении; не перезаписывать события».

Для разграничения доступа к архивам журналов Администратор безопасности должен написать скрипт, который будет запускаться по расписанию с правами администратора, и копировать архивы журналов 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.

4.5 Регистрация пользователей и СУ в сети ViPNet

Регистрацию пользователей и СУ в сети ViPNet осуществляют Администраторы, входящие в группу Администраторов ЦУС, с использованием ViPNet ЦУС 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.

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 Administrator

Все действия по обслуживанию и настройкам ПК ViPNet Administrator должны производиться следующими лицами: Администратором безопасности и Администратором ЦУС или УКЦ согласно их полномочиям по работе с комплексом.

Помимо требований и рекомендаций, изложенных в данном документе, в процессе эксплуатации ПК ViPNet Administrator должны выполняться требования и рекомендации, приведенные в правилах пользования на СКЗИ ViPNet CSP 4.2 [4].

5.1 Контроль целостности ТС и ПО

До включения ПК ViPNet Administrator пользователь обязан убедиться в отсутствии:

- внешних признаков вскрытия системного блока;
- подключенного дополнительного оборудования, не предусмотренного Актом о вводе в эксплуатацию.

ПК ViPNet Administrator оснащен встроенными механизмами проверки целостности ПО, справочной и ключевой информации. Проверка производится при каждом старте ПК ViPNet Administrator. Кроме того, встроены механизмы периодического тестирования работоспособности и целостности криптографических библиотек и ключевой информации.

Для ПК ViPNet Administrator исполнения 1 требования по контролю целостности реестра Windows не предъявляются.

Для ПК ViPNet Administrator исполнений 2, 3 целостность разделов реестра Windows обеспечивается с помощью средства защиты от НСД типа «электронный замок».

В ПК ViPNet Administrator исполнений 2, 3 контроль целостности исполняемых модулей ОС Windows осуществляется с помощью средства защиты от НСД типа «электронный замок».

ПК ViPNet Administrator исполнения 1 оснащен встроенными механизмами проверки целостности исполняемых модулей ОС. После установки ПК ViPNet Administrator исполнения 1 необходимо сформировать список исполняемых модулей ОС и вычислить контрольные суммы этих модулей. Типовой перечень исполняемых модулей ОС приведен в приложении 2 данного документа (соответствует содержимому файла C:\ProgramData\Infotecs\ViPNet CSP\os.prg). Часть файлов 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 вычисления контрольных сумм файлов из перечня os.prg необходимо в каталоге ViPNet CSP запустить с правами администратора утилиту make_ext_crg 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 (для редактирования этого файла требуются права администратора 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:

- команду 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

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

  Он не должен содержать ошибок.
- проверку целостности из контрольной панели ViPNet Administrator.

Компьютер, на который установлен ПК ViPNet Administrator, должен перезагружаться не реже одного раза в месяц.

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 ошибок при загрузке программного обеспечения Администратор безопасности или Администратор ЦУС/УКЦ в зависимости от своих полномочий обязан:

- отключить ТС с ПК ViPNet Administrator от ЛВС до устранения неисправностей;
- провести исследование с целью выяснения возможных причин возникновения неисправностей;
- произвести проверку работоспособности технических средств, на которых установлен ПК ViPNet Administrator;
- провести анализ журналов аудита с целью выявления попыток несанкционированного доступа и сетевых атак;
- при обнаружении признаков несанкционированного доступа к ПК ViPNet Administrator уведомить Администратора УКЦ о возможной компрометации ключей узла;
- устранить обнаруженные причины возникновения неисправностей или искажений;
- при необходимости произвести переустановку ПК ViPNet Administrator;
- 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 Administrator. 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.

Контрольная проверка на ПК ViPNet Administrator осуществляется в следующих случаях:

- при вводе ПК ViPNet Administrator 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.

5.3 Обновление ПК ViPNet Administrator

Под обновлением понимается повышение версионности ПО ViPNet Administrator.

Обновление ПО ViPNet Administrator осуществляется только локально, путем запуска штатной процедуры установки сертифицированного обновления на локальном компьютере. Установка обновления производится Администратором безопасности. Другие способы обновления ПО недопустимы. Перед обновлением должна быть выполнена проверка целостности файла дистрибутива ПО ViPNet Administrator путем сравнения контрольной суммы файла с контрольной суммой, указанной в формуляре [6].

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

5.4 Восстановление работоспособности при сбоях

Все действия по восстановлению работоспособности ПК ViPNet Administrator производятся только Администратором безопасности.

ViPNet ЦУС и ViPNet УКЦ независимо друг от друга обращаются к общей базе данных ПК ViPNet Administrator, в которой хранится информация о структуре сети, поэтому изменения одной программы незамедлительно отображаются в другой. Общая база данных позволяет избежать перерывов в обработке информации в случае временного выхода из строя ViPNet ЦУС и (или) ViPNet УКЦ. Однако нарушение целостности или потеря базы данных могут привести к серьезным последствиям с точки зрения возможности дальнейшей эксплуатации защищенной сети ViPNet. В связи с этим необходимо создавать резервные копии всех данных ПК ViPNet Administrator в ViPNet УКЦ. Резервные копии могут создаваться автоматически или вручную.

Автоматически резервное копирование осуществляется периодически согласно настройкам – но не реже 1 раза в сутки (если программа ViPNet УКЦ включена). Перенос и хранение резервных копий необходимо осуществлять в соответствии с организационно-техническим регламентом по осуществлению резервного копирования, принятым в организации.

Вручную резервное копирование выполняется с использованием мастера восстановления конфигурации. Рекомендуется выполнять резервное копирование перед обновлением ПК ViPNet Administrator. Созданную резервную копию можно использовать для восстановления конфигурации сети в случае нарушения работоспособности ПК ViPNet Administrator или сети ViPNet после обновления. Штатная процедура восстановления описана в документе [2].

При установке на новый компьютер следует провести заново инсталляцию программы согласно п.5.1 и восстановить конфигурацию ПК ViPNet Administrator из последней резервной копии, предварительно скопировав ее на новый компьютер.

5.5 Порядок вывода из эксплуатации и утилизации СКЗИ

ПК ViPNet Administrator эксплуатируется в соответствии с разделом 5 «Эксплуатация ПК ViPNet Administrator». Порядок удаления ПК ViPNet Administrator и всех ключей описан в документах [1] и [2]. Утилизация ПК ViPNet Administrator регламентируется разделом III «Порядок обращения с СКЗИ», утвержденным приказом ФАПСИ от 13 июня 2001 г. № 152.

Эксплуатация и утилизация устройства типа «электронный замок» и ТС, на котором функционирует ПК ViPNet Administrator, осуществляется производителем в соответствии с документацией на него.

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

6.1 Общие положения

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

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

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

6.3 Требования по защите от НСД при эксплуатации ПК ViPNet Administrator

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. 4.5. Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

Запрещается:

- оставлять без контроля ПК ViPNet Administrator после прохождения процесса аутентификации на СУ;
- вносить какие-либо изменения в программное обеспечение ПК ViPNet Administrator;
- 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 Administrator;
- записывать на ключевые носители постороннюю информацию.

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

- на ТС должна быть установлена только одна ОС;
- в зависимости от целей использования ПК ViPNet Administrator 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;
- в ОС должна быть исключена возможность удалённого (сетевого) администрирования для всех групп пользователей ОС, в том числе удалённое редактирование системного реестра.

Необходимо организовать затирание (по окончании сеанса работы) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы ПК ViPNet Administrator. Затирание следует выполнять путем запуска утилиты `clean.exe`, входящей в состав СКЗИ ViPNet CSP 4.2 и расположенной в каталоге установки СКЗИ ViPNet CSP 4.2.

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 Administrator к общедоступным сетям передачи данных 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.

7 Ключевая информация

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 формировании дистрибутива ключей для пользователя в его состав помещается РНПК.

На СУ аутентификация может быть выполнена следующими способами:

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

2 Устройство. При этом способе аутентификации используются устройство аутентификации (подробно виды устройств аутентификации и ограничения по применению устройств приведены в [2]) и ПИН-код устройства.

При использовании данного способа возможны два типа аутентификации:

- Персональный ключ на устройстве. Для доступа к СУ необходимо подключить устройство аутентификации, на котором сохранен персональный ключ пользователя, и ввести ПИН-код.
- Сертификат на устройстве. Для доступа к СУ необходимо подключить устройство аутентификации, на котором сохранены сертификат ключа проверки электронной подписи и соответствующий ключ электронной

подписи, и ввести ПИН-код. В данном варианте необходимо использовать устройство аутентификации, поддерживающее интерфейс PKCS#11, а также учитывать ограничения, приведенные в [2].

3 Сертификат аутентификации. Для доступа к СУ пользователю требуется контейнер ключей и сертификат ключа проверки ЭП, не закрепленный за каким-то определенным устройством и хранящийся на компьютере пользователя либо в защищенном хранилище организации. Данный тип аутентификации может быть использован для настройки аутентификации пользователя по общему сертификату в ОС Windows, ПО ViPNet и других специализированных программах. При настройке данного способа аутентификации администратору УКЦ не требуется контейнер ключей ЭП пользователя, за счет этого обеспечивается защита ключей от доступа третьих лиц. Данный тип аутентификации не поддерживается ПК ViPNet Client и ПК ViPNet Coordinator.

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.

Примечание: В соответствии с требованиями к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, использование парольной аутентификации в исполнениях 2 и 3 (класс КС2 и класс КС3) недопустимо.

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.

При изменении структуры сети ViPNet в ходе ее эксплуатации информация, находящаяся в составе дистрибутива ключей, становится неактуальной. Для актуализации справочно-ключевой информации вместо повторного использования дистрибутива ключей 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 на узле 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 обновления ключевой информации при смене мастер-ключа персональных ключей или при увеличении 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 Администратором УКЦ 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 ViPNet 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. 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 должна быть сделана соответствующая отметка.

7.4 Плановая смена и обновление ключей

Обновление ключей узлов при изменении структуры сети и плановая смена ключей узлов и пользователей производится централизованно. Плановая смена ключей осуществляется в ViPNet УКЦ одним из способов:

- путем увеличения варианта ключей узлов и ключей пользователей. Под вариантом ключей узла понимается порядковый номер ключей обмена и ключей защиты, которые идут в составе ключей узла. Под вариантом ключа пользователя понимается 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 в присутствии Администратора безопасности. Администратор безопасности должен подключить съемный носитель с РНПК этого пользователя для обновления ключей на узле.

При смене мастер-ключа персональных ключей в программе ViPNet Administrator формируются специализированные ключевые наборы, содержащие РНПК, сформированные на новом мастер-ключе. Доставка таких обновлений производится по доверенному каналу. Это необходимо для предотвращения последствий возможной неявной компрометации наборов РНПК на узлах сети.

Если у пользователя имеется ключ ЭП, инициатива создания которого принадлежит Администратору УКЦ, 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.

В зависимости от типа ключевой информации, к которой утрачено доверие, а также от положения узла со скомпрометированными ключами в структуре сети ViPNet, возможны различные варианты обновления ключевой информации при компрометации ключей.

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

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения ключей;
- возникновение подозрений на утечку информации;
- нарушение печати на сейфе с ключевыми носителями.

Первые четыре события должны трактоваться как явная компрометация действующих ключей. Остальные события (неявная компрометация), которые требуют специального рассмотрения в каждом конкретном случае. Ключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно вывести из действия. О выводе ключей из действия Администратор безопасности обязан сообщить Администратору УКЦ.

Администратор безопасности прекращает использование скомпрометированных ключей. После получения новых ключевых документов Администратор безопасности выполняет действия, аналогичные первичной установке ключевых документов.

7.5.1 Компрометация пароля пользователя и пароля Администратора СУ

При подозрении, что посторонним лицам может быть известен пароль доступа к ключам, которые используются в приложении ViPNet, но доступ к ключам этих посторонних лиц был и остается невозможен (ключи не скомпрометированы), следует сменить пароль. Смена пароля пользователя осуществляется локально на узле в соответствии с процедурой локального изменения.

Смена пароля Администратора СУ осуществляется в ПО ViPNet УКЦ. После смены пароля Администратора СУ необходимо сформировать и отправить на СУ обновление ключей в соответствии с процедурой централизованного обновления [1], [2].

7.5.2 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.

7.5.3 Компрометация персонального ключа пользователя и ключей узла

Если ключи узла скомпрометированы, то ключи пользователя также считаются скомпрометированными. В этом случае необходимо применить новый вариант персонального ключа пользователя и новый вариант ключей СУ, после чего осуществить обновление ключей пользователя и узла и ключей на узлах, связанных с этим узлом.

Если скомпрометированы персональные ключи пользователя, но доверие к ключам узла не утрачено (например, утеряно устройство аутентификации, но доступ к ключам узла у потенциального злоумышленника отсутствует), то для обновления ключей необходимо применить новый вариант персонального ключа пользователя в соответствии с процедурой, описанной в [2].

7.5.4 Компрометация РНПК

Утрата доверия к РНПК наступает в случае получения злоумышленником доступа к дистрибутиву ключей, в котором находится РНПК, либо непосредственно к файлу РНПК, если он хранится отдельно.

При утрате доверия к РНПК (автоматически утрачено доверие к персональному ключу пользователя и ключам узла) требуется выполнить одно из действий:

- удалить учетную запись скомпрометированного пользователя и узел из структуры сети ViPNet и создать новую учетную запись пользователя и узел;
- провести внеплановую смену мастер-ключа персональных ключей, которая проводится аналогично плановой смене ключей, см. раздел 7.4.

7.5.5 Компрометация мастер-ключей ViPNet УКЦ

В случае утраты доверия к мастер-ключам ViPNet УКЦ, необходимо удалить все имеющиеся мастер-ключи, создать новые, для всех узлов сети создать дистрибутивы ключей и провести инициализацию узлов с новыми дистрибутивами.

В случае утраты доверия к Администратору УКЦ необходимо удалить ключи защиты ViPNet УКЦ, сертификат уполномоченного лица и осуществить процедуру развертывания ViPNet УКЦ и создания ключевой информации для первичной инициализации всех узлов сети.

7.5.6 Компрометация ключей одного из нескольких пользователей узла

Данная необходимость может возникнуть при наличии на узле нескольких пользователей, ключи одного из которых скомпрометированы.

В этом случае необходимо:

1 Удалить скомпрометированного пользователя.

2 Ключам узла увеличить номер варианта и отправить новые ключи на узел.

3 Заново зарегистрировать пользователя на узле.

4 Сформировать новый дистрибутив ключей в ViPNet УКЦ для пользователя и развернуть его на узле.

5 Остальным связанным узлам сети выслать обновление ключей из ViPNet ЦУС.

8 Список документов

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

2. ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора, ОАО «ИнфоТеКС», 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. Средство криптографической защиты информации ViPNet CSP 4.2. Правила пользования, ФРКЕ.00106-04 99 01 ПП.

5. ViPNet CSP 4.2. Руководство пользователя, ОАО «ИнфоТеКС», ФРКЕ.00106-04 34 01.

6. Программный комплекс ViPNet Administrator 4. Формуляр, ФРКЕ.00109-07 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
ЦР	–	центр регистрации
ЭП	–	электронная подпись

ПРИЛОЖЕНИЕ 1

Протокол

контрольной проверки ПК ViPNet Administrator

«___» _____ 20___ г.

ПК ViPNet Administrator 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 (+/-)	Примечания. Отметки об устранении
1.	Перезапуск и проверка аутентификации в ПО Administrator	ПО Administrator перезапустилось, потребовалось прохождение аутентификации		
2.	Добавление нового пользователя	Успешное добавление нового пользователя		
3.	Создание дистрибутива ключей для СУ (ключей узла и ключей пользователя)	Успешное создание дистрибутива ключей		
4.	Выпуск тестового сертификата для тестового пользователя	Успешный выпуск тестового сертификата		
5.	Проверка журналов событий ViPNet УКЦ и ViPNet ЦУС	В журналах событий содержатся записи о следующих событиях: • аутентификация администратора; • добавлен пользователь; • созданы ключи узла; • созданы ключи пользователя; • издан сертификат пользователя.		
6.	Отзыв тестового сертификата тестового пользователя	Сертификат помечен, как аннулированный		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
7.	Выпуск CRL	Успешный выпуск очередного CRL		Рекомендуется совместить контрольную проверку с выпуском очередного CRL, чтобы избежать выпуск внеочередного CRL

Администратор безопасности

" "_____20___г.

Пользователь

" "_____20___г.

ПРИЛОЖЕНИЕ 2

Перечень исполняемых модулей ОС Windows и разделов реестра, подлежащих контролю целостности

Перечень исполняемых модулей ОС Windows и разделов реестра, подлежащих контролю целостности приведен в документе «Средство криптографической защиты информации ViPNet CSP 4.2. Правила пользования», ФРКЕ.00106-04 99 01 ПП, ОАО «ИнфоТеКС».

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	1, 2, 3, 5, 6, 8, 10, 11, 12, 13, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 33	-	-	7	36	Извещение №1 ФРКЕ.00109.1-2018	-	Лопатина А.Б.	20.04.2018