УТВЕРЖДЕН

ФРКЕ.00177-02 30 01 ФО-ЛУ

Система обнаружения вторжений

ViPNet IDS HS

ФОРМУЛЯР

ФРКЕ.00177-02 30 01 ФО

2019

Содержание

1 Общие указания

1.1 Перед эксплуатацией продукта необходимо ознакомиться с настоящим формуляром, правилами пользования и другими эксплуатационными документами на продукт, указанными в настоящем формуляре.

1.2 Формуляр должен постоянно храниться у пользователя (в эксплуатирующей организации).

1.3 Ведение формуляра подразумевает своевременное внесение пользователем (лицом, ответственным за ведение формуляра) в процессе эксплуатации продукта (при необходимости) записей в соответствующие разделы формуляра: «Сведения о рекламациях», «Сведения о хранении», «Сведения о закреплении при эксплуатации», «Сведения об изменениях», «Особые отметки». Краткая пояснительная информация об условиях внесения записей приведена в указанных разделах.

1.4 Все записи в формуляре должны выполняться чернилами (шариковой ручкой) отчетливо и аккуратно. Не допускаются записи карандашом или смывающимися чернилами.

1.5 Не допускается внесение в настоящий формуляр записей, не заверенных подписью или личным штампом пользователя (ответственного лица).

1.6 Не допускаются подчистки и использование штриха-корректора. Неправильная запись должна быть аккуратно зачеркнута, рядом должна быть записана новая запись, которую пользователь (ответственное за внесение исправления лицо) заверяет своей подписью.

1.7 Изменения в подлинник формуляра вносит изготовитель продукта с обязательным заполнением листа регистрации изменений.

1.8 Изменения в копии формуляра, находящиеся у пользователей (в эксплуатирующей организации), вносят на основании полученных от изготовителя бюллетеней (информационных сообщений), содержащих информацию о необходимости внесения изменений, с обязательным заполнением раздела «Сведения об изменениях».

2 Общие сведения о продукте

2.1 Основные сведения

2.1.1 Обозначение продукта: ФРКЕ.00177-02.

2.1.2 Тип продукта: программный комплекс.

2.1.3 Наименование: Система обнаружения вторжений ViPNet IDS HS (далее – ViPNet IDS HS или продукт).

2.1.4 Изготовитель: открытое акционерное общество «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»), 127287, Россия, Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, тел. (495) 737-61-92, лицензия ФСТЭК России на осуществление разработки и производства средств защиты конфиденциальной информации № 0636 от 24.03.2010 (бессрочная), лицензия ФСБ России на осуществление разработки и производства средств защиты конфиденциальной информации № 12282 К от 18.06.2012 (бессрочная)..

2.2 Назначение

2.2.1 ViPNet IDS HS представляет собой программный комплекс (далее – ПК), который предназначен для автоматического обнаружения вторжений (атак) на узле информационной системы (далее – ИС) на основе сигнатурного и эвристического методов анализа информации, а также позволяет упростить процесс установления источников компьютерных инцидентов.

2.2.2 ViPNet IDS HS может использоваться для защиты информации ограниченного доступа (в том числе персональных данных, служебной и коммерческой тайн и другой информации), не содержащей сведений, составляющих государственную тайну, в целях повышения уровня защищенности ИС, центров обработки данных (далее – ЦОД), рабочих станций пользователей, серверов и коммуникационного оборудования государственных и коммерческих структур.

2.3 Область применения

2.3.1 ViPNet IDS HS соответствует 4 классу защиты систем обнаружения вторжений, 4 уровню доверия и предназначен для использования в государственных информационных системах (далее – ГИС) до класса защищенности[1] К1 включительно, на верхнем уровне (уровне диспетчерского управления) в автоматизированных системах управления производственными

[1] Устанавливается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. №17.

и технологическими процессами (далее – АСУ ТП) до класса защищенности[2] К1 включительно, в ИС персональных данных для обеспечения уровня защищенности[3] персональных данных до 1 уровня включительно, в ИС общего пользования II класса[4], в том числе для обеспечения следующих базовых и адаптированных мер защиты информации в соответствии с требованиями, утвержденными приказами ФСТЭК России №17 от 11.02.2013, №21 от 18.02.2013 и №489 от 31.08.2010:

- ИАФ.1* – Идентификация и аутентификация пользователей, являющихся работниками оператора;
- ИАФ.5* – Защита обратной связи при вводе аутентификационной информации;
- УПД.1* – Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- УПД.4* – Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- УПД.6* – Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- УПД.10* – Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- РСБ.1 – Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- РСБ.З – Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- РСБ.4* – Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- РСБ.5 – Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- РСБ.7* – Защита информации о событиях безопасности;

[2] Устанавливается в соответствии с Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденными приказом ФСТЭК России от 14 марта 2014 г. №31.

[3] Устанавливается в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

[4] Устанавливается в соответствии с Требованиями о защите информации, содержащейся в информационных системах общего пользования, утвержденными приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

– СОВ.1 – Обнаружение вторжений;
– СОВ.2 – Обновление базы решающих правил;
– АНЗ.3* – Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
– ОЦЛ.1* – Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
– ОЦЛ.3* – Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;
– ИНЦ.2 – Обнаружение, идентификация и регистрация инцидентов;
– ИНЦ.3* – Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
– ИНЦ.4* – Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий.

2.3.2 Также ViPNet IDS HS может использоваться в автоматизированных системах управления (далее – АСУ), ИС и информационно-телекоммуникационных сетях (далее – ИТС), которые отнесены к значимым объектам критической информационной инфраструктуры (далее – КИИ) до категории значимости[5] К1 в соответствии со статьей 7 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в том числе для выполнения следующих базовых и адаптированных мер защиты информации и мер по обеспечению безопасности значимых объектов КИИ Российской Федерации в соответствии с требованиями, утвержденными приказами ФСТЭК России №31 от 14.03.2014 и № 239 от 25.12.2017:

– ИАФ.1* – Идентификация и аутентификация пользователей и инициируемых ими процессов;
– ИАФ.7* – Защита аутентификационной информации при передаче;
– УПД.1* – Управление учётными записями пользователей;
– УПД.4* – Разделение полномочий (ролей) пользователей;
– УПД.6* – Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему;

[5] Устанавливается в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 года № 239.

– УПД.10* – Блокирование сеанса доступа пользователя при неактивности;
– АУД.2* – Анализ уязвимостей и их устранение;
– АУД.4 – Регистрация событий безопасности;
– АУД.5 – Контроль и анализ сетевого трафика;
– АУД.6 – Защита информации о событиях безопасности;
– АУД.7 – Мониторинг безопасности;
– АУД.8 – Реагирование на сбои при регистрации событий безопасности;
– АУД.9 – Анализ действий отдельных пользователей;
– СОВ.1 – Обнаружение и предотвращение компьютерных атак;
– СОВ.2 – Обновление базы решающих правил;
– ОДТ.3* – Контроль безотказного функционирования средств и систем;
– ОЦЛ.1* – Контроль целостности программного обеспечения;
– ОДТ.6* – Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях;
– ИНЦ.1 – Выявление компьютерных инцидентов;
– ИНЦ.2 – Информирование о компьютерных инцидентах;
– ИНЦ.3 – Анализ компьютерных инцидентов.

Примечание. В отношении мер защиты информации и мер по обеспечению безопасности значимых объектов КИИ, отмеченных «*», обеспечивается их выполнение не в рамках защищаемой системы в целом, а для самого ViPNet IDS HS как компонента защищаемой системы.

2.3.3 ViPNet IDS HS предназначен для использования на территории Российской Федерации в 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.

3 Основные характеристики

3.1 Состав продукта

3.1.1 В состав ViPNet IDS HS входят следующие компоненты:

– ViPNet IDS HS Агент (далее – Агент) – выполняет функции датчика (сенсора) и анализатора (собирает необходимую информацию о функционировании ИС в режиме сбора с заданной периодичностью и выполняет первичный анализ собранных данных с применением базы решающих правил (далее – БРП) для обнаружения вторжения (атаки) в контролируемую ИС). Агент устанавливается на защищаемые узлы ИС;

– ViPNet IDS HS Сервер (далее – Сервер IDS HS) – служит для получения и хранения информации от Агентов, хранения и рассылки правил, команд и настроек для Агентов. На Сервере IDS HS также производится анализ и агрегирование данных, полученных от Агентов. При соответствующих настройках данные, полученные от Агентов, передаются в сторонние программные средства по протоколам CEF и SNMP;

– ViPNet IDS HS Консоль управления (далее – Консоль управления) – предоставляет графический интерфейс для мониторинга и управления Агентами. При соответствующих настройках функции Консоли управления может выполнять ПК ViPNet IDS MC.

Примечание. Количество подключаемых к Серверу IDS HS Агентов определяется лицензией на ViPNet IDS HS.

3.2 Функциональные возможности

3.2.1 ViPNet IDS HS обеспечивает обнаружение и (или) блокирование следующих основных угроз безопасности информации, относящихся к вторжениям (атакам):

– преднамеренный несанкционированный доступ (далее – НСД) или специальное воздействие на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;

– преднамеренный НСД или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в ИС.

3.2.2 Помимо вышеуказанных угроз безопасности информации, ViPNet IDS HS обеспечивает обнаружение угроз безопасности информации, которым подвержены сами системы обнаружения вторжений (атак). К таким угрозам относятся:

- нарушение целостности программного обеспечения (далее – ПО);
- нарушение целостности данных, собранных или созданных ViPNet IDS HS (данных ViPNet IDS HS);
- отключение или блокирование нарушителями компонентов ViPNet IDS HS;
- несанкционированное изменение конфигурации ViPNet IDS HS;
- несанкционированное внесение изменений в логику функционирования ViPNet IDS HS через механизм обновления БРП.

Примечание. Блокирование указанных угроз безопасности информации обеспечивается механизмами самого ViPNet IDS HS или внешними по отношению к ViPNet IDS HS механизмами и мерами защиты информации, реализуемыми в среде функционирования ViPNet IDS HS.

3.2.3 ViPNet IDS HS реализует следующие функциональные возможности:

- возможность сбора информации о сетевом трафике, проходящем через контролируемые узлы ИС, о событиях, регистрируемых в журналах аудита и реестре операционной системы (далее – ОС), прикладного ПО, о вызове функций, об обращении к ресурсам;
- возможность выполнения анализа собранных данных о сетевом трафике, запущенным процессам и файловой активности в режиме, близком к реальному масштабу времени, и фиксации по результатам анализа информации о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения (атаки);
- возможность обнаружения вторжений (атак) по отношению к контролируемым узлам ИС в режиме, близком к реальному масштабу времени, на уровне отдельных узлов;
- возможность выполнения анализа собранных данных с целью обнаружения вторжений (атак) с использованием сигнатурного и эвристических методов;
- возможность выполнения анализа собранных данных с целью обнаружения вторжений (атак) с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика и аномалий в действиях пользователя ИС, на заданном уровне эвристического анализа;

- возможность фиксации факта обнаружения вторжений (атак) или нарушений безопасности в журналах аудита;
- возможность уведомления администратора ViPNet IDS HS об обнаруженных вторжениях (атаках) и нарушениях безопасности с помощью отображения соответствующего сообщения на Консоли управления, а также посредством электронной почты;
- возможность обнаружения вторжений (атак) на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;
- возможность автоматизированного обновления БРП;
- возможность администрирования ViPNet IDS HS;
- возможность со стороны администраторов ViPNet IDS HS управлять режимом выполнения функций безопасности ViPNet IDS HS;
- возможность со стороны администраторов ViPNet IDS HS управлять данными, используемыми функциями безопасности;
- поддержка определенных ролей для ViPNet IDS HS и их ассоциации с конкретными администраторами ViPNet IDS HS и пользователями ИС;
- возможность управления данными функций безопасности ViPNet IDS HS (данными ViPNet IDS HS) в части установления и контроля ограничений на эти данные;
- возможность тестирования (самотестирования) функций безопасности ViPNet IDS HS (контроль целостности исполняемого кода ViPNet IDS HS);
- возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;
- возможность отображения информации из записей аудита для чтения;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность ограничения доступа к чтению записей аудита;
- возможность поиска, сортировки, упорядочения данных аудита;
- возможность интеграции ViPNet IDS HS с ПК ViPNet IDS MC, а также с внешними системами мониторинга событий;
- возможность синхронизации информации об узлах системы с Active Directory и ПК ViPNet Client;
- предоставление услуг мониторинга угроз безопасности информации в сети различным организациям;

– контроль файлов, содержащих вредоносное ПО;
– регистрация событий, связанных с обнаружением вредоносного ПО;
– обнаружение вредоносной активности RemSec;
– отслеживание установки системных обновлений ОС Windows;
– выгрузка информации о событиях в файл для ГосСОПКА.

3.2.4 Также в ViPNet IDS HS реализованы:

– возможность создания правил безопасности, доступная администратору ViPNet IDS HS;
– формирование отчетной информации;
– отслеживание изменений в журнале событий ОС Windows и в журналах приложений;
– контроль файловой активности (отслеживание изменений в каталогах или группах файлов);
– контроль системного реестра ОС Windows;
– контроль процессов, запущенных на компьютере с установленным Агентом;
– контроль установки нового ПО на компьютер с установленным Агентом;
– контроль состояния Агента.

3.2.5 ViPNet IDS HS поддерживает совместную работу с программными и программно-аппаратными продуктами ViPNet производства ОАО «ИнфоТеКС», включая ПК ViPNet Client, ПК ViPNet IDS MC, ПК ViPNet StateWatcher, программно-аппаратный комплекс (далее – ПАК) ViPNet TIAS, с внешними системами мониторинга событий (ArcSight и прочие), а также со службами Active Directory.

3.2.6 При выполнении требований и рекомендаций, изложенных в правилах пользования ФРКЕ.00177-02 99 01 ПП и другой эксплуатационной документации на продукт, ViPNet IDS HS соответствует:

– требованиям документа ФСБ России «Требования к средствам обнаружения компьютерных атак», установленным для класса Б;
– требованиям документа «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011);
– требованиям документа «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012);
– требованиям документа «Система обнаружения вторжений ViPNet IDS HS. Задание по безопасности» ФРКЕ.00177-02 98 01;

– требованиям документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018).

3.3 Системные требования

3.3.1 Компоненты ViPNet IDS HS функционируют на компьютерах, поддерживающих архитектуру x86, x86-64 с минимально рекомендуемой производителем ОС аппаратной конфигурацией (с учетом требований, изложенных в пп. 3.3.2-3.3.3), а также в среде виртуализации, поддерживающей эти архитектуры.

3.3.2 Требования к компьютеру для установки Агента и Консоли управления:

– процессор – Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;
– объем оперативной памяти – не менее 1 Гбайт;
– свободное место на жестком диске – не менее 500 Мбайт (рекомендуется 600 Мбайт);
– наличие сетевого адаптера или модема.

3.3.3 Требования к компьютеру для установки Сервера IDS HS:

– процессор – Intel Core 2 Quad или другой схожий по производительности x86-совместимый процессор с количеством ядер 4 и более;
– объем оперативной памяти – не менее 8 Гбайт;
– свободное место на жестком диске – не менее 100 Гбайт;
– наличие сетевого адаптера или модема.

3.3.4 Компоненты ViPNet IDS HS функционируют под управлением ОС, перечисленных в таблице 1.

Таблица 1 – Поддерживаемые операционные системы

Агент	Сервер IDS HS	Консоль управления
Microsoft Windows 8.1 (32/64-разрядная)	Microsoft Windows 8.1 (64-разрядная)	Microsoft Windows 8.1 (64-разрядная)
Microsoft Windows 10 (32/64-разрядная)	Microsoft Windows 10 (64-разрядная)	Microsoft Windows 10 (64-разрядная)
Microsoft Windows Server 2012 (64-разрядная)	Microsoft Windows Server 2012 (64-разрядная)	Microsoft Windows Server 2012 (64-разрядная)
Microsoft Windows Server 2012 R2 (64-разрядная)	Microsoft Windows Server 2012 R2 (64-разрядная)	Microsoft Windows Server 2012 R2 (64-разрядная)
Microsoft Windows Server 2016 (64-разрядная)	Microsoft Windows Server 2016 (64-разрядная)	Microsoft Windows Server 2016 (64-разрядная)

Агент	Сервер IDS HS	Консоль управления
Astra Linux Special Edition 1.5 релиз «Смоленск» (64-разрядная), ядро 4.2		
Astra Linux Special Edition 1.6 релиз «Смоленск» (64-разрядная), ядро 4.15.3-1		
Debian 8.5 (64-разрядная), ядро 3.16.51-2		
Альт Линукс СПТ 7.0 (64-разрядная), ядро 3.10.17		
CentOS 7.5 (64-разрядная), ядро 3.10		
Ред ОС 7.2 (64-разрядная), ядро 4.19.79		

3.3.5 Функционирование компонентов ViPNet IDS HS гарантируется на виртуальных машинах (под управлением ОС, перечисленных в п. 3.3.4) в следующих средах виртуализации:

- VMware vSphere 6.5;
- VMware Workstation Pro 14.1;
- Oracle VM VirtualBox 5.2.

Примечания:

1. Аппаратная конфигурация компьютера должна соответствовать рекомендуемой производителем ОС.
2. Рекомендуется установить последний пакет обновлений ОС и все известные критические обновления, опубликованные производителем ОС.
3. Порядок и сроки эксплуатации ОС определяются производителем ОС. Стабильность работы ViPNet IDS HS и безопасность информации при эксплуатации ОС, поддержка которых прекращена производителем ОС, не гарантируется.

3.3.6 На компьютеры, предназначенные для работы с компонентами Сервер IDS HS и Консоль управления, должно быть установлено следующее ПО, входящее в комплект поставки:

- ViPNet CSP версии 4.2.2 и выше;
- Microsoft .NET Framework версии 4.5[6];
- Microsoft Visual C++ 2013 Redistributable Package (x86)[6];
- Microsoft Visual C++ 2015 Redistributable Package (x64)[6];

[6] Для данного ПО должны быть установлены последние обновления безопасности.

– СУБД PostgreSQL 9.5 (только для компонента Сервер IDS HS)[7].

3.3.7 На компьютер, предназначенный для работы с компонентом Агент для ОС Windows, должно быть установлено следующее ПО, входящее в комплект поставки:

– Microsoft .NET Framework версии 4.5[6];
– Microsoft Visual C++ 2013 Redistributable Package (x86)/(x64)[6].

Примечание. Если требуется, чтобы данные, передаваемые Агентом на Сервер IDS HS, были зашифрованы по алгоритму ГОСТ, необходимо дополнительно установить на компьютер, предназначенный для работы с компонентом Агент, ПО ViPNet CSP версии 4.2.2 и выше.

[7] Устанавливается автоматически вместе с компонентом Сервер IDS HS.

4 Комплектность

4.1 Комплектность ViPNet IDS HS приведена в таблице 2.

Таблица 2 – Комплектность ViPNet IDS HS

Наименование составной части	Обозначение	Примечание
Программное обеспечение		
MCSetup-x64_RUS_1.5.0.63137.msi	ФРКЕ.00177-02 94 01	Прим. 1
AgentSetup-x86_RUS_1.5.0.63137.msi	ФРКЕ.00177-02 94 02	Прим. 1
AgentSetup-x64_RUS_1.5.0.63137.msi	ФРКЕ.00177-02 94 03	Прим. 1
vipnet-ids-hs-agent-1.5.0.223-x86_64.deb	ФРКЕ.00177-02 94 04	Прим. 1
vipnet-ids-hs-agent-1.5.0.223-x86_64.rpm	ФРКЕ.00177-02 94 05	Прим. 1
vipnet-ids-hs-agent-1.5.0.223-with-astra-1.6-sign-x86_64.deb	ФРКЕ.00177-02 94 06	Прим. 1
GSSetup-x64_RUS_1.5.0.65200.msi	ФРКЕ.00177-02 94 07	Прим. 1, 5
ViPNet_CSP_RUS_4.2.2.36190.exe	ФРКЕ.00106-03 94 01	Прим. 1
infotecs_pub.gpg		Прим. 1
NDP452-KB2901907-x86-x64-AllOS-ENU.exe		Прим. 1
vc_redist.x64.exe		Прим. 1
vcredist_x86 2013.exe		Прим. 1
Документация		
Система обнаружения вторжений ViPNet IDS HS. Формуляр	ФРКЕ.00177-02 30 01 ФО	Прим. 3
Система обнаружения вторжений ViPNet IDS HS. Правила пользования	ФРКЕ.00177-02 99 01 ПП	Прим. 2
Система обнаружения вторжений ViPNet IDS HS. Руководство администратора	ФРКЕ.00177-02 32 01	Прим. 2
ViPNet IDS HS. Лицензионные соглашения на компоненты сторонних производителей	ФРКЕ.00177-02 90 14	Прим. 2
Система обнаружения вторжений ViPNet IDS HS. Руководство по выгрузке событий в ГосСОПКА	ФРКЕ.00177-02 32 02	Прим. 2, 5
Копия сертификата соответствия ФСТЭК России	—	Прим. 2
Копия сертификата соответствия ФСБ России	—	Прим. 2
Носитель информации		
Оптический диск	—	

Примечания:

1. ViPNet IDS HS и дополнительное ПО поставляются на оптическом диске.
2. Документация на ViPNet IDS HS (за исключением формуляра), в том числе копии сертификатов соответствия ФСБ России и ФСТЭК России, поставляется в электронном виде на оптическом диске.
3. Формуляр на ViPNet IDS HS поставляется в печатном виде.

4. Файл с лицензией поставляется в электронном виде по запросу пользователя (эксплуатирующей организации).
5. Утилита ViPNet IDS HS GS, предназначенная для настройки и выгрузки данных из ViPNet IDS HS в систему ГосСОПКА, а также документация на нее поставляются и используются для соответствия ViPNet IDS HS требованиям документа ФСБ России «Требования к средствам обнаружения компьютерных атак».

5 Свидетельство о маркировке, упаковке и приемке

ViPNet IDS HS ФРКЕ.00177-02,

серийный номер дистрибутива _____,

знак соответствия для маркировки сертифицированной продукции в системе сертификации № РОСС RU.0001.01БИ00

Место для знака соответст-вия

изготовлен, упакован, промаркирован, принят в соответствии с техническими условиями ФРКЕ.00177-02 97 01 ТУ и признан годным к эксплуатации.

Дата выпуска программного обеспечения _____

Дата упаковки _____

Изделие упаковал _____
(подпись)

Упакованное изделие принял _____
(подпись)

М. П.

6 Гарантии изготовителя

6.1 Изготовитель гарантирует работоспособность продукта ViPNet IDS HS ФРКЕ.00177-02 в соответствии с заявленными характеристиками только при соблюдении пользователем (эксплуатирующей организацией) требований и рекомендаций правил пользования ФРКЕ.00177-02 99 01 ПП и других эксплуатационных документов на продукт.

6.2 Гарантийные обязательства в отношении продукта ViPNet IDS HS ФРКЕ.00177-02 предоставляются в объеме и на условиях, предусмотренных лицензионным соглашением с конечным пользователем, прилагаемым к продукту ViPNet IDS HS ФРКЕ.00177-02.

6.3 В случае нарушения функционирования продукта ViPNet IDS HS ФРКЕ.00177-02 в период гарантийного срока по причине программных дефектов, нарушения процедуры поставки или иных проблем, не вызванных несоблюдением со стороны пользователя (эксплуатирующей организации) требований и рекомендаций правил пользования ФРКЕ.00177-02 99 01 ПП и других эксплуатационных документов на продукт, изготовитель обязуется осуществить гарантийное обслуживание в кратчайший срок после получения соответствующей рекламации. Сведения о порядке предъявления рекламаций приведены в следующем разделе настоящего формуляра.

6.4 Сообщить о возникшей проблеме также можно по электронной почте hotline@infotecs.ru, телефону +7 (495) 737-6196 или заполнив форму на странице сайта: https://infotecs.ru/support/request.

6.5 Гарантийное обслуживание не включает в себя:

1) обучение пользователей практическим навыкам работы с продуктом;
2) периодическое обслуживание в соответствии с требованиями и рекомендациями, изложенными в правилах пользования ФРКЕ.00177-02 99 01 ПП и другой эксплуатационной документации на продукт;
3) настройку конфигурации продукта и подбор оптимальных параметров под требования пользователя (эксплуатирующей организации).

6.6 Гарантийные обязательства также не распространяются на следующие случаи:

1) наличие дефектов, вызванных нарушениями со стороны заказчика или пользователя (эксплуатирующей организации) требований и рекомендаций правил пользования ФРКЕ.00177-02 99 01 ПП и других эксплуатационных документов на продукт, в том числе:

    а) нарушением условий транспортирования, хранения и эксплуатации (воздействие повышенной влажности, агрессивных сред, некачественная

электрическая сеть, короткое замыкание, перегрузки, наличие механических, тепловых и электрических повреждений);

б) нарушением целостности программного обеспечения в результате попыток несанкционированного изменения (модификации);

2) наличие проблем, связанных с продуктами сторонних производителей;

3) наличие дефектов, вызванных форс-мажорными обстоятельствами, в том числе наводнениями, пожарами, другими стихийными бедствиями и техногенными катастрофами.

6.7 Если в результате диагностики будет установлено, что на данный случай не распространяются гарантийные обязательства, то делается заключение об отказе в гарантийном обслуживании с указанием причины отказа и предложением постгарантийного обслуживания.

6.8 Постгарантийное обслуживание осуществляется только после заключения отдельного соглашения (договора), регламентирующего условия его предоставления.

7 Сведения о рекламациях

7.1 В течение гарантийного срока пользователь (эксплуатирующая организация) имеет право предъявить рекламацию изготовителю при несоответствии продукта ViPNet IDS HS ФРКЕ.00177-02 заявленным характеристикам и сопроводительной документации.

7.2 Рекламации предъявляются в письменном виде с указанием даты обнаружения некомплектности и (или) неисправности (дефекта), описанием дефекта и условий его возникновения и обнаружения.

7.3 Рекламации направляются в адрес ОАО «ИнфоТеКС»: 127287, Россия, Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1.

7.4 Срок рассмотрения рекламаций – 1 месяц со дня получения.

7.5 Содержание рекламаций и меры, принятые по ним, записываются пользователем (ответственным лицом) в таблицу 3:

Таблица 3 – Учет предъявленных рекламаций

Дата	Содержание рекламации	Меры, принятые по рекламации	Должность, Ф.И.О., подпись ответственного лица

8 Сведения о хранении

Таблица ниже заполняется при постановке носителя информации с ViPNet IDS HS на хранение. Требования и рекомендации по условиям хранения ViPNet IDS HS изложены в правилах пользования ФРКЕ.00177-02 99 01 ПП.

Дата		Условия хранения	Должность, Ф.И.О., подпись лица, ответственного за хранение
постановки на хранение	снятия с хранения		

9 Сведения о закреплении при эксплуатации

Таблица ниже заполняется при назначении или смене пользователя (лица, ответственного за эксплуатацию) ViPNet IDS HS. Требования и рекомендации по эксплуатации ViPNet IDS HS изложены в правилах пользования ФРКЕ.00177-02 99 01 ПП.

Должность ответственного лица	Ф.И.О. ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

10 Сведения об изменениях

Таблица ниже заполняется при необходимости внесения изменений в формуляр, в том числе при получении от изготовителя ViPNet IDS HS бюллетеня (информационного сообщения) с информацией о необходимости внесения изменений.

Основание изменения (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, Ф.И.О. и подпись лица, ответственного за проведение изменения	Подпись лица, ответственного за эксплуатацию изделия

11 Контрольные суммы

11.1 Настоящий раздел содержит контрольные суммы дистрибутивов и исполняемых файлов продукта ViPNet IDS HS, прошедшего сертификационные испытания.

11.2 Контрольные суммы рассчитаны с использованием утилиты ViPNet HashCalc по алгоритму ГОСТ Р 34.11-2012, 256 бит и с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.2 (разработчик ЗАО «ЦБИ-сервис») по алгоритму «Уровень-3», программно.

11.3 Вычисленные контрольные суммы приведены в таблице 4.

Таблица 4 – Контрольные суммы файлов

Файл	Длина (байт)	Контрольная сумма
Контрольные суммы, рассчитанные с использованием утилиты ViPNet HashCalc по алгоритму ГОСТ Р 34.11-2012, 256 бит		
MCSetup-x64_RUS_1.5.0.63137.msi	72900608	30CCBC3BCB149616503E89D420F71D19DFB409D8C8DE70A420E5ACA61DAA3CAF
AgentSetup-x86_RUS_1.5.0.63137.msi	8556544	92D4FF8CE2696318D6444FEDED3120322748157711040E369CA940945E57E62F
AgentSetup-x64_RUS_1.5.0.63137.msi	9134080	04FEA15353B5839800F752A19E314712B643EFB7E2F8D0401193C1ADF62230A7
vipnet-ids-hs-agent-1.5.0.223-x86_64.deb	4848890	0E842AE13A3371BA98286ACF096F01E96028FF90F93FAF81B91CEFEC156A7DF4
vipnet-ids-hs-agent-1.5.0.223-x86_64.rpm	6833046	6407A51339AEFAA18C459CC3D52F9DACB3F9A61E23889C03E3E49D59B6F7D4E5
vipnet-ids-hs-agent-1.5.0.223-with-astra-1.6-sign-x86_64.deb	4850772	EDF54ADADAE64949902C1CA92C547CC35B268B375B87B0EBF493686F56620816
GSSetup-x64_RUS_1.5.0.65200.msi	18116608	D2D9B4DB8B8A4610E1F7442C54DFA7E5026BB01661079130B6F3AD4585F89BF4
infotecs_pub.gpg	540	067B40F81B2957190D8AA69CC2D0EAE9E4F3C1F4DCEAED3203E5ED836B91FB5A
NDP452-KB2901907-x86-x64-AllOS-ENU.exe	69999448	AE566E6DE2BAB70459218A1C9843F67ADE77D00332D76BE35D0333B50F2DD4B5
vc_redist.x64.exe	14572000	2273E5CD4AD1BAE24D3E9E2E69533667B23CF34ED6C1831C93B6FFF9F6EF886C
vcredist_x86 2013.exe	6506256	26259DBD75BE52458DD7115A67826C91B743CCEF75796238ED3D468105F486A2
ViPNet_CSP_RUS_4.2.2.36190.exe	37346128	F8A2C07497E0B32E846BD3C23B866120BD419B9056803DF11D0EE288A4A508E2
Контрольные суммы, рассчитанные с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.2 (разработчик ЗАО «ЦБИ-сервис») по алгоритму «Уровень-3», программно		
MCSetup-x64_RUS_1.5.0.63137.msi	72900608	e94e748d
AgentSetup-x86_RUS_1.5.0.63137.msi	8556544	ba39a309
AgentSetup-x64_RUS_1.5.0.63137.msi	9134080	63be4dfe

Продолжение таблицы 4

Файл	Длина (байт)	Контрольная сумма
vipnet-ids-hs-agent-1.5.0.223-x86_64.deb	4848890	1b61e447
vipnet-ids-hs-agent-1.5.0.223-x86_64.rpm	6833046	41ee3b47
vipnet-ids-hs-agent-1.5.0.223-with-astra-1.6-sign-x86_64.deb	4850772	4d6c890f
GSSetup-x64_RUS_1.5.0.65200.msi	18116608	07c7a495
infotecs_pub.gpg	540	cfa9550d
NDP452-KB2901907-x86-x64-AllOS-ENU.exe	69999448	c7c79afd
vc_redist.x64.exe	14572000	f756bc35
vcredist_x86 2013.exe	6506256	186a974e
ViPNet_CSP_RUS_4.2.2.36190.exe	37346128	7f94ddbc

12 Особые отметки

В данном разделе ставятся особые отметки, предусмотренные в соответствии с требованиями и рекомендациями, изложенными в правилах пользования ФРКЕ.00177-02 99 01 ПП и других эксплуатационных документах на продукт, в том числе отметки о результатах периодического контроля.

12 Особые отметки

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					