УТВЕРЖДЕН

643.95486689.UTM-01 30-ЛУ

Изделие

«Универсальный шлюз безопасности «UserGate UTM»

Пакет модификаций (Service pack) UserGate UTM 5. Вносимые изменения (Release notes)

643.95486689.UTM-01 30

Разработал

Д. Р. Шагимарданов

«____»_____ 201_ г.

Проверил

В. В. Белавин

«____»_____ 201_ г.

Нормоконтроль

А. В. Кистанов

«____»_____ 201_ г.

Утвердил

А. В. Левченко

«____»_____ 201_ г.

2019

Подп. и дата	Инв.№ дубл.	Взам. инв.№	Подп. и дата	Инв.№ подл.

Изм	Лист	№ докум.	Подп.	Дата

Перв. примен.

Справ. №

Подп. и дата

Инв.№ дубл.

Взам. инв.№

Подп. и дата

Инв.№ подл.

Содержание

Принятые сокращения

Термин, сокращение		Определение
БРП	-	База решающих правил
ИС	-	Информационная система
МЭ	-	Межсетевой экран
ОО	-	Объект оценки
ПО	-	Программное обеспечение
СОВ	-	Система обнаружения вторжений
ТУ	-	Технические условия

1 Общие указания

1.1 Настоящий документ содержит перечень исправлений и патчей, внесенных в пакет модификаций изделия «Универсальный шлюз безопасности «UserGate UTM» (далее по тексту – изделие, объект оценки) версии 5.

2 Общие сведения

2.1 Наименование изделия и его обозначение: «Универсальный шлюз безопасности «UserGate UTM», 643.95486689.UTM-01.

2.2 Тип продукта: программное обеспечение, программное-техническое средство (в зависимости от исполнения).

2.3 Изделие представляет собой программное (вариант поставки в виде виртуальной машины) или программно-техническое средство (вариант поставки в виде программно-аппаратного комплекса), реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков, а также функции по обнаружению и предотвращению вторжений, и используемое в целях обеспечения защиты (не криптографическими методами) информации ограниченного доступа.

Изделие обеспечивает нейтрализацию следующих угроз безопасности информации:

- несанкционированный доступ к информации, содержащейся в информационной системе;

- отказ в обслуживании информационной системы и (или) ее отдельных компонентов;

- несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;

- несанкционированное воздействие на МЭ, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;

- несанкционированное получение сведений о сети информационной системы (автоматизированной системы управления), а также об ее узлах;

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних

нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;

- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

2.4 Изделие является межсетевым экраном типа «А» четвертого класса защиты, межсетевым экраном типа «Б» четвертого класса защиты и системой обнаружения вторжений уровня сети четвертого класса защиты в случае поставки в виде программно-аппаратного комплекса. Изделие является межсетевым экраном типа «Б» четвертого класса защиты и системой обнаружения вторжений уровня сети четвертого класса защиты в случае поставки в виде виртуальной машины.

2.5 Логически изделие разделяется на 2 подсистемы (рисунок 1, рисунок 2):

- подсистема управления, реализующая интерфейс для пользователя и администратора изделия;

- подсистема защиты информации, реализующая функции безопасности МЭ и СОВ.

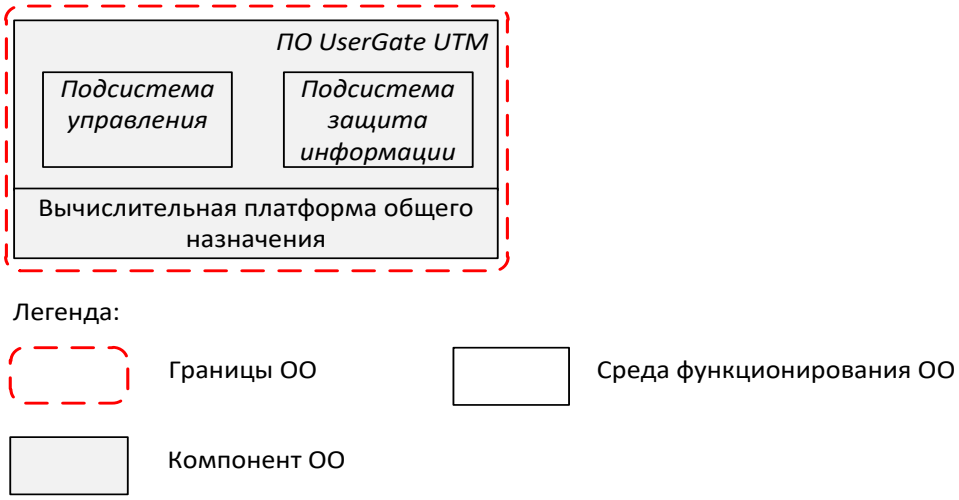

Рисунок 1 - Физические границы ОО (вариант поставки в виде программно-аппаратного комплекса)

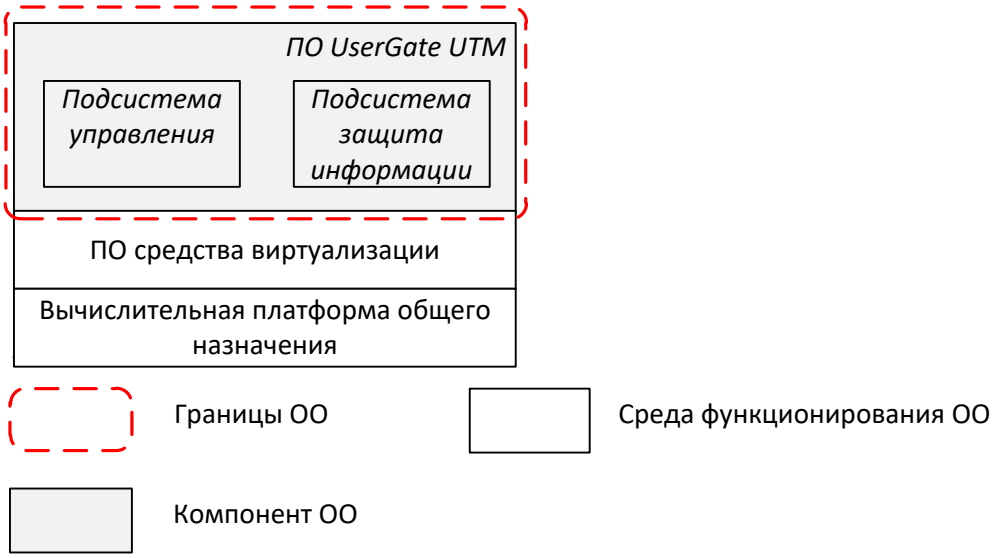

Рисунок 2 - Физические границы ОО (вариант поставки в виде виртуальной машины)

2.6 Предприятие-разработчик и изготовитель продукции: ООО «еСЛ Девелопмент» (630090, г. Новосибирск, ул. Николаева, д.11, оф. 602, ИНН 5408243746).

3 Перечень изменений

В таблице Таблица 3.**1** приведен полный перечень изменений, внесенных в обновление UserGate UTM.

Номер во внутренней системе отслеживания задач	Пояснение
UGDNS-6656	Исправлен некорректный вывод в CLI на двойное нажатие Esc
UGDNS-6799	Исправлена ошибка отображения страницы Captive-портала при отсутствии явного указания зоны источника в правиле Captive-портала
UGDNS-6783	Исправлена ошибка отправки запроса на изменение категории сайта
UGDNS-6694	Исправлена ошибка при создании резервной копии на внешний носитель, проявляющаяся в некоторых случаях
UGDNS-6605	Исправлена ошибка, при которой создаётся некорректное правило межсетевого экрана, если указать у сервиса порты источника и назначения
UGDNS-6645	Исправлена ошибка, периодически проявляющаяся при развёртывании образа на аппаратные платформы
UGDNS-6597	Исправлена ошибочное ограничение логина пользователя SMPP в 15 символов
UGDNS-6709	Исправлена проблема блокировки сайта skif.minfin74.ru модулем СОВ
UGDNS-6639	Исправлена проблема медленной работы UTM при включенном экспорте журналов на внешний сервер syslog, недоступный в данный момент
UGDNS-6526	Исправлена проблема обновления ПО UTM в случае наличия кластера
UGDNS-6896	Исправлена проблема обновления БРП СОВ, если файл обновления содержит некорректные данные
UGDNS-6856	Исправлена проблема отображения пользователей с русскими именами в списке запросов сайтов в белый список
UGDNS-6811	Исправлена проблема синхронизации пользователей Active Directory из OU, в которых используются русские буквы и пробелы
UGDNS-6641	Исправлена проблема увеличения размера жёсткого диска на виртуальной платформе Microsoft Hyper-V
UGDNS-6545	Исправлена проблема DNS-фильтрации в случае присутствия символа * в списке доменов
UGDNS-6679	Исправлена проблема, при которой защита DoS не отбрасывала пакеты, превышающие порог защиты
UGDNS-6651	Исправлена проблема, при которой принудительная проверка обновлений продукта не происходила в некоторых случаях
UGDNS-6891	Исправлена проблема зависания модуля генерации SSL-сертификатов
UGDNS-4996	Исправлено падение сервера статистики с сообщением ошибки invalid byte sequence for encoding UTF8

UGDNS-6886	Улучшена производительность отображения пользователей Active Directory, уменьшена нагрузка на сервера AD
UGDNS-6730	Улучшена стабильность работы UTM при обновлении баз решающих правил
UGDNS-6762	Уменьшены затраты UTM на применение правил межсетевого экрана при аутентификации пользователя
UGDNS-6728	Добавлена возможность создавать правила защиты от DoS с ограничением более 10000 пакетов в секунду
UGDNS-7068	Добавлена возможность передавать на ICAP-сервер имя пользователя (X-Authenticated-User) в кодировке base64
UGDNS-7083	Добавлена возможность установить несколько кластерных IP-адресов на один интерфейс
UGDNS-7030	Исправлена ошибка таймаута DNS, проявляющаяся в некоторых случаях
UGDNS-7044	Исправлена ошибка, возникающая при обновлении списка сайтов онлайн-переводчиков
UGDNS-7074	Исправлена проблема авторизации компьютеров через тип авторизации Kerberos вместо пользователей этих компьютеров
UGDNS-7100	Исправлена проблема работы MailSecurity, при использовании протокола STARTLS
UGDNS-7101	Исправлена проблема циклического редиректа при наличии блокирующего всё правила контентной фильтрации и указании внешней страницы блокировки
UGDNS-7006	Улучшено время, требуемое для применения правил межсетевого экрана
UGDNS-7308	Исправлена ошибка добавления URL, начинающегося с точки
UGDNS-7260	Исправлена ошибка "Сервер занят" при изменении порта, используемого HTTP прокси сервера
UGDNS-7307	Исправлена ошибка Mailsecurity при указании условий на Envelop-to, Envelop-From
UGDNS-7289	Исправлена проблема в агенте авторизации Windows, приводящая к появлению в определенных условиях пользователей Unknown
UGDNS-7399	Исправлена проблема открытия веб-ресурсов при явно указанном прокси сервере, проявляющаяся в некоторых случаях
UGDNS-7263	Исправлена проблема передачи почтовых сообщений от серверов Google gmail на сервера exchange
UGDNS-7291	Исправлена проблема применения политик фильтрации к стандартной группе Active Directory Domain Users
UGDNS-7280	Исправлена проблема с публикацией DNAT с изменением портов назначения
UGDNS-7229	Исправлена проблема фильтрации по морфологическому списку ФЗ-436
UGDNS-6856	Исправлено некорректное отображение имен пользователей, содержащих кириллицу, в списке запросов URL на добавление в белый список
UGDNS-7550	Исправлена проблема доставки почты через UTM с почтовых серверов Google на Exchange через TLS соединение
UGDNS-7554	Исправлена ошибка проверки списков фильтрации при отсутствии модуля ATP в лицензии
UGDNS-7535	

UGDNS-7530 UGDNS-7505 UGDNS-6495 UGDNS-7276	Исправлены ошибки веб-консоли "Сервер занят", проявляемые при определенных условиях
UGDNS-7512	Исправлена ошибка авторизации пользователя через Kerberos в случае присутствия пользователя в двух или более доменах Active Directory
UGDNS-7034	Добавлена поддержка Веб-портал
UGDNS-7128	Добавлены отчеты о действиях пользователей, системных событиях, событиях безопасности
UGDNS-7223	Добавлена возможность управления протоколами АСУ ТП
UGDNS-7247	Реализована настройка политик безопасности при помощи сценариев
UGDNS-5005	Добавлена поддержка динамических протоколов маршрутизации OSPF
UGDNS-4403	Добавлена поддержка динамических протоколов маршрутизации BGP
UGDNS-5542	Добавлена поддержка кластера отказоустойчивости Active-Active
UGDNS-2981 UGDNS-3996 UGDNS-5693 UGDNS-4354 UGDNS-7404	Добавлены дополнительные методы аутентификации пользователей
UGDNS-5830	Улучшена возможность авторизации с помощью Kerberos и NTLM без указания прокси-сервера в браузере
UGDNS-3416 UGDNS-5267	Добавлена поддержка новых типов сетевых интерфейсов и режимов их работы: агрегированный интерфейс (бонд) с использованием протокола LACP (link aggregation control protocol), мост
UGDNS-5567	Добавлена поддержка FTP поверх HTTP
UGDNS-5690	Добавлена возможность инжектирования произвольного кода на веб-страницы
UGDNS-5482	Добавлена поддержка ролевого доступа администраторов к элементам управления UserGate
UGDNS-5680	Улучшена производительность системы обнаружения и предотвращения вторжений (СОВ)
UGDNS-3991	Улучшен функционал работы с внешними серверами ICAP, добавлена возможность отсылать только избранный трафик на эти сервера, а также работать с фермами ICAP-серверов
UGDNS-3173	Добавлен режим t-proxy для HTTP и DNS
UGDNS-4000	Добавлена возможность отрицания условия в правилах (negate)
UGDNS-4261	Улучшена процедура обработки некорректных и отозванных сертификатов SSL
UGDNS-4298	Исправлены ошибки при работе с веб-консолью из браузера Internet Explorer
UGDNS-4327	Добавлена возможность захвата сетевых пакетов для диагностики
UGDNS-4717	Добавлена возможность диагностирования правил, срабатывающих при пользовательском запросе
UGDNS-4857	Добавлены уровни рисков к URL-категориям

UGDNS-4861	Добавлены уровни рисков к сигнатурам СОВ
UGDNS-4863	Добавлены диагностические утилиты ping, traceroute в веб-консоль
UGDNS-4864	Добавлена возможность поиска пользователей по имени, фамилии, назначенному IP-адресу
UGDNS-3184	Добавлена поддержка интерфейсов PPPoE
UGDNS-7828	Добавлены дополнительные символы, разрешаемые для использования в SNMP community string
UGDNS-7861	Исправлена ошибка журнала веб-доступа, при которой не отображались заблокированные MIME-типы
UGDNS-7691	Исправлена проблема высокой загрузки процессора, вызываемой трафиком приложения teamviewer
UGDNS-7871	Исправлена проблема невозможности логина пользователя Administrator, если используется 2 или более доменов Active directory
UGDNS-7888	Исправлена проблема некорректного определения категории сайтов, в которых присутствует знак вопроса
UGDNS-7851	Исправлена проблема обновления сертификатов для сайтов, срок действия сертификата которых истек и которые были обновлены
UGDNS-7853	Исправлена проблема, при которой SNMP сервис не может стартовать
UGDNS-7838	Исправлена проблема, при которой SNMP сервис не отдавал все требуемые значения на запросы
UGDNS-7892	Улучшена обработка имени пользователя в Captive-портале, добавлено удаление пробелов
UGDNS-7823	Улучшена производительность http-проксирования
UGDNS-7784	Улучшена работа коннекторов AD и FreeIPA
UGDNS-7884	Улучшено отображение ошибки некорректной авторизации пользователя
UGDNS-5253	Улучшено представление журнала трафика, добавлены дополнительные поля и поиск
UGDNS-3525	Добавлена возможность создавать профили сигнатур СОВ и использовать их в правилах
UGDNS-8103	Добавлена возможность использовать MAC-адрес в правилах маршрутизации (PBR).
UGDNS-7905	Добавлена возможность устанавливать обновления UserGate при отсутствии подключения к интернет (offline updates).
UGDNS-7715	Добавлена поддержка форматов выгрузки логов - BSD syslog protocol (RFC - 3164), syslog protocol (RFC - 5424), CEF (ArcSight Common Event Format).
UGDNS-8169	Добавлена возможность экспортировать список запросов в белый список.
UGDNS-8128	Добавлена возможность подключаться напрямую к опубликованному сервису через веб-портал.
UGDNS-8098	Добавлена возможность показывать графики в дашборде за неделю, месяц, год.
UGDNS-7553	Добавлена возможность создания сетевых мостов с функцией байпас для ПАК UserGate D, E, F.
UGDNS-5923	Добавлена возможность гибкой защиты от DoS.
UGDNS-8136	Улучшена фильтрация пакетов с некорректными флагами TCP.

UGDNS-8018	Добавлен тип интерфейса Mirror.
UGDNS-5486	Добавлена возможность работы СОВ с трафиком, поступающим на интерфейсы типа Mirror.
UGDNS-7850	Добавлена возможность фильтровать доступ к веб-сайтам на основе значения referrer.
UGDNS-8010	Добавлены новые URLF категории: Криптомайнеры, Военные сайты, Справочная информация, Нетрадиционная сексуальная ориентация, Литература и книги, Здоровое питание и диеты, Домашние животные.
UGDNS-7815	Добавлена возможность использовать виртуальную клавиатуру при авторизации через Captive-портал.
UGDNS-7042	Добавлена возможность создания правила типа netmap для подмены адреса источника/назначения для подсетей.
Без номера	Исправлена ошибка в BIOS для ПАК UserGate D/D+, приводящая к периодическому зависанию ПАК во время загрузки.
Без номера	Добавлен процессор Intel® Xeon® Processor E5-2650L v4 для использования в ПАК UserGate E+.
Без номера	Добавлен жесткий диск DES25-A28M41BW1DC-A90 для использования в ПАК UserGate X1.

Таблица 3.1

Перв. примен.	
Справ. №	

4 Особые отметки

Инв.№ подл.	Подп. и дата	Взам. инв.№	Инв.№ дубл.	Подп. и дата	

Приложение А

Контрольные суммы инсталляционного пакета ПО изделия.

№ пп	Контрольная сумма	Имя файла
1	2E872CBC	utm_5_0_6_3600f_1_public_hd.bz2
2	F3EA0ED8	utm_5_0_6_3600f_1_public_hy.zip
3	1EA47450	utm_5_0_6_3600f_1_public.mf
4	918EBE27	utm_5_0_6_3600f_1_public.ovf
5	8BBCA066	utm_5_0_6_3600f_1_public_d.vmdk
6	D9FB4875	Интегральная контрольная сумма