СОГЛАСОВАНО	УТВЕРЖДАЮ
Начальник 2 управления	Генеральный директор
ФСТЭК России	ООО «Вэлл-Сервис»
В.С. Лютиков	В.В. Подзоров
« ___ » _____ 2015 г.	« ___ » _____ 2015 г.

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

Программа защиты информации от несанкционированного доступа

ARMlock

Формуляр

ЛИСТ УТВЕРЖДЕНИЯ

RU.60945681.501410-01 30-ЛУ

2015

УТВЕРЖДЕН
RU.60945681.501410-01 30-ЛУ

Программа защиты информации от несанкционированного доступа ARMlock

Формуляр

RU.60945681.501410-01 30

Листов 25

2015

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

СОДЕРЖАНИЕ

ОБЩИЕ УКАЗАНИЯ

Перед эксплуатацией необходимо внимательно ознакомиться с соответствующими эксплуатационными документами:

Программа защиты информации от несанкционированного доступа ARMlock. Формуляр. RU.60945681.501410-01 30;

Программа защиты информации от несанкционированного доступа ARMlock. Описание программы. RU.60945681.501410-01 13;

Программа защиты информации от несанкционированного доступа ARMlock. Описание применения. RU.60945681.501410-01 31;

Программа защиты информации от несанкционированного доступа ARMlock. Руководство администратора. RU.60945681.501410-01 34»;

Формуляр входит в комплект поставки и должен находиться в подразделении, ответственном за эксплуатацию программного изделия.

Сведения разделов 8 – 13 настоящего формуляра заполняются лицом, ответственным за ведение формуляра.

Все записи в формуляре должны производиться чернилами или пастой черного, фиолетового или синего цвета четко и аккуратно и заверяться подписью лица, ответственного за ведение формуляра. Исправления записей должны быть оговорены и засвидетельствованы подписью лица, внесшего исправления, и скреплены печатью. Подчистки в записях не допускаются.

Правильность и своевременность заполнения формуляра контролируется должностными лицами.

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование

Полное наименование изделия: Программа защиты информации от несанкционированного доступа ARMlock.

Краткое наименование: ПЗИ НСД ARMlock.

1.2. Условное обозначение - ARMlock.

1.3. Предприятие - разработчик

ООО «Вэлл-Сервис»
ИНН 7802467177, КПП 780201001

194156, Санкт-Петербург, пр.Энгельса д.37 офис 402

1.4. Изделие сертифицировано в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 на соответствие требованиям руководящих документов:

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности;

– «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля.

Изделие имеет сертификат соответствия требованиям по безопасности информации № _____, выданный ФСТЭК России « » _____ 2015 г.

Изделие может быть использовано:

– при создании защищенных автоматизированных систем до класса защищенности 1Г включительно (руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));

– в государственных информационных системах до 1 класса защищённости включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных

системах» для реализации мер защиты: УПД.2, ЗНИ.8, ИАФ.1, РСБ.3, ОЦЛ.1, ОЦЛ.3;

– для обеспечения до 1 уровня защищенности персональных данных включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных») для реализации мер защиты: УПД.2, ЗНИ.8, ИАФ.1, РСБ.3, ОЦЛ.1, ОЦЛ.3;

– при создании защищенных информационных систем 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 до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований 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») при условии соблюдения ограничений, указанных в разделе 13 настоящего формуляра.

1.5. Программа защиты информации от несанкционированного доступа ARMlock функционирует в операционных системах:

– Microsoft Windows XP;
– Microsoft Windows Server 2003 R2;
– Microsoft Windows Server 2008;
– Microsoft Windows Server 2008 R2;
– Microsoft Windows 7;
– Microsoft Windows 8;
– Microsoft Windows 8.1 Update;
– Microsoft Windows Server 2012;
– Microsoft Windows Server 2012 (R2);
– Microsoft Windows 10.

ПЗИ НСД ARMlock поддерживает как 32-битные версии ОС, так и 64-битные.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. Общие положения

ПЗИ НСД ARMlock представляет собой программное средство защиты информации в ОС семейства Windows.

Система защиты устанавливается на автоматизированные рабочие места (АРМ), как автономные, так и в составе локально-вычислительной сети для защиты локальных ресурсов этих АРМ.

ПЗИ НСД ARMlock предназначена для защиты персонального компьютера:

- от доступа к информации в нарушение установленных прав доступа сотрудников;
- от несанкционированного доступа к конфиденциальной информации;
- от подключения незарегистрированных в системе защиты носителей информации;
- от доступа к информации в объеме, превышающем необходимый для выполнения служебных обязанностей.

2.2. Основные характеристики ПЗИ НСД ARMlock:

ПЗИ НСД ARMlock обеспечивает выполнение:

– дискреционного принципа контроля доступа в соответствие с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности;

– предотвращения доступа субъекту к остаточной информации в соответствие с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности;

– идентификации и аутентификации в соответствие с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности;

– регистрации событий безопасности в соответствие с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности;

– требования «целостность» в соответствие с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности.

2.3. Для размещения файлов ПЗИ НСД ARMlock требуется не менее 50 МБ пространства на системном разделе жесткого диска.

2.4. Для использования аппаратных идентификаторов необходимо наличие в аппаратной части АРМ USB-порта или COM-порта, а также соответствующего считывателя аппаратных идентификаторов.

3. КОМПЛЕКТНОСТЬ

3.1. Комплектность поставки ПЗИ НСД ARMlock приведена в таблице 1.

Таблица 1

Обозначение	Наименование	Количество	Примечание
RU.60945681.501410-01	Программа защиты информации от несанкционированного доступа ARMlock. Дистрибутив	1	на компакт-диске
RU.60945681.501410-01 30	Программа защиты информации от несанкционированного доступа ARMlock. Формуляр	1	твердая копия
RU.60945681.501410-01 34	Программа защиты информации от несанкционированного доступа ARMlock. Руководство администратора	1	на компакт-диске
	Бланк простой (неисключительной) лицензии	1	В бумажном виде
	Копия сертификата соответствия ФСТЭК России	1	В бумажном виде
	Знак соотвествия сертифицированной продукции	1	

3.2. Контрольные суммы файлов дистрибутива ПЗИ НСД ARMlock приведены в таблицах 2 и 3.

Таблица 2

Имя файла	КС (ГОСТ Р 34.11-94)
Console.v.0.2.8.exe	f336a17e58ba9edf599fdc9771097ae71442ad4536d32e1301afb6435772a3d1
SetupClient.v.0.2.8.msi	7bc5ae4c0a68696694a0f7cc7e74ddb1933a499b9968e4935fcb83a085be62e1

Примечание: Контрольные суммы файлов рассчитаны с использованием программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (сертификат соответствия ФСТЭК России № 2031 03.02.2010).

Таблица 3

№ пп	Имя файла	Длина, байт	Длина, строк	КС
1	Console.v.0.2.8.exe	4214024	-	6949ed8b
2	SetupClient.v.0.2.8.msi	5005312	-	04bf4395
итого: файлов - 2		**9219336**	**0**	**6df6ae1e**

Примечание: Контрольные суммы рассчитаны с использованием программы ФИКС 2.0.2 (разработчик – ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548 от 15.01.2008) по алгоритму КС «Уровень-3».

3.3. Контрольные суммы исполняемых файлов, устанавливаемых на ПК и подлежащих контролю приведены в таблицах 4 – 7.

Таблица 4 - Контрольные суммы исполняемых файлов ПЗИ НСД ARMlock, установленных в 32-разрядных операционных системах

Имя файла	КС (ГОСТ Р 34.11-94)
CheckOs.dll	4ef3fae2886c9e4eb9624dcee8c34bcb3a3d3b42ea733a10a5e30183084ac6c3
Events.dll	6deb99894dc1e483623a0189d5beddd8c4d4ca9a359702a72f3f5046f47d7126
Proj10CredentialProvider.dll	99947e435a499446616052bea799e99c1302b2357215d335a83282016e419db6
Proj10Driver.sys	720aeb658341f1a0e04ea3e1f072ffd36aaf22bf3225c0ade653b69ff2650d09
Proj10Gina.dll	a8ad2bb020f57a271886756ae29204b32a3b4ad8f2d31228d86c5d09d5142aaa
Proj10Library.dll	87bee26419947cad77d895d2d1a7b0503d5d058ea2bf5e7ed66bd0b7d29a9a24
Proj10Library86.dll	a2e6d66e1fdabbe26d54e16c45421b5e04bb2a1c05cb688356c6430b4ffb0443
Proj10Service.exe	8584bcdb4f6c3e35ecfa5544c7a93ca62943e4c6ce1d7e81cfb01d912ad63e57
Shreder.dll	a2928d6d15469454914fd2b9471c95aa3c47ad73f29f0fd23ee735d6a5e0a5e0

Таблица 5 - Контрольные суммы исполняемых файлов ПЗИ НСД ARMlock, установленных в 64-разрядных операционных системах

Имя файла	КС (ГОСТ Р 34.11-94)
CheckOs.dll	4ef3fae2886c9e4eb9624dcee8c34bcb3a3d3b42ea733a10a5e30183084ac6c3
Events.dll	0f0bbbdb64ff6288bfb466caf7860da8713fca88ef5694fd4305293f97c4f2b8
Proj10CredentialProvider.dll	ef220301e33c13e7529c54db60709c9dc377ad1a5b9fce6111202ae95567f058
Proj10Driver.sys	469dc132a51c0761a046b9e043063026426e27be1608913225456c777fa236ba
Proj10Gina.dll	3f0a12695dd387408037643d184b7beaefd54faa2741a5a7adac024eb6dc5330
Proj10Library.dll	60a408f79f7c2535edda19b0bfd329829030f350604d99a112112a46aceb8036
Proj10Library86.dll	f2355386f3417e8f556344d86f93d9c5f777db571714862e5a18e77760bae376
Proj10Service.exe	c081dd3cb8d5328692ff7063a21b03c50124b7dd836952a5929ae52097192276
Shreder.dll	3ed364085c83704107218956695f919a014fa86e53d9797955d0b7abfc4c35d6

Примечание: Контрольные суммы файлов рассчитаны с использованием программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (сертификат соответствия ФСТЭК России № 2031 03.02.2010).

Таблица 6 - Контрольные суммы исполняемых файлов ПЗИ НСД ARMlock, установленных в 32-разрядных операционных системах

№ пп	Имя файла	Длина, байт	Длина, строк	КС
Каталог C:\ARMlock				
1	CheckOs.dll	345864	-	311e8f3d
2	Events.dll	15112	-	b67c96b9
3	Proj10CredentialProvider.dll	1187592	-	108ddbef
4	Proj10Driver.sys	27400	-	a393dad5
5	Proj10Gina.dll	1089800	-	3a48a4d8
6	Proj10Library.dll	519432	-	667e469a
7	Proj10Library86.dll	519432	-	200cf832

8	Proj10Service.exe	518408	-	7064d648
9	Shreder.dll	269064	-	2a304aac
итого: файлов - 9		**4492104**	**0**	**12129e2a**

Таблица 7 - Контрольные суммы исполняемых файлов ПЗИ НСД ARMlock, установленных в 64-разрядных операционных системах

№ пп	Имя файла	Длина, байт	Длина, строк	КС
Каталог C:\ARMlock				
1.	CheckOs.dll	345864	-	311e8f3d
2.	Events.dll	16136	-	42311fef
3.	Proj10CredentialProvider.dll	1426184	-	0c7cf937
4.	Proj10Driver.sys	30472	-	545f8ad3
5.	Proj10Gina.dll	1189640	-	f05dae4e
6.	Proj10Library.dll	595208	-	459afa74
7.	Proj10Library86.dll	519432	-	fa19c673
8.	Proj10Service.exe	649480	-	2b5d7ad8
9.	Shreder.dll	316168	-	15cb40a3
итого: файлов - 9		**5088584**	**0**	**5a444b04**

Примечание: Контрольные суммы рассчитаны с использованием программы ФИКС 2.0.2 (разработчик – ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548 от 15.01.2008) по алгоритму КС «Уровень-3».

4. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

Контролю подлежат контрольные суммы файлов на компакт-диске и исполняемых файлов ПЗИ НСД ARMlock, приведенные в разделе 3 настоящего формуляра.

Проверяемая характеристика		Дата проведения измерения					
наименование измерения	величина	20___г.		20___г.		20___г.	
		фактическая величина	замерил (должность, подпись)	фактическая величина	замерил (должность, подпись)	фактическая величина	замерил (должность, подпись)

5. СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программа защиты информации от несанкционированного доступа ARMlock

наименование программного изделия

RU.60945681.501410-01

обозначение

_____

серийный номер

соответствует требованиям технических условий RU.60945681.501410-01 91 и признана годной для эксплуатации

Дата выпуска «___»_____20 г.

Номер лицензии: _____

Количество ПЭВМ, на которые распространяется лицензия _____

Ответственное за приемку лицо _____ _____

подпись расшифровка подписи

М .П.

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Программа защиты информации от несанкционированного доступа ARMlock

наименование программного изделия

RU.60945681.501410-01

обозначение

_____

серийный номер

упакована _____

наименование или код предприятия (организации)

согласно требованиям, предусмотренным инструкцией

обозначение

Дата упаковки «___»_____20 г.

Номер знака соответствия _____

Знак соответствия для маркировки сертифицированной продукции в Системе сертификации № РОСС RU.0001.01БИ00

Место нанесения знака соответствия

Упаковку произвел _____ _____

подпись расшифровка подписи

Примечание. Форму заполняют на предприятии, производившем упаковку.

7. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

7.1 Изготовитель гарантирует соответствие поставляемых экземпляров ПЗИ НСД ARMlock эталонному экземпляру (сертификат № _____ от ___.___._____г.)

7.2 Организация-изготовитель гарантирует работоспособность ПЗИ НСД ARMlock в соответствии с объявленными характеристиками при соблюдении пользователем требований эксплуатационных документов на данное программное средство (ПС).

7.3 Гарантийный срок - 12 (двенадцать) месяцев. Расширенная гарантия может быть предусмотрена договором с конечным пользователем и/или лицензией на изделие.

7.4 Начальной датой исчисления гарантийного срока является дата поставки ПС.

7.5 При отсутствии даты поставки начальной датой исчисления гарантийного срока является дата выпуска, указанная в разделе 5 Формуляра.

7.6 На сертифицированную версию изделия распространяется гарантийная поддержка на срок, указанный в Лицензии на изделие, при условии соблюдения правил эксплуатации, транспортировки и хранения.

7.7 В течение действия гарантийной поддержки предоставляется возможность загрузки выпущенных сертифицированных обновлений изделия с Центра сертифицированных обновлений – https://armlock.pro.

7.8 Реквизиты для доступа к Центру сертифицированных обновлений могут быть получены у поставщика ПЗИ НСД ARMlock по запросу конечного пользователя.

7.9 Процедура обновления ПЗИ НСД ARMlock выполняется в следующем порядке:

7.9.1Загрузка обновлённой версии дистрибутива с сайта https://armlock.pro

7.9.2Проверка контрольных сумм файлов загруженной версии дистрибутива.

7.9.3Удаление старой версии программного продукта путём запуска вновь загруженного дистрибутива (согласно процедуре, описанной в «Руководстве администратора»).

7.9.4Установка новой версии программного обеспечения с помощью вновь загруженного дистрибутива.

Вместо п.3 и п.4 возможно выполнить удаление и установку вновь загруженной версии ПЗИ НСД ARMlock в один этап с помощью стандартной системной команды msiexec.

Пример:

msiexec.exe /i SetupClient.v.0.2.3.msi INSTALLLOCATION="C:\ARMlock2015"

AUTHTYPE="WITHCARDS" SERVERSANDPORTS="srv-armlock:88" REINSTALLMODE=voums /passive /forcerestart /log %TEMP%\result.log

где INSTALLLOCATION – путь установки ПЗИ НЗД «ARMlock»

AUTHTYPE – тип аутентификации, который может принимать значение WITHCARDS (двухфакторная аутентификация с использованием аппаратных идентификаторов) или WITHOUTCARDS (аутентификация по имени и паролю)

SERVERSANDPORTS – адреса и номера портов серверов ARMlock (при их наличии) в формате server1:port1;server2:port2;…;serverN:portN

В случае локальной установки переменная SERVERSANDPORTS не используется или в её значении указывается «пробел».

После выполнения процедуры обновления требуется перезагрузка ПЭВМ.

7.10 Изготовитель производит периодическое тестирование ПЗИ НСД ARMlock на наличие уязвимостей. В случае выявления уязвимостей Изготовитель разрабатывает обновление, направленное на устранение уязвимостей средства защиты информации, организует проведение инспекционного контроля средства защиты информации с установленным обновлением в испытательной лаборатории. Пользователь при появлении сообщения о выходе обновленной версии ПЗИ НСД ARMlock самостоятельно осуществляет процедуру обновления в соответствии с п. 7.9 настоящего формуляра RU.60945681.501410-01 30.

7.11 Действие гарантийных обязательств прекращается при истечении гарантийного срока, либо при нарушении пользователем в течение гарантийного срока правил эксплуатации, транспортировки и хранения ПС, которые привели к появлению дефектов в ПС.

7.12 В случае выявления в течение гарантийного срока в ПС дефектов, не связанных с нарушением пользователем правил эксплуатации, транспортирования и хранения, ПС подлежит рекламации и организация - изготовитель обязуется при получении рекламации устранить дефекты своими силами и средствами вплоть до поставки нового ПС.

7.13 Гарантийное обслуживание изделия не производится в перечисленных ниже случаях:

- внесение изменений в ПЗИ НСД ARMlock без согласования с Разработчиком;
- несоблюдение правил установки и эксплуатации;
- утрата формуляра;
- небрежное хранение и (или) транспортировка потребителем, торговой или транспортной организацией;
- механические повреждения, воздействия химическими веществами;

- использование изделия в целях, для которых оно не предназначено.

7.14 За технической поддержкой обращаться:

а) по адресу 194156, Санкт-Петербург, пр. Энгельса д. 37 офис 402;

б) по адресу электронной почты - support@armlock.pro;

в) на веб-сайт - armlock.pro.

8. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

Рекламации, связанные с эксплуатацией ПС, должны направляться в письменном виде организации - изготовителю по адресу:

ООО «Вэлл-Сервис», 194156, Санкт-Петербург, пр. Энгельса, д. 37 офис 402, info@wellsrv.ru.

Срок рассмотрения рекламации - 1 (один) месяц со дня получения рекламации.

Содержание рекламаций и меры, принятые по ним, записывают в настоящем формуляре.

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

9. СВЕДЕНИЯ О ХРАНЕНИИ

Сведения о хранении программного продукта должны предоставляться в следующем виде:

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятие с хранения		

10. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

11. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

В форме “Сведения об изменениях” программного продукта указывают основание для внесения изменений, содержание изменений с указанием его порядкового номера, а также должность, фамилию и подпись лица, ответственного за проведение изменения.

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

12. ОСОБЫЕ ОТМЕТКИ

13. ОГРАНИЧЕНИЯ ПО ЭКСПЛУАТАЦИИ

Для обеспечения выполнения требований к пятому классу защищенности необходимо выполнение организационно-технических мероприятий перечисленных ниже.

13.1. Установка изделия на автоматизированные рабочие места должна проводиться с дистрибутива изделия, расположенного на компакт-диске в составе верифицированного установочного комплекта, или загруженного с Центра сертифицированных обновлений Производителя (https://armlock.pro). Реквизиты для доступа к Центру сертифицированных обновлений могут быть получены у поставщика ПЗИ НСД ARMlock по запросу конечного пользователя.

13.2. Использование ПЗИ НСД ARMlock для обработки информации, содержащей сведения, составляющие государственную тайну запрещено.

13.3. Настройка, использование и контроль средств защиты информации изделия должны проводиться ответственным за эксплуатацию изделия (администратором безопасности) в соответствии с утвержденной политикой безопасности организации, организационно-методическими документами принятой системы защиты информации, Руководством администратора изделия и настоящим формуляром.

13.4. Перед началом эксплуатации сертифицированной версии ПЗИ НСД ARMlock администратору безопасности необходимо изменить существующие (заводские и тестовые) установки паролей, настроить изделие в соответствии с Требованиями по безопасной настройке, указанными в Руководстве администратора на изделие. Пароли должны сохраняться в секрете и периодически меняться.

13.5. Администратором должно проводиться периодическое тестирование функций защиты изделия, включающее контроль настроек безопасности изделия, а также проверку целостности его текущей конфигурации.

13.6. В случаях и в порядке, предусмотренном нормативными документами ФСТЭК России в зависимости от уровня защищённости персональных данных и/или класса защищённости информационной системы, должна проводиться периодическая проверка на отсутствие уязвимостей с использованием средства анализа защищенности.

13.7. Для пользователей ПЗИ НСД ARMlock в среде функционирования на базе сертифицированных ОС Windows XP, Windows Server 2003 и Windows Server 2003 R2, в соответствии с информационными сообщениями ФСТЭК России № 240/24/1208 от 07 апреля 2014 года и № 240/24/2497 от 19 июня 2015 года рекомендуется:

1. Спланировать мероприятия по переводу до декабря 2016 г. для Windows XP и до августа 2017 г. для Windows Server 2003 R2 информационных систем на сертифицированные по требованиям безопасности информации операционные системы, поддерживаемые их производителями.

2. До перехода на сертифицированные по требованиям безопасности информации операционные системы с учетом моделей угроз безопасности информации принять следующие дополнительные меры защиты информации, направленные на минимизацию рисков реализации угроз безопасности информации:

- установить все актуальные обязательные сертифицированные обновления сертифицированных версий операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2, выпущенных российскими производителями (заявителями);
- установить запрет на автоматическое обновление сертифицированных версий операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2;
- провести настройку и обеспечивать периодический контроль механизмов защиты сертифицированных версий операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2 в соответствии с руководствами по безопасной настройке и контролю сертифицированных версий операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2;
- по возможности исключить подключение к сети Интернет и к ведомственным (корпоративным) локальным вычислительным сетям средств вычислительной техники или сегментов информационных систем, работающих под управлением операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2;
- при невозможности отключения от сети Интернет и (или) от ведомственных (корпоративных) локальных вычислительных сетей средств вычислительной техники или сегментов информационных систем, работающих под управлением операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2, применять в обязательном порядке меры по сегментированию информационных систем и защите периметра информационной системы и выделенных сегментов (в том числе путем применения сертифицированных межсетевых экранов, средств антивирусной защиты, систем обнаружения вторжений, средств защиты от несанкционированной передачи (вывода) информации (DLP - систем), средств управления потоками информации);
- обеспечить регулярное резервное копирование информации, программного обеспечения и средств защиты информации, содержащихся на средствах вычислительной техники или в сегментах информационных систем, работающих под управлением операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2, на внешние носители информации;
- регламентировать и обеспечивать контроль за применением съемных машинных носителей информации, исключив при этом использование не зарегистрированных в информационной системе машинных носителей информации и не проверенных средствами антивирусной защиты;

- проводить периодический анализ уязвимостей сегментов информационных систем, работающих под управлением операционных систем Windows XP, Windows Server 2003 и Windows Server 2003 R2, с использованием сертифицированных средств контроля (анализа) защищенности информации, а также периодический контроль целостности установленных операционных систем;

- проводить мониторинг общедоступных источников, публикующих сведения об уязвимостях, на предмет появления в них информации об уязвимостях в операционных системах Windows XP, Windows Server 2003 и Windows Server 2003 R2 и принимать меры, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителями выявленных уязвимостей (в том числе за счет применения дополнительных средств защиты информации);

- разработать и внедрить правила и процедуры действий должностных лиц в случае выявления уязвимостей в операционных системах Windows XP, Windows Server 2003 и Windows Server 2003 R2 или возникновения инцидентов информационной безопасности, связанных с ее применением.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					