Утвержден
ЕАРМ.5090005.032-03 30 01-ЛУ

Средство защиты информации

«Secure Pack Rus»

Версия 3.0

Формуляр

ЕАРМ.5090005.032-03 30 01

Листов 24

Компания «КРИПТО-ПРО»

2021

ООО «КРИПТО-ПРО»
Адрес 127018, г. Москва, ул. Сущевский Вал, дом 18
Телефон +7 (495) 995-4820
e-mail info@cryptopro.ru
Web www.cryptopro.ru

Оглавление

Список сокращений 4
1. Общие указания 5
2. Общие сведения об изделии 6
3. Основные технические характеристики 10
4. Комплектность 12
5. Контроль целостности дистрибутива 15
6. Свидетельство о приемке 16
7. Свидетельство об упаковке 17
8. Гарантии изготовителя (поставщика) 18
9. Сведения о рекламациях 19
10. Сведения о хранении 20
11. Сведения о закреплении изделия при эксплуатации 21
12. Сведения об изменениях 22
13. Особые отметки 23
Список литературы 24

Список сокращений

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ЗПС	Замкнутая программная среда
ИС	Информационная система
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СЗИ	Средство или система защиты информации
СКЗИ	Средство криптографической защиты информации
СХКИ	Средство хранения конфиденциальной информации

1. Общие указания

Формуляр на изделие средство защиты информации «Secure Pack Rus» версия 3.0 (сокращенные названия изделия – Secure Pack Rus 3.0 или SPR 3.0) является документом, удостоверяющим гарантированные предприятием-изготовителем основные характеристики, определяющим комплект поставки, содержащим сведения о произведенных изменениях и другие данные за весь период эксплуатации.

Порядок обеспечения информационной безопасности при использовании SPR 3.0 определяется руководителем эксплуатирующей организации на основе требований, изложенных в эксплуатационной документации на изделие.

Эксплуатация SPR 3.0 должна проводиться в соответствии с эксплуатационной документацией, предусмотренной настоящим Формуляром. Перед установкой SPR 3.0 необходимо внимательно ознакомиться с условиями применения, указанными в [1].

Администратор безопасности SPR 3.0 должен изучить и выполнять требования и рекомендации, изложенные в [2], [3], [4], [5] и [6].

Пользователь должен изучить и выполнять требования и рекомендации, изложенные в [7].

Формуляр входит в комплект поставки изделия и должен постоянно храниться в подразделении, ответственном за эксплуатацию изделия.

Все записи в формуляре производятся отчетливо и аккуратно. Незаверенные исправления не допускаются.

2. Общие сведения об изделии

SPR 3.0 предназначен для обеспечения защиты информационных ресурсов АИС, состоящих из АРМ и серверов, функционирующих под управлением ОС компании Microsoft (Таб. 1), и совместно с другими средствами защиты усиливает штатные механизмы ОС, обеспечивающие информационную безопасность АИС.

Таб. 1. Операционные системы, поддерживаемые SPR 3.0 (исполнения 5, 6)

Операционная система	Необходимые обновления
Microsoft Windows 7 Professional/Enterprise/Ultimate[1]	KB976932 (Service Pack 1), KB2479943, KB2491683, KB2506212, KB2560656, KB2564958, KB2579686, KB2585542, KB2620704, KB2621440, KB2631813, KB2653956, KB2654428, KB2685939, KB2690533, KB2698365, KB2705219, KB2727528, KB2758857, KB2770660, KB2807986, KB2813430, KB2847927, KB2862330, KB2864202, KB2868038, KB2871997, KB2884256, KB2893294, KB2900986, KB2973201, KB2977292, KB2978742, KB2984972, KB2991963, KB2992611, KB3004375, KB3010788, KB3011780, KB3019978, KB3021674, KB3030377, KB3033929, KB3035126, KB3042058, KB3045685, KB3046017, KB3046269, KB3059317, KB3060716, KB3067903, KB3071756, KB3086255, KB3093513, KB3108371, KB3108664, KB3109103, KB3109560, KB3110329, KB3115858, KB3126587, KB3138910, KB3139398, KB3139914, KB3155178, KB3156016, KB3159398, KB3161949, KB2604115, KB2729452, KB2736422, KB2742599, KB2789645, KB2840631, KB2861698, KB2894844, KB2911501, KB2931356, KB2937610, KB2943357, KB2968294, KB2972100, KB2978120, KB3023215, KB3037574, KB3072305, KB3074543, KB3097989, KB3127220, KB4470641, KB4480063, KB4483458, KB4495606, KB4507004, KB4532945, KB3124275, KB4474419, KB4490628, KB4536952, KB4534310
Microsoft Windows 7 x64 Professional/Enterprise/Ultimate Edition[1]	KB976932 (Service Pack 1), KB2479943, KB2491683, KB2506212, KB2560656, KB2564958, KB2579686, KB2585542, KB2620704, KB2621440, KB2631813, KB2653956, KB2654428, KB2685939, KB2690533, KB2698365, KB2705219, KB2706045, KB2727528, KB2758857, KB2770660, KB2807986, KB2813430, KB2847927, KB2862330, KB2864202, KB2868038, KB2871997, KB2884256, KB2893294, KB2900986, KB2973201, KB2977292,

	KB2978742, KB2984972, KB2991963, KB2992611, KB3004375, KB3010788, KB3011780, KB3019978, KB3021674, KB3030377, KB3033929, KB3035126, KB3042058, KB3045685, KB3046017, KB3046269, KB3059317, KB3060716, KB3067903, KB3071756, KB3086255, KB3093513, KB3108371, KB3108664, KB3109103, KB3109560, KB3110329, KB3115858, KB3126587, KB3138910, KB3139398, KB3139914, KB3155178, KB3156016, KB3159398, KB3161949, KB2604115, KB2931356, KB2937610, KB2943357, KB2968294, KB2972100, KB2978120, KB3023215, KB3037574, KB3072305, KB3074543, KB2729452, KB3097989, KB3127220, KB4470641, KB4480063, KB4483458, KB4495606, KB4507004, KB4532945, KB2736422, KB2742599, KB2789645, KB2840631, KB2861698, KB2894844, KB2911501, KB3124275, KB4474419, KB4490628, KB4536952, KB4534310
Microsoft Windows Server 2008 R2 Standard/Enterprise[1]	KB976932 (Service Pack 1) KB2479943, KB2491683, KB2506212, KB2560656, KB2564958, KB2579686, KB2585542, KB2620704, KB2621440, KB2631813, KB2653956, KB2654428, KB2685939, KB2690533, KB2698365, KB2705219, KB2706045, KB2727528, KB2758857, KB2770660, KB2807986, KB2813430, KB2847927, KB2862330, KB2864202, KB2868038, KB2871997, KB2884256, KB2893294, KB2900986, KB2973201, KB2977292, KB2978742, KB2984972, KB2991963, KB2992611, KB3004375, KB3010788, KB3011780, KB3019978, KB3021674, KB3030377, KB3033929, KB3035126, KB3042058, KB3045685, KB3046017, KB3046269, KB3059317, KB3060716, KB3067903, KB3071756, KB3086255, KB3093513, KB3108371, KB3108664, KB3109103, KB3109560, KB3110329, KB3115858, KB3126587, KB3138910, KB3139398, KB3139914, KB3155178, KB3156016, KB3159398, KB3161949, KB2604115, KB2729452, KB2736422, KB2742599, KB2789645, KB2840631, KB2861698, KB2894844, KB2911501, KB2931356, KB2937610, KB2943357, KB2968294, KB2972100, KB2978120, KB3023215, KB3037574, KB3072305, KB3074543, KB3097989, KB3127220, KB4470641, KB4480063, KB4483458, KB4495606, KB4507004, KB4532945, KB3124275, KB4474419, KB4490628, KB4536952, KB4534310
Microsoft Windows 8.1 Pro/Enterprise[1]	KB3021910, KB2919355, KB2962140, KB2973201, KB2976897, KB3010788, KB3019978, KB3023266,

	KB3042058, KB3045685, KB3045999, KB3046017, KB3059317, KB3061512, KB3062760, KB3071756, KB3076949, KB3082089, KB3084135, KB3086255, KB3109103, KB3109560, KB3110329, KB3115858, KB3126434, KB3126587, KB3138910, KB3138962, KB3139398, KB3139914, KB3146723, KB3155178, KB3156059, KB3159398, KB3161949, KB3175024, KB3178539, KB3187754, KB2894856, KB2977765, KB2978041, KB2978126, KB3023222, KB3037579, KB3097997, KB3074228, KB3074548, KB3098779, KB3135994, KB3185319, KB4603004, KB5001403, KB5005076
Microsoft Windows 8.1 x64 Pro/Enterprise Edition[1]	KB3021910, KB2919355, KB2962140, KB2973201, KB2976897, KB3010788, KB3019978, KB3023266, KB3042058, KB3045685, KB3045999, KB3046017, KB3059317, KB3061512, KB3062760, KB3071756, KB3076949, KB3082089, KB3084135, KB3086255, KB3109103, KB3109560, KB3110329, KB3115858, KB3126434, KB3126587, KB3138910, KB3138962, KB3139398, KB3139914, KB3146723, KB3155178, KB3156059, KB3159398, KB3161949, KB3175024, KB3178539, KB3187754, KB2894856, KB2977765, KB2978041, KB2978126, KB3023222, KB3037579, KB3097997, KB3074228, KB3074548, KB3098779, KB3135994, KB3185319, KB4603004, KB5001403, KB4535680, KB5005076
Microsoft Windows Server 2012 R2 Standard/Enterprise[1]	KB3021910, KB2919355, KB2973201, KB2976897, KB3010788, KB3019978, KB3023266, KB3042058, KB3045685, KB3045999, KB3046017, KB3059317, KB3061512, KB3071756, KB3076949, KB3082089, KB3084135, KB3086255, KB3109103, KB3109560, KB3110329, KB3115858, KB3126434, KB3126587, KB3133043, KB3138910, KB3138962, KB3139398, KB3139914, KB3146723, KB3156059, KB3159398, KB3161949, KB3175024, KB3178539, KB2894856, KB2977765, KB2978041, KB2978126, KB3023222, KB3037579, KB3097997, KB3074228, KB3074548, KB3098779, KB3135994, KB4603004, KB3185319, KB5001403, KB4535680, KB5005076
Microsoft Windows 10 Version 20H2 Pro/Enterprise[1]	KB5004331, KB5005033
Microsoft Windows 10 Version 20H2 x64 Pro/Enterprise Edition[1]	KB5005033, KB5005033

Microsoft Windows Server 2016 Standard/Enterprise[1]	KB5001402, KB4535680, KB5004752, KB5005043

Примечания: [1] Порядок и сроки эксплуатации ОС определяются производителем ОС.

3. Основные технические характеристики

SPR 3.0 поставляется в четырех исполнениях.

ОС Microsoft Windows (Таб. 1) со встроенными и дополнительными интегрированными механизмами обеспечения безопасности, реализуемыми SPR 3.0 (исполнения 5), обеспечивает уровень защиты АК3 в соответствии с [8] и реализует:

- Возможность доменной аутентификации пользователей на основе метода двухфакторной аутентификации с использованием сертификатов стандарта X.509.
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к именованным объектам системы (файлы, процессы и.т.д.).
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к устройствам (отчуждаемые хранилища данных, мобильные устройства, принтеры, порты ввода/вывода и.т.д).
- Обнуление освобожденной оперативной памяти системы.
- Возможность аудита входа/выхода субъектов доступа (пользователей) в систему/из системы.
- Возможность аудита.
- Возможность периодического контроля целостности объектов файловой системы.
- Возможность задания администратором списка разрешенных на выполнение программных модулей.
- Возможность задания администратором списка разрешенных для установки в систему инсталляционных пакетов.
- Возможность задания администратором списка разрешенных на выполнение сценариев.
- Возможность криптографической защиты информации, передаваемой по канал связи, с посредством создания аутентичного защищенного соединения с использованием протокола КриптоПро TLS и/или посредством защиты IP-соединений с использованием протоколов КриптоПро IKE, КриптоПро ESP, КриптоПро AH. Криптографическая защита информации осуществляется по классу КС3.
- Возможность криптографической защиты информации, записываемой на съемные хранилища данных посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС3.
- Возможность криптографической защиты информации, записываемой на жестких дисках АРМ и серверов посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС3.
- Возможность централизованного удаленного управления через механизм групповых политик ОС Microsoft Windows (Таб. 1).

ОС Microsoft Windows (Таб. 1) со встроенными и дополнительными интегрированными механизмами обеспечения безопасности, реализуемыми SPR 3.0 (исполнения 6), обеспечивает уровень защиты АК2 в соответствии с (8) и реализует:

- Возможность доменной аутентификации пользователей на основе метода двухфакторной аутентификации с использованием сертификатов стандарта X.509.
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к именованным объектам системы (файлы, процессы и.т.д.).
- Возможность дискреционного разграничения доступа именованных субъектов системы (пользователей) к устройствам (отчуждаемые хранилища данных, мобильные устройства, принтеры, порты ввода/вывода и.т.д).
- Обнуление освобожденной оперативной памяти системы.
- Возможность аудита входа/выхода субъектов доступа (пользователей) в систему/из системы.
- Возможность аудита.
- Возможность периодического контроля целостности объектов файловой системы.
- Возможность задания администратором списка разрешенных на выполнение программных модулей.
- Возможность задания администратором списка разрешенных для установки в систему инсталляционных пакетов.
- Возможность задания администратором списка разрешенных на выполнение сценариев.
- Возможность криптографической защиты информации, передаваемой по канал связи, с посредством создания аутентичного защищенного соединения с использованием протокола КриптоПро TLS и/или посредством защиты IP-соединений с использованием протоколов КриптоПро IKE, КриптоПро ESP, КриптоПро AH. Криптографическая защита информации осуществляется по классу КС2.
- Возможность криптографической защиты информации, записываемой на съемные хранилища данных посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС2.
- Возможность криптографической защиты информации, записываемой на жестких дисках АРМ и серверов посредством шифрующей файловой системы КриптоПро EFS. Криптографическая защита информации осуществляется по классу КС2.
- Возможность централизованного удаленного управления через механизм групповых политик ОС Microsoft Windows (Таб. 1).

4. Комплектность

SPR 3.0 поставляется в четырех комплектациях.

В Таб. 2 представлена комплектация SPR 3.0 (исполнение 5), соответствующая уровню защиты АК3 в соответствии с [8].

Таб. 2. Комплектация SPR 3.0 (исполнение 5)

Наименование	Обозначение	Кол-во
Средство защиты информации «Secure Pack Rus» версия 3.0 (дистрибутив АК3)	EAPM.5090005.032-03	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Ведомость эксплуатационных документов	EAPM.5090005.032-03 20 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Формуляр.	EAPM.5090005.032-03 30 01	1
Средство защиты информации Secure Pack Rus 3.0 Описание применения.	EAPM.5090005.032-03 31 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности.	EAPM.5090005.032-03 90 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Установка.	EAPM.5090005.032-03 90 02	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Аутентификация.	EAPM.5090005.032-03 90 03	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности.	EAPM.5090005.032-03 90 04	1

Политики управления приложениями.		
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Аудит.	ЕАРМ.5090005.032-03 90 05	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Мандатное шифрование. Концепция.	ЕАРМ.5090005.032-03 91 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство пользователя.	ЕАРМ.5090005.032-03 34 01	1
Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 3-Base/4.0 R4 3-Base в комплектации согласно [9][1]	ЖТЯИ.00089	1

Примечания: [1] Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 должно иметь действующий сертификат соответствия ФСБ России.

В Таб. 3 представлена комплектация SPR 3.0 (исполнение 6), соответствующая уровню защиты АК2 в соответствии с [8].

Таб. 3. Комплектация SPR 3.0 (исполнение 6)

Наименование	Обозначение	Кол-во
Средство защиты информации «Secure Pack Rus» версия 3.0 (дистрибутив АК2)	ЕАРМ.5090005.032-03	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Ведомость эксплуатационных документов	ЕАРМ.5090005.032-03 20 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Формуляр.	ЕАРМ.5090005.032-03 30 01	1
Средство защиты информации Secure Pack Rus 3.0	ЕАРМ.5090005.032-03 31 01	1

Описание применения.		
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности.	EAPM.5090005.032-03 90 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Установка.	EAPM.5090005.032-03 90 02	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Аутентификация.	EAPM.5090005.032-03 90 03	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Политики управления приложениями.	EAPM.5090005.032-03 90 04	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство администратора безопасности. Аудит.	EAPM.5090005.032-03 90 05	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Мандатное шифрование. Концепция.	EAPM.5090005.032-03 91 01	1
Средство защиты информации «Secure Pack Rus» версия 3.0 Руководство пользователя.	EAPM.5090005.032-03 34 01	1
Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 2-Base/4.0 R4 2-Base в комплектации согласно [10][1].	ЖТЯИ.00088	1

Примечания: [1] Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 должно иметь действующий сертификат соответствия ФСБ России.

5. Контроль целостности дистрибутива

Для расчета контрольной суммы дистрибутива SPR 3.0 необходимо использовать утилиту CtrlSum версии 2.0 (инв. № Д48/39).

При расчете контрольной суммы для SPR 3.0 (исполнения 5, 6) в качестве целевой папки необходимо указать папку «Distribs\CAN\spr-3.0 (editions 5, 6)». Также необходимо выставить флаги «Process Subfolders» и «Check Total».

6. Свидетельство о приемке

Изделие средство защиты информации «Secure Pack Rus» версия 3.0 (ЕАРМ.5090005.032-03),

серийный номер дистрибутива _____

носители:

☐ CD-ROM _____ шт.

соответствует эталону, хранящемуся в ООО "СиЭйЭн", и признано годным для эксплуатации.

Дата выпуска: «_____» _____ 20_____ г.

М.П.

Приемку произвел _____

(Подпись лица ответственного за приемку)

7. Свидетельство об упаковке

Изделие средство защиты информации «Secure Pack Rus» версия 3.0 (ЕАРМ.5090005.032-03),

серийный номер дистрибутива _____

упаковано в

☐ бумажный конверт

☐ коробку

☐ пластиковый конверт

☐ _____

Дата упаковки: «_____» _____ 20_____ г.

М. П.

Упаковку произвел _____

(Подпись)

8. Гарантии изготовителя (поставщика)

Пользователь приобретает изделие и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.

Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками при соблюдении пользователем требований эксплуатационной документации на изделие.

В случае выявления в программном обеспечении дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации, и предприятие-изготовитель обязуется по получении рекламации в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки нового изделия, а также принять меры, исключающие эти дефекты во всех остальных экземплярах изделия.

Гарантийный срок изделия – 12 месяцев с момента поставки.

Примечание: При отсутствии данных о дате поставки изделия гарантийный срок отсчитывается от даты его выпуска, указанной в разделе 5 «Свидетельство о приемке».

Данные о поставке (продаже) изделия:

SPR 3.0

ООО «СиЭйЭн»

(наименование организации-поставщика (продавца) изделия)

Дата поставки: «_____» _____ 20_____ г.

М.П.

_____

(подпись)

9. Сведения о рекламациях

10. Сведения о хранении

11. Сведения о закреплении изделия при эксплуатации

12. Сведения об изменениях

13. Особые отметки

Список литературы

1. **Компания "СиЭйЭн".** Описание применения. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 31 01.

2. —. Руководство администратора безопасности. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 01.

3. —. Руководство администратора безопасности. Установка. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 02.

4. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 03.

5. —. Руководство администратора безопасности. Политики управления приложениями. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 04.

6. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 90 05.

7. —. Руководство пользователя. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 34 01.

8. **ФСБ России.** Требования по защите конфиденциальной информации от несанкционированного доступа в автоматизированных информационных системах, расположенных на территории Российской Федерации.

9. **Компания "КРИПТО-ПРО".** Формуляр. *Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 3-Base.* ЖТЯИ.00089-01 30 01.

10. —. Формуляр. *Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 2-Base.* ЖТЯИ.00088-01 30 01.

11. —. Формуляр. *Средство криптографической защиты информации «КриптоПро CSP» версия 4.0 R4 3-Base.*

12. **Компания "СиЭйЭн".** Мандатное шифрование. Концепция. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 91 01.

13. —. Формуляр. *Средство защиты информации «Secure Pack Rus» версия 3.0.* ЕАРМ.5090005.032-03 30 01.