# ОПИСАНИЕ РЕЛИЗА

**Наименование продукта**

Privacy-SPS, LIS-SPS

**Поддерживаемые версии продуктов**

Privacy-SPS 1.1.4.0 и выше

LIS-SPS 1.2 и выше

**Наименование базы данных**

База данных угроз, средств и мер защиты

**Версия релиза**

2.0

**Дата релиза**

20.01.2016 09.00

**Описание базы данных**

Интерфейс «Типы активов»:

- установка базы данных внесет следующие Типы активов (если они были ранее удалены):

- Персональный компьютер
- Терминальный клиент
- Сервер приложений
- Сервер баз данных
- Хранилище
- Сетевой принтер
- Сканер
- Устройство обработки видеоизображения
- Голосовой шлюз
- Коммутатор
- Концентратор
- Маршрутизатор
- Каналообразующее оборудование
- Факс
- Сотовый телефон
- Стационарный телефон
- Планшет
- Внешний канал связи
- Помещение
- Здание
- Канал связи с ССОП
- Внутренний канал связи

- добавлены новые Типы активов:

- Точка доступа
- Съемный машинный носитель информации
- Средства и системы обеспечения

- обновлены иконки для следующих Типов активов:

- Персональный компьютер
- Терминальный клиент
- Сервер приложений
- Сервер баз данных
- Хранилище
- Сетевой принтер
- Сканер
- Устройство обработки видеоизображения
- Голосовой шлюз
- Коммутатор
- Концентратор
- Маршрутизатор
- Каналообразующее оборудование
- Факс
- Сотовый телефон
- Стационарный телефон
- Планшет
- Внешний канал связи
- Внутренний канал связи

Интерфейс «Угрозы»:

- в целях унификации изменены названия последствий реализации угроз (Свойств безопасности):

- нарушение конфиденциальности (на Конфиденциальность),
- нарушение целостности (на Целостность),
- нарушение доступности (на Доступность),

- добавлены следующие Свойства безопасности:

- Неотказуемость
- Владение
- Подотчетность
- Аутентичность
- Достоверность

- вносятся следующие Типы угроз (если были удалены ранее):

- Угрозы утечки акустической информации
- Угрозы утечки видовой информации
- Угрозы утечки информации по каналам ПЭМИН
- Угрозы связанные с ошибками проектирования и разработки
- Угрозы связанные с локальным доступом к компонентам ИС
- Угрозы связанные с сетевым взаимодействием
- Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия
- Угрозы программно-математических воздействий
- Угрозы несанкционированного доступа к съемным носителям информации
- Угрозы доступа к ТС и системам обеспечения
- Угрозы разглашения информации
- Неопределенный

- Угрозы связанные с природными факторами
- Угрозы использования ресурсов ИС в сторонних целях

- добавляется новый Тип угроз:

- Угрозы связанные с обманом и мошенничеством

- изменены (дополнены, актуализированы) названия следующих Угроз:

| Старое название | Новое название |
|---|---|
| использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет "микрофонного эффекта" в ТС обработки ПДн и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений) | использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет «микрофонного эффекта» в технических средствах обработки информации и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений) |
| применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении ТС обработки ПДн и второстепенных ТС и систем ВЧ-сигналом | применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении технических средств обработки информации и ВТСС ВЧ-сигналом |
| применение акустооптических модуляторов на базе волоконно-оптических линий, находящихся в поле акустического сигнала ("оптических микрофонов") | применение акустооптических модуляторов на базе волоконно-оптических линий, находящихся в поле акустического сигнала («оптических микрофонов») |
| визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИС | визуальный просмотр информации на экранах дисплеев ИС, документах на бумажном носителе, других носителях визуальной информации |
| визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИС | визуальный просмотр информации с помощью оптических (оптикоэлектронных) средств на экранах дисплеев ИС, документах на бумажном носителе, других носителях визуальной информации |
| использование специальных электронных устройств съема видовой информации (видеозакладки) | использование специальных электронных устройств съема видовой информации (видеозакладок) |
| применение специальных средств регистрации ПЭМИН, от ТС и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры) | применение специальных средств регистрации ПЭМИН от технических средств и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры) |

| Старое название | Новое название |
|---|---|
| применение токосъемников для регистрации наводок информативного сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений | применение токосъемников для регистрации наводок информативных сигналов, обрабатываемых техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны |
| применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИСПДн или при наличии паразитной генерации в узлах ТС | применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав технических средств ИС или при наличии паразитной генерации в узлах технических средств |
| применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИСПДн в которых проводится обработка информативных сигналов - параметрических каналов утечки | применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения технических средств ИС, в которых проводится обработка информативных сигналов (параметрические каналы утечки) |
| преднамеренное внесение уязвимостей при проектировании и разработке системного ПО, недекларированные возможности системного ПО | преднамеренное внесение уязвимостей при проектировании и разработке системного ПО, использование недекларированных возможностей системного ПО |
| преднамеренное внесение уязвимостей при проектировании и разработке ППО, недекларированные возможности ППО | преднамеренное внесение уязвимостей при проектировании и разработке прикладного ПО, использование недекларированных возможностей прикладного ПО |
| использование неверных настроек ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное) | использование неверных настроек ПО, изменение режимов работы технических средств и ПО (случайное либо преднамеренное) |
| доступ в операционную среду (локальную ОС отдельного ТС ИС) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ | доступ в операционную среду (локальную ОС отдельного технического средства ИС) с возможностью выполнения НСД вызовом штатных процедур или запуском специально разработанных программ |
| доступ в среду функционирования прикладных программ (локальная СУБД, например) | доступ в среду функционирования локальных прикладных программ (локальное приложение, база данных) |

| Старое название | Новое название |
|---|---|
| анализ сетевого трафика при его передаче в пределах ЛВС для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены | анализ сетевого трафика при его передаче в пределах локальной вычислительной сети для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены |
| внедрение специализированных троянов | внедрение специализированных программ типа «троянский конь» |
| повреждение носителя информации | нарушение функционирования съемного машинного носителя информации |
| утрата носителя информации | утрата съемного машинного носителя информации |
| хищение носителя информации | хищение съемного машинного носителя информации |
| подключение к ТС и системам | подключение к техническим средствам и системам |
| нарушение функционирования кабельных линий связи, оборудования | нарушение функционирования кабельных линий связи |
| нарушение функционирования ТС обработки информации, НЖМД | нарушение функционирования технических средств обработки информации (компьютеров, принтеров, коммутаторов и т.п.) |
| сбои в работе ТС и ПО компьютерного оборудования (рабочих станций, серверов и т.п.) | сбои в работе технических средств и ПО компьютерного оборудования (рабочих станций, серверов и т.п.) |
| копирование информации на незарегистрированный носитель информации, в том числе печать | копирование информации на незарегистрированный носитель информации, в том числе печать такой информации |
| сбои в работе ТС и ПО технологического оборудования (коммутаторы, маршрутизаторы и т.п.) | сбои в работе технических средств и ПО технологического оборудования (коммутаторы, маршрутизаторы и т.п.) |
| использование ресурса в личных целях (развлечения в рабочее время) | использование компьютерного оборудования в личных целях (развлечения в рабочее время) |

- вносятся следующие Угрозы (если были удалены ранее):

- использование направленных (ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала
- использование "контактных микрофонов" для съема виброакустических сигналов

- использование "лазерных микрофонов" для съема виброакустических сигналов
- использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет «микрофонного эффекта» в технических средствах обработки информации и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений)
- применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении технических средств обработки информации и ВТСС ВЧ-сигналом
- применение акустооптических модуляторов на базе волоконно-оптических линий, находящихся в поле акустического сигнала («оптических микрофонов»)
- визуальный просмотр информации на экранах дисплеев ИС, документах на бумажном носителе, других носителях визуальной информации
- визуальный просмотр информации с помощью оптических (оптикоэлектронных) средств на экранах дисплеев ИС, документах на бумажном носителе, других носителях визуальной информации
- использование специальных электронных устройств съема видовой информации (видеозакладок)
- применение специальных средств регистрации ПЭМИН от технических средств и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)
- применение токосъемников для регистрации наводок информативных сигналов, обрабатываемых техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны
- применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав технических средств ИС или при наличии паразитной генерации в узлах технических средств
- применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения технических средств ИС, в которых проводится обработка информативных сигналов (параметрические каналы утечки)
- преднамеренное внесение уязвимостей при проектировании и разработке системного ПО, использование недекларированных возможностей системного ПО
- преднамеренное внесение уязвимостей при проектировании и разработке прикладного ПО, использование недекларированных возможностей прикладного ПО
- использование неверных настроек ПО, изменение режимов работы технических средств и ПО (случайное либо преднамеренное)
- доступ к информации и командам, хранящимся в BIOS с возможностью перехвата управления загрузкой ОС и получения прав доверенного пользователя
- доступ в операционную среду (локальную ОС отдельного технического средства ИС) с возможностью выполнения НСД вызовом штатных процедур или запуском специально разработанных программ

- доступ в среду функционирования локальных прикладных программ (локальное приложение, база данных)
- локальный доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности
- сканирование сети для изучения логики работы ИС, выявления протоколов, портов
- анализ сетевого трафика при его передаче в пределах локальной вычислительной сети для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены
- применение специальных программ для выявления пароля (IP-спуффинг, разные виды перебора)
- реализация угрозы отказа в обслуживании
- внедрение специализированных программ типа «троянский конь»
- сетевые атаки
- применение утилит администрирования сети
- подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети
- внедрение программных закладок
- внедрение вредоносных программ (случайное или преднамеренное, непосредственное)
- нарушение функционирования съемного машинного носителя информации
- утрата съемного машинного носителя информации
- хищение съемного машинного носителя информации
- подключение к техническим средствам и системам
- нарушение функционирования кабельных линий связи
- нарушение функционирования технических средств обработки информации (компьютеров, принтеров, коммутаторов и т.п.)
- доступ к системам обеспечения, их повреждение
- доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)
- сбои в работе технических средств и ПО компьютерного оборудования (рабочих станций, серверов и т.п.)
- разглашение информации лицам, не имеющим права доступа к ней
- передача защищаемой информации по открытым каналам связи
- копирование информации на незарегистрированный носитель информации, в том числе печать такой информации
- передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации
- пожар
- наводнение, ураган, землетрясение
- сбои в работе технических средств и ПО технологического оборудования (коммутаторы, маршрутизаторы и т.п.)
- сбой, отказ проводной линии связи
- сбой, отказ оптической линии связи
- кража устройства, оборудования
- финансовое мошенничество с использованием компьютера
- использование Интернет ресурсов в личных целях

- использование компьютерного оборудования в личных целях (развлечения в рабочее время)
- сбой, отказ системы электропитания на время до 30 минут
- сбой, отказ системы электропитания на время до 60 минут
- сбой, отказ системы электропитания на время более 60 минут
- анализ сетевого трафика при его передаче по внешним каналам связи для изучения логики работы ИС, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены

- добавлены новые Угрозы:

- социальный инжиниринг
- отказ от авторства
- доступ в среду функционирования сетевых прикладных программ (сетевые сервисы, базы данных и т.п.)

- обновлена привязка Угроз к Свойствам безопасности,

- обновлена привязка Угроз к Типам активов, на которые они могут влиять.

Интерфейс «Классы средств и мер защиты»:

- изменены (дополнены, актуализированы) названия следующих Классов средств и мер защиты:

| Старое название | Новое название |
|---|---|
| Средства межсетевого экранирования | Межсетевые экраны |
| Средства анализа уязвимостей | Сканеры уязвимостей |
| Меры предотвращения просмотра видовой информации | Мероприятия по предотвращению просмотра видовой информации |
| Меры повышения звуконепроницаемости | Мероприятия по повышению звуконепроницаемости |
| Меры физической защиты оборудования и систем | Мероприятия по физической защите оборудования и систем |
| Меры по защите от разглашения | Мероприятия по защите от разглашения |
| Меры контроля ПО на отсутствие ошибок, закладок и т.п. | Мероприятия по контролю ПО на отсутствие ошибок, недекларированных возможностей, закладок |
| Меры контроля носителей данных | Мероприятия по управлению носителями данных |
| Средства контроля целостности ПО | Средства контроля целостности файлов |
| Меры управления идентификацией и аутентификацией | Мероприятия по управлению идентификацией и аутентификацией |
| Меры по управлению разграничением доступа | Мероприятия по управлению разграничением доступа |
| Меры по защите беспроводного доступа | Мероприятия по управлению беспроводным доступом |
| Меры по управлению программным обеспечением | Мероприятия по управлению программным обеспечением |
| Меры по управлению событиями безопасности | Мероприятия по управлению событиями безопасности |

| Старое название | Новое название |
|---|---|
| Меры по контролю защищенности технических средств, ПО и средств защиты | Мероприятия по контролю защищенности активов |
| Меры по управлению инцидентами | Мероприятия по управлению инцидентами |
| Меры по управлению изменениями ИС и системы защиты | Мероприятия по управлению изменениями ИС и системы защиты |

- добавлены новые Классы средств и мер защиты:

- Общие организационные мероприятия по информационной безопасности
- Общие мероприятия по управлению средствами защиты информации
- Мероприятия по уничтожению не используемой конфиденциальной информации
- Средства управления доступом к данным приложений и баз данных
- Мероприятия по защите от обмана и мошенничества
- Мероприятия по управлению СКЗИ
- Мероприятия по обучению вопросам ИБ
- Средства контроля печати
- Средства централизованного управления механизмами защиты
- Средства контроля сетевых коммуникаций

- обновлена привязка Классов средств и мер защиты к Угрозам, на которые данные классы влияют.

Интерфейс «Общие/Параметры/Классы, уровни средств защиты»:

- изменены (дополнены, актуализированы) названия следующих Уровней сертификации по требованиям информационной безопасности:

| Старое название | Новое название |
|---|---|
| МЭ | МЭ по НМД ФСТЭК России |

- внесен новый Уровень сертификации, по «Техническим условиям»,

- внесен новый Уровень сертификации «АПМДЗ по НМД ФСБ России», на соответствие требованиям ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ, значения:

- Класс 1А
- Класс 1Б
- Класс 1В
- Класс 1Г
- Класс 2А
- Класс 2Б
- Класс 2В
- Класс 2Г
- Класс 3А
- Класс 3Б
- Класс 3В

- Класс 3Г

- внесен новый Уровень сертификации «АС», на соответствие требованиям РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», решение председателя Гостехкомиссии России от 30 марта 1992 г., значения:

- Класс 1А
- Класс 1Б
- Класс 1В
- Класс 1Г
- Класс 1Д
- Класс 2А
- Класс 2Б
- Класс 3А
- Класс 3Б

- внесен новый Уровень сертификации «СДЗ», на соответствие «Требованиям к средствам доверенной загрузки», приказ ФСТЭК России от 27 сентября 2013 г. N 119, зарегистрированный Минюстом России 16 декабря 2013 г., рег. N 30604, значения:

- 1 класс
- 2 класс
- 3 класс
- 4 класс
- 5 класс
- 6 класс

- внесен новый Уровень сертификации «Средства контроля СМНИ», на соответствие «Требованиям к средствам контроля съемных машинных носителей информации», приказ ФСТЭК России от 28 июля 2014 г. № 87, зарегистрирован Минюстом России 5 сентября 2014 г., регистрационный № 33994, значения:

- 1 класс
- 2 класс
- 3 класс
- 4 класс
- 5 класс
- 6 класс

- внесен новый Уровень сертификации «ОУД», на соответствие РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий – Часть 3.Требования доверия к безопасности», Гостехкомиссии России, 2002, значения:

- ОУД1
- ОУД2
- ОУД3
- ОУД4
- ОУД5
- ОУД6
- ОУД7

- внесен новый Уровень сертификации «МЭ по НМД ФСБ России», на соответствие требованиям ФСБ России к устройствам типа межсетевые экраны, значения:

- 1 класс
- 2 класс
- 3 класс
- 4 класс
- 5 класс

- внесен новый Уровень сертификации «СКЗИ», на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам, значения:

- КА
- КВ2
- КВ1
- КС3
- КС2
- КС1

- внесен новый Уровень сертификации по «Заданию по безопасности», на соответствие РД «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», Гостехкомиссии России, 2002

- внесен новый Уровень сертификации «СОА по НМД ФСБ России», на соответствие требованиям ФСБ России к системам обнаружения компьютерных атак, значения:

- Класс А
- Класс Б
- Класс В
- Класс Г

Интерфейс «Средства и меры защиты»:

- внесены новые средства защиты, в составе:

- Аккорд NT/2000 v.3.0
- Аккорд-Win32
- Аккорд-Win64
- Аккорд-АМДЗ
- Аккорд-В.
- Аккорд-Х
- Аккорд-РАУ
- Secret Net 6
- Secret Net 6 (Вариант К)
- Secret Net 7 – Клиент
- Secret Net 7 – Сервер безопасности
- Secret Net 7 – Программа управления
- Secret Net LSP
- Соболь
- Соболь 3.0
- Security Studio Endpoint Protection 7.7
- АПКШ "Континент" 3.6 Крипто Шлюз
- Детектор атак "Континент" 3.7
- СКЗИ "Континент-АП" 3.6 (исполнение 3)
- СКЗИ "Континент-АП" 3.6 (исполнение 4)
- АПКШ "Континент" 3.М
- vGate R2

- vGate для Hyper-V
- TrustAccess
- Secret Disk 4
- Secret Disk Server NG 3.8
- Secret Disk Enterprise
- eToken Network Logon 5
- ViPNet Coordinator (Windows) 3.2
- ViPNet Coordinator (Linux) 3.2
- ViPNet Client 3.2 (исполнение 2)
- ViPNet Client 3.2 (исполнение 1)
- ViPNet Administrator 3.2 (исполнение 1)
- ViPNet Administrator 3.2 (исполнение 2)
- ПАК ViPNet IDS 2000 Q2 версии 2.0
- ПАК ViPNet IDS 2000 Q1 версии 2.0
- ПАК ViPNet IDS 1000 Q1 версии 2.0
- ViPNet SafeDisk 4.1
- ПАК ViPNet Coordinator KB1000 Q2
- ПАК ViPNet Coordinator KB100 X2
- ПАК ViPNet Coordinator HW
- DeviceLock 8
- NetworkLock 8
- XSpider 7.8.24

Интерфейс «Партии средств защиты»:

- внесены актуальные данные по сертификатам соответствия требованиям по безопасности информации указанных средств защиты