ОПИСАНИЕ РЕЛИЗА

Наименование продукта

Privacy-SPS.

Версия релиза

1.1.0.4

Дата релиза

24.06.2013 09.00

Описание ключевых изменений

Выполнен ряд правок связанных с принятием Приказа ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»:

- внесены новые классы средств защиты (интерфейс «Классы средств и мер защиты»):

  - Средства управления доступом к сети
  - Средства контроля целостности ПО
  - Средства защиты от спама
  - Меры управления идентификацией и аутентификацией
  - Меры по управлению разграничением доступа
  - Меры по защите беспроводного доступа
  - Меры по управлению программным обеспечением
  - Меры по управлению событиями безопасности
  - Меры по контролю защищенности технических средств, ПО и средств защиты
  - Меры по управлению инцидентами
  - Меры по управлению изменениями ИС и системы защиты
  - Средства защиты виртуальной инфраструктуры

- в интерфейсе «Функции безопасности» удалены не актуальные функции:

  - анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов
  - анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы
  - идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов
  - аутентификация взаимодействующих объектов сетей
  - двухфакторная аутентификация пользователей
  - доверенная загрузка операционной системы
  - идентификация программ, томов, каталогов, файлов, записей, полей записей по именам
  - идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам

- идентификация технических средств информационных систем и каналов связи, внешних устройств информационных систем по их логическим адресам (номерам)
- контроль копирования информации на съемные носители
- контроль отсутствия НДВ в программном обеспечении средств защиты информации
- обеспечение целостности программных средств системы защиты, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации
- обеспечение целостности программных средств системы защиты, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ
- обеспечение целостности программных средств системы защиты, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по наличию имен (идентификаторов) ее компонент, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;
- возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа
- регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства)
- регистрация кода или пароля, предъявленного при неуспешной попытке доступа в систему
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла
- регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам,

узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер))

- физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации
- физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации
- физическая охрана технических средств информационных систем (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания
- централизованное управление системой защиты
- аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных
- аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети
- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации
- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам
- контроль целостности своей программной и информационной части
- локальная сигнализация попыток нарушения правил фильтрации на межсетевом экране
- предотвращение доступа через МЭ неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась
- регистрация действия администратора межсетевого экрана по изменению правил фильтрации
- регистрация запуска программ и процессов (заданий, задач)
- регистрация и учет запросов на установление виртуальных соединений
- регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации)
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления
- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов,

процесса идентификации и аутентификации администратора межсетевого, экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления
- трансляция сетевых адресов для скрытия структуры информационной системы
- фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя
- фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя
- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов
- фильтрация с учетом даты и времени
- фильтрация с учетом любых значимых полей сетевых пакетов
- резервирование программных средств ИС

- в интерфейс «Функции безопасности» добавлены новые функции:

- обновление базы данных признаков вредоносных компьютерных программ (вирусов)
- обновление базы решающих правил
- обеспечение возможности восстановления ПДн с резервных машинных носителей ПДн (резервных копий) в течение установленного временного интервала
- идентификация и аутентификация пользователей, являющихся работниками оператора
- идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
- защита обратной связи при вводе аутентификационной информации
- идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
- реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между информационными системами
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС
- ограничение неуспешных попыток входа в ИС (доступа к ИС)

- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
- регламентация и контроль использования в ИС технологий беспроводного доступа
- регламентация и контроль использования в информационной системе мобильных технических средств
- управление взаимодействием с ИС сторонних организаций (внешние информационные системы)
- обеспечение доверенной загрузки средств вычислительной техники
- управление установкой (инсталляцией) компонентов ПО, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО
- установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
- управление доступом к машинным носителям персональных данных
- уничтожение (стирание) или обезличивание ПДн на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания
- определение событий безопасности, подлежащих регистрации, и сроков их хранения
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
- защита информации о событиях безопасности
- выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей
- контроль установки обновлений ПО, включая обновление ПО средств защиты информации
- контроль работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации
- контроль состава технических средств, ПО и средств защиты информации
- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС
- контроль целостности ПО, включая ПО средств защиты информации
- обнаружение и реагирование на поступление в ИС незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию ИС (защита от спама)

- контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
- идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
- регистрация событий безопасности в виртуальной инфраструктуре
- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
- контроль целостности виртуальной инфраструктуры и ее конфигураций
- резервное копирование данных, резервирование технических средств, ПО виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры
- реализация и управление антивирусной защитой в виртуальной инфраструктуре
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки ПДн отдельным пользователем и (или) группой пользователей
- контроль и управление физическим доступом к ТС, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены
- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
- разделение в ИС функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты ПДн, функций по обработке ПДн и иных функций ИС
- обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
- защита архивных файлов, параметров настройки средств защиты информации и ПО и иных данных, не подлежащих изменению в процессе обработки ПДн
- разбиение ИС на сегменты (сегментирование ИС) и обеспечение защиты периметров сегментов ИС
- защита беспроводных соединений, применяемых в информационной системе
- определение лиц, ответственных за выявление инцидентов и реагирование на них
- обнаружение, идентификация и регистрация инцидентов
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
- принятие мер по устранению последствий инцидентов

- планирование и принятие мер по предотвращению повторного возникновения инцидентов
- определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и системы защиты ПДн
- управление изменениями конфигурации ИС и системы защиты ПДн
- анализ потенциального воздействия планируемых изменений в конфигурации ИС и системы защиты ПДн на обеспечение защиты ПДн и согласование изменений в конфигурации ИС с должностным лицом (работником), ответственным за обеспечение безопасности ПДн
- документирование информации (данных) об изменениях в конфигурации ИС и системы защиты ПДн
- защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)

- в интерфейсе «Функции безопасности» заменены названия функций:

Старое название	Новое название
применение антивирусных средств	реализация антивирусной защиты
регистрация результата попытки в систему входа (успешная или неуспешная)	регистрация результата попытки входа в систему (успешная или неуспешная)
криптографическая защита канала связи	обеспечение защиты ПДн от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
обнаружение атак в сетевом потоке	обнаружение вторжений
резервирование защищаемых данных обрабатываемых в информационной системе	периодическое резервное копирование ПДн на резервные машинные носители ПДн

- в интерфейсе «Зависимость функций безопасности от архитектуры ИСПДн» и интерфейсе «Зависимость функций безопасности от угроз» появились дополнительные связи для новых функций указанных выше

- в интерфейс «Средства и меры защиты» добавлены новые средства (меры) защиты:

- Управление событиями безопасности (сбор, хранение, анализ, защита)
- Управление программным обеспечением (задание порядка установки, обновления, контроля работы)
- Контроль защищенности технических средств, ПО и средств защиты
- Меры физической защиты технических средств (контроль, разграничение доступа, резервирование)
- Управление инцидентами (обнаружение, ответственность, анализ, принятие мер)
- Управление изменениями ИС и системы защиты (ответственность, анализ и документирование изменений)

- изменен порядок формирования документа «Описание системы защиты» для более полного включения новых средств и мер защиты.

Обновляемые шаблоны документов

Описание системы защиты персональных данных

Порядок установки

1. Скопируйте файл обновления в директорию, где установлена серверная частью программы, по умолчанию «C\IRADD\SMS_srv»

2. Запустите файл, укажите параметры подключения к серверу:

- имя пользователя имеющего административные полномочия по доступу к базе данных, как правило «sa»,

- пароль пользователя,

- сервер в формате «доменное имя компьютера\имя экземпляра базы данных»,

- имя базы данных (по умолчанию «risk»).

3. Дождитесь окончания процесса обновления - в окне состояниям отобразится строка «Обновление завершено»