УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В СООТВЕТСТВИИ С ПРИКАЗОМ ФСТЭК РОССИИ № 21 ОТ 18 ФЕВРАЛЯ 2013 Г.

И.А. Щербинина, Н.А. Леонтьева

МГУ им. адм. Г.И. Невельского, Владивосток, Россия

Аннотация: Выбор мер защиты информации в информационных системах, обрабатывающих персональные данные представляет определённою сложность для специалистов практиков. Статья посвящена обзору возможностей наиболее распространённых средств защиты информации и соответствия их возможностей мерам по обеспечению безопасности персональных данных, определённым ФСТЭК России.

Ключевые слова: информационные системы персональных данных (ИСПДн), персональные данные (ПДн) средства защиты информации (СрЗИ), несанкционированный доступ (НСД).

Сегодня для большинства организаций, являющихся операторами информационных систем персональных данных, особую сложность представляет выбор необходимых средств защиты информации, соответствующих законодательству, в том числе СрЗИ от несанкционированного доступа. Несмотря на то, что рынок предлагает множество различных сертифицированных СрЗИ, многим специалистам пока сложно разобраться, как их функциональные возможности соответствуют приказу 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».

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках систем защиты ПДн с учётом актуальных угроз безопасности ПДн и применяемых информационных технологий, в соответствии с приказом ФСТЭК России № 21 входят:

* идентификация и аутентификация субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн;
* регистрация событий безопасности;
* антивирусная защита;
* обнаружение (предотвращение) вторжений;
* контроль (анализ) защищённости ПДн;
* обеспечение целостности информационной системы и ПДн;
* защита среды виртуализации;
* защита технических средств;
* защита ИС, её средств, систем связи и передачи данных;
* выявление инцидентов и реагирование на них;
* управление конфигурацией ИС и системы защиты ПДн.

В настоящее время среди основных игроков рынка СрЗИ от НСД можно выделить следующие продукты: Secret Net, Dallas Lock, Страж NT. СрЗИ Secret Net 7.0, Dallas Lock 8.0-C и Страж NT 3.0 соответствуют 2-му уровню контроля отсутствия недекларированных возможностей и 3-му классу защищённости от НСД (сертификаты ФСТЭК России № 2707, № 2945 и № 2145 соответственно), и могут использоваться для защиты информации в ИСПДн до 1-го класса включительно.

Приведём в таблице функциональные возможности вышеперечисленных СрЗИ от НСД в соответствии с приказом ФСТЭК России № 21.

Технические меры по обеспечению безопасности в соответствии с приказом ФСТЭК России № 21 и СрЗИ от НСД, помогающие их выполнить\*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Условное обозначение и номер меры | Меры по обеспечению безопасности ПДн | Уровни защищённости ПДн | Secret Net 7.0 | Dallas Lock 8.0-C | Страж NT 3.0 |
| 4 | 3 | 2 | 1 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Идентификация и аутентификация субъектов доступа и объектов доступа |
| 1 | ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | + | + | + | + | + | + |
| 2 | ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных и портативных |  |  | + | + | - | + | + |
| 3 | ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | + | + | + | + | + | + |
| 4 | ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | + | + | + | + | + | - |
| 5 | ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | + | + | + | + | + | + |
| 6 | ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + | + | + | + | - | + | + |
| Управление доступом субъектов доступа к объектам доступа |
| 7 | УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей, в том числе внешних пользователей | + | + | + | + | + | + | + |
| 8 | УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | + | + | + | + | + | + |
| 9 | УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС | + | + | + | + | + | + | + |
| 10 | УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС | + | + | + | + | - | + | + |
| 11 | УПД.6 | Ограничение неуспешных попыток входа в ИС (доступа к ИС) | + | + | + | + | + | + | + |
| 12 | УПД.8 | Оповещение пользователя после успешного входа в ИС о его предыдущем входе в ИС |  |  |  |  | - | + | - |
| 13 | УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учётной записи пользователя ИС |  |  |  |  | - | + | - |
| 14 | УПД.10 | Блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу |  | + | + | + | + | - | + |
| 15 | УПД.11 | Разрешение (запрет) действий пользователей, разрешённых до идентификации и аутентификации |  | + | + | + | + | + | + |
| 16 | УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе её хранения и обработки |  |  |  |  | + | + | + |
| 17 | УПД.14 | Регламентация и контроль использования в ИС технологий беспроводного доступа | + | + | + | + | + | + | + |
| 18 | УПД.15 | Регламентация и контроль использования в ИС мобильных технических средств | + | + | + | + | + | + | + |
| 19 | УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |  |  | + | + | + | + | + |
| Ограничение программной среды |
| 20 | ОПС.1 | Управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО |  |  |  |  | + | + | + |
| 21 | ОПС.2 | Управление установкой (инсталляцией) компонентов ПО, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО |  |  | + | + | - | - | + |
| 22 | ОПС.3 | Установка (инсталляция) только разрешённого к использованию ПО и (или) его компонентов |  |  |  | + | - | + | + |
| Защита машинных носителей ПДн |
| 23 | ЗНИ.1 | Учёт машинных носителей ПДн |  |  | + | + | + | - | + |
| 24 | ЗНИ.2 | Управление доступом к машинным носителям ПДн |  |  | + | + | + | - | + |
| 25 | ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием ПДн, хранящихся на машинных носителях, и (или) использования носителей ПДн в иных ИС |  |  |  |  | - | + | + |
| 26 | ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители ПДн |  |  |  |  | + | + | + |
| 27 | ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители ПДн |  |  |  |  | + | + | + |
| 28 | ЗНИ.7 | Контроль подключения машинных носителей ПДн |  |  |  |  | + | + | + |
| 29 | ЗНИ.8 | 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 |  | + | + | + | + | + | + |
| Регистрация событий безопасности |
| 30 | РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | + | + | + | + | + | + |
| 31 | РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | + | + | + | + | + | + |
| 32 | РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + | + | + | + | + | + | + |
| 33 | РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объёма (ёмкости) памяти |  |  |  |  | + | - | + |
| 34 | РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |  |  | + | + | + | + | + |
| 35 | РСБ.7 | Защита информации о событиях безопасности | + | + | + | + | + | + | + |
| Контроль (анализ) защищенности ПДн |
| 36 | АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ |  | + | + | + | + | + | - |
| 37 | АНЗ.4 | Контроль состава технических средств, ПО и СрЗИ |  | + | + | + | + | + | - |
| 38 | АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС |  |  | + | + | + | - | - |
| Обеспечение целостности информационной системы и персональных данных |
| 39 | ОЦЛ.1 | Контроль целостности ПО, включая ПО СрЗИ |  |  | + | + | + | + | + |
| 40 | ОЦЛ.2 | Контроль целостности ПДн, содержащихся в базах данных ИС |  |  |  |  | + | - | + |
| 41 | ОЦЛ.3 | Обеспечение возможности восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций |  |  |  |  | + | + | - |
| 42 | ОЦЛ.5 | Контроль содержания информации, передаваемой из ИС (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из ИС  |  |  |  |  | + | + | - |
| 43 | ОЦЛ.6 | Ограничение прав пользователей по вводу информации в ИС |  |  |  |  | + | + | - |
| Обеспечение доступности персональных данных |
| 44 | ОДТ.2 | Резервирование технических средств, ПО, каналов передачи информации, средств обеспечения функционирования ИС |  |  |  |  | + | - | - |
| 45 | ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |  |  |  | + | + | - | - |
| Защита среды виртуализации |
| 46 | ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + | + | + | + | + | + | - |
| 47 | ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |  | + | + | + | - | + | - |
| 48 | ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией |  |  |  |  | - | + | - |
| 49 | ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и её конфигураций |  |  | + | + | - | + | - |
| Защита информационной системы, ее средств, систем связи и передачи данных |
| 50 | ЗИС.1 | Разделение в ИС функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты ПДн, функций по обработке ПДн и иных функций ИС |  |  |  | + | + | - | + |
| 51 | ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и СрЗИ (функциями безопасности СрЗИ) |  |  |  |  | + | - | - |
| 52 | ЗИС.5 | Запрет несанкционированной удалённой активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |  |  |  |  | + | - | - |
| 53 | ЗИС.14 | Использование устройств терминального доступа для обработки ПДн |  |  |  |  | + | - | - |
| 54 | ЗИС.15 | Защита архивных файлов, параметров настройки СрЗИ и ПО и иных данных, не подлежащих изменению в процессе обработки ПДн |  |  | + | + | + | + | - |
| 55 | ЗИС.18 | Обеспечение загрузки и исполнения ПО с машинных носителей ПДн, доступных только для чтения, и контроль целостности данного ПО |  |  |  |  | + | - | - |
| 56 | ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти |  |  |  |  | + | - | - |
| Выявление инцидентов и реагирование на них |
| 57 | ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов |  |  | + | + | + | - | - |
| 58 | ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами |  |  | + | + | + | - | - |

\*Таблица составлена на основе информации, предоставленной разработчиками средств защиты [1], [2], [3] и в соответствии с приказом ФСТЭК России № 21.

Как видно из таблицы, каждое из описываемых СрЗИ имеет свои преимущества. СрЗИ Secret Net имеет больше функциональных возможностей в соответствии с приказом ФСТЭК России № 21, чем Dallas Lock и Страж NT, однако при этом в отличие от Dallas Lock имеет ограничения:

* несовместимость с редакциями операционных систем Windows, в которых отсутствует возможность подключения к домену и управление средствами групповых политик;
* необходимость установки русского языка в региональных настройках операционных систем Windows.

СрЗИ Страж NT в отличие от Secret Net и Dallas Lock функционирует в операционной системе Windows 2000, но не поддерживает работу в операционных системах Windows 8 (8.1) и Windows Server 2012 (R2).

Поэтому при выборе того или иного средства защиты необходимо учитывать не только формальное выполнение требований руководящих документов по защите информации, но и актуальные угрозы безопасности ПДн, применяемые информационные технологии в организации, совместимость с операционными системами защищаемых компьютеров и другие критерии, важные для организации.

Литература:

1. Подробная информация о выполнении мер защиты, определенных Приказом ФСТЭК России от 18.02.2013 г. № 21, при помощи продуктов компании «Код Безопасности»;
2. Возможность выполнения мер по защите информации с помощью Dallas Lock 8.0-C;
3. Сводная таблица по составу мер защиты информации для соответствующего класса защищенности информационной системы и реализация в СЗИ «Страж NT» (версия 3.0);
4. 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».