ТЕХНИЧЕСКИЕ НАУКИ

Кляус Татьяна Константиновна
студентка
Сухостат Валентина Васильевна
канд. техн. наук, доцент

ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
г. Санкт-Петербург

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ПРИМЕНЯЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация: *в данной статье авторами проведен сравнительный анализ наиболее распространенных средств защиты информации (СЗИ) от несанкционированного доступа (НСД), применяемых для защиты персональных данных в информационных системах персональных данных. Критерии сравнения выбраны исходя из характеристик СЗИ от НСД. Разработана методика сравнительного анализа СЗИ от НСД.*

Ключевые слова: *средства защиты информации, несанкционированный доступ, персональные данные, информационная система, персональные данные, методика сравнительного анализа.*

Для защиты информации в компьютерных системах от атак на уровне операционной системы, системы сетевого программного обеспечения и системы управления базами данных [1, с. 27] применяются средства защиты информации от несанкционированного доступа (СЗИ от НСД). Определяющим фактором выбора СЗИ от НСД в информационной системе персональных данных (ИСПДн) является соответствие нормам и требованиям уполномоченных органов в сфере

обработки персональных данных. Наиболее распространенными средствами защиты информации от несанкционированного доступа в ИСПДн семейства MS Windows являются средства: «Secret Net 7», «Dallas Lock 8.0-K», «Панцирь-К», «Аура 1.2.4» (могут быть применены для ИСПДн 1 уровня защищенности включительно) [3–7].

Все вышеперечисленные СЗИ являются сертифицированными программными средствами защиты информации, поддерживающими автономный и сетевой режим работы. Кроме того, они выполняют схожие функции, такие как:

1. Идентификация и аутентификация пользователей.

2. Разграничение и контроль доступа пользователей к ресурсам системы, терминалам, ЭВМ, узлам сети ЭВМ, внешним устройствам, программам, томам, каталогам, файлам и т. д. (реализуется дискреционный принцип контроля доступа).

3. Учет носителей информации.

4. Контроль целостности защищаемых ресурсов.

5. Контроль компонентов СЗИ.

6. Контроль вывода на печать и маркировка документов.

7. Уничтожение (затирание) содержимого файлов при их удалении.

8. Регистрация событий безопасности в журнале.

9. Теневое копирование выводимой информации.

В сетевом режиме СЗИ выполняют следующие функции:

1. Централизованное управление настройками СЗИ.

2. Централизованный сбор информации о событиях безопасности на защищаемых компьютерах.

Методика сравнительного анализа СЗИ от НСД «Secret Net 7», «Dallas Lock 8.0-K», «Панцирь-К», «Аура 1.2.4» приводится ниже.

Критериями для сравнительного анализа в настоящей работе выбраны следующие технические характеристики СЗИ от НСД [3–6]:

1. Класс защищенности.

2. Уровень контроля НДВ.

3. Класс автоматизированных систем.

4. Дополнительные аппаратные требования: требуемый объем свободного места на жестком диске для размещения СЗИ.

5. Дополнительная аппаратная поддержка: есть или нет.

Критерий стоимости СЗИ от НСД в настоящей работе не рассматривается.

Указанные технические характеристики для выбранных СЗИ от НСД приводятся в таблице 1.

Таблица 1

Технические характеристики СЗИ от НСД

Критерии сравнения	*Secret Net 7*	*Dallas Lock 8.0-K*	*Панцирь-К*	*СЗИ Аура 1.2.4*
Класс защищенности	По 3 классу защищенности	По 5 классу защищенности	По 5 классу защищенности	По 5 классу защищенности
Уровень контроля НДВ	По 2 уровню контроля	По 4 уровню контроля	По 4 уровню контроля	По 4 уровню контроля
Класс автоматизированных систем	До класса 1Б включительно	До класса 1Г включительно	До класса 1Г включительно	До класса 1Г включительно
Дополнительные аппаратные требования: свободное место на жестком диске	2,000 Гб	0,030 Гб	0,020 Гб	0,060 Гб
Дополнительная аппаратная поддержка	есть (Secret Net Card, ПАК «Соболь»)	нет	есть (ПАК контроля активности КСЗИ)	нет

Для оценки рейтинга СЗИ от НСД по критерию сравнения необходимо построить следующую матрицу показателей A_{ij} (таблица 2):

Таблица 2

Матрица показателей

Критерии сравнения	*Secret Net 7*	*Dallas Lock 8.0-K*	*Панцирь-К*	*СЗИ Аура 1.2.4*
Класс защищенности	*A11*	*A12*	*A13*	*A14*
Уровень контроля НДВ	*A21*	*A22*	*A23*	*A24*

Критерии сравнения	*Secret Net 7*	*Dallas Lock 8.0-K*	*Панцирь-К*	*СЗИ Аура 1.2.4*
Класс автоматизированных систем	*A31*	*A32*	*A33*	*A34*
Дополнительные аппаратные требования: свободное место на жестком диске	*A41*	*A42*	*A43*	*A44*
Дополнительная аппаратная поддержка	*A51*	*A52*	*A53*	*A54*

В данной матрице каждому показателю A_{ij} присваивается определенное числовое значение.

Поясним назначение числовых значений показателей A_{ij} на примере СЗИ от НСД «Secret Net 7». Класс защищенности, уровень контроля НДВ и класс автоматизированной системы выше, чем у остальных СЗИ, принятых для сравнительного анализа. С другой стороны, требуемый объем жесткого диска для реализации этого СЗИ значительно больше, что вводит ограничения на возможности аппаратных средств. Теперь необходимо ввести следующее правило для количественной оценки показателя A_{ij}: *показатель должен принимать тем большее значение, чем выше значимость выбранного критерия для принятия решения*. В данном конкретном случае, количественную оценку показателей для принятых критериев сравнения будем выполнять следующим образом:

A_{1J} = 1 / (Класс защищенности: 3 или 5);

A_{2J} = 1 / (Уровень контроля НДВ: 2 или 4);

A_{3J} = 1 / (Класс автоматизированных систем: 2 – для класса 1Б или 4 – для класса 1Г);

A_{4J} = 1 / (Требуемый объем жесткого диска в Гб);

$$A_{5J} = \begin{cases} 1 - \text{дополнительная аппаратная поддержка есть;} \\ 0 - \text{дополнительной аппаратной поддержки нет.} \end{cases}$$

Таким образом, нетрудно получить числовые значения матрицы показателей (таблица 3):

Таблица 3

Матрица показателей. Числовые значения

Критерии сравнения	*Secret Net 7*	*Dallas Lock 8.0-K*	*Панцирь-К*	*СЗИ Аура 1.2.4*
Класс защищенности	*1/3 = 0,333*	*1/5 = 0,200*	*1/5 = 0,200*	*1/5 = 0,200*
Уровень контроля НДВ	*1/2 = 0,500*	*1/4 = 0,250*	*1/4 = 0,250*	*1/4 = 0,250*
Класс автоматизированных систем	*1/2 = 0,500*	*1/4 = 0,250*	*1/4 = 0,250*	*1/4 = 0,250*
Дополнительные аппаратные требования: свободное место на жестком диске	*1/2,000 = 0,500*	*1/0,030 = 33,333*	*1/0,020 = 50,000*	*1/0,06 = 16,667*
Дополнительная аппаратная поддержка	*1,000*	*0,000*	*1,000*	*0,000*

Дальнейший сравнительный анализ проводится с помощью расчета рейтинга по критериям сравнения [2, с. 70–101].

Рейтинг по критерию сравнения определяется по формуле (1):

$$Rij = \frac{Aij - Ai\,min}{Ai\,max - Ai\,min} \times 100 \times Ki, \qquad (1)$$

где *Aij* – текущее значение показателя;

Aimin – минимальное значение показателя для указанного критерия;

Aimax – максимальное значение показателя для указанного критерия;

Ki – весовой коэффициент.

Далее по формуле (2) определяется итоговый рейтинг СЗИ от НСД:

$$Rj = \sum_{i=1}^{m} Rij, \qquad (2)$$

где *m* – количество критериев средства защиты информации.

Пример расчета по предложенной методике приводится ниже в таблицах 4 и 5. Весовые коэффициенты назначены из условия приоритетных требований по первым трем критериям сравнения.

Таблица 4

Исходные данные для расчета итогового рейтинга СЗИ от НСД

Критерии сравнения	*Secret Net 7*	*Dallas Lock 8.0-K*	*Панцирь-К*	*СЗИ Аура 1.2.4*	*Ai min*	*Ai max*	*Ki*
Класс защищенности	*0,333*	*0,200*	*0,200*	*0,200*	*0,200*	*0,333*	*0,30*
Уровень контроля НДВ	*0,500*	*0,250*	*0,250*	*0,250*	*0,250*	*0,500*	*0,30*
Класс автоматизированных систем	*0,500*	*0,250*	*0,250*	*0,250*	*0,250*	*0,500*	*0,30*
Дополни-тельные аппаратные требования: свободное место на жестком диске	*0,500*	*33,333*	*50,000*	*16,667*	*0,500*	*50,000*	*0,05*
Дополнитель-ная аппаратная поддержка	*1,000*	*0,000*	*1,000*	*0,000*	*0,000*	*1,000*	*0,05*

Таблица 5

Расчет итогового рейтинга СЗИ от НСД

Критерии сравнения	*Secret Net 7*	*Dallas Lock 8.0-K*	*Панцирь-К*	*СЗИ Аура 1.2.4*
Класс защищенности	*30,000*	*0,000*	*0,000*	*0,000*
Уровень контроля НДВ	*30,000*	*0,000*	*0,000*	*0,000*
Класс автоматизированных систем	*30,000*	*0,000*	*0,000*	*0,000*
Дополнительные аппаратные требования: свободное место на жестком диске	*0,000*	*3,316*	*5,000*	*1,633*
Дополнительная аппаратная поддержка	*5,000*	*0,000*	*5,000*	*0,000*
Итоговый рейтинг СЗИ от НСД Rj	*95,000*	*3,316*	*10,000*	*1,633*

Выводы.

1. В настоящей работе предложена методика сравнительного анализа СЗИ от НСД для выбранных критериев оценки.

2. С точки зрения технического уровня, из числа рассмотренных средств защиты информации, бесспорным преимуществом обладает СЗИ от НСД «Secret Net 7». Однако необходимо учитывать, что данное СЗИ может применяться не только для защиты конфиденциальной информации, но и для защиты секретной (сертифицирован по 3 классу защищенности СВТ и по 2 уровню контроля НДВ),

поэтому для защиты ИСПДн «Secret Net 7», в данном случае, избыточен. Далее приоритеты распределяются следующим образом: «Панцирь-К», «Dallas Lock 8.0-K» и СЗИ «Аура 1.2.4». Данное распределение носит лишь иллюстративный характер и в первую очередь, зависит от выбора критериев сравнения и весовых коэффициентов.

3. При выполнении сравнительного анализа средств защиты информации от несанкционированного доступа, следует учитывать также и стоимость приобретения и технической поддержки СЗИ от НСД.

Список литеоратуры

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.

2. Ивченко Б.П., Мартыщенко Л.А., Монастырский М.Л. Теоретические основы информационно-статистического анализа сложных систем. – СПб.: Лань, 1997. – 320 с.

3. Комаров А. СЗИ от НСД. Обзор рынка [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/blog/personal/zlonov/24114.php

4. Код безопасности. СЗИ от НСД Secret Net [Электронный ресурс]. – Режим доступа: http://www.securitycode.ru/products/secret_net/

5. Информационные технологии в бизнесе. КСЗИ Панцирь–К [Электронный ресурс]. – Режим доступа: http://www.npp-itb.spb.ru/products/nsdk.shtml

6. СЗИ от НСД Dallas Lock. Dallas Lock 8.0-K [Электронный ресурс]. – Режим доступа: http://www.dallaslock.ru/dallas-lock-80-k

7. НИО ПИБ. Система защиты информации «Аура 1.2.4» [Электронный ресурс]. – Режим доступа: http://www.cobra.ru/prod/aura1_24