DOI: https://doi.org/10.15688/NBIT.jvolsu.2022.4.3

УДК 004.056
ББК 32.97

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Наталья Алексеевна Головачева

Старший преподаватель, кафедра информационной безопасности,
Волгоградский государственный университет
golovacheva.natalya@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Никита Петрович Карпов

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBAS-191_665328@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье анализируются основные методы защиты конфиденциальной информации. Выделены критерии для адекватной оценки методов защиты конфиденциальных данных. В рамках экспериментальных исследований выявлен наилучший метод защиты конфиденциальных данных.

Ключевые слова: информационная безопасность, защита информации, угроза информационной безопасности, персональные данные, конфиденциальная информация, несанкционированный доступ, криптографическая защита информации.

В настоящее время большое внимание уделяется защите конфиденциальной информации – то есть информации, на доступ к которой имеет право ограниченный круг лиц. Это могут быть персональные данные граждан или секреты коммерческой деятельности фирм, или служебные и государственные тайны, или материалы судопроизводства. Для обеспечения защиты конфиденциальной информации требуется не только разработка отдельных механизмов и методов защиты, а необходим комплексный системный подход – комплекс мер, таких как использование программных, аппаратных, инженерных и криптографических средств; правовых и организационных мер. Среди способов сохранения конфиденциальных данных наиболее распространенными являются: сертификация данных, лицензирование, категоризация, аттестация.

Говоря о нормативно-правовых актах, мы обращаемся прежде всего к двум законам. К закону 152-ФЗ, описывающему правила работы с персональными данными, регулирующему работу с персональными данными конкретных лиц. Те, кто собирает и хранит эти данные (компании, которые ведут базу данных клиентов или сотрудников), должны их соблюдать. Этот закон гласит, что, если вы собираете личную информацию, вы должны хранить ее в секрете и защищать от посторонних. К закону 98-ФЗ, который определяет, что считается коммерческой тайной компаний. В нем объясняется, что такое коммерческая тайна, как ее защитить и что произой-

дет, если она станет известна посторонним. В нем определяется коммерческая тайна как информация, которая помогает компании увеличить доход, избежать расходов или помогает получить какую-либо коммерческую выгоду. А также мы обращаемся к Статьям 23, 24 Конституции РФ; к Статье 727 Гражданского кодекса РФ; Федеральному закону № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

Раскрытие конфиденциальной информации является одним из основных рисков безопасности. Конфиденциальность информации ограниченного доступа нарушается в случае разглашения или утечки.

Несанкционированный доступ (НСД) определяется в руководящем документе Государственной технической комиссии «Защита от несанкционированного доступа. Термины и определения» как доступ к информации, который нарушает правила контроля доступа с использованием стандартных инструментов, предоставляемых инструментами вычислительной техники или автоматизированными системами [2]. Самое главное в этом виде угроз – определить кто и к каким данным должен иметь доступ. НСД – это активное воздействие, использующее системные ошибки. С целью легализации он обращается к требуемому набору данных или действует на информацию о НСД. Любой системный объект может быть подвержен НСД.

Рассмотрим основные методы защиты конфиденциальной информации:

1. SIEM-системы.

Это комбинация двух классов программных продуктов: SEM (управление событиями безопасности) и SIM (управление информацией о безопасности). Первым классом пользуются для изучения безопасности в реальном времени, вторым – при долгосрочном хранении данных или при анализе в организациях информационных объектов.

2. Средства защиты информации от несанкционированного доступа (СЗИ от НСД).

Это программно-аппаратные средства, предотвращающие попытки НСД, в том числе уничтожение конфиденциальных данных.

3. Межсетевые экраны (брандмауэр).

Это программно-аппаратный элемент компьютерной сети, который осуществляет контроль и фильтрацию проходящего через нее сетевого трафика по установленным правилам. С помощью брандмауэра общую сеть разделяют на 2 и более части и применяют правила, которые определяют условия прохода пакетов с данными из одной части в другую. В большинстве случаев брандмауэры защищают локальную сеть компании либо от злоумышленников из глобальной сети Интернет, либо от атак из внутренней сети компании, к которой подключена локальная сеть компании.

4. Системы обнаружения вторжений (СОВ).

Это программно-аппаратные средства, которые используют для выявления фактов НСД к информационной системе или компьютерной сети, а также для выявления фактов несанкционированного управления ими через сеть Интернет [3]. СОВ повышают уровень безопасности рабочего места или сети.

5. Средства криптографической защиты информации (СКЗИ).

Это аппаратные, программные и программно-аппаратные средства, системы и комплексы, которые реализуют алгоритмы криптографического преобразования информации и которые предназначены для защиты информации при передаче по каналам связи от НСД при ее обработке и хранении. Шифрование считается одной из самых надежных форм защиты данных, так как защищает не доступ к информации, а саму информацию. Криптографически преобразованная информация имеет более высокую степень защиты, сохраняя большую секретность.

6. Сканеры безопасности.

Это средства проверки и мониторинга информационной безопасности, предназначенные для проверки информационной безопасности в корпоративных сетях.

7. Антивирусная защита.

Это комплекс профилактических и диагностических мер, которые применяются для защиты информационных систем от заражения вирусами – вредоносными программами, распространяющиеся по каналам связи с целью внедрения в код другого программного обеспечения, его блокировки или

нарушения работы программно-аппаратных комплексов [4].

Выделим организационные и технические меры защиты конфиденциальной информации в соответствии с ГОСТ Р 50922-2006:

1) защита конфиденциальной информации от утечки;

2) защита конфиденциальной информации от несанкционированного воздействия;

3) защита информации от непреднамеренного воздействия;

4) защита информации от разглашения;

5) защита информации от несанкционированного доступа;

6) защита информации от преднамеренного воздействия [1].

В связи с этим для анализа методов защиты конфиденциальных данных необходимо ввести следующие критерии для адекватной оценки:

– К1 – обеспечение защиты конфиденциальной информации от несанкционированного воздействия;

– К2 – обеспечение защиты конфиденциальной информации от утечки;

– К3 – обеспечение защиты информации от непреднамеренного воздействия;

– К4 – обеспечение защиты от информации от разглашения;

– К5 – обеспечение защиты от информации от несанкционированного доступа;

– К6 – обеспечение защиты от преднамеренного воздействия;

– К7 – эффективность обнаружения подозрительной активности;

– К8 – простота эксплуатации и настройки.

Качественные характеристики всех восьми критериев имеют низкое (н), среднее (с) и высокое (в) значения.

В таблице 1 указано значение критериев для оценки каждого метода защиты конфиденциальных данных.

Так как ни один из методов не обладает наилучшим набором значений критериев, необходимо разработать программное средство для автоматизации выбора наилучшего метода защиты конфиденциальных данных.

Была разработана математическая модель программного средства:

1. Входными параметрами является пользовательский набор требования, где каждое требование указывает на необходимость наличия функционала, согласно критерию оценивания.

2. Требования пользователя формируют вектор требований:

$$T = \{t_0, \ldots t_8\}, \quad (1)$$

где t_i – необходимость наличие функционала.

3. Множество средств защиты конфиденциальных данных:

$$A = \{a_0, \ldots a_6\}, \quad (2)$$

где a_j – средство: SIEM-системы; СЗИ от НСД; межсетевые экраны; СОВ; СКЗИ; сканеры безопасности; антивирусная защита.

4. Каждое средство также обладает вектором функциональных возможностей, определяемых матрицей, представленной в таблице 1.

Наиболее подходящее средство определяется по формуле:

$$AV = \max (AV_j), \quad (3)$$

где AV_j – оценка соответствия системы заявленным требованиям.

Таблица 1

Определение значений критериев для оценки каждого метода защиты

Метод защиты	Критерий							
	К1	К2	К3	К4	К5	К6	К7	К8
SIEM-системы	н	с	н	с	с	в	в	с
СЗИ от НСД	в	с	н	с	в	в	с	с
Межсетевые экраны	с	в	с	в	в	с	в	н
СОВ	в	с	с	в	в	в	в	с
СКЗИ	н	в	в	в	в	в	н	с
Сканеры безопасности	н	с	н	с	с	с	в	в
Антивирусная защита	в	н	с	с	с	в	с	в

Чем выше оценка AV_j, тем больше средство подходит при наборе требований.

Экспериментальные исследования по поиску наилучшего метода защиты конфиденциальных данных были проведены для трех случаев:

1. На вход программного средства подаются средние требования к методу защиты конфиденциальных данных.

2. На вход программного средства подаются высокие требования к методу защиты конфиденциальных данных.

3. На вход программного средства подаются низкие требования к методу защиты конфиденциальных данных.

В первом случае наилучшим при заданных требованиях является метод, при котором используются системы обнаружения вторжений (СОВ), набравший в результате оценки 8 условных единиц.

Во втором случае наилучшим при заданных требованиях являются:

– использование систем обнаружения вторжения (СОВ);

– использование средств криптографической защиты информации (СКЗИ).

Каждый из представленных методов набрал по 5 условных единиц оценки.

В третьем случае все представленные методы набирают максимально возможное количество баллов, это обуславливается тем, что мы требуем от методов защиты конфиденциальных данных наименьших обязательных показателей, которые априори должны соблюдаться.

В ходе анализа экспериментальных исследований была составлена таблица 2 для обобщения полученных результатов.

Исходя из результатов экспериментальных исследований, можно сделать вывод, что программное средство позволяет адекватно определить наилучший метод защиты конфиденциальных данных согласно требованиям и нуждам пользователя. Исходя из трех рассмотренных выше случаев, наилучшим методом являются системы обнаружения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Гончаров, А. М. Защита конфиденциальной информации (сведений конфиденциального характера) / А. М. Гончаров // RTM Group : [сайт]. – Электрон. текстовые дан. – Режим доступа: https://rtmtech.ru/articles/zashhita-konfidentsialnoj-informatsii/ (дата обращения: 18.11.2022). – Загл. с экрана.

2. Редькина, Н. С. Информационные технологии в вопросах и ответах / Н. С. Редькина. – Новосибирск : Изд-во ГПНТБ СО РАН, 2010. – 224 с.

3. Тезик, К. А. Фаервол Comodo Firewall : метод. указания по выполнению практ. работ студ. всех

Таблица 2

Результаты экспериментальных исследований

№ п/п	Требования	Определенные оценки	Наилучший метод
1	Средние требования по каждому критерию	SIEM-системы – 6 СЗИ от НСД – 7 МЭ – 7 СОВ – 8 СКЗИ – 6 Сканеры безопасности – 6 АВЗ – 7	СОВ
2	Высокие требования по каждому критерию	SIEM-системы – 2 СЗИ от НСД – 3 МЭ – 4 СОВ – 5 СКЗИ – 5 Сканеры безопасности – 2 АВЗ – 3	СОВ и СКЗИ
3	Низкие требования по каждому критерию	SIEM-системы – 8 СЗИ от НСД – 8 МЭ – 8 СОВ – 8 СКЗИ – 8 Сканеры безопасности – 8 АВЗ – 8	

форм обучения / К. А. Тезик. – Курск : Изд-во ЮЗГУ, 2018. – 15 с.

4. Энциклопедия «Касперского». – Электрон. текстовые дан. – Режим доступа: https://encyclopedia.kaspersky.ru/ (дата обращения: 18.11.2022). – Загл. с экрана.

REFERENCES

1. Goncharov A.M. *Zashhita konfidencial'noj informacii (svedenij konfidencial'nogo haraktera)* [Protection of Confidential Information (Confidential Information)]. URL: https://rtmtech.ru/articles/zashhita-konfidentsialnoj-informatsii/ (accessed 18 November 2022).

2. Redkina N.S. *Informacionnye tehnologii v voprosah i otvetah* [Information Technologies in Questions and Answers]. Novosibirsk, Izd-vo GPNTB SO RAN, 2010. 224 p.

3. Tezik K.A. *Faervol Comodo Firewall: metod. ukazanija po vypolneniju prakt. rabot stud. vseh form obuchenija* [Comodo Firewall: Methodological Instructions on the Implementation of Practical Works of Students of All Forms of Education]. Kursk, Izd-vo JuZGU, 2018. 15 p.

4. *Jenciklopedija «Kasperskogo»* [Kaspersky Encyclopedia]. URL: https://encyclopedia.kaspersky.ru/ (accessed 18 November 2022).

RESEARCH OF METHODS OF PROTECTION OF CONFIDENTIAL DATA

Natalia A. Golovacheva

Senior Lecturer, Department of Information Security,
Volgograd State University
golovacheva.natalya@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Nikita P. Karpov

Student, Department of Information Security,
Volgograd State University
IBAS-191_665328@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article analyzes the main methods of protecting confidential information. Organizational and technical measures to protect it are considered. Criteria for an adequate assessment of methods for protecting confidential data are highlighted. Within the framework of experimental studies, the best method of protecting confidential data has been identified. Currently, much attention is paid to the protection of confidential information - that is, information that a limited number of people have the right to access. This may be personal data of citizens or secrets of commercial activity of firms, official and state secrets, or materials of legal proceedings. As a result of the leakage of secret information, there is a loss of customers, a decrease in income, etc. Attackers can seize valuable information, damage the reputation of citizens, gain access to bank accounts, private and state secret documents. To ensure the protection of confidential information, not only the development of separate mechanisms and methods of protection is required, but a whole systematic approach is needed - a set of measures, such as the use of software and hardware, engineering and cryptographic tools; legal and organizational measures. The complex nature of protection arises from the complex actions of intruders who seek to obtain important information for them by any means. Among the methods of preserving confidential data, the most common are: data certification, licensing, categorization, certification. Disclosure of confidential information is one of the main security threats. The implementation of threats is the result of one of the actions and events: disclosure of confidential information, leakage of confidential information and unauthorized access to protected information. In case of disclosure or leakage, the confidentiality of restricted access information is violated.

Key words: information security, information protection, threat to information security, personal data, confidential information, unauthorized access, cryptographic information protection.