ОСНОВНЫЕ МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

И.А. Какорин, *студент*
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2023-2-2-22-24

Аннотация. *В статье описаны основные методы защиты конфиденциальной информации. К методам защиты информации относят средства, меры и практики, которые должны защищать информационное пространство от угроз – случайных и злонамеренных, внешних и внутренних. Рассмотрены следующие методы: использование надежных паролей, NGFW, прокси-сервера, антивирусов, SIEM, разграничение доступом, проведение аудита.*

Ключевые слова: *информационная безопасность, антивирусные программы, брандмауэр, методы защиты.*

Цифровые технологии представляют собой мощный потенциал развития современного общества, но они также могут нанести ущерб недооценивающим основные риски кибербезопасности. Необходимо защищать свою информацию, свои информационные системы. Рассмотрим основные полезные инструменты для защиты компьютерных данных [1-3].

1. Использование надежных паролей.

Доступ к компьютеру или к файлу по имени пользователя и паролю является первой формой защиты. Пароль должен быть индивидуальным, трудно угадываемым и храниться в тайне. Поэтому его не следует писать ни на каком носителе. Необходимо внедрить строгую политику управления паролями: пароль должен содержать не менее 8 символов, включая цифры, буквы и специальные символы, и должен часто обновляться (например, каждые 3 месяца).

2. Брандмауэр следующего поколения (NGFW Next Generation Firewall) для предотвращения вторжений.

Это система сетевой безопасности, которая обнаруживает и блокирует кибератаки, вмешиваясь на уровне приложения (обнаружение вредоносного программного обеспечения) и на уровне оборудования, применяя правила безопасности к порту или протоколу связи, через который проходят ваши цифровые потоки.

3. Прокси для защиты ваших данных.

Посредник между вашим веб-браузером и Интернетом, прокси-сервер позволяет защитить доступ к вашим данным, скрывая определенную информацию в случае анонимных прокси (IP-адрес, операционная система, веб-страницы). Подобно брандмауэру, он повышает безопасность, обнаруживая вредоносное ПО и блокируя подключение внешних компьютеров к вашему. Также прокси позволяет применять правила фильтрации согласно политике безопасности вашей организации (блокировка определенных сайтов, сайты, признанные опасными, не имеющими отношения к профессиональной деятельности, юридически или морально предосудительными и т.д.). А также возможна система аутентификации для ограничения доступа во внешнюю сеть, с возможностью ведения журналов (посещенные сайты, просмотренные страницы, пользователи и т.д.).

4. Использование антивирусных программ.

Антивирусная защита представляет собой основу для защиты ваших данных от известных вирусов, троянов и червей. Это программное обеспечение позволяет выявлять вредоносные программы, выявленные на ранней стадии распространения (вредоносное ПО) устраняется путем удаления или помещения в карантин.

5. Антиспам: остерегайтесь фишинговых писем.

Большая часть спама представляет собой просто нежелательные сообщения, часто рекламного характера. Но встречаются письма, которые вынуждают перейти по вредоносной ссылке, отправить данные через поддельную форму и т.д. Первая мера безопасности – никогда не открывать вложение незапрашиваемого сообщения, особенно если отправитель точно не идентифицирован. Таким образом, защита от спама является эффективным средством фильтрации сообщений от неизвестных отправителей. Но будьте осторожны, некоторые сообщения якобы отправлены вашими коллегами или знакомыми.

6. Информация о безопасности и управление событиями (SIEM).

Решения по управлению информацией и событиями безопасности (SIEM) обеспечивают анализ журналов безопасности, которые записываются сетевым оборудованием, серверами и программными приложениями, в режиме реального времени. Решения SIEM не только объединяют и коррелируют входящие события, но также могут выполнять ряд событий: удалять несколько отчетов в одном экземпляре, а затем действовать в соответствии с критериями оповещения и срабатывания. Как правило, они также предоставляют набор инструментов анализа, позволяющих находить только интересующие вас события, например события, связанные с безопасностью данных. Решения SIEM необходимы для расследований безопасности данных.

7. Контроль доступа.

В большинстве случаев пользователям не должно быть разрешено копировать или хранить конфиденциальные данные локально; вместо этого они должны быть вынуждены пользоваться данными удаленно. В идеале конфиденциальные данные никогда не должны храниться ни в одной локальной системе. Все системы должны требовать подключения того или иного типа и иметь условия для блокировки системы в случае сомнительного использования. Кроме того, доступ к конфиденциальным файлам должен иметь только авторизованный пользователь. Разрешения должны предоставляться пользователям в строгом соответствии с принципом наименьших привилегий. Список управления доступом (ACL) указывает, кто может получить доступ к какому ресурсу и на каком уровне. Это может быть внутренний компонент операционной системы или приложения. Списки контроля доступа могут быть белыми или черными списками. Белый список – это список разрешенных элементов; черный список – это список запрещенных вещей. В процессе управления файлами чаще используются белые списки управления доступом, и они настраиваются на уровне файловой системы. Например, в Microsoft Windows, вы можете настроить разрешения NTFS и создать из них NTFS ACL.

8. Аудит.

Чтобы должным образом защитить вашу конфиденциальную информацию, вам также необходимо проверять изменения в ваших системах и попытки доступа к вашим важным данным. Например, любая учетная запись, в которой превышено максимальное количество неудачных попыток входа в систему, должна автоматически сообщаться администратору информационной безопасности для расследования. Крайне важно иметь возможность обнаруживать изменения в конфиденциальной информации и соответствующих разрешениях. Необходимо знать, как используются конфиденциальные данные, кто их использует и как они перемещаются, это поможет разработать эффективные и точные стратегии для защиты информации и предвидеть потенциальные угрозы, влияющие на безопасность. Этот процесс также позволяет выявить ранее неизвестные риски.

Заключение. Важно понимать, что ни одна система безопасности не способна дать 100% гарантию на защиту данных. Но многоуровневая комплексная система защиты информации однозначно эффективнее, чем применение отдельных методов обеспечения информационной безопасности.

Библиографический список

1. Попов, Г.А. Анализ методов обнаружения DDOS-АТАК / Г.А. Попов, С.В. Петренко // Безопасность информационных систем и технологий в условиях цифровой экономики: Материалы IX Всероссийской научно-практической конференции с международным участием, Волгоград, 27-28 октября 2021 года / Редколлегия: О.А. Какорина, Ю.С. Бахрачева, Т.А. Попова. – Волгоград: Волгоградский государственный университет, 2021. – С. 72-76.
2. Дегтярев, Д.И. Безопасная компиляция и архитектуры защищенных модулей / Д.И. Дегтярев, О.А. Какорина // Безопасность информационных систем и технологий в условиях цифровой экономики: Материалы IX Всероссийской научно-практической конференции с международным участием, Волгоград, 27-28 октября 2021 года / Редколлегия: О.А. Какорина, Ю.С. Бахрачева, Т.А. Попова. – Волгоград: Волгоградский государственный университет, 2021. – С. 23-26.
3. Автоматизация процесса определения класса защищенности информационной системы и мер для ее защиты / С.П. Сазонов, Н.И. Федонюк, М.А. Кузнецова [и др.] // Защита информации. Инсайд. – 2021. – № 3 (99). – С. 44-46.

KEY METHODS OF PROTECTING CONFIDENTIAL INFORMATION

I.A. Kakorin, *Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *The article describes the main methods of protecting confidential information. Methods of information protection include means, measures and practices that should protect the information space from threats – accidental and malicious, external and internal. The following methods are considered: the use of strong passwords, NGFW, proxy server, antiviruses, SIEM, access control, auditing.*

Keywords: *information security, anti-virus programs, firewall, methods of protection.*