

УДК 001.8

DOI 10.51691/2541-8327_2023_4_24

***ПРИМЕНЕНИЕ НАУЧНО-ТЕХНИЧЕСКИХ МЕТОДОВ ДЛЯ ЗАЩИТЫ
ИНФОРМАЦИИ В ИНТЕРНЕТЕ***

Клейменкин Д.В.

магистрант,

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в

г. Шахты,

Шахты, Россия

Аннотация

Статья посвящена проблеме развития научно-технических методов и расширению возможностей интернета, из-за возрастания числа угроз для информационной безопасности. Автор утверждает, что современные научно-технические методы, такие как криптография, контроль доступа и системы обнаружения и предотвращения вторжений, позволяют защитить информацию от несанкционированного доступа. Автор считает, что многие научные методы постоянно совершенствуются, что предоставляет возможность эффективно бороться с новыми угрозами. Автор приходит к выводу о том, что применение научно-технических методов для защиты информации в интернете выступает ключевым фактором обеспечения информационной безопасности в современном мире.

Ключевые слова: научный метод, шифрование, контроль доступа, защита информации.

***APPLICATION OF SCIENTIFIC AND TECHNICAL METHODS TO PROTECT
INFORMATION ON THE INTERNET***

Kleimenkin D.V.

master's student,

Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,

Shakhty, Russia

Abstract

The article is devoted to the problem of the development of scientific and technical methods and the expansion of the Internet, due to the increase in the number of threats to information security. The author argues that modern scientific and technical methods, such as cryptography, access control and intrusion detection and prevention systems, can protect information from unauthorized access. The author believes that many scientific methods are constantly being improved, which makes it possible to effectively deal with new threats. The author comes to the conclusion that the use of scientific and technical methods to protect information on the Internet is a key factor in ensuring information security in the modern world.

Keywords: scientific method, encryption, access control, information protection.

В век компьютерных технологий проблема защиты информации на сегодняшний день стоит так остро, как никогда ранее. Несомненно, существование глобальной сети привнесло достаточно много положительных моментов в жизнь миллионов людей в плане работы с информацией, однако сейчас становится все труднее сохранять конфиденциальность любых личных данных. Особенно сложной является защита информации в сети Интернет, где все данные имеют достаточно большой доступ широкому кругу пользователей [1]. Ни один пользователь не может быть застрахован от того, что в его личное пространство не вторгнется посторонний и получит возможность воспользоваться полученной информацией по своему усмотрению.

ЭЛЕКТРОННЫЙ НАУЧНЫЙ ЖУРНАЛ «ДНЕВНИК НАУКИ»

Для развития и большей применимости научно-технических методов обратимся к характеристикам основных теоретических методов.

Можно выделить основные теоретические методы научного исследования, это, прежде всего, индукция и дедукция, они отражают типы и ход мышления[2]:

1. Индукция представляет собой движение мысли от частного к общему.

Проблематичный характер большинства индуктивных выводов требует их многократной проверки практикой, сопоставления с опытом следствий, выводимых из индуктивного обобщения. По мере того, как эти следствия совпадают с результатом опыта, увеличивается степень достоверности индуктивного вывода. В этом процессе обоснование знаний, полученных путём индукции, обязательно предполагает движение от индуктивных обобщений к тому или иному частному случаю. Тем самым, можно резюмировать то, что индукция дополняется дедукцией, что и обеспечивает переход от вероятностного к достоверному знанию.

2. Противоположным методом является дедукция, ее возможность в том, что частное вытекает из общего.

В технических науках чаще всего срабатывает аксиоматический метод. Это тот, который был основан в Древней Греции в V веке до нашей эры. Сфера его применения – геометрия. Фундаментальная работа этого этапа «Элементы Евклида», хотя считается, что до него древнегреческий математик Пифагор уже разработал аксиоматический метод. Таким образом, Древние греки принимают определенные факты за аксиомы, утверждения, не требующие каких-либо логических доказательств, то есть без необходимости демонстрации, поскольку содержащиеся в них постулаты неоспоримы. Намного позже в XIX веке немецкий математик Д. Гильберт формализует математический научный язык, где составляющие были позиционированы как формулы или последовательности знаков, которые сами по себе не имеют никакого значения.

Они приобретают смысл только в определенной интерпретации, в рамках математического поля. В старой системе аксиоматическая теория основана на доказательстве утверждений. В то время как основа формальной теории дана демонстрацией непротиворечивости ее аксиом. Математические методы являются полноценной иллюстрацией применения дедуктивного метода.

Специфика дедуктивного метода состоит в начале процесса задается набор базовых положений, они не требуют доказательств и принимаются за явные, по сути, являются аксиомой.

Применение научно-технических методов в области защиты информации является необходимым условием для обеспечения надежной защиты информации. В настоящее время, для обеспечения надежной защиты информации используются различные научные методы, такие как шифрование, контроль доступа, методы обнаружения и предотвращения атак [3].

Один из наиболее распространенных методов защиты информации в технических науках – это шифрование. Метод шифрования – это процесс преобразования информации в нечитаемый вид (шифр), который может быть прочитан только с помощью ключа дешифрования. Целью шифрования является защита конфиденциальности данных от несанкционированного доступа или чтения. Существует множество методов шифрования, включая симметричные и асимметричные шифры, шифры замены и перестановки, блочные и поточные шифры, и многие другие. Каждый метод имеет свои преимущества и недостатки, и выбор метода зависит от конкретных потребностей и требований к защите информации. Создано множество атак, которые могут быть использованы для взлома шифрования, включая атаки перебора, атаки словаря и многие другие. Поэтому важно выбирать достаточно сильный метод шифрования и ключ дешифрования должен храниться в безопасном месте. Кроме того, разработчики метода шифрования должны постоянно следить за новыми уязвимостями и улучшать свои методы

шифрования, чтобы предотвратить возможные атаки и обеспечить безопасность данных.

Другой метод защиты информации – контроль доступа [4]. Он основан на определении прав доступа для каждого пользователя или группы пользователей. Права доступа могут определять, какая информация доступна для чтения, записи или обновления, и могут быть установлены на уровне пользователя, группы или роли. Целью метода контроля доступа является обеспечение конфиденциальности и целостности данных, а также предотвращение несанкционированного доступа к информации.

Также для защиты информации используются методы обнаружения и предотвращения атак. Для этого используются методы анализа сетевого трафика, анализа поведения пользователей и технологии машинного обучения.

Существует множество приемов, разработанных в рамках научно-технических методов для обнаружения и предотвращения «атак», включая следующие [5]:

- Создание препятствий для предполагаемого злоумышленника с помощью физических и программных средств.
- Управление или влияние на элементы защищаемой системы.
- «Маскирование» или преобразование данных с использованием криптографических методов.
- Регулирование или разработка законодательства и комплекса мер, направленных на поощрение надлежащего поведения пользователей, работающих с базами данных.
- Принуждение или создание условий, при которых пользователь будет вынужден соблюдать правила обращения с данными.
- Поощрение или создание среды, которая мотивирует пользователей действовать должным образом.

Каждый метод реализуется с помощью различных средств. Основными средствами являются организационные и технические.

В заключении отметим, что использование научных методов в области защиты информации является необходимым условием для обеспечения надежной защиты информации. Развитие данных методов и их применение в практике позволяют существенно повысить уровень защиты информации от внешних угроз. При помощи анализа и специфики модели можно построить систему контроля информации в интернете и защитить пользователей от несанкционированного доступа к личным данным.

Библиографический список

1. Protecting information on the Internet – is it important [Электронный ресурс] — Режим доступа — URL: <https://ilovevaquero.com/zakon/112730-zaschita-informacii-v-internete-vazhna-li-ona.html> (Дата обращения: 10.04.2023).

2. Основные методы научного исследования [Электронный ресурс] — Режим доступа — URL: <https://sibac.info/blog/osnovnye-metody-nauchnogo-issledovaniya#2-kakie-byvajut-teoreticheskie-metody> (Дата обращения: 10.04.2023)

3. Мавлянова Л. Т. Защита информации в интернет // ORIENSS. 2022. №1. Режим доступа — URL: <https://cyberleninka.ru/article/n/zaschita-informatsii-v-internet> (Дата обращения: 11.04.2023).

4. Дударь З. В., Збитнева М. В. Анализ средств контроля доступа и защиты информации от сетевых атак // Радиоэлектроника и информатика. 2007. №1. Режим доступа — URL: <https://cyberleninka.ru/article/n/analiz-sredstv-kontrolya-dostupa-i-zaschity-informatsii-ot-setevyh-atak> (Дата обращения: 11.04.2023).

5. Methods to Protect Information | Methods and Tools for Data Protection [Электронный ресурс] — Режим доступа — URL: <https://searchinform.com/infosec-blog/2019/11/06/data-protection/methods-to-protect-information/> (Дата обращения 11.04.2023).

Оригинальность 92%