УДК 004

МЕТОДЫ И ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Станислав Владимирович Самородов
студент
samorodovs@yandex.ru
Наталия Владимировна Пчелинцева
старший преподаватель
natas79@mail.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассматриваются общие вопросы организации методов и средств защиты информации, а также представлены принципы защиты и виды угроз.

Ключевые слова: защита информации, конфиденциальность, угрозы, криптография.

В современном мире информация играет огромную роль. При помощи информаци человечество может передавать свой опыт, сохранять память о прошлом, стимулировать развитие различных сфер общественной жизни, таких как экономика, политика и тд. Но с развитием информационных технологий возникла проблема угроз, которые связанны с похищением, повреждением и распространением личной и секретной информации. Поэтому были созданы определенные методы и принципы защиты данных.

Защита информации основывается на трех принципах:

1. Конфиденциальность. Принцип заключается в том, что все данные переводят в шифр, непригодный и неразборчивый вид, в основном используют алгоритм шифрования. Это защищает информацию от незаконного доступа или утечки во вне.

2. Целостность. Информация не должна видоизменяться без разрешения владельца. Для защиты аккаунта от взлома рекомендуется использовать двухфакторную аутентификацию. Для того, чтобы не произошел взлом защиты корпоративных данных, рекомендуется давать сотрудникам только те данные, которые необходимы непосредственно для работы.

3. Доступность. Специальные сотрудники должны иметь больший доступ, чтобы в случае утечки или нечаянных сбоев можно было восстановить данные или резервно скопировать их, при этом не мешая работе [1, 2].

Для того, чтобы определить, что необходимо делать при угрозе защиты информации необходимо узнать какой это вид угроз: естественный или искусственный.

Естественные угрозы – вызванный воздействием на автоматизированную систему, ее частей из вне. Также это могут быть природные явления, не имеющие отношения к человеку.

Икусственные - угроза информации, напрямую связаная с человеком. Среди них можно выделить:

- преднамеренные – связаные с корыстными целями;

•непреднамеренные – вызванные ошибками в программном обеспечении, ошибках в проектировании и т. д.

Также существуют несколько основных видов угрозы информационной безопасности:

•Несанкционированный доступ. Доступ к информационным системам могут получиь постороние люди или злоумышленники, не имеющие развршенного доступа.

•Нарушение целостности – подразумевает неизменность информации. Угроза нарушения информационной безопасности может означать случайное или намеренное изменение данных без согласия пользователя.

•Раскрытие информации. Данный тип угрозы означает утечку и оглашение информации, которая должна быть исключительно конфиденциальной.

Методы защиты – способы и приспособления для обеспечения безопасности и конфиденциальности информационных данных. Эти методы помогают предотвратить изменение, уничтожение информации.

Физическая защита представляет собой меры, которые принимаются для физической защиты доступа к информации. Принципы физической защиты:

• Контроль доступа. Это двери, замки и любые другие физические барьеры, способные ограничить доступ к помещению, в котором содержится оборудование с информацией.

• Физическая охрана. Наличие службы безопасности позволяют обеспечить патрулирование территории, проверку удостоверений личности и быстрое реагирование на экстренные ситуации.

• Видеонаблюдение. Камеры видеонаблюдения помогают контролировать и записывать действия, происходящие внутри помощения [3, 4].

Криптографическая защита.

Криптография – наука о методах, позволяющих обеспечить конфиденциальность и целостность инфомации.

Криптографическая защита – защита с помощью криптографических алгоритмов. Она пользуется большой популярностью, поскольку его используют для защиты экономических действий, личных данных.

Основные методы включают в себя:

- Асимметричное шифрование разделяется на несколько ключей: публичный и приватный. Публичный ключ используют для шифровки данных, а приватный для их расшифровки.
- В симметричном шифровании используют один и тот же ключ как для шифрования, так и для расшифровки.

Аутентификация и авторизация.

Аутентификация – процесс проверки на подлинность устройства или пользователя. Осуществляется за счет проверки пароля, логина, иногда даже отпечатка пальца. Целью такой проверки является установление личности пользователя, и является ли он тем, за кого себя выдает. Методы аутентификации бывают самые разные. Например, биометрическая аутентификация основывается на уникальных физических данных: формах лица, сетчатке глаза, отпечатке пальца.

Авторизация – процесс определения прав доступа пользователя к определенным информационным данным. У нее есть уникальная особенность, потому что у кажого человека имеется своя определенная роль, определяющая право доступа [5].

Есть еще масса принципов и методов, помогающих защитить информацию как от внешнего вмешательства, так и от нечаянного действия: принцип защиты информации, защита от вредоносного программного обеспечения и т. д. Каждый из этих методов дополняет друг друга, помогая создавать мощное средство защиты.

Методы и принципы защиты информации представляют собой полноценную систему, направленную на обеспечение защиты от различных угроз. Но из-за постоянного развития технологий, необходимо постоянно совершенствовать методы защиты информации.

Список литературы:

1. Матросова С. А., Пчелинцева Н. В., Мещерякова А. А. Цифровизация в животноводстве (на примере предприятий Тамбовской области) // Наука и Образование. 2022. Т. 5. № 2.

2. Прокопов Д.С. Защита информации. Виды защиты информации // В сборнике: Передовые инновационные разработки. Перспективы и опыт использования, проблемы внедрения в производство. сборник научных статей по итогам второй международной научной конференции. 2019. С. 133-134.

3. Пчелинцева Н.В. Цифровизация животноводства: проблемы и перспективы развития // В сборнике: НАУКА, ОБРАЗОВАНИЕ И ИННОВАЦИИ ДЛЯ АПК: состояние, проблемы и перспективы. Материалы VII Международной научно-практической онлайн-конференции. Майкоп. 2022. С. 273-275.

4. Пчелинцева Н.В., Чепраков И.В., Гущина А.А. К вопросу применения криптографии // Наука и Образование. 2022. Т. 5. № 2.

5. Чехун Г.Н. Защита информации. Цели защиты информации // Говор: альманах. 2013. № 10-1. С. 286-293.

UDC 004

METHODS AND PRINCIPLES OF INFORMATION PROTECTION

Stanislav V. Samorodov
student
samorodovs@yandex.ru
Natalia V. Pchelintseva
senior lecturer
natas79@mail.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Annotation. The article discusses the general issues of the organization of methods and means of information protection, as well as the principles of protection and types of threats.

Keywords: information protection, confidentiality, threats, cryptography.

Статья поступила в редакцию 03.05.2024; одобрена после рецензирования 13.06.2024; принята к публикации 27.06.2024.

The article was submitted 03.05.2024; approved after reviewing 13.06.2024; accepted for publication 27.06.2024.