ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ОБЯЗАННОСТИ)

Зарипова Г.К.[1], Рамазонов Ж.Ж.[2]

[1]Зарипова Гулбахор Камиловна - кандидат педагогических наук, доцент,
кафедра гуманитарных наук,
Бухарский государственный университет;
[2]Рамазонов Жахонгир Жалолович – ассистент,
кафедра гуманитарных наук
Бухарский филиал
Ташкентский институт инженеров ирригации и механизации сельского хозяйства,
г. Бухара, Республика Узбекистан

Аннотация: *статья посвящена обеспечению информационной безопасности и защите информации, безопасности информации. Кроме того, информация в электронном вирусе является надежным инструментом для эффективной работы антивирусного программного обеспечения.*
Ключевые слова: *информационная безопасность, шифрование, декодирование цифровой подписи, идентификация, криптография, компьютерные вирусы, программные компоненты антивирусов, программа предусмотрены блоки для защиты в комплексе от внешних угроз.*

Информационная безопасность означает, что мы используем случайные или предсказуемые природные или искусственные неблагоприятные последствия, включая информацию, которая используется для нарушения информационной инфраструктуры, включая информацию мы понимаем, что информация защищена их владельцами. Защита информации – это комплекс мер, направленных на обеспечение информационной безопасности.

Основными организаторами информационной безопасности являются следующие категории: предоставление инфраструктуры и поддержка конфиденциальности, целостности и доступности информационных ресурсов. Первый Президент Республики Узбекистан Ислам Каримов в своей книге: «Национальная экономика, политика, идеология»: «сотрудничество с западным миром современных технологий, привлечение инвестиций в отрасли, ведущей сеть, открывает путь к комплексному использованию природного сырья. Важно оказывать помощь хорошо подготовленным специалистам, особенно в области банковского дела и управления, создавать информационные сети, устанавливать отношения с ведущими мировыми рынками и изучать зарубежный опыт». В школе, академических лицеев и профессиональных колледжей и системы высшего образования и применять их в результате независимой страны, которая полностью отвечает требованиям международных стандартов, молодежи возможность достичь совершенной человеческой формы, как [1, 59].

Использование – это возможность получить необходимое информационное обслуживание в течение определенного периода времени. Целостность – это доступность информации, защищенная от разрушения и несанкционированная модификация. Возможность изменять информацию должна быть доступна только тем, кто имеет право на участие. Конфиденциальность. Эта информация защищена от несанкционированного доступа и может быть предоставлена только для информации.

Основными методами защиты информации являются контроль доступа, который является способом защиты использования всех информационных систем и ресурсов информационных технологий. Такие методы должны исключать доступ к несанкционированному доступу к информации. Управление разрешениями включает в себя следующие защитные функции: идентификация пользователей, персонала и системных ресурсов (предоставление персональной идентификации каждому объекту); Идентификация объектов или предметов по указанному идентификатору (подлинность); проверить, что они имеют право на использование; Регистрация ссылок на охраняемые ресурсы; включая сенсорные предупреждения, выключение системы, выключение системы, игнорирование запросов при попытке доступа к несанкционированному доступу.

Идентификация и аутентификация могут рассматриваться как важный программно-технический инструмент, поскольку остальные службы предназначены только для самих субъектов. Идентификация и аутентификация – это отправная точка для доступа к корпоративной информации. Сочетание процедур идентификации и аутентификации признается в качестве процедуры авторизации. Идентификация позволяет субъектам (пользователям, действиям и субъектам от имени конкретного пользователя) идентифицировать свою личность. Аутентификация позволяет узнать, кто на самом деле другой. Иногда слово «аутентификация» используется как синоним «аутентификации».

Аутентификация имеет два типа: односторонний (обычно аутентификация клиент-клиент) и двухсторонний (обе стороны подтверждают подлинность). Примером односторонней миграции аутентификации является возможность входа в систему.

Один из способов аутентификации компьютерных систем, введя имя пользователя, просто набрав логин (английское имя – список) и пароль - это какая-то конфиденциальная информация. Надежные пароли и логин хранятся в конкретной базе данных.

Простая аутентификация состоит из следующих общих алгоритмов: Преемник запрашивает доступ к системе и вводит персональный идентификатор и пароль; возвращенные нежелательные данные сравниваются со стандартом на сервере аутентификации; Успешным является тот случай, когда данные соответствуют аутентификации сертификата, в противном случае будет неудачным.

Существуют также криптографическая криптографическая защита (приветствия с приветствиями), представляющая собой набор идей и методов, связанных с изменением информации для защиты информации от неавторизованных пользователей, Информация представлена в виде текстового сообщения. Такая информация называется открытым текстом. Изменение его в защищенный режим, шифрование, шифрование и модифицированный текст – криптография. Криптография, т. Е. Перенос текста в чистый текст, осуществляется путем дешифрования. Используется дополнительная информация, которая используется в качестве ключа для шифрования и расшифровки. Ключ является ключом к шифрованию. Чтение криптографов в течение ограниченного периода времени без знания ключа должно быть чрезвычайно сложным или невозможным. Шифрование является одним из компонентов притологии и является информацией о передаче информации из неавторизованного доступа. Шифрование, как описано, шифруется и дешифруется секретным ключом данных. Другой компонент криптографии – криптоанализ – должен заниматься теорией удаления информации без криптографии [4]. Современное шифрование состоит из четырех основных разделов: симметричных криптосистем; криптосистемы с открытым исходным кодом; системы электронной цифровой подписи, управление ключами.

Симметричные криптосистемы включают алгоритмы, которые реализуют шифрование и дешифрование с помощью одного ключа. Эти алгоритмы иногда называют секретными алгоритмами. При работе с такими системами отправитель и получатель должны иметь возможность использовать ключ, который вы хотите использовать с ранее скрытым каналом. Эффективные криптографические системы защиты включают в себя четкие криптоанализаторы, другими словами асимметричные криптосистемы. В таких системах, если ключ используется для шифрования данных, для дешифрования используется другой ключ (отсюда слово асимметрично). Первый ключ известен всем пользователям системы и используется для шифрования данных. Данные не могут быть декодированы с помощью открытого ключа. Дешифрованные данные используются пользователем для дешифрования второго ключа – секретногоключа. Обратите внимание, что ключ дешифрования не может быть найден с использованием ключа, используемого при шифровании.

Электронная цифровая подпись (ЕДС) является доказательством электронного документа, используемого для защиты электронного документа от фальсификации и подтверждения источника информации. Цифровая подпись состоит из серии символов, созданных криптографическим изменением электронного документа. ЭДС будет добавлен в блок данных для защиты источника данных от источника данных, целостности целостности данных. Электронная цифровая подпись генерируется криптографическим изменением с помощью специального программного обеспечения и секретного ключа электронной цифровой подписи. ЭДС улучшает поток электронных документов и обеспечивает надежность документа. Если исходный текст будет изменен добровольно, ЭДС не будет действительным. Каждый, кто использует электронную цифровую подпись, участвуя в обмене электронными документами, сможет генерировать один открытый и секретный криптографический ключ. Важным элементом этого является секретный ключ: он зашифрован электронными документами и создается электронная цифровая подпись [2]. Секретный ключ также доступен пользователю через отдельных носителей: они могут быть гибким диском, смарт-картой. Он должен храниться в секрете от других пользователей в сети. Открытый ключ используется для проверки подлинности ЭДС. Копия открытых ключей хранится в Центре сертификации. Центр сертификации будет защищать ваш реестр и защищать открытый ключ от ошибок и фальсификаций. Средства защиты от вирусов включают в себя защиту информации [3].

Компьютерный вирус – это специализированная программа, которая создает копию без взаимодействия с пользователем и позволяет им развертывать различные объекты компьютерных систем и сетей. Эта копия позволит вам распространять ее позже. Основная антивирусная программа – это антивирусное программное обеспечение, и существует несколько основных способов обнаружения и защиты вирусов. Это: сканеры – последовательность файлов для сканирования для поиска известных сигнатур вирусов. Его можно использовать для поиска известных и узнаваемых вирусов, таких как: обнаружение полиморфных и полиморфных вирусов, которые могут полностью модифицировать свой код при обнаружении новой программы или загрузочного сектора; анестезиологический анализ – идентификация неизвестных вирусов; Использование антивирусного мониторинга. Автоматическая проверка всех запущенных программ, созданных, открытых и сохраненных в Интернете документов или

копирование с дискеты или компакт-диска на жесткий диск; обнаруживать изменения в характеристиках всего диска через предустановленного программиста; Использование антивируса, доступного в БИОС вашего компьютера, – это управление вашим жестким диском и загрузочными секторами.

Антивирусные программные компоненты и базы данных обнаружения вирусов должны постоянно обновляться для эффективной работы. Информационные системы имеют внутренние и внешние угрозы, а основной угрозой безопасности ИТ (ИТ) является появление корпоративных секретов, тенденций развития, исследований и анализа рынка в этой области.

Таким образом, для эффективного противодействия вредоносному программному обеспечению требуется комплексный подход к защите от внешних угроз информационной безопасности. Существует четыре основных угрозы безопасности для информационной безопасности на рынке ИТ: антивирусное программное обеспечение; отображение корпоративной сети; личные сундуки; система борьбы с нападениями. Правильное использование этих ресурсов, несомненно, обеспечит безопасность информации.

Список литературы

1. *Каримов И.А.* Узбекистан: национальная независимость, экономика, политика, идеология. Том 1. Ташкент: «Узбекистан», 1996.
2. *Арипов М.М.* Основы Интернета и электронной почты. Ташкент: Университет, 2000.
3. *Абдукодиров А.* Глоссарий терминов дистанционного обучения. Президент Республики Узбекистан, Фонд «Истедод», Ташкент, 2005. Б. 24.
4. *Гуломов С. и другие.* Информационные системы и технологии: учебник для студентов высших учебных заведений совместно редактирует академик С. Гулямов. Ташкент: «Шарк», 2000. 592 с.