Emro Science and Education
Open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 1 (2023) · “Axborot oqimlari va intellektual tizimlarning ijtimoiy, iqtisodiy va texnik-texnologik tarmoqlardagi o‘rni” mavzus...

Xalqaro ilmiy-amaliy anjuman materiallar to‘plami *Andijan 2023 yil 10-noyabr*

Обеспечение информационной безопасности: разработка методов для криптографической защиты информации

Boboyorov B.N.-доцент, доктор философии (PhD),
Нурафшанский филиал ТУИТа
Бобоёров Шоҳжахон - Магистр Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми

Annotatsiya: Mazkur maqolada axborot xavfsizligini ta’minlash masalalari, jumladan, axborotni kriptografik himoya qilish metodlari tahlil qilingan.

Аннотация: В данной статье проанализированы вопросы обеспечения информационной безопасности, в том числе методы криптографической защиты информации.

Annotation: This article analyzes the issues of information security, including methods of cryptographic protection of information.

Kalit so‘zlar: axborot xavfsizligi, axborot texnologiyalari, kriptografik protokollar, maxfiy shifrlash, samaradorlik.

Ключевые слова: информационная безопасность, информационные технологии, криптографические протоколы, секретное шифрование, эффективность.

Key words: information security, information technology, cryptographic protocols, secret encryption, efficiency.

Современные тенденции в мире, нестабильность на мировых рынках, дефицит топливно-энергетических ресурсов негативно сказываются на экономическом развитии практически всех стран, а борьба за природные ресурсы приводит к обострению военно-политической обстановки в ряде стран. В такой ситуации активизируются силы, борющиеся за «права человека» и, по сути, двигающиеся за право собственности на природные ресурсы.

Использование такими силами информационных факторов, а также возможностей информационных и коммуникационных технологий для распространения, поглощения и пропаганды националистических идей, дестабилизации стабильности многонациональных государств, распространения, усвоения и продвижения националистических идей является причиной большое беспокойство у населения. Информация стала мощным оружием в нынешнюю эпоху идеологической борьбы.

Обеспечение информационной безопасности, принятие мер по недопущению попадания сведений о государственной, военной и служебной тайне в руки противника - создает необходимость совершенствования криптографии и криптографических протоколов.Для разработки методов преобразования информации (или шифрования) с целью ее защиты от незаконных пользователей и возникла наука криптография. Криптология происходит от греческих слов kryptos — «тайна» и logos — «слово».

На сегодняшний день одним из самых надежных средств обеспечения информационной безопасности является криптографическая защита

Published: 10.11.2023

Cite this article: Boboyorov B.N, Бобоёров Шоҳжахон (2023). Обеспечение информационной безопасности: разработка методов для криптографической защиты информации. Emro Science and Education, 1(1). https://journal.emro.uz/public/maqola/653

© 2023 The Author(s). Published by Emro Science and Education. This is an open access article.

информации. Одной из основных задач постановления Президента Республики Узбекистан от 3 апреля 2007 года PQ-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан» является подготовка высококвалифицированных кадров в области криптографическая защита информации. Также распоряжением Президента Республики Узбекистан от 7 февраля 2017 года «О стратегии действий по пяти приоритетным направлениям дальнейшего развития Республики Узбекистан на 2017-2021 годы» № ПФ-4947 предусмотрено ускорение работ по обеспечению информационной безопасности как одной из пять приоритетных направлений [1, 2с].

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Современная криптография является отдельным научным направлением на стыке математики и информатики. Практическое применение криптографии стало неотъемлемой частью жизни современного общества. Она используется во многих отраслях, например, в электронном документообороте, электронной коммерции, телекоммуникациях и т.д.

Классификация криптографических методов преобразования информации по типу воздействия на исходные данные включает следующие виды: **шифрование, стенография, кодирование, сжатие** [2, 3с].

Шифрование предполагает видоизменение исходника посредством логических, математических, комбинаторных и других операций. В итоге таких преобразований первоначальные данные приобретают вид хаотически расположенных символов (цифр, букв и т.д.) и кодов двоичной системы.

Инструментами создания шифра служат алгоритм преобразования и ключ.

В определенных методах шифрования применяется постоянная преобразовательная последовательность. Ключ включает управляющие данные, определяющие выбор видоизменения на конкретных пунктах алгоритма и размер используемых в ходе шифрования операндов.

Шифрование является основным криптографическим способом видоизменения данных в компьютерах. Чтобы обеспечить эффективную борьбу против криптоатак (атак на шифр, криптоанализа), методы шифрования должны отвечать ряду требований:

Криптостойкость (стойкость перед криптоанализом), позволяющая вскрыть шифр лишь через полный перебор ключей.

Стойкость шифра благодаря конфиденциальности ключа, а не алгоритма преобразования.

Соразмерность объемов исходного текста и шифротекста.

Исключение искажений и потерь данных, последовавших за ошибками в ходе шифрования.

Небольшое время шифрования.

Согласованность стоимости шифрования и стоимости исходной информации. Выделяют два вида шифрования:

Симметричное: с использованием одного криптографического ключа.

Асимметричное: с открытым ключом [3, 3c].

Стенография – этот метод, единственный среди криптографических способов, позволяет скрыть не только информацию, но и сам факт ее хранения и передачи. В основе стенографии лежит маскирование секретных данных среди общедоступных файлов. Иными словами, закрытая информация скрывается, а вместо нее создаются дубликаты.

Кодирование - преобразование данных по этой методике происходит по принципу замещения слов и предложений исходника кодами. Закодированные данные могут выглядеть как буквенные, цифровые или буквенно-цифровые комбинации. Для кодирования и раскодирования применяют специальные словари или таблицы.

Рассматриваемый метод удобно использовать в системах с небольшим набором смысловых конструкций. Недостаток кодирования заключается в том, что необходимо хранить и распространять кодировочные таблица, а также достаточно часто их менять во избежание нежелательного рассекречивания информации.

Сжатие - данный способ представляет собой сокращение объема исходной информации. Понятие сжатия относят к криптографическим с некоторыми оговорками. С одной стороны, сжатые данные требуют обратного преобразования для возможности их прочтения. С другой стороны, средства сжатия и обратного преобразования общедоступны, поэтому этот способ не является надежным в части защиты информации.

На сегодняшний день широкое применение получили следующие алгоритмы шифрования: Data Encryption Standard (DES), 3DES и International Data Encryption Algorithm (IDEA) [4, 4c].

В целях защиты информации, обеспечения информационной безопасности и предотвращения угроз криптографическим протоколам мы выдвигаем следующие рекомендации:

- разработка рекомендаций национальным пользователям по использованию эффективных программно-аппаратных средств предотвращения несанкционированного доступа к информационным системам;
- оказание консультационных услуг и технической помощи отечественным пользователям по вопросам состояния компьютерной безопасности в информационных системах и государственных предприятиях, и организациях;
- организация обучения и тренингов для специалистов государственных предприятий, операторов и провайдеров, по вопросам обеспечения безопасности криптографических протоколов.

Практика показывает, что для достижения достаточного уровня прогресса в защите информации необходима совместная реализация правовых, организационных и технических мер. Он определяется конфиденциальностью защищаемой информации, классификацией угрозы и наличием мер.

Список литературы

[1, 2c] Указ Президента Республики Узбекистан № ПФ-4947 «О стратегии действий по пяти приоритетным направлениям дальнейшего развития Республики Узбекистан на 2017-2021 годы». Ташкент, 7 февраля 2017 года.

Постановление Президента Республики Узбекистан PQ-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан». - Ташкент, 3 апреля 2007 г.

[2, 3c]. Введение в криптографию / Под общ. ред. В. В. Ященко. СПб.: Питер, 2001.

[3, 3c]. Алферов А. П., Зубов А.Ю., Кузмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2001.

[4, 4c]. Акбаров Д.Е. «Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши» - Т.: «Ўзбекистон маркаси», 2009. - 424 б

PARFYUMERIYA DO’KONINI DASTURIY TAMINOTINI YARATISH

Abidov Adxamjon Abdumajid o'g'li, Assisent, Andijon mashinasozlik instituti

Rahmatova Nargiza Mahmudjon qizi, 4- bosqich talabasi, Andijon mashinasozlik instituti

Annotatsiya. Ushbu parfyumeriya do’konini dasturiy taminotini yaratish haqida. Do’kon faoliyatining natijalarini, sotilgan mahsulotlar statistikasini va mijozlarning afzalliklarini hisoblash uchun ma’lumotlar tarqatish va hisobotlar tuzishni o’z ichiga oladi.

Kalit so’zlar. Do’kon, mahsulot, mijoz, ombor, tizim, dasturiy, tuzish.

Parfyumeriya do’konining dasturiy taminoti yaratish uchun qadamlar quyidagilardir.

Ma’lumot tizimi. Mahsulotlaringiz, ularning turlari, yetkazib berish va ombor boshqaruv tizimini yaratish. Ma’lumotlar bazasida har bir mahsulot uchun ma’lumotlar (nomi, turi, narxi, qolgan miqdori, katalog raqami, rasm, tavsiflar, vaqtincha chegirma, to’lov shartlari) saqlanishi kerak.

Onlayn sotish. Onlayn platforma (veb-sayt yoki mobil ilova) orqali mahsulotlar sotilishi uchun tizim tuzilishi. Mijozlar uchun oson va qulay tizim tuzish.

Xaridorlar boshqarish tizimi. Mijozlar ro’yxati, ularning tarixi va harakatlarini boshqarib, mijozlar bilan aloqa qilish uchun CRM (Xaridor Muharriri Tizimi) tuzilishi.

Ombor boshqarish. Mahsulotlar ombori, kirim-chiqimlar, qolgan mahsulotlar, va yetarli miqdorlar monitoring qilish uchun ombor boshqarish tizimini o’rnating.

Xaridorlar bilan aloqalar. Xaridorlarga chegirmalar, takliflar, yangiliklar yuborish uchun avtomatlashtirilgan xabarlar va e-rasmlar yuborish tizimini yaratish.

Hisobot va statistika. Do’kon faoliyatining natijalarini, sotilgan mahsulotlar statistikasini va mijozlarning afzalliklarini hisoblash uchun ma’lumotlar tarqatish va hisobotlar tuzish.

Tayyor mahsulot retsenziyalari va sharhlar. Mijozlar uchun tayyor mahsulot reytinglari va sharhlarni qo’llash tizimini o’rnating.

To’lov tizimi. Turli to’lov usullarini qo’llash tizimini tuzish. Kredit kartalari, onlayn to’lov shakllari, naqd pul va boshqa usullar orqali to’lov qabul qilish imkoniyatini yaratish.

Mijozlarga maxsus takliflar va chegirmalar. Xaridorlar tarixini va o’z xususiyatlari bo’yicha mahsulotlar uchun maxsus chegirmalar va takliflarni avtomatlashtirish.