Васяева Д.О.
*Научный руководитель: к.т.н., доцент каф. ФПМ К.В. Макаров*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: v-dasha95@yandex.ru*

**Сравнительный анализ алгоритмов симметричного шифрования**

Многие предприятия не пользуются преимуществами технологий шифрования, опасаясь, что это слишком сложно. Шифрование особо ценных данных ненамного сложнее, чем запуск антивирусного сканера или резервного копирования данных.

Шифрование данных – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит способом соблюдения конфиденциальности передаваемой информации.

Причины потери данных:

1. Отправка серверов или жестких дисков в ремонт;
2. Перевозка компьютеров из одного офиса в другой, например, при переезде;
3. Утилизация компьютеров, серверов, жестких дисков и лент;
4. Хранение магнитных лент в специальном депозитарии (off-site storage);
5. Перевозка ленты, например, в депозитарий;
6. Кража или потеря жестких дисков или лент.

В связи с этим анализ, существующих методов защиты информации является актуальной научно-технической задачей.

Безопасность, обеспечиваемая традиционной криптографией, зависит от нескольких факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Классическим примером таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

- Простая подстановка
- Одиночная перестановка по ключу
- Гаммирование

Объекты исследования в данной работе – алгоритмы шифрования: простая подстановка, одиночная подстановка по ключу и гаммирование, предмет исследования – использование одного из выше перечисленных алгоритмов шифрования защиты данных.

Целью исследования является обзор анализ и выбор одного из алгоритмов шифрования: простая подстановка, одиночная подстановка по ключу и гаммирование, для реализации его в приложении виртуальная криптографическая лаборатория для защиты данных.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор выше заявленных алгоритмов шифрования.

2. Анализ выбранных методов.
3. Представить результаты исследования.

Обзор алгоритмов шифрования

Одиночная перестановка по ключу

При шифровании простой перестановкой ключевое слово с неповторяющимися символами или цифровой ключ. Число колонок в таблице задаётся количеством символов в ключе, а число строк может быть фиксировано или может задаваться длиной сообщения. Шифруемый текст записывается последовательными строками под символами ключа. Для заполнения пустых клеток (если объём текста меньше ёмкости таблицы) можно использовать любые символы. Затем текст выписывается колонками в той последовательности, в которой располагаются в алфавите буквы ключа или в порядке следования цифр, если ключ цифровой. В качестве примера рассмотрим шифрование сообщения: «БУДЬТЕ ОСТОРОЖНЫ С ПРЕДСТАВИТЕЛЕМ ФИРМЫ «СПЕКТР». Применим цифровой ключ - 5 1 8 3 7 4 6 2. Выписывая текст по колонкам, получаем абракадабру: УОРТМССВИТЬОДЛСЕНТМЕБТПИРРОЫАФКТЖСЕПДРЕЕЫ.

Дешифрование выполняется в следующем порядке. Подсчитываем число знаков в зашифрованном тексте и делим на число знаков ключа (41: 8=5 и 1 знак в остатке). Под знаками ключа в соответствующей последовательности записываем вертикально (колонками) символы зашифрованного текста в определенном выше количестве. В каждой колонке по 5 символов, а в одной (первой слева) - 6 символов (5+1 буква в остатке). По строкам таблицы (горизонтально) читаем исходный текст. Выше, в «Истории тайнописи», упоминается шифр называемый в некоторых книгах по криптографии «Сцитала» (наматывание ленты на жезл). Это не что иное, как перестановка по таблице с простым ключом - 1 2 3 4 …

Простая подстановка

Каждая из 33 букв русского алфавита заменяется на другую букву того же алфавита (моноалфавитная подстановка). Такой шифр (одноалфавитная замена) имеет низкую (временную) стойкость, т. к. зашифрованный (закрытый) текст имеет те же статистические характеристики, что и исходный (открытый) - каждая буква имеет свою частоту появления. Поэтому использовать этот метод целесообразно для шифрования только короткого текста.

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

Гаммирование

Метод гаммирования состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой.

В потоковых криптосистемах на основе ключа вырабатывается гамма, которая затем накладывается на текст сообщения. Наложение осуществляется посредством сложения по модулю 2 (операции XOR).

Зашифрование производится следующим образом:

$c_i = m_i \otimes k_i$ для i=1,2,3...

где $c_i$ - знак шифротекста;

$m_i$ - знак открытого текста;

$k_i$ - знак ключевой последовательности;

$\otimes$ - сложение по модулю 2.

Поскольку повторное применение операции XOR восстанавливает первоначальное значение, расшифрование производится повторным наложением гаммы:

$m_i = c_i \otimes k_i$ для i=1,2,3...

Преобразование текста осуществляется потоком по мере выработки гаммы. Поэтому поточные шифры подходят для шифрования непрерывных потоков данных - голоса, видео и т.д.

Принцип шифрования гаммированием заключается в генерации бесконечного ключа (гаммы шифра) с помощью датчика псевдослучайных чисел (ПСЧ) и наложении полученной гаммы на исходные данные обратимым образом. Процесс расшифровки данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то зашифрованный текст можно раскрыть только путем прямого перебора.

Сравнительный анализ методов шифрования

После проведенного обзора было выявлено, что шифрование методом простой подставки совершенно не эффективно, так как его можно расшифровать после несложного анализа. Алгоритм одиночной перестановки гораздо надежнее подстановки, но если ключ используется несколько раз, то его можно проанализировать и взломать. Из трех проанализированных методов, алгоритм методом гаммирования является самым эффективным.

Таблица 1. Сравнительный анализ алгоритмов симметричного шифрования

| | Простая подстановка | Одиночная перестановка по ключу | Гаммирование |
|---|---|---|---|
| Методы взлома | Шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифр тексте | При своей несложности система легко уязвима. Если злоумышленник имеет шифрованный и соответствующий исходный текст | Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма |
| Параметры ключа | Число возможных ключей мало | Число возможных ключей ограничено | Длинна шифрующей гаммы должна быть не менее защищаемого сообщения |
| Передача ключа | Отправитель и получатель должны некоторым тайным образом получить копии секретного ключа и сохранить их в тайне | | |
| Стойкость | Имеет низкую стойкость | Имеет стойкость более высокую чем подстановка | Исходный текст практически невозможно восстановить без ключа |
| Недостатки | Использовать этот шифр целесообразно только для шифрования коротких текстов | Если ключ используется несколько раз его можно проанализировать и взломать | Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей |

Результат

В результате проведенного исследования было выяснено, что из трех выбранных алгоритмов шифрования самым более надежными является алгоритм гаммирования, так как данный алгоритм обладает рядом преимуществ, а именно: имеет высокую криптостойкость (исходный текст не возможно восстановить без ключа), не требует больших вычислительных мощностей, что позволяет использовать его любому лицу, а также прост в использовании.

Волков Д.А.
*Научный руководитель: к.т.н., доцент каф. ФПМ А.В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail:madehim333@yandex.ru*

**Обзор и анализ метода аутентификации с использованием протокола с нулевым разглашением секрета Фиата-Шамира**

Защита информации является неотъемлемой составной частью общей проблемы информационной безопасности, роль и значимость которой во всех сферах жизни и деятельности общества и государства на современном этапе неуклонно возрастают.

Сначала сеть Интернет проектировалась и рассматривалась как система обработки и передачи информации в военной среде. Вопрос безопасности данных и в те времена являлся особо важным, но из-за ограниченного числа машин, имеющих доступ к сети, предпринимались только меры безопасности на физическом уровне. Под этим подразумевалась изоляция объектов от посторонних лиц, и данные меры являлись оправданными из-за, как указано выше, невысокого количества ЭВМ. Со временем, Интернет получил распространение в гражданской среде. В связи с этим в сети появилось множество различной информации, часть из которой является общедоступной, а другая часть доступна только для ограниченного числа людей. Следовательно, для защиты второй категории данных от несанкционированного доступа и необходимо обеспечивать безопасность передачи данных. В связи с этим разработка новых и совершенствование существующих методов защищенной передачи информации и аутентификации является актуальной научно-технической задачей.

Объекты исследования в данной работе – протокол с нулевым разглашением секрета Фиата-Шамира, предмет исследования – использование протокола с нулевым разглашением секрета в клиент-серверных приложениях для аутентификации.

Целью исследования является обзор и анализ методов аутентификации, реализуемого в клиент-серверных приложениях для защиты информации на примере протокола с нулевым разглашением секрета Фиата-Шамира.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор метода аутентификации;
2. Анализ метода;
3. Результаты исследования.

Обзор метода аутентификации. Аутентификация - это проверка соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, в простейшем случае - с помощью имени входа и пароля.

В ходе исследования был рассмотрен следующий метод:

Протокол Фиата–Шамира. Основной идеей алгоритма является сложность извлечения квадратного корня по составному модулю, который включает не менее двух больших простых множителей[1]. При этом считается, что разложение этих множителей неизвестно. Доказывающим происходит выбор двух простых чисел (преимущественно больших) p и q и вычисляется модуль n = p * q. Затем в качестве своего личного секретного ключа выбирается случайное число s, такое, что $1 \leq s \leq n-1$, и вычисляется значение $y = s^2 \bmod n$.(Это делается для того, чтобы доказывать проверяющему, то что он знает квадратный корень из y.) Значение y, которое объявляется всем участникам протокола, играет роль открытого ключа в смысле его использования для проверки того, что доказывающий знает s.

Алгоритм протокола состоит из z-кратного повторения раундов, содержащих следующие шаги:

1. Доказывающим выбирается число k, которое удовлетворяет условию $1 \leq k \leq n-1$. Далее происходит вычисление значения $u = k^2 \bmod n$, называемое фиксатором, и это значение отправляется проверяющему. (Число k играет роль разового секретного ключа, это применяется для

обеспечения защиты и личного секретного ключа от разглашения при направлении ответа, зависящего от s.);

2. Проверяющий отправляет доказывающему равновероятный случайный бит r ($r = 1$ или $r = 0$);

3. Доказывающий производит вычисление значение $w = k*s^r \bmod n$ и отправляет его проверяющему.

При выполнении равенства $w^2 = u*y^r \bmod n$, проверяющий считает ответ верным.

Вероятность правильного прохождения раунда нарушителем равна $2^{-1}$, следовательно, пройти проверку и выдать себя за пользователя, знающего секрет, возможно лишь с вероятностью $2^{-z}$[3].

Анализ методов аутентификации. Для сравнительного анализа были выбранные следующие критерии:

Вычислительные затраты и предвычисления - число модульных умножений для обоих сторон.

Требования к памяти – необходимое количество памяти для записи ключей.

Гарантии безопасности – защита от злоумышленника, пытающегося получить доступ к секретной информации.

Кроме вышеупомянутого протокола Фиата-Шамира, для сравнения выбраны протоколы Гуилоу-Куйсквуатера и Шнорра[2]:

1.Вычислительные затраты. Менее требовательным к вычислительным затратам является протокол Фиата-Шамира, для него необходимо от 11 до 20 шагов. Далее идет протокол Шнорра, порядка 30 шагов. Заключает список протокол Гуилоу-Куйсквуатера с количеством шагов равным 60. Эти данные получены при kt=20 и размере n в 512 бит. Так же можно отметить, что неоптимизированный алгоритм RSA требует порядка 768 шагов;

2.Предвычисления. По совокупности вычислений проверяющей и доказывающей стороны данные протоколы приблизительно одинаковы. Протокол Шнорра имеет меньше вычислений у доказывающей стороны, из-за необходимости выполнения всего лишь одного модульного умножения (возвести в степень можно в ходе выполнения предвычислений), но у проверяющей стороны требуется большие вычисления, чем в протоколах Фиата-Шамира и Гуилоу-Куйсквуатера;

3.Требования к памяти и коммуникационные затраты. В протоколе Гуилоу-Куйсквуатера имеется возможность снизить требования к необходимой памяти и часть коммуникационных затрат. В других рассматриваемых протоколах данная возможность отсутствует;

4.Гарантии безопасности. Все вышеупомянутые протоколы способны обеспечить эффективное противодействие злоумышленнику, так как основываются на сложных математических операциях. Протокол Фиата-Шамира требует извлечения из числа корня по составному модулю, Гуилоу-Куйсквуатера основывается на невозможности получения из числа v корней по составному модулю, Шнорра требует вычисление дискретного логарифма по модулю простого числа.

В результате сравнения, протокол Фиата-Шамира является наилучшим вариантом, т.к. требованиями к памяти на текущий момент развития ЭВМ можно пренебречь.

Результаты исследования. В результате проведенного исследования было выяснено, что выбранный метод аутентификации, основанный на протоколе с нулевым разглашением секрета Фиата-Шамира является безопасным для защиты конфиденциальной информации. Так же, в ходе анализа были рассмотрены различные протоколы с нулевым разглашением секрета и выявлено, что выбранный протокол наиболее оптимальный для ряда основных критериев.

**Литература**

1. Протокол Фиата — Шамира [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/Протокол_Фиата_—_Шамира (дата обращения: 05.03.2017).

2. Сравнение протоколов с нулевым разглашением [Электронный ресурс] // Cryptowiki : энциклопедия теоритической и прикладной криптографии URL: http://cryptowiki.net/index.php?title=Доказательства_с_нулевым_разглашением_знания (дата обращения: 06.03.2017).

3. Молдовян А.А., Молдовян Д.Н., Левина А.Б. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с. - экз.

Ермошина В.А.
*Научный руководитель: к.т.н., инженер вычислительного центра А.В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: valentina_ermoshina@mail.ru*

**Создание системы контроля лицензий**

Основным документом, который определяет права и обязанности пользователя программного обеспечения, является лицензионное соглашение (licence agreement), которое прилагается к приобретенному продукту либо в виде бумажного документа, либо в электронном виде. Именно это соглашение определяет правила использования данного экземпляра продукта. По сути, лицензия выступает гарантией того, что издатель ПО, которому принадлежат исключительные права на программу, не подаст в суд на того, кто ею пользуется[1]. Иными словами, издатель программного обеспечения ставит определенные защитные рамки по использованию его программного обеспечения. Во времена прогресса информационных технологий возникает вопрос, как обезопасить себя от злоумышленников. В итоге придумывают много различных систем для ограничения доступа к информации. Одна из этих систем лицензирование. С помощью лицензирования можно не только обезопасить информацию но и управлять как функционалом так и временем использования программой.

Целью работы является разработка программы для лицензирования приложения.

Для достижения поставленной цели необходимо выполнить следующие задачи:

- Изучение актуальности лицензирования;
- Анализ процесса лицензирования популярных программ;(обзор систем аналогов)
- Разработка системы лицензирования (формирование требований к * на основании сравнительного анализа систем аналогов;

Рассмотрим аналоги приложения:

Таблица 1. Сравнение приложений-аналогов

| Аналоги | Особенности | | | |
|---|---|---|---|---|
| | Генерация регистрационных ключей | Создание нескольких типов лицензий | Зашифровывание MotherBoard ID Processor ID | Низкая стоимость |
| The Enigma Protector | + | - | - | - |
| ASProtect | + | + | - | - |
| Реализуемая программа | + | + | + | + |

Требования:

Для более надежного варианта подходит зашифровывание ID MotherBoard, Processor, так как у всех компьютеров он разный[2]. Так же программа должна записывать зашифрованный ключ в отдельный файл в формате(*.dat)|*.dat". Потом с помощью проверки ключа активировать приложение. Так как, материнская плата и процессор самые долго не заменяемые детали компьютера, их номера используют для шифрования ключей в целях безопасности и невозможности распространения. Далее они будут записываться в файл, который после передается разработчику для генерирования ключа. При этом пользователь будет оповещен, что файл с данными нужно переслать разработчику для обработки информации, после получает файл с ключом, который активирует программу. Необходим так же генератор ключа и дешифратор файла ключа. Дешифрование файла ключа происходит у пользователя после его получения и входа в программу. Приложение сверяет файл у пользователя с файлом ключом

после дешифрования  и при их соответствии выдает уже полный доступ к приложению. При неверности соответствия пользователю повторно нужно отправлять файл разработчику для проверки.

Вывод: в ходе исследовательской деятельности были разработаны требования к программе на основе изучения аналогов приложения.

**Литература**

1. А. И. Савельев Лицензирование программного обеспечения в России: законодательство и практика – М.: Инфотропик Медиа, 2012. – 432 с.

2. Бабаш Л.В Криптографические и теоретико-автоматные аспекты современной защиты информации. Криптографические средства защиты / Издательский центр ЕАОН, 201 с.215.

Зайцева Е.С.
*Научный руководитель: к.т.н., инженер вычислительного центра А. В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: katlabutova@yandex.ru*

**Реализация групповой политики безопасности**

В системе должна быть единая политика безопасности, которая определяет правила обращения с информацией так, чтобы исключить или снизить угрозы ущерба. Единая политика нужна, чтобы исключить противоречия между правилами обращения с одной и той же информацией в разных подразделениях организации. В самом простом случае, это дискреционная политика. При такой политике у каждого информационного объекта системы есть хозяин, который определяет правила доступа субъектов к объектам. Для реализации дискреционной политики безопасности каждый субъект и объект должны быть идентифицированы, а каждый субъект должен подтвердить свой идентификатор (аутентификация) [1]. Обычно дискреционную политику безопасности усиливают аудитом, отслеживая активность пользователей или субъектов, которые действуют от их имени, в компьютерной системе. Исходя из этого реализация групповой политики безопасности информационной системы является актуальной научно-технической задачей.

Целью исследования является реализация групповой политики безопасности.

Кроме дискреционной политики безопасности как минимум необходимо организовать защиту целостности информационных ресурсов от модификации или уничтожения. Идентификация и аутентификация, правила разграничения доступа, аудит и защита целостности должны реализовываться механизмами защиты. На каждом рабочем месте и на серверах установлены операционные системы, которые, как правило, обладают набором механизмов защиты, обеспечивающих идентификацию и аутентификацию, разграничение доступа, аудит на данном компьютере. Серьезные прикладные системы типа СУБД также обладают локальным набором механизмов защиты, обеспечивающих идентификацию и аутентификацию, разграничение доступа и аудит. Основными механизмами защиты целостности являются резервное копирование (backup), электронно-цифровая подпись (ЭЦП) и коды аутентификации [3].

Сравним эти механизмы:

| Название | Криптостойкость | Целостность | Разграничение доступа |
|---|---|---|---|
| Резервное копирование | - | + | - |
| ЭЦП | + | + | + |
| Коды аунтефикации | - | + | + |

В ходе исследования можно увидеть на основе сравнения механизмов защиты, наиболее надежной защитой информации и данных является ЭЦП, так как у нее больше преимуществ перед другими механизмами защиты.

**Литература**

1. Кияев В., Граничин О. «Безопасность информационных систем: курс». 2016 г.
2. Скрипник Д. А. «Общие вопросы технической защиты информации», 2016 г.
3. Блинов А. М. «Информационная безопасность», 2010 г.

Кирбинев Ю.В.
*Научный руководитель: к.т.н., доцент каф. ФПМ А.В. Провоторов*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*provotorovalexey@gmail.com*

**Создание системы контроля лицензий на основе сертификатов**

Активация – это технология противодействия компьютерному пиратству, которая определяет соответствие использования ключа продукта требованиям лицензионного соглашения. При активации необходимо использование лицензионного ключа продукта.

Однако условия лицензионных соглашений могут быть нарушены и копии программного обеспечения могут незаконно распространяться. Если это происходит, то имеет место нарушение лицензионного соглашения – незаконное копирование, что является нарушением законодательства Российского Кодекса о защите авторских прав.

Именно поэтому создание систем контроля лицензий является актуальной научно-технической задачей.

Целью работы было создание системы лицензирования, способной выполнять следующие функции:

1. Возможность создания, пересылки, проверки и продления лицензий;
2. Возможность использования различного типа лицензий (нет лицензии, лицензия получена, срок лицензии истек)

В ходе работы были проанализированы самые распространенные аналоги систем лицензионной активации – операционные системы (Windows, Linux) и антивирусы (Касперский, DoctorWeb, Avast). В результате были выделены следующие критерии для создания системы контроля лицензий:

1. Создание лицензии для конкретного программного обеспечения;
2. Пересылка лицензии пользователю, использующему конкретное программное обеспечение.
3. Проверка лицензии на подлинность и действительность на конкретном устройстве
4. Продление лицензии путем обращения к разработчику используемого программного обеспечения

Привязка к конкретному устройству была реализована с помощью формирования лицензионного сертификата. Выдача лицензионных сертификатов обязательна для всех пользователей. Если программное обеспечение не имеет привязки сертификату, то дальнейшая работа с программой на данном устройстве невозможна.

Для формирования лицензионного сертификата, разработчику программного обеспечения необходимо указать время действительности сертификата, а также указать уникальный идентификационный ключ. Он формируется путем сохранения данных устройства, на котором была запущена программа. Данный ключ отсылается разработчику, и на его основе система лицензирования формирует уникальный сертификат, который отправляется обратно пользователю и служит для доступа к программе на срок действия сертификата. При попытке отправить сертификат другому пользователю или активировать на другом устройстве, сертификат становится недействительным. При истечении срока лицензии необходимо отправить разработчику соответствующий запрос, на основании которого будет сформирован новый сертификат.

Таким образом, в ходе работы была реализована система контроля лицензий на основе сертификатов, способная решать важную и актуальную задачу защиты программного обеспечения от несанкционированного использования.

Козырева Е.С.
*Научный руководитель: к.т.н., инженер вычислительного центра А. В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: elena.kozireva666@yandex.ru*

**Разработка алгоритма шифрования текста**

Вопрос защиты ценной информации путем ее видоизменения, исключающего ее прочтение незнакомым лицом тревожила лучшие человеческие умы еще с самых древних времён. История шифрования - почти что ровесница истории человеческой речи. Кроме того, изначально письмо само по себе было криптографической системой, поскольку в древних обществах подобным знанием обладали лишь избранные. Священные манускрипты различных древних государств тому примеры[2].

Понятие "Безопасность" охватывает широкий круг интересов как отдельных лиц, так и целых государств. В наше мобильное время видное место отводится проблеме информированной безопасности, обеспечению защиты конфиденциальной информации от ознакомления с ней конкурирующих групп[1].

Целью работы является разработка алгоритма шифрования текста.

Для достижения цели были поставлены следующие задачи:

– разработать свой код шифрования текста;
– выявить недостатки существующих алгоритмов (таблица 1).

Итак шифр Елены – представляет собой матрицу 6х5, столбцы и строки которого нумеруются цифрами от 1 до 5 и 6 соответственно. В каждую клетку этого квадрата записывается одна буква. Буквы расположены в алфавитном порядке. В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путём нахождения буквы, стоящей на пересечении строки и столбца.

Сравним три существующих алгоритма и разработанный шифр.

Таблица 1 – Сравнение существующих программ-аналогов

| Название | Криптостойкость | Процедура расшифрования | Удобный в использование |
|---|---|---|---|
| Цезарь | - | + | + |
| Атбаш | - | - | + |
| АзбукаМорзе | - | + | - |
| Елена | + | + | + |

Проанализировав криптографическую устойчивость трех существующих шифров и разработанного, пришли к выводу, что самый лучший идеальный вариант по всем пунктам: шифр Елены.

Все поставленные цели были выполнены путем решения всех указанных задач.

**Литература**

1. Бабаш А. В. “Криптографические и теоретико – автоматные аспекты современной защиты информации.” Учебно-методическое пособие. Издательский центр «ЕАОИ» 2011 г , 215 стр.

2. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2012.

Круглов К.А.
*Научный руководитель: к.т.н., доцент М. В. Макаров*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: kruglov.kos@yandex.ru*

**Определение критериев при выборе системы контроля и управления доступом на предприятии на основе сравнительного анализа**

В современном мире, информационная безопасность – важнейшее условие успешной экономической деятельности любого предприятия. Системы контроля и управления доступом (СКУД) – один наиболее действенных методов управления информационной безопасностью на предприятии. СКУД способна уберечь предприятие от рисков, связанных с несанкционированным проникновением на объект. В связи с этим сравнительный анализ СКУД является актуальной научно-технической задачей. Исходя из этого, основной целью данной исследования является определение критериев при выборе СКУД на основе сравнительного анализа основных типов данных систем.

На сегодняшней день СКУД активно применяются практически во всех сферах деятельности. Тип применяемой СКУД определяется особенностями объекта: размерами, важностью, уровнем секретности, его финансовым состоянием, целями и задачами предприятия.

Автономная система контроля доступа – предназначены для обеспечения контроля и управления доступом в отдельное помещение. Такая система состоит из автономного контроллера, хранящего в себе базу данных идентификаторов и управляющего работой остальных элементов системы. В качестве исполнительного устройства используется электромагнитный замок, либо защелка. Для идентификации пользователя используются различные типы карт с соответствующими считывателями (магнитные, проксимити, штриховые)

Сетевая система контроля доступа СКУД представляет собой несколько СКУД, объединенных в единую сеть с помощью кабельных линий или беспроводного оборудования. Управление комплексом осуществляется с одного или нескольких компьютеров, на которых установлено специальное программное обеспечение. Сетевые СКУД позволяют отслеживать нахождение сотрудников на рабочем месте, вести учет рабочего времени, настраивать доступ к помещениям, территориям по времени, вносить посетителей и персонал в электронную картотеку и выполнять другие сложные задачи.

Биометрические СКУД используют для идентификации биометрических параметров, являющихся уникальными для каждого человека: отпечаток пальца или рисунок радужной оболочки глаза. Использование для идентификации биометрических параметров позволяет обеспечить больший уровень безопасности, чем при использовании ключей или паролей.

При проведении исследований использовался метод сравнительного анализа по многим критериям. При использовании такого метода, анализ сравниваемых объектов предполагает какую-то оценку его основных характеристик, исходя из выбранных критериев. Основой для выбора критериев являются технические требования, физические параметры объекта, показатели качества, целевые функции, факторы и т.п. В результате проведенного сравнительного анализа трех основных типов СКУД были получены результаты, представленные в таблице 1. Данные результаты позволяют определить критерии, которые необходимо использовать в процессе выбора СКУД для конкретного предприятия.

Таблица 1. Сравнительный анализ СКУД

| Тип СКУД | Недостатки | Преимущества |
|---|---|---|
| Автономная СКУД | 1. Контроллер автономной СКУД не хранит информацию о входах и выходах пользователей.<br>2. Отсутствие централизованного управления.<br>3. В простых контроллерах доступа как правило нет возможности удалить отдельный ключ из памяти; чтобы удалить потерянные ключи, необходимо стереть всю память и заполнить заново актуальными | 1. Невысокая цена<br>2. Автономные системы просты в установке и использовании. |
| Сетевая СКУД | 1. Возможность взлома системы. Карты доступа могут быть потеряны или украдены, ими может воспользоваться злоумышленник.<br>2. Высокая стоимость оборудования, трудоемкий процесс установки и повышенные требования к квалификации обслуживающего персонала | 1. Возможности получения постоянной информации о передвижениях сотрудников.<br>2. Сетевая СКУД может быть интегрирована в единую систему безопасности объекта наряду с системой видеонаблюдения, охранно-пожарной сигнализацией. |
| Биометрические СКУД | 1. Биометрические системы контроля доступа дороже аналогичных систем, использующих для доступа бесконтактные карты.<br>2. Временные пропуски невозможны<br>3. При числе пользователей более 1000 необходимо введение двухфакторной системы идентификации: по карте доступа и отпечатку. | 1. Биометрические показатели невозможно подделать.<br>2. Проверка личности пользователя занимает всего несколько секунд.<br>3. Сетевой контроллер доступа хранит журнал событий: входов, выходов пользователей и аварийных открытий двери.<br>4. Сотрудникам различных подразделений могут задаваться разные расписания и зоны доступа. |

В результате проведенного исследования было выяснено, что эффективный выбор СКУД зависит от учета следующих параметров предприятия: размера, финансового состояние, цели и задачи предприятия.

**Литература**

1. Виды СКУД. [Электронный ресурс] Режим доступа: http://www.quantech.ru/articles/resheniya-dlya-skud/vidy-skud/

2. Контроль управления доступом [Электронный ресурс] Режим доступа: http://www.itrade-group.ru/solutions/physical_security_systems/skud2/

3. Системы контроля и управления доступом [Электронный ресурс] Режим доступа: http://www.rluxe.ru/skud

Решетников Д.В.
*Научный руководитель: к.т.н, доцент каф. СГПД М.В. Макаров*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail:student.reshetnikov@mail.ru*

**Обзор и анализ механизма распознавания радужной оболочки глаза для систем аутентификации пользователей с использованием технологии Windows Hello**

Целью данной работы является обзор и анализ механизма распознавания радужной оболочки глаза для систем аутентификации пользователей с использованием технологии Windows Hello.

Основной параметр деятельности всех биометрических систем распознавания радужной оболочки состоит в том, что при сканировании области глаза захватывается район зрачка и самой радужной оболочки. При этом радужная оболочка настолько неповторимый параметр, что даже не самый удачный в плане шумов или чёткости снимок даст достоверный результат. Отсканированная область с помощью вшитого программного обеспечения очищается от шумов и бликов, которые исходят, например, от очков. Далее считанная информация охватывается в прямоугольный формат – Iris Code, который несёт всю информацию о персональных параметрах объекта в черно-белом виде, подобно штрих-коду. Далее Iris Code проверяет изображение по готовой базе с хранящимися в системе шаблонами. Скорость обрабатываемых данных при этом крайне высокая, что позволяет применять систему для работы с большими базами данных, в том числе выполняя задачи правоохранительных органов и различных государственных организаций.

Более подходящую под обычных пользователей технологию биометрической аутентификации разработали в компании Microsoft. Их система под названием Windows Hello, помимо основных методов аутентификации, например, по отпечатку пальца или по голосу, так же имеет в своём составе сканирование радужной оболочки глаза.

Для использования сканирования необходима только соответствующая камера, поддерживающая данную технологию. Кроме камеры нужен светодиод и датчик, которому будет поступать отраженная информация. Как правило, глаз освещается инфракрасными лучами таким образом, чтобы камера смогла отсканировать оболочку.

Windows Hello может использоваться не только для входа в свой профиль, но и при авторизации в приложениях, корпоративных сервисах и на сайтах, что существенно повышает защиту персональных данных. При этом разработчикам сторонних приложений вовсе не нужно разбираться в шифровании, биометрике или технологии работы с учетными записями Microsoft.

Для анализа системы был выбран ряд основных критериев:

1. Безопасность – позволяет оценить вероятность того насколько сложно обмануть систему и получить несанкционированный доступ. В результате эксперимента Windows Hello ни разу не допустил в систему ложного близнеца.

2. Возможность перехвата данных по сети. Все полученные данные хранятся в локальной базе данных Windows Hello на устройстве пользователя для безопасности от хакеров. Они не перемещаются и не передаются на внешние устройства или серверы.

3. Доступность. Технология Windows Hello может использоваться в обычных пользовательских ноутбуках, смартфонах и планшетах. Стоимость данных девайсов в разы ниже, чем специальных аппаратов на производственных или государственных службах.

4. Простота и удобство в использовании. Любой пользователь может настроить для себя данную технологию распознавания радужной оболочки глаза без любых проблем с помощью имеющихся в свободном доступе документаций.

В результате анализа были выявлены следующие достоинства данной технолгогии, приведенные в таблице 1.

Таблица 1. Результаты анализа технологии Windows Hello

| Технология | Безопасность | Возможность перехвата данных по сети | Доступность | Простота и удобство в использовании |
|---|---|---|---|---|
| Система аутентификации пользователей с использованием технологии Windows Hello | Windows Hello допускает ошибку реже чем 1 раз в 100000 | Все данные хранятся на локальном устройстве. | Доступен каждому обычному пользователю | Максимальная для пользователя |

В результате проведенного исследования было выяснено, что выбранная технология распознавания радужной оболочки глаза для аутентификации пользователей с использованием системы Windows Hello отвечает всем необходимым требованиям пользователя. Она сочетает надёжную безопасность с доступностью и простотой, необходимую для обычного пользователя.

**Литература**

1. Аутентификация по радужной оболочке глаза [Электронный ресурс] // wikipedia.org: интернет портал URL: https://ru.wikipedia.org/wiki/Аутентификация по радужной оболочке глаза (дата обращения: 7.04.2017).

2. Управление проверкой личности с помощью Windows Hello [Электронный ресурс] // habrahabr.ru. URL: https://habrahabr.ru/company/microsoft/blog/314822/ (дата обращения: 7.04.2017).

3. Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. РУКОВОДСТВО ПО БИОМЕТРИИ. - Издательство: Техносфера, Серия: Мир цифровой обработки, Год издания: 2007.

Титков Е.В.
*Научный руководитель: доцент каф. ФПМ, к.т.н. Р.А. Штыков*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: rm4life95@gmail.com*

**Обзор и анализ методов криптографии**

С каждым годом компьютерная информация играет все более важную роль в нашей жизни, и все большую актуальность приобретают проблемы ее защиты. Каждый пользователь при общении хочет иметь защищённую сеть для обмена данными что бы передача данных была безопасной и не один злоумышленник не смог прочитать конфиденциальные данные. Для безопасной передачи данных криптография используется в беспроводных и проводных сетях, где простой текст преобразуется в шифр, а шифр преобразуется в простой текст.

Целью исследования является обзор и анализ методов крифтографии.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор методов криптографии.
2. Анализ выбранных криптосистем.
3. Результаты исследования.

Обзор методов криптографии

Криптография делится на симметричную и асимметричную. В симметричной один и тот же ключ используется обоими сторонами. Отправитель использует такой ключ для шифрования данных, а получатель для их расшифровки. В асимметричной используются два ключа, открытый и закрытый. Закрытый ключ хранится у получателя и защищен паролем, который известен только владельцу, а открытый ключ известен всем пользователям. Рассмотрим некоторые широко используемые асимметричные криптосистемы: RSA (Rivest Shamir and Adleman), Diffie-Hellman, DSA(Digital Signature Algorithm), ECC (Elliptic curve cryptography).

RSA

Алгоритм асимметричной криптосистемы с открытым ключом основанный на предполагаемой сложности факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования (обратной операции) за разумное время необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложение числа на простые множители.

Diffie-Hellman

Данный алгоритм позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены, канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования.

Digital Signature Algorithm (DSA)

Криптографический алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования (в отличие от RSA и схемы Эль-Гамаля). Подпись создается секретно, но может быть публично проверена. Это означает, что только один субъект может создать подпись сообщения, но любой может проверить её корректность. Алгоритм основан на вычислительной сложности взятия логарифмов в конечных полях.

Elliptic Curve Cryptography (ECC)

Раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день не известно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования.

Таблица 1. Анализ криптосистем

| № | Криптосистема | Анализ |
|---|---|---|
| 1 | Rivest Shamir and Adleman (RSA) | RSA может использоваться в мобильной связи так как она уязвимая ко многим атакам. |
| | | RSA не подходит для WSN (беспроводная сенсорная сеть) из за высокой сложности |
| 2 | Diffie-Hellman Algorithm | Ключи передаются между двумя пользователями неизвестными друг другу |
| | | Преследуют две цели: проверка подлинности закрытого ключа и подтверждение открытого ключа |
| | | Может использоваться в интернете и почти в каждой криптосистеме используемой в интернете (SSL, SSH, IPSec) |
| 3 | Digital Signature Algorithm (DSA) | Используется приемником для проверки отсутствия изменений в принятом сообщении. Цифровая подпись используется для этой задачи. |
| | | Результат хеш-функции зависит от размера данных |
| 4 | Elliptic Curve Cryptography (ECC) | Алгоритмы с открытым ключом которые могут предоставлять более короткую длину ключа и имеют большую производительность над системами основанными на факторизации и дискретных логарифмах |
| | | Производительность ECC в 5, 15, 20, 60, а иногда и в 400 раз быстрее чем у других. |

Результаты исследования

После рассмотрения всех вышеперечисленных криптосистем, можно сделать вывод что ECC быстрее чем RSA, потому что используются меньшие ключи. Но математически его операция сложна как у RSA. В алгоритме Diffie-Hellman секретный ключ обменивается между двумя пользователями. В то время как цифровая подпись используется получателем в DSA для подтверждения отсутствия изменений в принятом сообщении.

**Литература**

1. RSA [Электронный ресурс] // wikipedia.org: интернет портал URL: https://ru.wikipedia.org/wiki/RSA (дата обращения: 7.04.2017).

2. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си — М.: Триумф, 2002

.

Чекалов Я.А.
*Научный руководитель: к.т.н., доцент каф. ФПМ А. В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: ChekYasha@yandex.ru*

**Разработка программы мониторинга действий пользователя**

Перед любым предприятием в современном мире остро стоит проблема защиты от несанкционированного доступа к своим материальным (помещения, здания) и виртуальным (компьютерные базы данных) ресурсам.

Система контроля действий пользователя - программный или программно-аппаратный комплекс, который позволяет отслеживать действия пользователя, осуществляя мониторинг рабочих операций на предмет их соответствия корпоративным политикам.

Необходимость возникновения данных комплексов была обусловлена увеличением внутренних угроз на предприятиях. В большинстве случаев причинами данных угроз являются:

-халатность сотрудников (невыполнение должностных инструкций, пренебрежение средствами защиты информации)

-намеренная кража информации сотрудником

Подобные системы предотвращают или помогают расследовать утечки конфиденциальной информации, а также выявить нецелевое использование рабочего времени.

Основными целями контроля являются: обеспечение информационной безопасности, выявление случаев некорректного, непрофессионального или нецелевого использования ресурсов, оценка характеристик функционирования сети и параметров использования ресурсов

Целью работы является разработка системы мониторинга действий пользователя.

Для выполнения данной цели были сформированы следующие задачи:

-обзор аналогов

-формирование требование к разработке системы мониторинга действий пользователя

Сравним существующие программы – аналоги:

Таблица 1 – Сравнение существующих программ-аналогов

| Название | Мониторинг экрана, USB-устройств, запущенных процессов, сайтов | Блокировка событий (запуск приложений, блокировка подключения) | Отчетность (генерация по расписанию, конвертация отчетов) |
|---|---|---|---|
| Spector 360 | + | - | + |
| Activity Monitor | + | + | - |
| Разрабатываемое приложение | + | + | + |

Проанализировав основные системы мониторинга действий пользователя, необходимо решить следующие задачи:

-осуществление наблюдения

-контроль действий пользователя на компьютере и предоставление информации о том, сколько времени провел пользователь за компьютером

-мониторинг запущенных программ

-контроль интернет-страниц, которые были посещены

-блокировка указанных событий (игровые, веб-общение, веб-серфинг, мультимедиа и др.)

-сбор и анализ статистики времени работы и активного использования программ и составление на её основе отчетов в удобных для просмотра графиках и таблицах.

Все ходе работы все поставленные цели были выполнены путем решения всех указанных задач.

**Литература**

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. –СПб.: Питер, 2015.-1120с.: ил. – (Серия «Классика computer science»).

2. Дж. Рихтер CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#. 4-е изд.

Шардин Т.О.
*Научный руководитель: к.т.н., доцент каф. ФПМ А.В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: tima.shardin@mail.ru*

**Обзор и анализ методов защищенной передачи данных на примере протокола рукопожатия с использованием криптосистемы RSA**

В настоящее время Интернет – открытая информационная среда. И не только в плане свободы информации, но и в плане несанкционированного доступа к этой информации. По различным историческим и технологическим причинам, большинство трафика, передаваемого разными способами по Интернету, пересылается открытым образом. То есть злоумышленник, подключившийся к каналу передачи данных, сможет беспрепятственно считывать данные, передаваемые пользователем и получаемые им из Интернета. И если содержимое сообщения в тематическом форуме не всегда заслуживает секретности, то номер кредитной карты – напротив, нуждается в хорошей защите. Поэтому разработчики программного обеспечения принимают меры по защите передаваемых данных, тем самым защищая их от злоумышленников. Зачастую это реализуется путем создания защищенного канала передачи данных. В связи с этим анализ, разработка новых и совершенствование существующих методов защищенной передачи информации является актуальной научно-технической задачей.

Объект исследования в данной работе – протокол рукопожатия с использованием криптосистемы RSA, предмет исследования – использование протокола рукопожатия в клиент-серверных приложениях для защиты передаваемых данных.

Целью исследования является обзор и анализ метода защищенного канала передачи данных, реализуемого в клиент-серверных приложениях для защиты информации на примере протокола рукопожатия с использованием криптосистемы RSA.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор метода защищенной передачи информации.
2. Анализ выбранного метода.
3. Результаты исследования.

Обзор метода защищенной передачи информации. На практике, процесс передачи информации через защищенный канал связи зачастую связан с использованием протоколов, основанных на различных криптосистемах. Большинство специалистов сделали вывод, что наилучшие результаты достигаются при использовании, в процессе передачи данных, открытого и закрытого ключа для идентификации клиента или сервера.

В ходе исследования был рассмотрен следующий метод:

Протокол рукопожатия – криптографический протокол, основанный на симметричном взаимном обмене информацией между участниками по схеме запрос – ответ [1]. При использовании криптосистемы RSA в данном протоколе позволяет участникам обмена изначально использовать необходимые параметры для безопасной передачи информации. RSA относится к так называемым асимметричным алгоритмам, у которых ключ шифрования не совпадает с ключом дешифровки. Закрытый ключ находится в тайне, а открытый ключ можно сообщать кому угодно или даже публиковать его. Открытый и закрытый ключи каждого участника обмена образуют согласованную пару в том смысле, что они являются взаимно обратными [2]. Злоумышленнику, перехватившему значение открытого ключа, потребуется большое количество времени или вовсе будет невозможно вычислить пару простых чисел для дальнейшего подбора закрытого ключа, при условии, что простые числа при генерации пары ключей изначально были большими. Тем самым это позволяет использовать данную систему для безопасного обмена информацией в клиент-серверных приложениях [3].

Анализ методов защищенной передачи информации. Для анализа были выбранные следующие критерии:

Требование к материальным затратам – позволяет оценить, рентабелен ли данный метод при разработке приложения, требуется ли материальные затраты для поддержания алгоритма.

Использование центров сертификации – позволяет оценить, необходимо ли дополнительно прибегать к использованию подтверждения подлинности ключей с помощью электронно-цифровой подписи.

Криптостойкость метода – позволяет оценить, обладает ли данный алгоритм достаточной способностью противостоять криптоанализу. Это один из важных критериев, так как при недостаточной или низкой криптостойкости, использование алгоритма для защиты информации между участниками обмена нецелесообразно.

Простота использования алгоритма – позволяет оценить, понятна ли работа для пользователя, работающего с интерфейсом алгоритма.

В результате анализа были выявлены следующие достоинства данного метода, приведенные в таблице:

Таблица 1 – Результаты анализа

| Вид | Требование к материальным затратам | Использование центров сертификации | Криптостойкость метода | Простота использования алгоритма |
|---|---|---|---|---|
| Протокол рукопожатия с криптосистемой RSA | Не требует материальных затрат | Не требует центров сертификации | Обладает высокой криптостойкостью при использовании большой длины ключа (большие простые числа) | Обладает простотой при использовании в приложениях |

Результаты исследования. В результате проведенного исследования было выяснено, что выбранный метод защищенного канала передачи информации, основанного на протоколе рукопожатия с использованием криптосистемы RSA является безопасным для защиты конфиденциальной информации. Данный метод обладает рядом преимуществ, а именно: выгоден по экономическим соображениям (затраты минимальные или их вовсе нет), не требует дополнительных центров сертификации, что позволяет использовать его любому лицу, а также простота в использовании.

**Литература**

1. Цифровые SSL сертификаты [Электронный ресурс] // Habrahabr.ru : интернет портал URL: https://habrahabr.ru/company/tuthost/blog/150433 (дата обращения: 28.03.2016).

2. RSA [Электронный ресурс] // Википедия : свободная энцикл. URL: https://ru.wikipedia.org/wiki/RSA (дата обращения: 28.10.2016).

3. Молдовян А.А., Молдовян Д.Н., Левина А.Б. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с. - экз.

Шитикова А.С.
*Научный руководитель: к.т.н., доцент каф. ФПМ А. В. Астафьев*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: anastasiya.shitikova.96@mail.ru*

**Разработка системы хранения паролей с помощью шифрования**

В последнее время очень актуален вопрос о защите персональных данных. Большинство людей активно пользуются сетью Интернет, регистрируются на множестве сайтов, требующих регистрацию пользователей. Как итог – большое количество паролей от различных аккаунтов сложно удержать в голове. Есть вариант использования одних и тех же данных, но это опасно, так как взломав один аккаунт, злоумышленник может получить доступ ко всем персональным данным.

При сохранении информации на первый план выходят не технические, а системные средства. К ним можно отнести также специальную процедуру ограничения доступа к информации или полный ее перенос в организованные места хранения (архивы, хранилища и др.) [1].

Целью работы является разработка системы хранения паролей в зашифрованном виде.

Для достижения цели были установлены следующие задачи:

- обзор аналогов;
- сформировать требования к разработке системы хранения паролей.

В результате выполнения работы должна быть разработана программа, позволяющая пользователю вносить в нее регистрационные данные своих аккаунтов, иметь к ним удобный доступ [2]. Храниться данные должны в зашифрованном виде в специальном файле.

Рассмотрим приложения-аналоги:

Таблица 1. Сравнение приложений-аналогов

| Аналоги | Особенности | | | |
|---|---|---|---|---|
| | Генерация паролей | Шифрование паролей | Использование «соленого» хеширования | Выбор способа кодирования информации |
| KeePass | + | + | - | - |
| LastPass | + | + | + | - |
| Реализуемая система | + | + | + | + |

После обзора аналогов можно увидеть, что реализуемая система включает в себя все особенности рассмотренных программ.

Хранение данных удобно производить в специализированной базе данных, но ввиду того, что объем данных приложения не будет очень большим (маловероятно, что у пользователя будет несколько сотен или тысяч данных авторизации), использование БД необоснованно и лишь затрудняет разработку программы и ее сопровождение, так как практически все БД требуют установки на компьютере сервера баз данных. Поэтому в программе будет использован бинарный файл. Данный тип файлов по умолчанию не открывается обычными программами редактирования и, соответственно, обеспечивается его сохранность от доступа посторонних лиц.

Требования к разработке системы хранения паролей:

1. Необходимо предусмотреть аутентификацию, для того, чтобы пользователь идентифицировался в системы со своим логином и паролем.

2. Возможность обработки довольно большого количества авторизационных данных пользователя.

3. Также пользователю необходимо вводить название сайта или аккаунта, логин и пароль от него, а также нужно предусмотреть поле для ввода какой-либо дополнительной информации.

Для обеспечения выбора метода кодирования [3] отлично подойдут переключатели, позволяющие пользователю осуществить выбора одного варианта из нескольких.

В ходе исследовательской деятельности были сформулированы требования к разработке системы хранения паролей на основе обзора особенностей приложений аналогов.

**Литература**

1. Зубкова, Т.М. Технология разработки программного обеспечения: Учебное пособие /Т.М. Зубкова. - Оренбург: ГОУ ОГУ, 2004. - 101 с.

2. Степанченко, И.В. Методы тестирования программного обеспечения: Учебное пособие /И.В. Степанченко. - Волгоград: ВолгГТУ, 2006. - 74 с.

3. Левин М.: PGP: Кодирование и шифрование информации с открытым ключом. - М.: Майор, 2001.

Шляпугин М.С.
*Научный руководитель: к.т.н., доцент каф. СГПД М.В. Макаров*
*Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»*
*602264, г. Муром, Владимирская обл., ул. Орловская, 23*
*E-mail: shliapugin.mihail@yandex.ru*

**Обзор и анализ технологии контроля доступа по отпечатку пальца для систем идентификации пользователей**

Целью данной работы является проведение обзора и анализа технологии контроля доступа по отпечатку пальца для систем идентификации пользователей и анализ её преимущества над аналогами. У всех людей отпечаток каждого пальца уникален, который не изменяется естественным образом в период жизни человека. Если же какой-либо из пальцев имеет повреждение, то при идентификации достаточно воспользоваться так называемым «резервным» отпечатком другого пальца, данные о котором, тоже заносят в биометрическую систему. Как правило, алгоритмы сканеров отпечатков пальцев берут характерные точки на пальцах: окончание линии узора, разветвлении линии, одиночные точки. Также дополняется это информацией о самой структуре отпечатка: линий папиллярного узора, «арочных» и спиральных линий. Различные особенности отпечатка перерабатываются в особый код, который использует всю необходимую информативность изображения самого отпечатка пальца. Непосредственно эти коды хранятся в базе персональных данных пользователя, которая используется для идентификации пользователя. Время преобразования полученного изображения отпечатка пальца в код и его идентификация не превышает одной секунды.

На данный момент используются два самых распространенных подхода к реализации систем идентификации по отпечаткам пальцев:

1) Оптическая система. На данный момент - это самый популярный способ сканирования отпечатка пальца исходит из использования оптики - призмы и нескольких линз со встроенным источником света. Свет, попадает на призму, в результате чего идёт отражение от поверхности, которая соприкасается с пальцем идентифицируемого пользователя, и выходит через вторую сторону призмы, попадая на особый оптический сенсор, где и формируется само изображение. Качество идентификации сильно исходит от параметров кожи пользователя – его сухости, наличия масла или бензина, прочих химических элементов. Как пример, у людей с сухой кожей наблюдается размытия изображения на оптическом сканере. Из-за чего происходи высокая доля ложных срабатываний.

2) Полупроводниковая технология. Такая технология применяет путь расчёта пальца электрического поля пользователя. Когда он помещает свой отпечаток в поле сенсора прибора, он является как бы частью пластин конденсатора. Следующая пластина конденсатора является сенсором, который состоит из кремниевого чипа, содержащего 90000 конденсаторных пластин с шагом считывания 500 dpi. Итогом выходит 8-битовое растровое изображение гребней и впадин пальца. Разумеется, в этом методе жировой баланс кожи и уровень чистоты рук не играет никакой функции. Что ещё важно, в этом способе система получается намного компактней, чем оптическая.

Идентификация по отпечатку пальца является самой распространенной и используемой. Она занимает около 54% от всей используемой биометрической идентификации. Анализ основных преимуществ такой системы вынесен в таблицу 1 и позволяет наглядно оценить преимущества в соотношении цены и качества технологии доступа посредством отпечатка пальца перед остальными.

Таблица 1 - Анализ основных преимуществ такой системы идентификации пользователя по отпечатку пальца

| Параметры | Аутентификация | | | |
|---|---|---|---|---|
| | Отпечаток пальца | Радужная оболочка глаза | 3-D распознавание лица | Голос |
| Уровень равной ошибки (EER) | 2 – 3,3% | 4,1 – 4,6% | 4,1% | 4-4,86% |
| Стоимость системы | Низкая | Очень высокая | Высокая | Низкая |
| Отказ в доступе пользователю | 2% | 7% | ~3% | 2-3% |
| Вероятность взлома | 2,5% | 6% | 4% | 3.25% |
| Вероятность пропуска ложной цели | 0,01% | 0,1% | 10% | 0,75% |

Технология контроля доступа по отпечатку не является самой лучшей системой для аутентификации пользователей. Силовые, правоохранительные и государственные структуры могут использовать в своем распоряжении намного более высокоточные системы аутентификации. Однако для средних торговых компаний, рассматриваемая технология является наиболее приемлемой в соотношении цены и качества и предоставляет собой наилучший выбор для использования, но в связи с непосредственной связью качества идентификации от окружающей среды и здоровья пользователя применение на производственных предприятиях нежелательно.

**Литература**

1. Молдовян АА., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета, Университет ИТМО, 2016 – 49с.

2. Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. РУКОВОДСТВО ПО БИОМЕТРИИ. - Издательство: Техносфера, Серия: Мир цифровой обработки, Год издания: 2007.

3. Современные биометрические методы идентификации [Электронный ресурс] // habrahabr.ru. URL: https://habrahabr.ru/post/126144// (дата обращения: 13.04.2017).

4. Сканеры отпечатков пальцев. Классификация и способы реализации [Электронный ресурс] // geektimes.ru. URL: https://geektimes.ru/post/116458// (дата обращения: 13.04.2017).