Евразийский национальный университет имени Л.Н. Гумилева

Тема дипломного работа: Создание системы информационной безопасности Алматинского районного ЦОНа г. Нур-Султан

Выполнил: Жумабаев Беген РЭТ-41

Дипломный руководитель: ф.-м.ғ.к, доцент Мукан Жасузак

Нур-Султан 2019

ВВЕДЕНИЕ

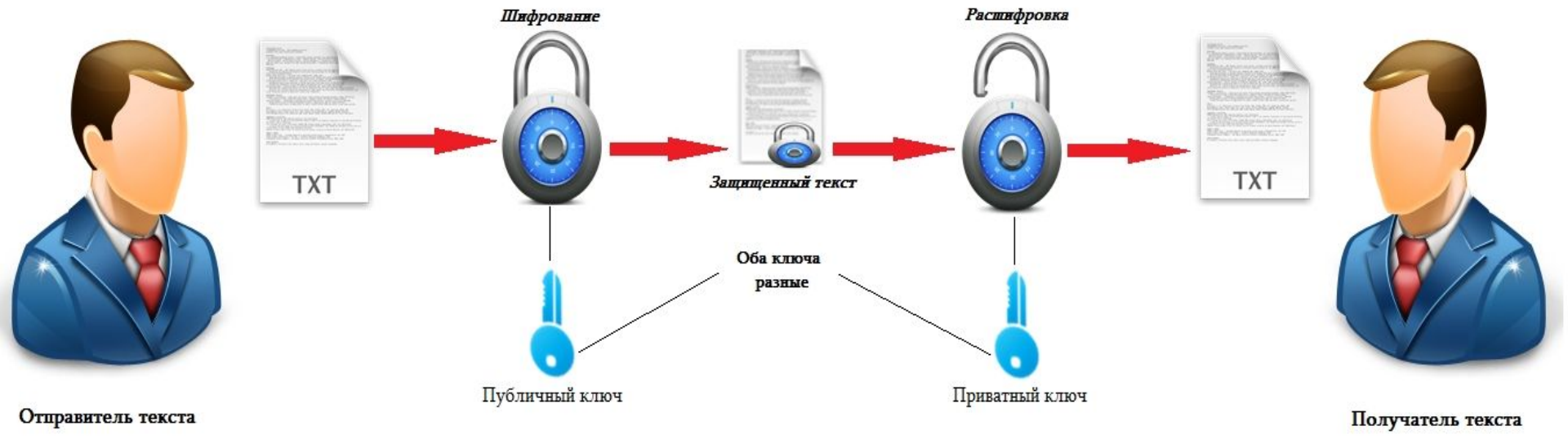
Криптография (от др.-греч. крипто «скрытый» + графия «пишу») наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства. Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных. Изначально криптография изучала методы шифрования информации - обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст. Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография - одна из старейших наук, её история насчитывает несколько тысяч лет.

АЛГОРИТМ - RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи.



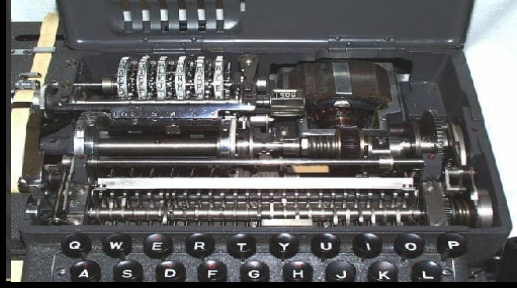
Цель дипломного работа

1. Защищать документы и программного обеспечения в центре обслуживания населения.

2. Создание цифрового подписи в центре обслуживания населения.

3. Профилактика способы предотвращения хакерских атак (информационной безопасность) в центре обслуживания населения.

ПЕРВАЯ ТЕОРЕТИЧЕСКАЯ ЧАСТЬ ОСНОВЫ КРИПТОГРАФИИ



История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.

Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами). Второй период (хронологические рамки — с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) — до начала XX века) ознаменовался введением в обиход полиалфавитных шифров. Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

Четвёртый период — с середины до 70-х годов XX века — период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости для различных известных атак — линейного и дифференциального криптоанализа. Однако, до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами (в предыдущие эпохи использование криптографии было исключительной прерогативой государства). Правовое регулирование использования криптографии частными лицами в разных странах сильно различается — от разрешения до полного запрета.

Современная криптография образует отдельное научное направление на стыке математики и информатики — работы в этой области публикуются в научных журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества — её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

Шифрование паролей enable и console. Cisco packet tracer.


```
Switch>
Switch>en
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# en
Switch(config)# enable pass
Switch(config)# enable password Begen
Switch(config)#ex
Switch#
Switch#show run
Building configuration...

Current configuration : 1100 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable password Begen
!
```

```
Switch>
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#service password-encryption
Switch(config)#service password-encryption
Switch(config)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show run
Building configuration...

Current configuration : 1106 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable password 7 080349490C17
!
!
!
```

Спасибо за внимание!