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

Определение состава виртуальной криптографической лаборатории

Криптография – область знаний, изучающая криптологию и методы ее раскрытия (криптоанализ). [1]

До недавнего времени все исследования в этой области были только закрытыми, но в последние несколько лет как в России, так и за рубежом стало появляться всё больше публикаций в открытой печати. Отчасти смягчение секретности объясняется тем, что стало уже невозможным скрывать накопленное количество информации. С другой стороны, криптография всё больше используется в гражданских отраслях, что требует раскрытия сведений. [2]

Криптографическая система – совокупность технических и программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей. [3]

Одна из основных целей криптографической системы заключается в том, чтобы зашифровать осмысленный исходный текст (также называемый открытым текстом), получив в результате совершенно бессмысленный на первый взгляд шифрованный текст. Получатель, которому он предназначен, должен быть способен дешифровать этот шифротекст, восстановив, таким образом, соответствующий ему открытый текст. [1]

В соответствии с государственными стандартами аппаратная часть криптографической лаборатории должна включать в себя отдел аппаратных средств вычислительной техники, оснащенный рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и сети Интернет, учебным сетевым программным обеспечением, обучающим программным обеспечением, а так же отделом программно-аппаратных средств обеспечения информационной безопасности, оснащенный антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации (включающими в том числе криптографические средства защиты информации). [2]

Как можно было заметить, для изучения криптографии требуется большое количество аппаратуры, которая в свою очередь требует не малых затрат. Как правило, не все учебные заведения могут позволить себе создать полноценную физическую криптографическую лабораторию, соответственно, возникла потребность в создании виртуальной криптографической лаборатории.

Для создания лаборатории необходимо опередить состав – это и является целью научного исследования.

Приобретение оборудования для лаборатории предполагает большие затраты, которые можно снизить за счет внедрения системы «Виртуальная лаборатория», которая требует на много меньше затрат, что будет позволять учебным заведениям тратить бюджет на другие не менее важные цели.

В большинстве случаев, для использования виртуальной криптографической лаборатории потребуется иметь в наличии персональный компьютер или же ноутбук. Все криптографические и связанные с ними процессы практически полностью будут моделироваться на работающей машине.

Для студентов будет возможным работа над проектами вне института, что повысит быстроту выполнения заданий, так как все необходимое всегда будет рядом в любое время.

Так же данная лаборатория будет составлять полный отчет о процессе работы по окончании тех или иных процессов, что в свою очередь так же поможет студентам при оформлении документации для сдачи.

В соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки Прикладная математика и информатика в состав виртуальной лаборатории должны входить следующие основные компоненты:

1. Модули работы с ассиметричными типами шифрования.
2. Модули работы с симметричными типами шифрования.
3. Модули анализа выше указанных типов шифрования.
4. Модули проверки криптостойкости алгоритмов.
5. Модули получения Хэш-функций.
6. Модуль формирования секретных ключей с использованием асимметричных алгоритмов.

Реализация всех модулей должна соответствовать данным требованиям:

1. Зашифрованное сообщение должно поддаваться чтению только при наличии ключа.
2. Знание алгоритма шифрования не должно влиять на надежность защиты.
3. Любой ключ из множества возможных должен обеспечивать надежную защиту информации.
4. Алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

Эти пункты являются основными в изучении криптографии, следовательно, их наличие обязательно для лаборатории.

В результате проведенного исследования был определен основной состав виртуальной криптографической лаборатории.

Криптография сегодня - это важнейшая часть всех информационных систем: от электронной почты до сотовой связи, от доступа к сети Интернет до электронной валюты. А в будущем, по мере того как коммерция и коммуникации будут все теснее связываться с компьютерными сетями, криптография станет неотъемлемой частью нашей жизни. Следовательно, мы должны способствовать развитию обучающего процесса, и возможно, что виртуальная криптографическая лаборатория станет одной из ступеней на этом тернистом пути.

Список источников

1. Криптография [Электронный ресурс] //Wikipedia.ru: интернет портал URL: «https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F» (дата обращения 21.03.2016)
2. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.
3. Сергей Баричев Основной вопрос криптографии – Санкт-Петербург : СПб: Университет ИТМО, 2015 – 25с. – экз.