УДК 517.1:519.6

ДОСЛІДЖЕННЯ ТА ОГЛЯД МОДЕЛЕЙ ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

Студ. Казабер Джеладзе, гр. МгЗІТ-1-18
Науковий керівник доц..Т.І.Астістова
Київський національний університет технологій та дизайну

Мета і завдання. Дослідити існуючі складові моделі технологій кібербезпеки та практичні аспекти мереж наступних поколінь, розробити варіант, який би перейняв переваги та врахував недоліки існуючих методів та моделей на ринку.

Об'єкт та предмет дослідження. Основним об'єктом дослідження є архітектура системи кібербезпеки інфокомунікацій, відповідно до вимог безпеки, модель довіри кібербезпеки та система існуючих сервісів програмно-апаратного забезпечення. Предметом дослідження виступають алгоритми криптографічних методів шифрування, розподілу ключів, запозичених фрагментів та підготовки матеріал для оцінки метода.

Методи та засоби дослідження. Теоретичною основою при вирішенні науково-технічної проблеми є праці провідних вчених в галузі кібербезпеки та захисту від кібератак, теорії мереж, математичного моделювання, математичного та програмного забезпечення. У теоретичних дослідженнях використано методи та алгоритми технології криптографії, а саме: цифрові підписи, шифрування, розподіл ключів.

Наукова новизна та практичне значення отриманих результатів. Даний програмний продукт відрязняється більш точними алгоритмами пошуку співпадінь, що гарантує більш високу якість захисту. Оптимізовані шляхи зрівняння дають більш високу швидкість роботи та отримати результат. Система має зручний інтуїтивний інтерфейс, який полегшує роботу з програмою

Результати дослідження. В результаті дослідження було проаналізовано ряд матеріалів Міжнародного союзу електрозв'язку. Серед пострадянських країн, охоплених дослідженням "Глобальний індекс кібербезпеки 2017" Міжнародного союзу електрозв'язку, Грузія вийшла на 8 місце. Росія зайняла 10 місце. Останніми виявилися Вірменія і Туркменістан. "Хворою точкою" Грузії є недолік галузевих центрів кібербезпеки (CERT), Росії - низький рівень стандартизації в області кібербезпеки для організацій. У звіті говориться, що уряд Грузії, після широкомасштабних кібератак на інтернет-простір країни в 2008 році, рішуче підтримав роботу по захисту державних ІТ-систем. Законом про інформаційну безпеку було створено Бюро кібербезпеки, основнимзавданням якого захист найважливіших ІКТ-систем Міністерства оборони Грузії .Сьогодні технічними можливостями комп'ютерів, їх програмним забезпеченням, мережею Інтернет, стільниковим зв'язком прагнуть скористатися кримінальні елементи, кількість яких з кожним днем зростає. На думку фахівців, темпи зростання злочинності в глобальній мережі Інтернет є найшвидшими на Кібербезпека являє собою набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту киберсреды, ресурсів організацій і користувачів. Кібербезпека має на увазі досягнення і збереження властивостей безпеки у ресурсів організації або користувачів, спрямованих проти відповідних кіберугроз.

Захист інформації, що передається й обробляється в мережах, полягає у створенні та підтримці в дієздатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення кібербезпеки оброблюваної

інформації та NGN у цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації. Система зазначених заходів, що забезпечує захист інформації в NGN, називається комплексною системою захисту інформації.

У процесі свого розвитку послуги та механізми безпеки переросли в закінчені технології, тобто сукупність методів, процесів, засобів і заходів, що використовуються для забезпечення кібербезпеки. Логіку забезпечення безпеки доцільно доповнити технологіями кібербезпеки, які зручно описувати ієрархічною послідовністю: "техніка кібербезпеки (technique – технічні прийоми) → категорії (category) технологій кібербезпеки → технології (technology) кібербезпеки"

Складові моделі класифікації технологій кібербезпеки:

– криптографія (Cryptography);
– контроль доступу (Access control);
– цілісність системи (System integrity);
– аудит і моніторинг (Audit and Monitoring);
– менеджмент (Management);

Однією з ефективних технологій захисту інформаційних ресурсів є застосування криптографічних методів. Методи криптографії поділяють на два основних типи: симетричного ключа та асиметричного ключа. На рисунку 1. представлена схема передачі інформації між двох осіб - A та B. Це можуть бути як фізичні особи так і організації

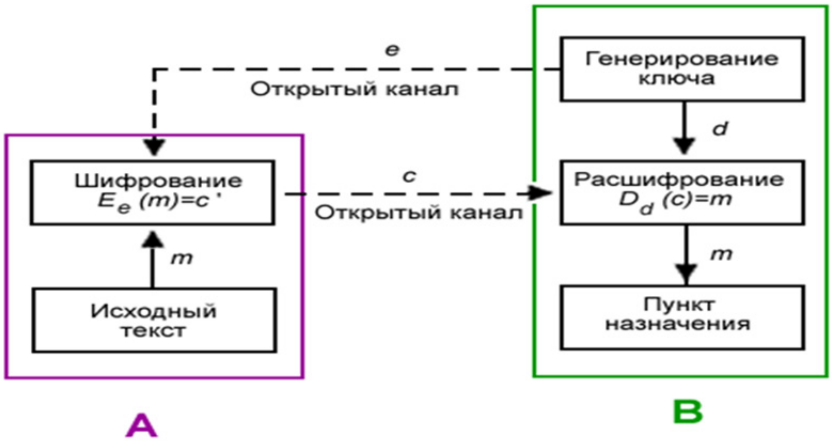

Рисунок 1 – Схема передачі інформації

Криптографія симетричного ключа використовує алгоритм шифрування RSA, в яких ключ шифрування та ключ дешифрування один і той самий та алгоритм узгодження ключів, які можна реалізувати на мові Python 3. RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису.

Висновки. В результаті дослідження були розроблені програмні продукт на основі алгоритмів криптографічного шифрування та програми, які забезпечують захист від проникнення , написані мовою Python.

Ключові слова: кібербезпека, алгоритм, Python , RSA, криптографія.

ЛІТЕРАТУРА

1. Валов С.Г. Инфокоммуникационные сети будущего: тормоза технологий переноса / С.Г. Валов, А.В. Голышко // Вестник связи. – 2013. – № 5. –109 с.

2. Тесля В.Я. Концептуальные подходы к технологии сетей нового поколения NGN / В.Я. Тесля, А.Л. Бабосюк, В.В. Сикорский, А.Е. Рудниченко //Зв'язок. – 2014. – № 2. – С.87.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C // Б.Шнайер // М.: Триумф, 2012. — 816 с.