РОЗДІЛ 4.
ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Виходець Юрій Олександрович
начальник Управління протидії кіберзлочинам в Одеській області
Департаменту кіберполіції Національної поліції України

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ В ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ КАК СТРУКТУРНЫЙ ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ АБСОЛЮТНОЙ БЕЗОПАСНОСТИ

1. На сегодняшний день информационная инфраструктура общества достигла колоссальных размеров. Такая информационная среда представляет собой сегментированную часть мирового механизма взаимодействия человечества. Как и в любом другом направлении, в сфере высокотехнологичных разработок присутствуют сектора, именуемые сегментами среды. К таким сегментам можно отнести: сегмент сотовой и мобильной связи; сегмент разработки настольных и мобильных компьютеров и суперкомпьютеров; сегмент создания и поддержки обслуживающих слоёв информационной инфраструктуры и другие. Для компаний, работающих в вышеупомянутых сегментах информационной среды, приоритетными направлениями развития механизмов абсолютной безопасности являются:

• Создание и тестирование устройств, для достижения безотказной работы;

• Обеспечение информационной безопасности, включая техническую безопасность;

- Разработка технологий комфортной работы.

Сохранение целостности и безопасности информации достигается благодаря информационным технологиям, основанным на протоколировании, а сущность протоколов состоит во внедрении в них различных алгоритмов сильного шифрования.

2. Наиболее ярко необходимость протоколирования просматривается в сегменте сотовой, компьютерной и транспортной инфраструктурах, отвечающих за сохранение и безопасную передачу конфиденциальной и персональной информации.

3. Для достижения наивысшей (абсолютной) безопасности при передаче данных, необходимо совокупное использование криптографических протоколов, а внутри них – симметричных и ассиметричных шифров. Криптографическое протоколирование необходимо в транспортных обслуживающих слоях информационной инфраструктуры, состоящее из набора приоритетов пользователей, правил распределения ролей, механизмов идентификации и аутентификации источника данных, отравителя и получателя, системы проверок подлинности пользователей благодаря технологиям ЭЦП.

4. В ходе данного исследования была предложена разработка такого криптографического протокола транспортных слоёв информационного сегмента, который обеспечивает целостность передачи данных, а также безопасную их транспортировку между субъектами сети – пользователями, серверами, другими ЭВУ, обеспечивающими работоспособность сети, и/или пользующимися услугами такой сети. За передачу информации о пользователях будет отвечать протокол Диффи-Хелмана, с разработанной защитой против атаки MIM, так же, данный протокол будет отвечать за передачу ключей доступа и идентификацию; алгоритм RSA 2048 bits будет отвечать за конфиденциальность данных, анонимность сторон передачи информации и невозможность прочтения данных в случае перехвата; за скорость определения экранов безопасности будет отвечать симметричный алгоритм AES128 bits;

за разграничение ролей и доступа будет отвечать специально усиленная система безопасности Белла-ЛаПадуллы.

5. Таким образом, используя предложенный протокол безопасности, можно говорить о том, что он представляет собой основу целостной информационной технологии, работающей на основании криптографического протоколирования и сильного шифрования для обеспечения абсолютной безопасности. Данная технология может быть использована в любой сегментированной области информационной инфраструктуры, использующей высокую степень безопасности данных в транспортных слоях передачи конфиденциальных данных.

Ключові слова: криптографічний протокол, інформаційна інфраструктура, кібербезпека.
Ключевые слова: криптографический протокол, информационная инфраструктура, кибербезопасность.
Keywords: cryptographic protocol, information infrastructure, cybersecurity.

Василенко Микола Дмитрович
Національний університет «Одеська юридична академія»
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

Новіков Вячеслав Пантелійович
Національний університет «Одеська юридична академія»
доцент кафедри кібербезпеки, к.т.н, доцент

Рачук Валерій Олександрович
Національний університет «Одеська юридична академія»
асистент кафедри кібербезпеки

БЕЗПЕКА ТА ВИКЛИКИ СУЧАСНОСТІ: РИЗИКИ ТА КІБЕРБЕЗПЕКА В ПЕРІОД ПАНДЕМІЇ

Інформація, яка надходить з різних країн світу свідчить про те, що в результаті пандемії з великим процентом ймовірності очікуються ризикові економічні та політичні негаразди.