41. В чому сутність моделі оцінки автентичності на основі ЕЦП, критерії оцінки?

У найбільш узагальненому вигляді під *криптографічним протоколом автентифікації* будемо розуміти криптографічний протокол встановлення достовірності твердження, що об'єкт (суб'єкт) має очікувані властивості. Як правило, достовірність твердження встановлюється з деякою ймовірністю. Тому має сенс застосування такого визначення протоколу автентифікації: *автентифікація об'єкта (суб'єкта) (en entity authentication) – це підтвердження із заданою ймовірністю того, що об'єкт (суб'єкт) є тим, за кого він себе видає.*

Важливими характеристиками криптографічного протоколу є автентичність суб'єктів, які взаємодіють, автентичність та криптографічна живучість ключів тощо. До основних також можна віднести такі характеристики криптографічних протоколів: **1) автентифікація суб'єктів; 2) автентифікація ключів; 3) вид автентифікації; 4) вид автентифікації ключів;** 5) вид підтвердження ключів; 6) новизна ключів; 7) управління ключами; 8) складність обчислень; 9) можливість попередніх обчислень; 10) захищеність від раніше переданих повідомлень; 11) вимоги до третьої сторони; 12) криптоживучість ключів; 13) складність криптографічного аналізу; 14) неспростовність; 15) число повторень (раундів, обмінів) тощо.

При оцінці рівня безпеки криптографічних протоколів у першу чергу необхідно вибрати (встановити) можливі моделі або модель порушника. *Порушник (зловмисник)* – це суб'єкт чи об'єкт, що навмисне чи ненавмисне реалізує загрози з метою нанесення втрат системі та/або власникам, користувачам тощо. Причому загроза – це потенційно існуюча небезпека нанесення втрат у системі в результаті реалізації деяких дій порушниками та зловмисниками. Загрози бувають активні й пасивні. *Пасивна* – загроза, у результаті реалізації якої не змінюється інформаційний стан системи, але збиток наноситься. *Активна* – загроза, в результаті реалізації якої змінюється стан інформаційної системи та наносяться збитки власникам та або користувачам системи.

В першу чергу порушник може бути *зовнішнім або внутрішнім*, *активним або пасивним*. Зовнішній порушник – порушник, що може мати тільки загальнодоступні дані криптографічного протоколу, а також мати доступ тільки до відкритих каналів зв'язку. Внутрішній порушник – порушник, який, крім інформації, доступної зовнішньому порушнику, може мати деяку специфічну інформацію (час і режим обміну інформацією, додаткові дані, що використовуються в протоколі).

Активний порушник – порушник, що при спробі розкриття криптосистеми здійснює активні дії, тобто дії, при яких порушник під час протоколу яким-небудь чином впливає на дані, передані в каналах зв'язки. Пасивний порушник – порушник, що виконує атаку на протокол за допомогою прослуховування каналу зв'язку та перехоплення всіх переданих між учасниками протоколу повідомлень і подальшого їх аналізу.

Крім наведених вище визначень порушника, існують рівні можливостей порушника. Визначення рівнів залежить від запланованих умов експлуатації засобів КЗІ та цінності інформації, що захищається:

- нульовий рівень – випадкове ненавмисне ознайомлення зі змістом інформації (випадкове прослуховування в каналі);

- перший рівень – порушник має обмежені кошти і самостійно створює засоби та методи атак на засоби КЗІ, а також інформаційно-телекомунікаційні системи із застосуванням доступних програмних засобів та електронно-обчислювальної техніки;

- другий рівень – порушник корпоративного типу має змогу створення спеціальних технічних засобів, вартість яких співвідноситься з можливими фінансовими збитками при втраті, спотворенні та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

- третій рівень – порушник має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави.

Існує велика кількість можливих атак на криптографічні протоколи. Вид атаки найбільшою мірою визначається видом, класом і властивостями протоколу, на який здійснюється атака.

Оцінка ступеня ефективності атаки може бути здійснена за рахунок проведення аналізу даних, якими володіє зловмисник, аналізу його можливостей та інших параметрів атаки. Основним методом оцінки можливостей зловмисника при атаці є створення моделі атаки.

Приклад моделі автентифікації на основі ЕЦП (з використанням асиметричної криптографії)

Усі криптографічні операції операції виконуються програмно, а приватний ключ формується на базі паролю. Обидва рішення використовують криптографію на базі ЕК, тому що вона більш стійка, ніж RSA, а це дозволяє використовувати коротші ключі й знижує вимоги до продуктивності.

Регистрация.

- Клиент выбирает *login* и *password*;
- На их основе формируется *PrivateKey = SHA256(login+password)*;
- На основе *PrivateKey* формируется *PublicKey*;
- *Login* и *PublicKey* отправляются на сервер и сохраняются в БД.

Аутентификация.

- Клиент вводит логин и пароль;
- На их основе формируется *PrivateKey = SHA256(login+password)*;
- Клиент получает от сервера случайное число(*RNDserver*) и генерирует свое случайное число(*RNDclient*);
- С помощью *PrivateKey* клиент формирует ЭЦП *Sign(SHA256(RNDserver+RNDclient))* и отправляет на сервер *Login, RNDclient* и *ЭЦП*;
- Сервер проверяет корректность ЭЦП с помощью *PublicKey* клиента, хранящегося в БД.