29. Які вимоги до засобів КЗІ в частині генерування ключів та як вони можуть бути виконані ?

Основною складовою, яка визначає якість ключів є генератори випадкових чисел (послідовностей). Випадкові числа використовуються для побудови гами в поточних криптосистемах, ключів для сеансів (сеансових) та інших ключів в блочних криптосистемах, початкових значень, для генерації параметрів в асиметричних крипто системахl, випадкових значень параметрів для багатьох систем електронного цифрового підпису, «випадкових наборів» даних в протоколах автентифікації тощо.

Визнаним є той факт, що криптографічна стійкість криптографічних перетворень і безпечність реалізації різноманітних криптографічних протоколів в суттєвій мірі залежить від того, яким чином генеруються та застосовуються різні види ключових даних (ключів). Загальним підходом до генерування ключів є застосування для цього генераторів випадкових послідовностей та/або детермінованих генераторів випадкових послідовностей (бітів). *Принциповою відмінністю чисто випадкових послідовностей від псевдовипадкових послідовностей (бітів) є те, що псевдовипадкова послідовність може бути відновлена в просторі і часі без попереднього її запису. Випадкова ж послідовність може бути відновлена тільки якщо її попередньо записати і в подальшому зберігати, розповсюджувати, вводити в дію і т.д.* Ще раз підкреслимо, що, як правило, при генеруванні ключів та ключової інформації вводять та застосовують ключ генератора ключів, який визначає його ентропію як джерела ключів.

Як до генераторів випадкових послідовностей(ГВП), так і до детермінованих генераторів випадкових послідовностей (ДГВП) (бітів), висуваються складні вимоги в частині генерування символів послідовності випадково, рівно ймовірно, незалежно та однорідно. При цьому факт компрометації ключа є критичним явищем в самій вищій мірі. Також повинно бути забезпечене оперативне відновлення ключа в просторі та часі.

Нині загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів та практичних (конкретних) алгоритмів їх генерування. При чому, як можна судити із ряду джерел, ці методи, механізми та алгоритми стараються захистити від розповсюдження особливо в частині генерування випадкових послідовностей. Також у зв’язку із суттєвим розвитком інфраструктури відкритих ключів виникла потреба в створенні апаратних, апаратно-програмних та програмних засобів генерування асиметричних пар ключів. Були розроблені та прийняті спочатку регіональні стандарти, а потім і міжнародні стандарти, в яких були визначені вимоги, методи, механізми та алгоритми реалізації генераторів. При чому у зв’язку з необхідністю відновлення ключів та ключової інформації в просторі і часі в них в повному обсязі розглядаються тільки детерміновані генератори випадкових бітів, що визначає їх особливу актуальність.

Основними вимогами, що висуваються до детермінованих генераторів випадкових бітів (ДГВБ) є непередбачуваність, просторова та тимчасова складність, відновлюваність в просторі і часі, необоротність, також період

повторення. Він повинен бути не менше заданого, подібно блочним симетричним шифрам, при чому в якості заданого може використовуватись:

- 2^{128} – нормальний рівень стійкості;
- 2^{256} – високий рівень стійкості;
- 2^{512} – надвисокий рівень стійкості;.

Запропоновано декілька підходів до визначення рівнів гарантій. Перший з них пов'язаний з тестування псевдовипадкових бітів (тобто випадкових бітів, сформованих детермінованим генератором випадкових бітів) на випадковість, для чого, наприклад, застосовується стандарт FIPS 140-1, або AIS 20. Більш детальними є вимоги та механізми реалізації, що визначені в AIS 20, що дозволяє реалізувати різні рівні гарантій – К1, К2, К3, К4. При цьому самим вищим рівнем гарантій являється рівень К4. В AIS 31 визначено два рівня гарантій Р1 і Р2, в яких, по суті, Р1 дещо еквівалентний К1, К2, а Р2 еквівалентний К3, К4. У випадку рівня гарантій К4 вимагається, щоб псевдовипадкові біти мали статистичні властивості, подібні до статистичних властивостей псевдовипадкових бітів, що генеровані ідеальним ДГВБ, була заданою ентропія джерела ключів (тобто наявність ключа генератора є обов'язковою), а також повинна бути практично виключена можливість обчислення попередніх та наступних бітів генератора при знанні поточного стану.

Необхідною умовою забезпечення криптографічної стійкості є формування ключів, ключової інформації та певних параметрів на основі використання одночасно як засобів формування фізично випадкових та детермінованих випадкових послідовностей. Якщо ця необхідна вимога не виконується, то говорити про певний рівень криптографічної стійкості немає сенсу. Крім того, є визнаним той факт, що криптографічні протоколи з нульовим розголошенням можуть бути реалізованими тільки за умови використання для формування ключів та ключової інформації і параметрів фізично випадкових засобів.

В цілому система управління ключів представляє собою комплексну організаційно-технічну систему, що забезпечує надання усіх послуг з питань генерування, реєстрації, накопичування, розподілення, збереження, передавання, приймання, уводу в дію, використання, архівування, знищення ключів та іншого ключового матеріалу, що використовуються при здійсненні криптографічних перетворень.

Так для реалізації потокового симетричного шифру до криптографічно стійкого генератора псевдовипадкової послідовності чисел (гами шифру) пред'являються три основних вимоги:

– період гами повинен бути досить великим для шифрування повідомлень різної довжини;

– гама повинна бути практично непередбачуваною, що означає неможливість передбачити наступний біт гами, навіть якщо відомі тип генератора й попередній відрізок гами;

– генерування гами не повинне викликати великих технічних складностей.

Із наведеного вище можна зробити висновок, що від якості випадковості формування ключів, ключової інформації та системних параметрів суттєво залежить криптографічна стійкість. Прн цьому Алгоритми генерації та тестування послідовностей випадкових чисел є базовими алгоритмами, що забезпечують дійсну криптографічну стійкість алгоритмів та механізмів криптографічного захисту інформації.

Базовими міжнародними стандартами, що стандартизують алгоритми генерації послідовностей випадкових чисел є :

– міжнародний стандарт ISO/IEC 18031 “Information technology – Random number generation”, який визначає алгоритми генерації псевдовипадкових та випадкових чисел, а також визначає статистичні тести перевірки генераторів;

– міжнародний стандарт ISO/IEC 18032 “Information technology – Prime number generation”, який визначає методи генерації простих чисел та методи тестування чисел на простоту;

– національний стандарт ДСТУ ISO/IEC19790 «Інформаційна технологія Методи захисту – Вимоги з захисту для криптографічних модулів».

Додаткові вимоги до алгоритмів та реалізацій методів і засобів генерації та тестування послідовностей випадкових чисел визначаються національними та промисловими стандартами США – FIPS 140-3, ANSI X9.17, ANSI X9.31 , ANSI X9.44 та ін., а також рекомендаціями NIST – NIST SP 800-22 і рекомендаціями органу зі стандартизації Німеччини – AIS-20, AIS-31 та ін.