Розділ 10

ВИМОГИ ДО ЗАСОБІВ КЗІ ТА УПРАВЛІННЯ КЛЮЧАМИ В ПЕРСПЕКТИВНИХ ІВК

Засоби ЕЦП є елементами системи ІВК (ЕЦП), що суттєвою мірою впливають на рівень безпеки та гарантій таких структур. Тому при створенні ІВК в першу чергу висувають вимоги до засобів КЗІ, що застосовуються для виконання таких криптографічних перетворень, як вироблення цифрового підпису, перевіряння цифрового підпису, генерування асиметричної пари ключів, виготовлення сертифікатів відкритих ключів, контроль цілісності й справжності ключів а також загальносистемних параметрів. У найбільш обґрунтованому системному вигляді вперше вимоги до засобів криптографічних перетворень в ІВК викладені в [116–118, 122–123]. У подальшому необхідно відзначити вимоги та рекомендації, що висунуті в нормативних і рекомендаційних документах Європейського Союзу [5, 226–228].

10.1. РІВНІ ГАРАНТІЙ ФЕДЕРАЛЬНОГО МОСТУ США

Згідно з [66–69, 117, 230–238] сторони, що взаємодіють, повинні оцінювати середовище і зв'язані загрози й уразливості та визначати рівень ризику, якому вони будуть піддаватися. Для забезпечення значної модульності згідно з Політикою сертифікації (СР) США можуть задаватись вимоги до захисту сертифікатів на п'ятьох рівнях гарантії: рудиментарному, базовому, середньому, середньо-апартному та вищому.

Згідно з Політикою сертифікації криптографічні модулі повинні атестуватися до рівнів, що визначені у FIPS-140. У відповідності до чинної Політики Федеральний центр Політики PKI має право на розгляд технічної документації, що пов'язана з будь-якими криптографічними модулями, призначеними для використання у FBCA. Також Федеральний Центр PKI Політики може визначати, що й інші діючі стандарти атестації, сертифікації або верифікації можуть застосовуватись для перехресної сертифікації з участю неамериканських урядових PKI.

Нижче в таблиці 10.1 наведено перелік мінімальних вимог до криптографічних модулів, які повинні виконуватися, залежно від рівня гарантії. В розділі 12 ми також наводимо перелік більш сурових вимог, наприклад до перспективних ІВК.

Таблиця 10.1. **Перелік мінімальних вимог до криптографічних модулів**

Рівень гарантії	CA (центр сертифікації)	Абонент	RA (центр реєстрації)
Рудиментарний	Рівень 1 (апаратні засоби або програмне забезпечення)	Не визначені	Рівень 1
Базовий	Рівень 2 (апаратні засоби або програмне забезпечення)	Рівень 1	Рівень 1 (апаратні засоби або програмне забезпечення)
Середній	Рівень 2 (апаратні засоби)	Рівень 1	Рівень 2 (апаратні засоби)
Середньоапартний	Рівень 2 (апаратні засоби)	Рівень 2 (апаратні засоби)	Рівень 2 (апаратні засоби)
Вищий	Рівень 3 (апаратні засоби)	Рівень 2 (апаратні засоби)	Рівень 2 (апаратні засоби)

Федеральний міст FBCA може видавати щонайменше один сертифікат з вищим рівнем гарантій. У таблиці 10.2 наведені вимоги до сертифікатів залежно від рівня гарантій, що мають бути забезпечені у відповідній інфраструктурі.

Таблиця 10.2. **Рівні гарантій для сертифікатів Федерального мосту США**

Рівень гарантії	Придатні для використання сертифікати
1	2
Рудиментарний	Цей рівень забезпечує найнижчу ступінь гарантії відносно ідентичності особи. Одна з головних функцій цього рівня є забезпечення цілісності даних відносно інформації, що підписується. Цей рівень відноситься до середовищ, у яких ризик зловмисних дій вважається низьким. Він не придатний для трансакцій, що вимагають автентифікацію, і звичайно недостатній для трансакцій, що вимагають конфіденційності, але може використовуватися коли сертифікати з більш вищими рівнями гарантії не доступні.
Базовий	Цей рівень забезпечує базовий рівень гарантії, який відноситься до середовищ, де є ризики і наслідки компрометування даних, але вони не вважаються сильно значущими. Це може включати доступ до особистої інформації, де можливість зловмисного доступу до інформації є не високою. Вважається, що на цьому рівні захисту користувачі не можуть бути зловмисниками.

Закінчення табл. 10.2

1	2
Середній	Цей рівень пов'язаний із середовищами, де ризики або наслідки від компрометації даних є помірними. Це може включати трансакції, які мають значиму грошову цінність або ризик підробки, або які включають доступ до особистої інформації, де можливість зловмисного доступу є великою
Середньоапаратний	Цей рівень пов'язаний із середовищами, де загрози для даних є великими або наслідки порушення послуг захисту є високими. Це може включати трансакції дуже високої цінності або такі, що можуть мати високі рівні ризику підробки
Вищий	Цей рівень резервується для перехресної сертифікації з участю державних об'єктів і придатний для середовищ, де загрози для даних є високими, або наслідки від порушення послуг захисту є високими. Це може включати трансакції дуже високої цінності або високі рівні ризику підробки

У табл. 10.3 наведено перелік вимог іменування субєктів, які згідно з Політикою СР повинні застосовуватись до кожного рівня гарантії.

Таблиця 10.3. **Рівні гарантій ідентифікації (іменування) Федерального мосту США**

Рудиметарний	**Ненульове ім'я суб'єкта або нульове ім'я суб'єкта, якщо альтернативне ім'я суб'єкта визнано й відмічено як критичне**
Базовий	Ненульове ім'я суб'єкта та опціональне альтернативне ім'я суб'єкта, якщо воно відмічено як некритичне
Середній (усі політики)	Ненульове ім'я суб'єкта та опціональне альтернативне ім'я суб'єкта, якщо воно відмічено як некритичне
Вищий	Ненульове ім'я суб'єкта та опціональне альтернативне ім'я суб'єкта, якщо воно відмічено як некритичне

10.2. АНАЛІЗ ТА ОБҐРУНТУВАННЯ ВИМОГ ДО ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІВК ТА ПРИНЦИПИ ЇХ ЗАБЕЗПЕЧЕННЯ

Аналіз джерел показав, що найбільш широко й системно вимоги до засобів КЗІ були визначені у федеральних стандартах США FIPS 140-1, FIPS 140-2 та в робочому проекті FIPS 140-3 [118], а також у [120–125]. Деякі відомості щодо вимог наведено в [123]. З них можна зробити висновок, що при побудуванні криптографічних систем необхідно обґрунтовувати та вибирати з відповідним рівнем захищеності криптографічні засоби, політики їх застосування, криптографічні перетворення та протоколи, протоколи управління та сертифікацію ключів тощо. При цьому, у першу чергу, необхідно враховувати таке:

– наскільки важливою є ІС чи ІТС для вирішення завдань організації;

– якою мірою повинні використовуватися національні та міжнародні стандарти;

– які вимоги щодо ефективності криптографічних механізмів повинні виконуватися (наприклад, пропускна здатність, час обробки, їх здатність протистояти діям порушників тощо);

– які вимоги повинні виконуватися щодо внутрішньосистемної здатності та міжсистемною здатністю й інтероперабільністю;

– вимоги щодо криптографічних алгоритмів, криптографічних протоколів та протоколів зв'язку тощо;

– мета та цілі безпеки інформації, мета та цілі застосування криптографічних засобів і механізмів;

– які послуги та за яким профілем повинні надаватися, наприклад, цілісність, справжність, конфіденційність, доступність, спостережливість, неспростовність;

– протягом якого періоду часу інформація повинна бути захищена;

– які регламенти та політики повинні бути застосовані;

– якою мірою користувачі проінформовані щодо криптографії та наскільки добре вони навчені;

– у чому полягає сутність фізичної та процедурної інфраструктури з криптографічного захисту інформації та даних, наприклад, збереження, облік та аудит, матеріальна й технічна підтримка тощо;

– відносно якої інформації та даних потрібно забезпечити зв'язок з використанням криптографічних перетворень і протоколів (у тому числі, наприклад, засоби та процедури фізичного захисту ключових даних та інформації).

Відповіді на вказані проблемні питання можуть бути використані при формулюванні підходу з розробки принципів інтеграції криптографічних систем і засобів в існуючі або нові ІС та ІТС. Причому обґрунтованим підходом з інтеграції криптографічних засобів і реалізації методів і механізмів є розробка вимог відповідно з цілями та політиками захисту.

Розглянемо вимоги щодо захисту засобів криптографічних перетворень (у подальшому – криптографічних модулів). На наш погляд, фізичні й логічні вимоги щодо захисту криптографічних модулів у найбільш прийнятному вигляді формулюються у FIPS 140-2 та в розширеному вигляді у FIPS 140-3.

У подальшому будемо враховувати етапи циклу життя системної розробки та завдання, пов'язані з безпекою, що повинні вирішуватися на кожному з етапів стосовно розроблення, придбання, впровадження та використання нових криптографічних систем і засобів.

У [25] наведено вимоги щодо безпеки й цілісності криптографічних модулів, що виконують криптографічні перетворення. Для кожного з уведених одинадцяти атрибутів безпеки визначено чотири рівні безпеки. Вважається, що криптографічні засоби управління надаються з використанням криптографічних модулів, що можуть включати такі можливості, як генерація та верифікація підпису, шифрування та розшифрування, генерація ключів і встановлення ключів.

На рис. 10.1 наведено загальну модель тестування рівнів безпеки, що включає тестування взагалі, у тому числі тестування криптографічних алгоритмів і криптографічних модулів [118, 122–123].

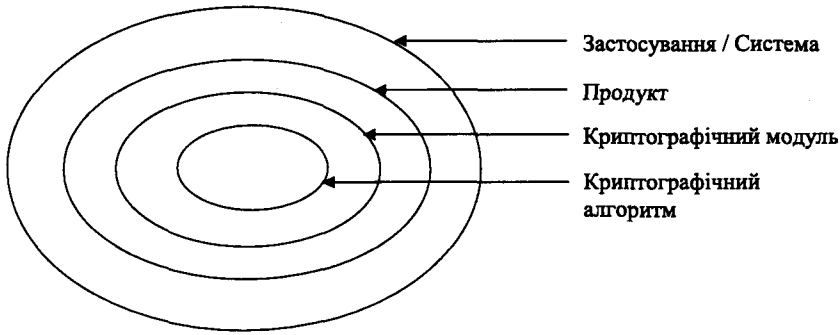

Рис. 10.1. Модель тестування рівнів і якостей безпеки

При такому підході криптографічні алгоритми й криптографічні модулі повинні тестуватися перед їх впровадженням в існуючу або нову систему. Криптографічні алгоритми й модулі тестуються розроблювачем і потім подаються для тестування у відповідності до нормативних документів, наприклад, для тестування криптографічного модуля можна використовувати федеральний стандарт США FIPS 140-2. Так, проведений аналіз показав, що в США для всіх державних відомств для захисту конфіденційної незасекреченої інформації обов'язковим є використання криптографічних засобів, що відповідають стандарту FIPS 140-2, якщо ці організації вважають, що такий криптографічний захист потрібен. Причому стандарт FIPS 140-2 необхідно застосовувати в комп'ютерних та телекомунікаційних системах, включаючи голосові системи, при проектуванні, створенні, тестуванні та застосуванні систем безпеки на базі використання криптографічних перетворень. Окрім того, NIST та Організація з Комунікаційної Безпеки (CSE) уряду Канади заснували спеціальну програму CMVP. Мета цієї програми – забезпечити державні організації метриками безпеки для використання при постачанні устаткування, що містить криптографічні модулі. Результати незалежного тестування забезпечуються акредитованими лабораторіями. Атестаційне тестування криптографічних модулів виконується з використанням похідних вимог тестування (DTR) для FIPS 140-2. У DTR перераховані всі вимоги до постачальника й організації, що здійснює тестування криптографічних модулів. Згідно з наведеними нормативними документами криптографічний модуль являє собою набір апаратних засобів, програмного забезпечення чи мікропрограмних (програмно-апапратних) засобів, або деякої їх комбінації, що реалізують криптографічну логіку або криптографічні перетворення. Прикладами криптографічних модулів можуть бути такі автономні пристрої, як шифратори зв'язку; шифрувальні плати розширення, вбудовані в комп'ютерні системи, та прикладні програми, що виконуються на мікропроцесорах, програми цифрового підпису тощо. Якщо криптографічна логіка реалізована у вигляді програмного забезпечення, то процесор, що використовує програмне забезпечення, також є частиною криптографічного модуля.

Основними перевагами використання атестованих модулів є такі:

– гарантія того, що модулі впроваджують необхідні властивості та дозволяють виконати певні вимоги;

– захист технічних активів і штатного часу технічного персоналу шляхом гарантії сумісності;

– можливість закупівлі модулів зі стандартними криптографічними перетвореннями, протоколами, інтерфейсами, а також стандартизація їх тестування;

– надання користувачам набору доступних і необхідних захисних елементів;

– підвищення гнучкості у виборі вимог захисту, що відповідають вимогам для конкретного застосування та середовища.

Варіант здійснення тестування криптографічних модулів наведено на рис. 10.2.

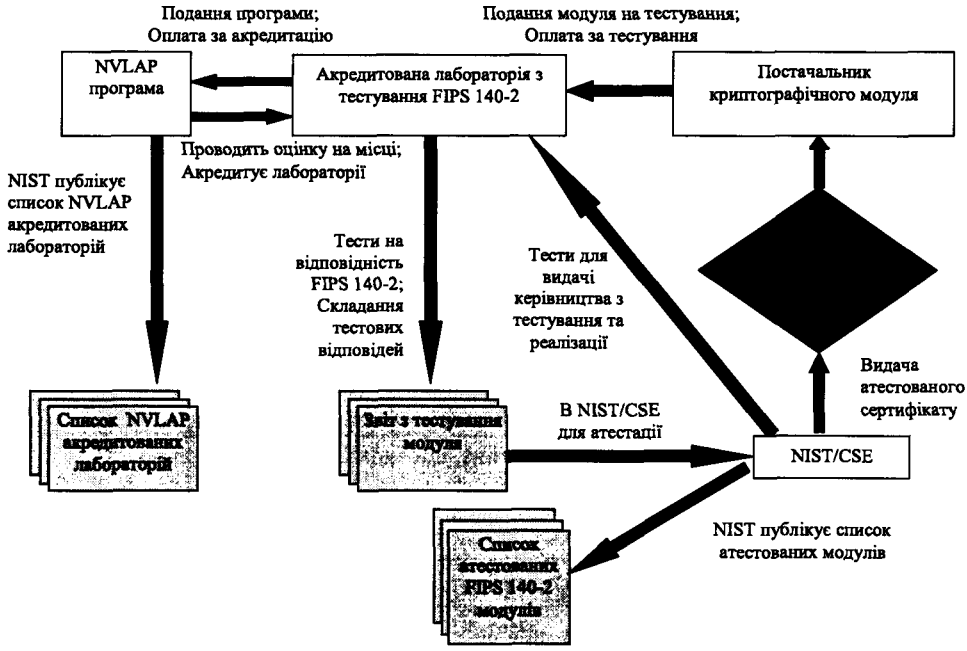

Рис. 10.2. Порядок тестування криптографічних модулів

Проведемо аналіз вимог до криптографічних модулів, що закладені у FIPS 140-2. У цілому, вимоги безпеки, що викладені в FIPS 140-2 охоплюють 11 галузей, пов'язаних із проектуванням та реалізацією криптографічного модуля. Так, у більшості галузей криптографічному модулю присвоюється, залежно від вимог, відповідний рівень захисту від 1 до 4, тобто від найнижчого до найвищого. Для інших галузей, у яких не передбачається захист з різними рівнями, криптографічному модулеві присвоюється оцінка, що відображає ступінь здійснення всіх вимог для цієї галузі. При цьому повна оцінка, що надається криптографічному модулеві, містить у собі мінімум незалежних оцінок, що присвоюються в галузях з відповідними рівнями захисту, а також ступінь забезпечення всіх вимог в інших галузях.

Окрім того, в атестаційному сертифікаті постачальника криптографічного модуля також вказується як загальна, так і окремі оцінки. В окремих випадках для постачальників та користувачів важливо зробити так, щоб повна оцінка криптографічного модуля не обов'язково була самою важливою оцінкою.

Це тому, що оцінка для окремої галузі в деяких випадках може бути важливішою, ніж повна оцінка, наприклад, залежно від середовища, у якому повинен використовуватися криптографічний модуль. Оцінка повинна також включати те, яким видам ризику та з якими допустимими втратами повинен запобігати криптографічний модуль. Модулі можуть відповідати для різних послуг різним рівням вимог захисту; наприклад, модуль може реалізувати автентифікацію з четвертим рівнем, а захист від підробки – на другому рівні тощо. У таблиці 10.4 наведено вимоги щодо забезпечення захисту, представлені у FIPS 140-2.

Таблиця 10.4. **Вимоги щодо забезпечення захисту, визначені в стандарті FIPS 140-2**

	Рівень захисту 1	**Рівень захисту 2**	**Рівень захисту 3**	**Рівень захисту 4**
1	2	3	4	5
Специфікація криптографічного модуля	Опис криптографічного модуля та граничних криптографічних властивостей. Перелік затверджених криптографічних алгоритмів та затверджених режимів застосування модуля. Опис криптографічного модуля, включаючи всі апаратні, програмні та програмно-апаратні (мікропрограмні) компоненти. Положення відносно політики захисту модуля			
Порти та інтерфейси криптографічного модуля	Необхідні інтерфейси та такі, що задаються опціонально			
Ролі, послуги та автентифікація	Логічний поділ	Автентифікація оператора на базі ролей чи на базі встановлення справжності		Автентифікація оператора на базі встановлення його справжності
Модель кінцевого стану	Опис моделі кінцевого стану. Необхідні стани й такі, що задаються опціонально. Діаграма переходу станів і описи станів			
Фізичний захист	Промислове маркіроване устаткування	Замки або засоби (знаки) захисту (tamper evidence)	Виявлення втручання та засоби захисту (захисні знаки) для кришок і дверей	Виявлення втручання та захисна оболонка із сигналізацією
Експлуатаційне середовище	Окремий оператор. Робоча програма. Затверджений механізм перевірки цілісності	Довідкові дані, оцінювання згідно EAL2 [108] із заданими механізмами розмежування й управління доступом і аудитом	Довідкові дані та довірчий канал, що оцінюється згідно EAL3 [108], а також моделювання політики захисту	Довідкові дані та довірчий канал з ключем, що повинен оцінюватися згідно EAL4 [108]

Закінчення табл. 10.4

1	2	3	4	5
Управління криптографічними ключами	Управління ключами в частині генерації випадкових чисел і ключів, установлення ключів, уведення/ виведення ключів, зберігання та надійне знищення ключів			
	Секретні й особисті ключі, що встановлюються за допомогою ручних методів, можуть вводитися або виводитися у відкритому вигляді	Секретні й особисті ключі, що встановлюються за допомогою ручних методів, причому ключі повинні вводитися або виводитися в зашифрованому вигляді або за допомогою протоколів розподілу таємниці		
Електромагнітна сумісність (EMI/ EMC)	Згідно з 47 CFR FCC Частина 15. Підчастина B, Клас A (Комерційне застосування). Вимоги, що застосовуються для FCC (радіозв'язку)	47 CFR FCC Частина 15. Підчастина B, Клас B (Побутове застосування)		
Самотестування	Кваліфікаційні тестування: тестування алгоритмів, тестування цілісності програмного забезпечення/ мікропрограмних засобів, критичні функціональні тестування. Умовні тестування			
Проектні гарантії	Рівень керування конфігурацією. Відповідність між проектом і політикою. Керівна документація	СМ система. Розподіл захисту. Функціональні вимоги	Реалізація мовою високого рівня	Формальна модель. Детальні пояснення (неформальні докази). Передумови та післяумови
Протидія іншим зловмисним діям	Опис способів протидії, відносно яких на цей час відсутні вимоги в частині тестування			

Розглянемо також інші вимоги.

Попередня доатестаційна відомість. Доатестаційна відомість надається тільки з метою інформування та носить рекомендаційний характер, тобто є необов'язковою. Стан кожного криптографічного модуля на такий момент якраз зазначено в доатестаційній відомості.

Особливості тестування. Тестування криптографічного модуля повинне здійснюватись акредитованою лабораторією в тісній взаємодії лабораторії та розробника. Разом з модулем повинна надаватись уся документація на модуль.

Надання результатів тестування. Після тестування повинно бути розроблено проект сертифікату, узагальнений опис модуля, детальний звіт за результатами тестування, політику захисту (причому вказане не повинно патентуватись). Може виконуватись також фізичне тестування. У цьому випадку спеціалізованій лабораторії надаються відповідні рекомендації.

Особливості тестування. Призначаються також експерти від NIST і CSE, що виконують попередню оцінку тестової документації (якщо це потрібно). У подальшому висунуті експертами NIST і CSE зауваження поєднуються в комплект зауважень, що відсилається в спеціалізовану лабораторію, яка здійснює або повинна здійснювати тестування.

Координація атестації. Спеціалізована лабораторія приймає від NIST та CSE зауваження та приймає рішення з їх урахуванням. Якщо потрібно, то проводиться також додаткове тестування, а також додатково розробляється документація. Приймається також рішення щодо зауважень, яке повторно подається на розгляд у NIST та CSE. Здійснюється оновлення тестової документації, яка повторно подається на розгляд у NIST та CSE. Відповіді на зауваження разом з виправленою документацією подаються на розгляд у NIST та CSE.

Завершальний етап атестації. Остаточне рішення щодо зауважень експертів подається на розгляд у NIST та CSE. На підставі цього рішення розробником виконується відновлення тестової документації та її подання на розгляд у NIST та CSE. Присвоюється також номер сертифікації. Ініціюється роздрукування сертифіката та процес його підписання.

Інформація щодо атестованого модуля вноситься в список атестованих модулів. При цьому для кожного модуля список атестованих модулів включає таку інформацію:

– що атестація виконана відповідно до FIPS 140-1 або FIPS 140-2;
– ім'я постачальника та контактна інформація;
– шифр модуля та номер версії;
– стандарт, FIPS 140-1 або 140-2, відповідно до якого виконана атестація;
– тип модуля (програмний, апаратний або мікропрограмний);
– дата атестації (та переатестації, якщо це доречно);
– рівень(і) атестації;
– зв'язок із сертифікатом, політикою захисту, web-сайтом компанії та технічні контакти.

Види перевірки щодо криптографічного модуля

Перевірка згідно FIPS 140-2 повинна виконуватися в такій послідовності. Проводиться аналіз вимог щодо кожної із послуг (галузей) застосування. Визначення тих вимог, що є специфічними, а також таких, що задані у FIPS 140-2, але спочатку не враховувалися. На базі допустимого ризику визначається прийнятний рівень щодо кожної з послуг (галузі) стандарту, завдання організації та ідентифікація активів.

Перевірка згідно з додатком А стандарту FIPS 140-2 «Затверджені функції захисту для FIPS 140-2» з метою визначення гарантії застосування криптографічного модуля. Перевірка затвердженого алгоритму та необхідної підтримки криптографічних операцій, сервісної функції(й) захисту, наприклад, симетричного ключа, асиметричного ключа, автентифікації повідомлень і гешування.

Перевірка згідно з додатком B стандарту FIPS 140-2 «Затверджені профілі захисту для FIPS 140-2» для визначення можливості застосування затвердженого профілю в операційній системі, у якій використовується криптографічний модуль.

Порівняння криптографічної структури, що пропонується, або специфікацій перспективних продуктів з вимогами додатка C стандарту FIPS 140-2 «Затверджені генератори випадкових чисел для FIPS 140-2» з метою визначення відповідності стандарту.

Порівняння криптографічної структури, що пропонується, або специфікації перспективних продуктів з вимогами додатка D стандарту FIPS 140-2 «Затверджені методи встановлення ключів» для визначення відповідності стандарту.

Одержання або розробка криптографічних модулів, що задовольняють або перевищують обрані рівні та/або задовольняють відповідному затвердженому профілю захисту.

У 2005 р. в США розпочато розробку стандарту FIPS 140-3, у якому визначено вимоги щодо захисту модулів криптографічного захисту. Згідно планів це буде виправлена версія FIPS 140-2.

NIST розробив FIPS 140-3 з урахуванням нових переглянутих вимог у відповідності з новими вимогами для федеральних органів, а також з урахуванням технологічних та економічних змін. На першому етапі NIST приймав коментарії та запити від суспільства, користувачів, представників IT індустрії, Федеральних, державних і місцевих урядових організацій у щодо нового стандарту.

NIST був особливо зацікавлений в одержанні коментаріїв з таких питань:

– сумісність з промисловими стандартами;

– новітні галузі технологій;

– уведення додаткових рівнів захисту;

– додаткові вимоги для фізичного захисту;

– корпоративні застосування, включаючи операційні системи на базі платформ та/або середовищ.

NIST розробив план на перехідний період для тестування та атестації модулів у відповідності з FIPS 140-3, а для організацій розробив плани придбання продуктів, що відповідають FIPS 140-3. Перехідний план також використовується Федеральними організаціями – виробниками криптографічних модулів, що пройшли атестацію на відповідність FIPS 140-1 та FIPS 140-2.

10.3. РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ АПАРАТНИХ ЗАСОБІВ ГЕНЕРУВАННЯ КЛЮЧІВ І ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ІВК

Аналіз ряду основоположних джерел [13, 21, 22, 37, 56, 116–123] показав, що управління ключовими даними є найбільш складною та критичною задачею, особливо щодо ІВК. Щодо управління ключами критичними є операції генерування випадкових бітів, генерування випадкових ключів, встановлення ключів, розподілення ключів, введення та виведення ключів, зберігання та знищення (обнулення) ключів. Згідно із загальновизнаним [13, 21, 22, 116–123], до критичних параметрів і ключів будемо відносити особисті та відкриті ключі. Причому відносно особистих ключів і параметрів треба забезпечувати послуги необхідної якості, такі як кон-

фіденційність, цілісність, справжність, доступність, неспростовність і надійність (CSP-параметри), а відносно відкритих – цілісність, справжність, доступність, неспростовність і надійність (PSP-параметри).

Вимоги щодо захисту для управління криптографічними ключами охоплюють повний життєвий цикл CSP- та PSP-параметрів, що застосовуються в криптографічному модулі. Криптографічний модуль може також використовуватись для управління ключами іншого криптографічного модуля. При оцінці також прийнято зашифрованими CSP називати параметри, які зашифровані з використанням затвердженого алгоритму або затвердженої функції захисту [116–123]. CSP-параметри, зашифровані з використанням незатвердженого алгоритму або власного алгоритму або методу, необхідно вважати відкритими. Основними вимогами до CSP-параметрів є те, що вони повинні бути захищені в межах криптографічного модуля від несанкціонованого розкриття, модифікації та підміни, а PSP-параметри повинні бути захищені в межах криптографічного модуля від несанкціонованої модифікації та підміни.

Криптографічний модуль може застосовувати генератори випадкових бітів (ГВБ), множину ГВБ або єдиний ГВБ. Усі ГВБ та їхнє використання повинні бути визначені. За умови якщо в криптографічному модулі використовується затверджений ГВБ і в затвердженому режимі, то повинні виконуватися такі вимоги [116–123]:

– джерело ГВБ повинне тестуватися на випадковість;

– детерміновані компоненти ГВБ також повинні тестуватися;

– дані, що отримані з ГВБ, повинні проходити повне тестування генератора випадкових бітів.

Окрім вказаних при генеруванні ключів, повинні враховуватись та/або виконуватись такі вимоги та рекомендації:

– з точки зору криптографічної стійкості та криптографічної живучості більш прийнятним є генерування ключів безпосередньо в криптографічному модулі;

– ключі, що призначені для використання в затвердженому криптографічному алгоритмі або функції захисту, повинні генеруватися також з використанням затвердженого генератора випадкових бітів;

– компрометація методу генерації ключів (наприклад, угадування початкового значення для ініціалізації детермінованого ГВБ) повинна вимагати щонайменше стільки ж операцій, скільки визначено значенням генерованого ключа;

– якщо початковий ключ вводиться під час процесу генерації ключів, то введення ключа має відповідати вимогам щодо введення встановлених ключів;

– якщо проміжні значення генерації ключів виводяться з криптографічного модуля, то значення повинні виводитися або в зашифрованому вигляді, або з розподілом таємниці, або з використанням обох методів;

Щодо механізмів встановлення ключів повинні виконуватись такі вимоги:

– здійснюватись за допомогою затверджених або стандартизованих електронних механізмів і протоколів;

– транспортування за допомогою затверджених або стандартизованих ручних методів, наприклад, за допомогою пристрою завантаження ключів, який транспортують вручну;

– встановлення за допомогою комбінації затверджених електронних і ручних методів транспортування;

– якщо в криптографічному модулі застосовуються затверджені методи встановлення ключів, то повинні використовуватися тільки затверджені методи генерування ключів;

– складність компрометації методу встановлення ключів (наприклад, компрометація захисту алгоритму, що використовується для встановлення ключів) повинна вимагати щонайменше стільки ж операцій, скільки дозволених ключів;

– якщо використовується метод передачі ключів, то переданий криптографічний ключ повинен відповідати вимогам щодо введення/ виведення ключів;

– якщо використовується метод узгодження ключів (наприклад, криптографічний ключ формується з використанням розподілених проміжних значень), то відносно розподілення таємниці вимоги щодо введення/ виведення ключів можуть бути послаблені.

Залежно від виду ключів і застосування, вони можуть вводитися або виводитися із криптографічного модуля. До механізмів введення/ виведення ключів висуваються такі вимоги:

– вони мають виконуватися з використанням ручних (наприклад, через клавіатуру) або електронних методів (наприклад, за допомогою старт-карт, токенів, PC карт або інших електронних пристроїв завантаження ключів або з'єднань);

– початковий ключ, якщо він вводиться під час генерації ключів, повинен вводитися таким же способом, як і криптографічні ключі;

– зашифровані секретні й особисті ключі, що вводяться або виводяться із криптографічного модуля та використовуються в затвердженому режимі операції, повинні бути зашифровані з використанням затвердженого алгоритму й, бажано, захищені від порушення цілісності;

– відкриті ключі можуть уводитися в криптографічний модуль або виводитися із криптографічного модуля у формі відкритого тексту і, як правило, мають бути захищені від порушення цілісності;

– криптографічний модуль повинен зв'язувати ключ (секретний, особистий або відкритий), що вводиться у модуль або виведений з модуля, з ідентифікатором відповідного об'єкта (наприклад, персони, групи або процесу), що є власником ключа;

– криптографічні ключі, що вводяться вручну, під час введення в криптографічний модуль, повинні бути перевірені на цілісність і справжність з використанням тестування ручного введення ключів;

– під час введення значення ключів, які вводять вручну, можуть бути тимчасово доступними для можливості візуальної верифікації й підвищення точності;

– якщо зашифровані криптографічні ключі або ключові компоненти вводяться в криптографічний модуль вручну, то відкриті значення криптографічних ключів або ключових компонентів не повинні бути доступними у відкритому вигляді.

Відповідні вимоги до модулів КЗІ центрів сертифікації ключів наведені в таблиці 10.5.

Аналіз основоположних джерел свідчить, що до управління ключами висуваються різні вимоги залежно від необхідного рівня захищеності та від додатків, у яких вони застосовуються. Так, у [116–117] вимоги розподілені за чотирма рівнями. Указані нормативні документи можна взяти за основу і в Україні, оскільки федеральний стандарт США FIPS 140-2 ще діє. У федеральному стандарті FIPS 140-3 [118, 122–123] запропоновано ввести п'ять рівнів захищеності.

Таблиця 10.5. **Вимоги щодо модулів КЗІ центрів сертифікації ключів**

	Рівень захисту 1	**Рівень захисту 2**	**Рівень захисту 3**	**Рівень захисту 4**	**Рівень захисту 5**
1	2	3	4	5	6
1. Опис криптографічного модуля	Опис модуля, меж, затверджених алгоритмів і затверджених режимів дії. Опис апаратних засобів і програмного забезпечення модуля. Документація модуля				
	Політика захисту визначає затверджений режим дії	Вказівка затвердженого режиму дії модуля			
2. Порти та інтерфейси криптографічного модуля	Потрібні та опціональні інтерфейси. Визначення всіх інтерфейсів і всіх вхідних і вихідних шляхів даних	Введення і виведення критичних параметрів захисту фізично або логічно відокремлених з використанням довірчого каналу від інших портів і інтерфейсів			
3. Ролі, послуги та автентифікація	Визначення ролей і послуг модуля	Автентифікація, заснована на ролі або ідентифікації	Автентифікація, заснована на ідентифікації оператора	Двохфакторна автентифікація	
4. Захист програмного забезпечення	Виконавчий код, затверджений метод перевірки цілісності, MSI, обмеження щодо читання й модифікації, обнулення при розвантаженні, перевірка формату	Тестування цілісності, засноване на цифровому підпису	MSI команда для ініціалізації тестування цілісності програмного забезпечення. Обнулення геш–значення	Шифрування і розшифрування CSP-параметрів і коду тестування цілісності	Шифрування і розшифрування PSP-параметрів і коду тестування цілісності

Продовження табл. 10.5

1	2	3	4	5	6
5. Операційне середовище	OS одного користувача або розмежувальний контроль доступу	Механізми контролю. Розмежувальний контроль доступу	Криптографічне програмне забезпечення, SSP і захист даних аудиту. Довірчий канал. Розширений аудит	Вимоги розширеного аудиту	
6. Фізичний захист	Промислові компоненти	Доказ втручання. Непрозоре покриття або корпус	Схема реагування на втручання й обнулення на знімних кришках і дверцятах. Захист вентиляції від зондування. Міцне покриття або корпус	EFP або EFT для температури і напруги. Схема виявлення втручання та обнулення для багатокристальних модулів	EFP для температури і напруги. Непрозоре для невізуальної радіаційної експертизи. Захист від вимкнення схеми виявлення втручання й обнулення
7. Неінвазивні атаки фізичного захисту	Ніяких додаткових вимог		Захист CSP-параметрів від атак тимчасового аналізу	Захист CSP-параметрів від SPA і DPA атак	Захист CSP-параметрів від EME атак
8. SSP управління	Вимоги для генераторів випадкових бітів, генерації SSP, встановлення SSP, введення і виведення SSP, зберігання SSP і обнулення CSP				
	Неелектронно транспортовані SSP можуть вводитися і виводитися у відкритій формі		Неелектронно транспортовані SSP, введені або виведені в зашифрованій формі або з використанням процедур розділу знання	Обнулення PSP	

Закінчення табл. 10.5

<table>
<tr><th>1</th><th colspan="2">2</th><th>3</th><th>4</th><th>5</th><th>6</th></tr>
<tr><td>9. Самотестування</td><td colspan="6">Передексплуатаційне самотестування: тестування цілісності програмного забезпечення, тестування криптографічного алгоритму і передексплуатаційне тестування обходу. Умовне самотестування: тестування парної узгодженості, тестування навантаження програмного забезпечення, тестування ручного введення ключів, безперервне RBG-тестування, тестування джерела RBG-ентропії та тестування умовного обходу</td></tr>
<tr><td rowspan="8">10. Керівна документація</td><td colspan="4">CMS для модуля, компонентів і документації. Кожен має бути унікально ідентифікований та відстежуваний протягом усього життєвого циклу</td><td colspan="2">Автоматизована CMS</td></tr>
<tr><td>Відповідність між модулем і Політикою захисту</td><td>Функціональна специфікація</td><td>Детальне проектування</td><td>Неформальний доказ відповідності між перед– і постумовами і функціональною специфікацією</td><td>Формальне моделювання і неформальний доказ відповідності між формальною моделлю та функціональною специфікацією</td></tr>
<tr><td colspan="6">Модель кінцевого стану</td></tr>
<tr><td colspan="3">Анотований початковий код, схематика або HDL мова</td><td colspan="3">Високорівнева мова програмного забезпечення. Високорівнева мова апаратного опису</td></tr>
<tr><td colspan="4">Функціональне тестування</td><td colspan="2">Низькорівневе тестування</td></tr>
<tr><td colspan="3">Процедури запуску</td><td>Процедури постачання</td><td colspan="2">Автентифікація оператора з використанням забезпеченої постачальником інформації автентифікації</td></tr>
<tr><td colspan="6">Керівництво адміністратора і неадміністратора</td></tr>
<tr><td>11. Протидія іншим атакам</td><td colspan="6">Ніяких механізмів протидії в Політиці захисту не вказано</td></tr>
</table>

Необхідно відзначити, що вимоги застосування в ЦСК апаратних модулів КЗІ є взаємно визнаними та закріплені у відповідних Політиках сертифікації. Так, Політика Сертифікації (СР) мостового центру США визначає сім політик сертифікації. Політики представляють п'ять різних рівнів гарантії (Рудиментарний, Базовий, Середній, Середньоапаратний і Високий) для сертифікатів відкритого ключа. Поняття рівня гарантії належить до стійкості зв'язку між відкритим ключем і особою, суб'єктне ім'я якої згадується у сертифікаті, механізмів, що використовуються для управління використанням особистого ключа, та захисту, що забезпечується самим РКІ. Суть у тому, що високий рівень гарантій забезпечується перш за все за рахунок виконання вимог до засобів КЗІ, що застосовуються у відповідних ЦСК.

10.4. АНАЛІЗ ТА ОБҐРУНТУВАННЯ ВИМОГ ДО СИСТЕМ УПРАВЛІННЯ ТА СЕРТИФІКАЦІЇ КЛЮЧІВ В ІВК ТА ПРИНЦИПИ ЇХ ЗАБЕЗПЕЧЕННЯ

У цьому параграфі наведено класифікацію існуючих типів ключів та обґрунтовуються вимоги до них, а також розглядаються сутність і вимоги до ключової інформації [119–120]. Розгляд здебільшого ведеться під кутом зору ІВК (системи ЕЦП).

Типи ключів та криптографічної інформації

При висуненні вимог до ІВК в першу чергу необхідно розробити вимоги до систем та засобів управління та сертифікації ключів. У подальшому під управлінням ключовими даними (у подальшому ключами), будемо розуміти дії, пов'язані з генеруванням або придбанням, реєструванням, розподіленням (розповсюдженням), сертифікацією, доставкою, уведенням в дію (інсталюванням), зміненням, зберіганням, архівуванням, скасуванням, блокуванням, поновленням, зняттям з реєстрації, обліком та знищенням ключової інформації (даних), а також носіїв ключових даних. Існує значна кількість різних типів ключів, що використовуються для різних типів криптографічних перетворень. Окрім того, в процесі криптографічних перетворень використовується інформація, що спеціальним чином пов'язана з криптографічними алгоритмами та ключами. Такого роду інформацію будемо називати криптографічною інформацією. Відповідно до використання рекомендується розділяти криптографічні ключі на відкриті, особисті та таємні. Щодо встановлення відкритих та особистих ключів класифікація може бути також за їхніми станами: статичний стан і сеансовий стан (ефемерний).

Як випливає з [119–120], в ІВК потенційно можуть використовуватися такі ключі:

– особистий ключ цифрового підпису;
– відкритий ключ перевіряння (верифікації) цифрового підпису;
– симетричний ключ автентифікації;
– особистий ключ автентифікації;
– відкритий ключ автентифікації;

– симетричний ключ шифрування даних;
– симетричний ключ шифрування ключів;
– симетричні й асиметричні ключі генерації випадкових чисел;
– симетричний майстер-ключ (головний);
– особистий ключ для передачі ключів;
– відкриті ключі передачі ключів;
– симетричний ключ узгодження ключів;
– особистий статичний ключ узгодження ключів;
– відкриті статичні ключі узгодження ключів;
– особисті сеансові ключі узгодження ключів;
– відкриті сеансові ключі узгодження ключів;
– симетричний ключ авторизації;
– особистий ключ авторизації;
– відкритий ключ авторизації.

У [119–120] також наведена інша криптографічна інформація та подана її загальна характеристика. Необхідність її розгляду пов'язана з очевидною необхідністю обґрунтування вимог також і до такої інформації. У цілому, іншою інформацією, що тією чи іншою мірою пов'язана з криптографічними перетвореннями та ключами, є така:

– параметри області криптографічних перетворень;
– вектори ініціалізації засобів перетворень;
– поділювані таємниці (секрети);
– випадкові (RNG) початкові числа;
– інша загальнодоступна інформація;
– проміжні результати криптографічних операцій;
– інформація з управління ключами;
– випадкові числа;
– паролі;
– інформація аудиту.

Основні вимоги до застосування ключів

У прикладній криптографії обґрунтовано та вважається загальновизнаним, що при криптографічних перетвореннях кожен ключ використовується тільки з однією метою (наприклад, направленого шифрування, автентифікації, захисту ключів, генерації випадкових чисел, цифрового підпису, авторизації тощо). Як показали дослідження, причинами цього є таке:

1. Використання одного й того самого ключа для двох різних криптографічних перетворень може послабити його захист;

2. Більш тяжкими будуть наслідки збитку, що можуть бути нанесені у разі компрометації ключа;

3. Деякі використання ключа впливають один на одного. Наприклад, розглянемо пари ключів, які використовуються для передачі ключів і для цифрових підписів. У цьому випадку особистий ключ використовується і як особистий ключ передачі ключів (для розшифрування ключів шифрування), і як особистий ключ цифрового підпису. За цих умов може знадобитися зберігати особистий ключ передачі ключів довше, ніж відповідний особистий ключ передачі ключів розшиф-

рування ключів. Особистий ключ підпису повинен знищуватися після закінчення свого строку дії (для запобігання його компрометації). У цьому випадку строк дії особистого ключа передачі ключів при розшифруванні та особистого ключа цифрового підпису суперечать один одному. У той же час, з використанням одного ключа можуть бути надані багато послуг – цифровий підпис з метою забезпечення неспростовності, цілісності й справжності, або коли один симетричний ключ шифрування даних може використовуватися для шифрування й автентифікації даних.

Однією з основних вимог, що висуваються до ключа, є наперед визначений криптографічний період $T_П$ [119–120], під яким розуміють період часу, протягом якого конкретний ключ санкціонується для використання законними об'єктами або ключі будуть залишатися в дії для заданої системи. Причому правильно обґрунтований і заданий криптоперіод:

– обмежує кількість інформації, що захищається заданим ключем і може бути доступною для криптоаналізу;

– обмежує ступінь розкриття деякого обсягу інформації в разі компрометації одного ключа;

– обмежує використання конкретного алгоритму криптографічного перетворення;

– обмежує час для спроб проникнення у фізичні, процедурні та логічні механізми доступу, що забезпечують захист ключа від несанкціонованого розкриття;

– обмежує період, протягом якого інформація може бути скомпрометована в результаті ненавмисного розкриття ключа несанкціонованим об'єктом;

– обмежує час, що доступний криптоаналітику (у застосуваннях, де не потрібен довгостроковий захист ключів). Як випливає із [119–120], криптоперіод можна визначити й через максимальну кількість даних, що захищаються ключем.

Для більш детального дослідження необхідно визначити та врахувати фактори ризику, які впливають на допустиму величину криптоперіоду.

Як зазначається в [119–120], до факторів, що впливають на ризик розкриття, необхідно віднести:

– стійкість криптографічних перетворень (наприклад, алгоритм, довжина ключа, розмір блоку і режим застосування тощо);

– вид реалізації криптографічних перетворень (наприклад, реалізація згідно FIPS 140-3 рівня 4 або програмна реалізація);

– середовище застосування (наприклад, засіб захисту обмеженого доступу, відкрите офісне середовище чи загальнодоступний термінал);

– обсяг інформаційного потоку або число трансакцій;

– час захисту даних;

– вид захисту (наприклад, шифрування даних, цифровий підпис, вироблення ключів, захист ключів тощо);

– метод криптографічного перетворення (наприклад, уведення через клавіатуру, шифрування за допомогою пристрою завантаження ключів, де людина не має прямого доступу до ключової інформації, вилучене перетворення в межах PKI);

– процес відновлення ключів або виведення ключів;

– число вузлів у мережі, що розділяють загальний ключ;

– число копій ключа та розподіл таких копій;

– вид загроз для інформації (наприклад, від кого інформація захищена, які технічні можливості, а також фінансові ресурси, що можуть бути застосовані для здійснення атаки, має можливий порушник).

Проведений аналіз дозволив виробити рекомендації щодо вибору криптоперіоду для конкретних типів ключа.

Криптоперіод, необхідний для заданого ключа, може залежати від типу ключа, а також середовища використання й характеристик даних, наведених вище. Нижче подано деякі загальні рекомендації щодо вибору криптоперіоду для різних типів ключа. Відзначимо, що подано значення грубого порядку для рекомендованих криптоперіодів. Більшість із них мають криптоперіод порядку декілька років, обґрунтування здійснено з урахуванням:

– вимоги відносно максимальної операційної ефективності;

– допущень за мінімальним критерієм, що пов'язаний із середовищем використання [див. 25, 29].

Указані вимоги необхідно уточнювати залежно від виду криптографічного перетворення.

Розглянемо ці вимоги залежно від криптографічних перетворень.

1. Криптографічне перетворення типу «Цифровий підпис»

Для особистого ключа цифрового підпису вважається, що:

– криптоперіод особистого ключа підпису може бути коротшим, ніж криптоперіод відповідного відкритого ключа перевіряння (верифікації) цифрового підпису;

– з урахуванням конкретного використання затверджених алгоритмів і розмірів ключа, а також з огляду на необхідність підвищення криптоживучості та з урахуванням критичності процесів, для яких надається ключ, максимальний рекомендований криптоперіод може бути до трьох років. Ключ має бути знищений після завершення зазначеного періоду.

Щодо відкритого ключа перевіряння підпису необхідно враховувати, що криптоперіод відкритого ключа перевіряння підпису може бути більшим, ніж криптоперіод відповідного йому особистого ключа підпису. По суті, це період, під час якого повинен бути перевірений будь-який документ або дані, що підписані за допомогою відповідного особистого ключа. Але збільшення криптоперіоду відкритого ключа накладає відносно мінімальні вимоги до його захисту. Як свідчить аналіз, необхідно враховувати, що для будь-якого криптографічного алгоритму та розміру ключа вразливість до криптоаналізу згодом збільшується. Причому, хоча вибір стійкого або найбільш стійкого алгоритму та ключа великого розміру може мінімізувати таку уразливість до криптоаналізу, це не впливає на наслідки від здійснення успішних атак на фізичні, процедурні та логічні механізми управління доступу для особистого ключа.

Автентифікація з використанням симетричного криптографічного перетворення

Як показав аналіз, допустима величина криптоперіоду таємного ключа автентифікації залежить від критичності інформації, що захищається з його використанням. Для дуже критичної інформації може знадобитися, щоб ключ автентифікації був унікальним. Для менш критичної інформації криптоперіод

може бути більшим. Також може знадобитися, щоб ключ був доступним для перевіряння (верифікації) MAC захищених даних навіть після закінчення періоду використання відправника (тобто період використання одержувача перевищує період використання відправника). Окрім того, якщо MAC-ключ буде скомпрометований, то для зловмисника з'являється можливість модифікації автентифікованих даних і повторного обчислення MAC. У [119–120] показано та рекомендовано для затверджених симетричних криптоалгоритмів і розмірів ключів, а також з урахуванням впливу середовища та критичності інформації, для забезпечення цілісності якої використовується ключ, встановлювати максимальний період використання таємного ключа автентифікації відправником до 2 років, а максимальний період використання при перевірянні – до 5 років.

Автентифікація з використанням асиметричних криптографічних перетворень

Розглянемо вимоги щодо особистого та відкритого перетворень. Особистий ключ автентифікації може використовуватись багаторазово. Зв'язаний з ним відкритий ключ може бути сертифікований, тобто з відкритого ключа виготовлений сертифікат. У більшості випадків криптоперіод особистого ключа автентифікації такий самий, як криптоперіод зв'язаного відкритого ключа. Залежно від середовища, у якому він використовується, та критичності автентифікованої інформації, період дії особистого ключа може складати декілька років. Щодо відкритого ключа, то в більшості випадків криптоперіод відкритого ключа автентифікації такий самий, як криптоперіод зв'язаного з ним особистого ключа автентифікації. Але, по суті, він може дорівнювати періоду, протягом якого повинна контролюватися інформація, захищена з використанням відповідного особистого ключа.

2. Симетричне криптографічне перетворення типу «Шифрування»

Для цього перетворення симетричний ключ шифрування використовується для забезпечення конфіденційності даних, повідомлень або сеансів зв'язку. Симетричний ключ шифрування даних повинен мати відносно короткий строк дії, головним чином через можливу компрометацію великих обсягів інформації за короткий період часу (наприклад, зашифрування каналу зв'язку). При цьому ключ шифрування, що використовується для шифрування меншого обсягу інформації, може мати більш довгий період використання для відправника.

При цьому строк застосування симетричного ключа зашифрування не повинен перевищувати криптоперіод. Однак може знадобитися, щоб ключ був доступний для розшифрування захищених даних після закінчення періоду використання відправника. За цих умов період дії ключа розшифрування може бути більшим за період дії ключа зашифрування. У цілому, період використання ключа зашифрування, що рекомендується для зашифрування великих обсягів інформації за короткі періоди часу (наприклад, для шифрування швидкісного каналу зв'язку) може складати порядку доби або тижня. Ключ зашифрування, що використовується для зашифровування менших обсягів інформації, може мати період використання відправника до одного місяця. При цьому максимальний період дії ключа розшифрування може складати до трьох років [119–120].

Щодо симетричних ключів шифрування, що використовуються для зашифровування окремих повідомлень або окремих сеансів зв'язку, то час їх дії може складати місяці або роки, оскільки зашифровані повідомлення можуть бути збережені для більш пізнього їх використання, а значить розшифрування. Причому коли інформація підтримується в зашифрованому вигляді за допомогою симетричних криптоперетворень, симетричні ключі шифрування також повинні підтримуватися, поки така інформація не буде перешифрована в новому ключі або знищена.

Симетричний ключ шифрування ключів

Симетричний ключ шифрування ключів, що використовується для шифрування дуже великого числа ключів за короткий період часу, повинний мати відносно короткий період використання відправника. Якщо такий ключ використовується для зашифрування невеликого числа ключів, то період використання ключа зашифрування ключів може бути довшим. При цьому може знадобитися, щоб ключ розшифрування використовувався після закінчення періоду дії ключа зашифрування (тобто може знадобитися, щоб період використання ключа розшифрування перевищував період дії ключа зашифрування). При відповідному обґрунтуванні деякі симетричні ключі шифрування ключів шифрування можуть використовуватись тільки для окремого ключа або сеансу зв'язку. Для таких короткочасних ключів шифрування ключів найбільш підходящим криптоперіодом (тобто який включає криптоперіоди ключа зашифрування та розшифрування) буде окремий сеанс зв'язку. Передбачається, що ключ, зашифрований ключем шифрування ключів, уже не буде залишатися у своєму зашифрованому вигляді. В інших випадках ключі зашифрування ключів можуть залишатися такими, щоб пізніше можна було відновити файли або повідомлення, зашифровані ключами шифрування. У цьому випадку період ключа розшифрування може бути значно більшим, ніж період використання ключа зашифрування. Таким чином, рекомендований період використання ключа зашифрування, що використовується для зашифрування дуже великої кількості ключів за короткий період часу, може або повинен складати порядку доби або тижня. Якщо потрібно зашифрувати відносно мале число ключів, то період використання ключа зашифрування ключів може досягати місяця. Коли ключ зашифрування використовується тільки для одного повідомлення або сеансу зв'язку, то його строк дії (криптоперіод) буде обмежений до одного сеансу зв'язку. За винятком останнього випадку, як максимальний період дії ключа розшифрування рекомендується 3 роки.

Симетричні й асиметричні ключі генераторів випадкових чисел

Симетричні й асиметричні ключі генераторів випадкових чисел використовуються у генераторах випадкових чисел. У більшості генераторів випадкових чисел закладені можливості змінювати ключі. Криптоперіод для таких додатків обґрунтовується окремо.

Головний (майстер)-ключ. Як правило, є симетричним ключем. Симетричний майстер-ключ може багаторазово використовуватися для виведення (обчислення) інших ключів за допомогою (однобічної) функції вироблення ключів. Тому для такого типу ключа необхідно розглядати тільки період перетворень типу зашифрування. У цілому обґрунтування та вибір необхідного криптоперіоду

залежить від характеру й особливостей застосування ключів, виведених з майстер-ключа, а також від вимог до них. При цьому криптоперіод ключа, виведеного з майстер-ключа, може бути відносно коротким, наприклад, коли він використовується один раз на сеансі зв'язку або транзакції. Окрім того, майстер-ключ може використовуватися більш довгий період часу для вироблення (або повторного вироблення) безлічі ключів для різних цілей. У цьому випадку криптоперіод вироблених ключів залежить від вимог до них та їх використання (наприклад, симетричні ключі шифрування або ключі автентифікації). Допускають, що підходящий криптоперіод для симетричного майстер-ключа може складати до одного року, залежно від середовища використання, критичності інформації, що захищається виробленими ключами, а також необхідного числа ключів, вироблених з використанням майстер-ключа.

Особистий ключ передачі ключів. Особистий ключ передачі ключів може використовуватись багаторазово для розшифрування. У зв'язку з можливою необхідністю розшифрування переданих ключів, через деякий час після їх зашифрування перед передачею криптоперіод особистого ключа передачі ключів може бути більшим за криптоперіод зв'язаного з ним відкритого ключа. Криптоперіод особистого ключа повинен бути не більше часу, протягом якого повинні бути розшифровані будь-які ключі, зашифровані за допомогою зв'язаного з особистим відкритого ключа передачі ключів. Величина криптоперіоду залежно від алгоритмів криптографічних перетворень, довжин ключів, обсягу інформації, що може бути захищена ключами, зашифрованими за допомогою зв'язаного відкритого ключа передачі, а також з огляду на можливу потребу підвищення криптоживучості ключів і критичність процесів, щодо яких здійснюється захист, рекомендується приймати максимальний криптоперіод до 2 років. У разі якщо прийняті повідомлення зберігаються у зашифрованому вигляді й розшифровуються пізніше, криптоперіод особистого ключа передачі ключів може перевищувати криптоперіод відкритого ключа передачі ключів.

Відкритий ключ передачі ключів. Застосовується для зашифрування. Криптоперіод для відкритого ключа передачі ключів повинен становити не менше часу, протягом якого відкритий ключ може використовуватися для фактичного зашифрування. Відкриті ключі передачі ключів можуть бути загальнодоступними. Основним фактором, що повинен враховуватись при визначенні криптоперіоду відкритого ключа передачі ключів, є криптоперіод зв'язаного з ним особистого ключа передачі ключів. Причому, як зазначено вище в п. 8, у зв'язку з можливою необхідністю розшифрування ключів через деякий час після їхнього зашифровування перед передачею криптоперіод відкритого ключа передачі ключів може бути коротшим, ніж криптоперіод зв'язаного з ним особистого ключа.

Симетричний ключ узгодження ключів. Симетричний ключ узгодження ключів може використовуватися багаторазово. У більшості випадків його криптоперіод дорівнює періодам використання ключа відправником та одержувачем. Причому конкретний вибір значення криптоперіоду таких ключів залежить від середовища, характеру (наприклад, типів і форматів) й обсягу ключів, а також особливостей застосовуваних алгоритмів і протоколів узгодження ключів. Причому симетричні ключі узгодження ключів можуть використовуватися як для встановлення симетричних ключів (наприклад, симетричних ключів шифрування

даних), так і для іншої криптографічної інформації (наприклад, векторів ініціалізації). Щодо вибору криптоперіоду, то за умови, що застосовуються дозволені або рекомендовані криптографічні алгоритми і функції вироблення ключів (наприклад сумісні зі стандартними), засіб КЗІ (пристрій) відповідає вимогам [119–120] і встановлено рівні ризику, довжина криптоперіоду для ключа узгодження ключів може складати 1–2 роки.

Особистий статичний ключ узгодження ключів. Особисті статичні ключі узгодження ключів можуть використовуватися для встановлення симетричних ключів (наприклад, ключів шифрування (упакування) ключів або іншої таємної криптографічної інформації. Кожен особистий статичний ключ узгодження ключів може використовуватись багаторазово. Як і у випадку симетричних ключів узгодження ключів, криптоперіод таких ключів залежить від середовища, характеру (наприклад, типів і форматів) й обсягу ключів, а також особливостей алгоритмів і протоколів узгодження ключів, що застосовуються. За умови, що при узгодженні ключів застосовуються особисті статичні ключі узгодження ключів, дозволені або рекомендовані криптографічні алгоритми і функції вироблення ключів (наприклад, сумісні зі стандартними), засіб КЗІ (пристрій) відповідає вимогам [118] і встановлено рівні ризику, то довжина криптоперіоду для ключа узгодження ключів може складати 1–2 роки. У ряді застосувань, (наприклад, електронній пошті), де прийняті повідомлення зберігаються й розшифровуються пізніше, криптоперіод особистого статичного ключа узгодження ключів може перевищувати криптоперіод відкритого статичного ключа узгодження ключів.

Відкритий статичний ключ узгодження ключів. Криптоперіод відкритого статичного ключа узгодження ключів повинен (може) бути такий самий, як криптоперіод зв'язаного з ним особистого статичного ключа узгодження ключів. Криптоперіод відкритого статичного ключа узгодження ключів може бути 1–2 роки.

Особистий ключ сеансу узгодження ключів. Особисті сеансові (ефемерні) ключі узгодження ключів є складовими елементами асиметричних пар ключів, що використовуються в окремій трансакції для встановлення одного чи більше ключів. Особисті ключі сеансу (ефемерні) узгодження ключів можуть використовуватися для встановлення симетричних ключів (наприклад, ключів шифрування (упакування) ключів) або іншої таємної криптографічної інформації. Вони використовуються для узгодження ключів в окремій транзакції. Однак особистий ключ сеансу може використовуватись багаторазово для встановлення одного й того самого симетричного ключа з багатьма сторонами під час однієї й тієї самої трансакції (для багатоадресної передачі). Криптоперіод особистого ключа сеансу узгодження ключів визначається як тривалість окремої трансакції узгодження ключів, так і числом трансакції.

Відкритий ключ сеансу узгодження ключів. Відкриті сеансові ключі узгодження ключів є відкритими ключовими елементами асиметричних пар ключів, що використовуються тільки раз для встановлення одного чи більше ключів. Вони використовуються тільки для окремої трансакції узгодження ключів. Криптоперіод відкритого ключа сеансу узгодження ключів визначається тривалістю окремої трансакції узгодження ключів.

Симетричний ключ авторизації. Симетричний ключ авторизації, залежно від захищуваних ресурсів і ролі об'єкта, що отримує санкцію на доступ, може використовуватися протягом розширеного періоду часу. Для цього типу ключа криптоперіод відправника й одержувача однакові. Обов'язковими при визначенні криптоперіоду для симетричних ключів авторизації є робастність ключа, адекватність криптографічному методові й адекватність механізмів і процедур механізмів захисту. При використанні затверджених алгоритмів криптографічних перетворень і розмірів ключа, а також з огляду на необхідність збереження ключів і використання середовища в міру збільшення критичності процесів авторизації рекомендується, щоб криптоперіоди становили не більше двох років.

Особистий ключ авторизації. Особистий ключ авторизації, залежно від захищуваних ресурсів і ролі об'єкта, що отримує санкцію на доступ, може використовуватися протягом розширеного періоду часу. При визначенні криптоперіоду для особистих ключів авторизації враховуються вимоги до стійкості ключа, адекватність криптографічного методу й адекватність механізмів і процедур механізмів захисту ключа. Криптоперіод особистого та відкритого ключів авторизації повинні бути однаковими. Для визначеного використання, затверджених криптографічних алгоритмів і розмірів ключа, а також з огляду на необхідність підвищення захисту для забезпечення криптографічної живучості збереження ключів, з урахуванням середовища та критичності процесів авторизації рекомендується, щоб криптоперіоди ключів авторизації становили не більше двох років.

Відкритий ключ авторизації. Відкритий ключ авторизації є загальнодоступним елементом асиметричної пари ключів, що використовується для верифікації привілеїв об'єкта, що володіє зв'язаним особистим ключем. Криптоперіод відкритого ключа авторизації має бути таким самим, як особистого ключа авторизації, тобто не більше двох років.

У таблиці 10.6 наведені узагальнені значення рекомендованих криптоперіодів.

Наведемо також рекомендації щодо криптографічної інформації для криптографічних перетворень. До іншої криптографічної інформації відносно криптоперіодів встановлених вимог немає. У той же час можна дати такі рекомендації [119–120].

1. Параметри області домену повинні залишатись в дії до їхньої зміни.

2. Вектор ініціалізації (IV) при криптографічних перетвореннях потрібно зберігати обмежений час.

3. Поділювані таємниці (секрети) повинні бути знищені відразу ж, як тільки вони стають непотрібними для виконання криптографічних перетворень.

4. Випадкові початкові числа (RNG) повинні бути знищені негайно після їх використання.

5. Інша загальнодоступна інформація не повинна зберігатися довше, ніж це потрібно для виконання криптографічних перетворень.

6. Проміжні результати повинні бути знищені негайно після їх використання.

Таблиця 10.6. **Рекомендовані криптоперіоди для різних типів ключів**

Тип ключа	Криптоперіод	
	Період використання відправника (OUP)	Період використання одержувача
1. Особистий ключ підпису	1–3 роки	
2. Відкритий ключ підпису	Декілька років (залежно від розміру ключа)	
3. Симетричний ключ автентифікації	≤ 2 роки	≤ OUP + 3 роки
4. Особистий ключ автентифікації	1 – 2 роки	
5. Відкритий ключ автентифікації	1 – 2 роки	
6. Симетричні ключі шифрування ключів	≤ 2 роки	≤ OUP + 3 роки
7. Симетричні ключі упакування ключів	≤ 2 роки	≤ OUP + 3 роки
8. Симетричні й асиметричні ключі генерування випадкових чисел	При повторному заданні початкового числа (reseeding)	
9. Симетричний майстер-ключ	Близько 1 року	
10. Особистий ключ передачі ключів	≤ 2 роки [14]	
11. Відкритий ключ передачі ключів	1–2 роки	
12. Симетричний ключ узгодження ключів	1–2 роки	
13. Особистий статичний ключ узгодження ключів	1–2 роки	
14. Відкритий статичний ключ узгодження ключів	1–2 роки	
15. Особистий сеансовий (ефемерний) ключ узгодження ключів	Одна трансакція узгодження ключів	
16. Відкритий сеансовий (ефемерний) ключ узгодження ключів	Одна трансакція узгодження ключів	
17. Симетричний ключ авторизації	≤ 2 років	
18. Особистий ключ авторизації	≤ 2 років	
19. Відритий ключ авторизації	≤ 2 років	

Проведений аналіз також показав, що відносно ключів і криптографічної інформації має бути забезпечений ряд гарантій щодо їх цілісності, справжності (вірогідності) параметрів області та вірогідності відкритих ключів. Гарантія вірогідності дає користувачеві впевненість у тому, що відкритий ключ є математично правильним. Це зменшує ймовірність використання слабких або викривлених ключів. Недостовірні відкриті ключі можуть призводити до недостатнього забезпечення захисту (включаючи цифровий підпис, установлення ключів, шифрування), а також до витоку деякої або всієї інформації про особистий ключ власника і витік деякої або всієї інформації про особистий ключ, який комбінований з недостовірним відкритим ключем (як це може бути зроблено при виконанні узгодження ключів або шифруванні з відкритим ключем). Методи одержання гарантії вірогідності відкритого ключа й алгоритмів узгодження ключів наведені в [21–22, 37, 119–120]. Одним із важливих способів одержання гарантії вірогідності є верифікація визначених математичних властивостей, які повинен мати відкритий ключ. Іншим способом є одержання гарантії від довірчої третьої сторони, яка проводить перевірку вірогідності властивостей.

Гарантія володіння особистим ключем призначена для того, щоб переконатися, що власник відкритого ключа дійсно володіє в деякий момент часу відповідним особистим ключем. Існує декілька способів одержання гарантії володіння особистим ключем [119–120, 156].

Інформація, що захищається криптографічними механізмами, буде захищеною тільки якщо алгоритми залишаються стійкими, а ключі не компрометовані. Компрометація ключів відбувається у разі порушення в механізмах захисту (наприклад, порушенні конфіденційності, цілісності або зв'язування ключа з його власником). У разі компрометації ключ більше не зможе заслуговувати довіри для забезпечення необхідного захисту. У разі компрометації ключа використання ключа для захисту інформації (наприклад, обчислення цифрового підпису або шифрування інформації) повинне бути заборонено, а компрометований ключ відкликано.

Однак при контрольованих ситуаціях може бути виправдане продовження використання ключа для зашифрування або верифікації, наприклад, для розшифрування або верифікації цифрового підпису). Це залежить від ризиків триваючого використання й Політики управління ключами організації.

Триваюче використання компрометованого ключа повинне бути обмежене до обробки захищеної інформації. У цьому випадку об'єкт, що використовує інформацію, має бути цілком обізнаний про небезпеку, на яку він наражається. Обмеження криптоперіоду ключа обмежує компрометацію ключа. Використання різних ключів для різних цілей (наприклад, для різних застосувань, а також різних криптографічних механізмів), а також обмеження кількості інформації, що захищається одним ключем, також забезпечує досягнення цієї мети.

Із [119–120] можна зробити висновки, що компрометація ключа може мати такі наслідки.

1. Несанкціоноване розкриття ключа означає, що інший об'єкт (несанкціонований об'єкт) може одержати ключ і зуміти застосувати такий ключ для виконання обчислень, що вимагають його використання.

2. Компрометація цілісності ключа означає, що ключ є неправильним – тобто ключ модифікований (навмисно або випадково) або замінений на інший. Компрометація ключа, використовуваного для забезпечення цілісності, ставить під питання цілісність всієї інформації, що захищається ключем. Ця інформація може бути змінена або створена хибна несанкціонованим об'єктом.

3. Компрометація використання ключа або зв'язування ключа означає, що ключ може використовуватися в неправильних цілях (наприклад, для встановлення ключа замість цифрових підписів) або для неправильного застосування, що може призвести до компрометації інформації, яка захищається ключем.

4. Компрометація засобом зв'язування ключа з власником або іншим об'єктом означає, що дійсність іншого об'єкта не може бути гарантованою (тобто невідомо, ким насправді є інший об'єкт) або що інформація не може бути правильно оброблена (наприклад, зашифрована або розшифрована за допомогою правильного ключа).

5. Компрометація засобом зв'язування ключа з іншою інформацією означає, що ніякого зв'язку взагалі не існує або що зв'язок здійснюється з неправильною «інформацією». Це може призвести до порушення криптографічних послуг, втрати інформації або компрометації інформації.

Проведені дослідження й практичний досвід дозволяють запропонувати з метою мінімізації ризиків при компрометації таке:

1. Обмеження часу перебування симетричного або особистого ключа у відкритому вигляді.

2. Протидія та запобігання можливості спостереження за симетричними й особистими ключами, коли вони у відкритому вигляді.

3. Запис, зберігання та використання симетричного й особистого ключів з фізично захищених контейнерів, у тому числі генератори ключів, пристрої передачі ключів, завантажники ключів, криптографічні модулі та ЗУ ключів.

4. Використання перевірок цілісності для гарантії того, що цілісність ключа або його зв'язку з даними не була скомпрометована. Наприклад, ключі можуть бути упакованими (тобто зашифрованими) таким чином, щоб можна було знайти несанкціоновані модифікації для упакування або зв'язування.

5. Застосування для гарантії того, що дійсно був установлений правильний ключ процедур затвердження ключів.

6. Здійснення безперервного спостереження за кожним доступом до симетричних і особистих ключів, коли вони у відкритому вигляді.

7. Забезпечення криптографічної перевірки цілісності на ключі (наприклад, MAC або цифровий підпис).

8. Використання довірчих тимчасових міток для підписаних даних.

9. Знищення ключів як тільки вони стають уже непотрібними.

Найзагрозливішою компрометацією є така, що не може бути виявлена. Проте, навіть у цьому випадку можуть бути запропоновані та впроваджені захисні міри. Так, системи управління ключами повинні бути спроектовані для ослаблення негативного впливу від компрометації ключів. Вони повинні бути побудовані так, щоб компрометація одного ключа викликала компрометацію як можна меншого числа інших ключів. Наприклад, один криптографічний ключ може використовуватися для захисту даних тільки одного користувача або обмеженого числа користувачів, а не великого числа користувачів.

План відновлення компрометованих ключів має суттєве значення для відновлення криптографічних послуг. Він може бути включений у практичні положення з управління ключами. Необхідно враховувати, що хоча відновлення з компрометованого стану є здебільшого локальною дією, наслідки від скомпрометованого ключа розділяються усіма, хто використовує систему або устаткування. Тому заходи щодо відновлення зі скомпрометованого стану повинні включати участь

усього співтовариства. Ннаприклад, відновлення з компрометації кореневого особового ключа підписання центра сертифікації (CA) вимагає, щоб усі користувачі інфраструктури одержували та інсталювали новий сертифікат центру сертифікації ключів. Для запобігання таких дорогих процедур може бути доцільним уведення ретельно розроблених запобіжних заходів щодо недопущення компрометації.

10.5. АНАЛІЗ ТА ОБҐРУНТУВАННЯ ВИМОГ ЩОДО ВИБОРУ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ І РОЗМІРІВ КЛЮЧІВ

У цьому пункті наведено результати, що стосуються узагальненого аналізу й обґрунтовано вимоги до криптографічних перетворень (алгоритмів). При цьому розглядаються стандартні криптографічні перетворення або такі, що мають відповідні рекомендації або позитивні висновки. Окрім того, у зв'язку з тим, що реальна стійкість значною мірою залежить від розмірів ключів, наведено результати аналізу стійкості залежно від розмірів ключів.

Розгляд ведеться з урахуванням вимог національних і міжнародних стандартів. У подальшому як безумовний факт вважається необхідність вибору криптографічних систем з алгоритмами, що забезпечують необхідний рівень стійкості. Як основоположні вихідні дані приймемо передбачуваний час застосування інформаційної системи $T_{зс}$ та час застосування самої криптографічної системи $T_{КРС}$ зі стійкістю, прийнятою при прогнозуванні.

Порівняння стійкості алгоритмів

Відомо, що криптографічні алгоритми забезпечують різні рівні криптографічної стійкості. Здебільшого вона залежить від криптографічного алгоритму, що використовується, та розміру ключа, що застосовується. Аналізуючи стійкість, необхідно задатися моделлю порушника, моделлю загроз і моделлю вразливості. Як основну будемо розглядати загрозу типу «Повне розкриття», у результаті реалізації якої порушник визначає особистий або таємний ключ, що застосовується. Аналізуючи далі, будемо вважати, що два алгоритми вважаються для заданих розмірів ключа L_x та L_y порівнянними за стійкістю, якщо кількість зусиль (складність, вартість), необхідних для «злому алгоритмів» або визначення ключів (із заданими розмірами ключа) з використанням однакових за спроможністю криптоаналітичних систем, приблизно однакові.

Для загального випадку стійкість криптографічного алгоритму для заданого розміру ключа перш за все будемо оцінювати складність, яку необхідно реалізувати, застосовуючи метод грубої сили випробовування всіх ключів для симетричного алгоритму із заданим ключем K_x). Це справедливо, якщо не існує ніяких спрощених атак (тобто коли найефективнішою атакою є випробовування всіх можливих ключів). Якраз у цьому випадку найкращою вважається атака, що здійснюється шляхом вичерпного пошуку (грубої сили). Алгоритм, що використовує L_y-бітовий ключ, стійкість якого порівняння з L_x-бітовим ключем такого симетричного алгоритму, вважається алгоритмом, що має L_x-бітову стійкість проти криптоаналізу. Будемо також вважати, що одна групова операція при криптоаналізі вимагає складності $I_{го}$ або часу $T_{го}$.

Класи розмірів ключів, що розглядаються та рекомендуються, базуються на оцінках з використанням сучасних відомих методів криптоаналізу. З часом досяг-

нення в галузі методів факторизації, а також вирішення дискретного логарифма і дискретного логарифма в групі точок еліптичної кривої, а також квантових обчислень можуть у майбутньому змінити в сторону погіршення отримані сьогодні результати. Можуть бути розроблені нові або поліпшені існуючі атаки або технології, що зроблять деякі із сучасних алгоритмів цілком нестійкими. Якщо атаки, що ґрунтуються на квантових обчисленнях, стануть практично здійсненними, то ряд асиметричних криптоперетворень, які мають субекспоненційну складність криптоаналізу, можуть стати нестійкими. Для цього необхідно періодично проводити відповідну експертизу та здійснювати перегляд, внаслідок чого розміри ключа повинні бути збільшені або алгоритми вважатимуться незахищеними. У цілому, більш довгі ключі можуть зменшити ймовірність того, що ключі будуть компрометовані.

При порівнянні та виборі алгоритму криптографічного перетворення, наприклад, FIPS-197 або ГОСТ 28147-89, розмір блоку також може впливати на стійкість.

У таблиці 10.7 наведено результати порівняння стійкості для визнаних національних, регіональних і міжнародних стандартів [119–120]. У стовпці 1 наведно число бітів ключа для симетричного перетворення. У стовпці 2 подано алгоритми симетричних криптографічних перетворень. У стовпці 3 поданий мінімальний розмір параметрів для стандартів, що ґрунтуються на перетвореннях у кінцевих полях. Прикладами таких алгоритмів можуть бути FIPS 186-3 та ГОСТ 34.310-95 – для цифрових підписів, а також алгоритм Діффі-Геллмана (DH) і алгоритм узгодження ключів MQV, як визначено в [46, 119–120], де L_e – розмір відкритого ключа, а L_o – розмір особистого ключа. У стовпці 4 подано значення k (розмір модуля перетворення) для криптографічних перетворень, що ґрунтуються на складності вирішення задач факторизації, наприклад RSA алгоритм ANSX9.31 і PKCS#1. Посилання на ці специфікації подані у FIPS 186-3 для цифрових підписів. Значення k зазвичай використовують для того, щоб указати розмір ключа. У стовпці 5 наведено порядок базової точки для криптографічних перетворень у групі точок еліптичних кривих, що подані для цифрових підписів у [46, 119–120], і для встановлення ключів у [119–120]. Значенням f позначено розмір ключа (порядок базової точки $n = 2^f$).

Таблиця 10.7. **Порівнянні стійкості стандартизованих криптоперетворень**

Довжина симетричного ключа	Симетричні криптоперетворення	Перетворення в полі (наприклад, ГОСТ 34.310, DSA, DH)	Перетворення в кільці (наприклад, RSA)	Перетворення ЕС (наприклад, ДСТУ 4145, ECDSA)
80	2TDEA	$L = 1024$, $N = 160$	$k = 1024$	f =160 – 223
112	3TDEA	$L = 2048$, $N = 224$	$k = 2048$	$f = 224 – 255$
128	AES-128	$L = 3072$, $N = 256$	$k = 3072$	$f = 256 – 383$
192	AES-192	$L = 7680$, $N = 384$	$k = 7680$	$f = 384 – 511$
≥256	ГОСТ 28147	$L = 15360$, N=512	k =15360	$f = 512 +$
256	AES-256	$L = 15360$, $N = 512$	$k = 15360$	$f = 512 +$

У таблиці 10.8 подано розмір функції гешування з порівнянням стійкості для перерахованих розмірів параметрів і ключів для цифрових підписів, HMAC, функцій вироблення ключів і генерації випадкових чисел.

Ця інформація міститься у [211–212]. Аналогічна інформація щодо розмірів повинна бути надана в стандартах, що описують HMAC, функції вироблення ключів, генератори випадкових чисел та інші алгоритми, що використовують функцію як складову при криптографічному захисті. Необхідно відзначити, що SHA-1, як нещодавно було продемонстровано, забезпечує менш ніж 80-бітовий захист для цифрових підписів. У [211–212] вона оцінена в 69 бітів. Тому SHA-1 не рекомендується для використання в нових системах. Нові криптографічні системи повинні використовувати одну з найбільш довгих функцій гешування. У таблицю 10.8 функція гешування включена для відображення свого широкого використання в існуючих системах.

Таблиця 10.8. **Стійкість функцій гешування при криптографічних застосуваннях**

Довжина симетричного ключа	Цифрові підписи з застосуванням функцій гешування	Коди автентифікації HMAC	Функції вироблення ключів	Генерація випадкових чисел	Інше (повинно бути визначено)
80	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 ГОСТ 34.311	Має бути визначено	Має бути визначено	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 ГОСТ 34.311	Має бути визначено
112	SHA-224 SHA-256 SHA-384 SHA-512 ГОСТ 34.311			SHA-1 SHA-224 SHA-256 SHA–384 SHA–512 ГОСТ 34.311	
128	SHA-256 SHA-384 SHA-512 ГОСТ 34.311			SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 ГОСТ 34.311	
192	SHA-384 SHA-512 ГОСТ 34.311			SHA-224 SHA-256 SHA-384 SHA-512 ГОСТ 34.311	
256	SHA-512 ГОСТ 34.311			SHA-256 SHA-384 SHA-512 ГОСТ 34.311	

Визначення здатних (допущених до застосування) комплектів алгоритмів

Проведені дослідження дозволили визначити криптографічні алгоритми та мінімальні розміри ключів для застосування в ІВК. У таблиці 10.9 наведено відповідні прогнози.

Алгоритми та розміри ключа, зазначені в таблиці 10.9, вважаються такими, що найбільше підходять для захисту даних під час заданих періодів часу. Алгоритми або розміри ключа, не зазначені для заданого діапазону років, не повинні використовуватися для захисту інформації під час такого періоду часу. Якщо безпечний час інформації перевищує один часовий період, зазначений у таблиці, і переходить у наступний часовий період (більш пізній часовий період), то повинні використовуватися алгоритми та розміри ключа, зазначені для більш пізнього часу.

Таблиця 10.9. **Рекомендовані алгоритми та мінімальні розміри ключа**

Безпечний період застосування	Симетричні криптоперетворення	Перетворення в полі (наприклад, ГОСТ 34.310, DSA, DH)	Перетворення в кільці (наприклад, RSA)	Перетворення ЕС (наприклад, ДСТУ 4145, ECDSA)
До 2010 р. (мін. 80 бітів стійкості)	2TDEA 3TDEA AES-128 AES-192 AES-256	Мін.: $L = 1024$; $N = 160$	Мін.: $k = 1024$	Мін.: $f = 160$
До 2030 р. (мін. 112 бітів стійкості)		Мін.: $L = 1048$; $N = 224$	Мін.: $k = 2048$	Мін.: $f = 224$
До 2030 р. (мін. 128 бітів стійкості)	AES-128 AES-192 AES-256	Мін.: $L = 3072$; $N = 256$	Мін.: $k = 3072$	Мін.: $f = 256$

Використання криптографічних примітивів

З точки зору стійкості, криптографічні примітиви (алгоритми), що застосовуються сумісно, кожен з яких забезпечує різну стійкість, зазвичай не використовують. Однак алгоритми з різними рівнями стійкості та розмірами ключів можуть застосовуватись із причин ефективності, доступності, інтероперабельності тощо за умови забезпечення деякого мінімального але достатнього рівня стійкості. У цьому випадку найслабший алгоритм і деякий мінімальний розмір ключа визначають стійкість захисту. Визначення стійкості захисту повинне здійснюватися не тільки щодо алгоритму(ів) і розміру(ів) ключів, а й також для будь-яких алгоритмів і розмірів ключів, що використовуються при встановленні ключа(ів), наприклад, у протоколах встановлення ключів. Далі подано перелік деяких комбінацій алгоритмів та наведено оцінки щодо їх ефективності при застосуванні в ІВК.

1. Коли для створення криптографічної інформації за допомогою одного чи більшого числа криптографічних алгоритмів (наприклад, ГОСТ 28147, AES або HMAC) застосовується схема встановлення ключів, то реальна стійкість повинна оцінюватися найслабшим алгоритмом з відповідним розміром ключа.

2. Коли функція гешування й алгоритм цифрового підпису використовуються для обчислення цифрового підпису в комбінації, то стійкість підпису визначається більш слабким алгоритмом із двох алгоритмів, що застосовуються.

3. Коли для генерування ключа використовується генератор випадкових бітів, призначений для забезпечення L_x-бітового захисту, то повинен використовуватися затверджений генератор випадкових бітів, що забезпечує щонайменше L_x-бітів захисту.

Якщо визначено, що для захисту даних потрібен конкретний рівень захисту, то необхідно вибирати набір алгоритму та ключа, за яких забезпечується мінімальний захист.

Заміна криптографічних алгоритмів і розмірів ключа

Як один з основних показників стійкості використовують безпечний час криптографічного алгоритму T_a. Під ним розуміють період часу, протягом якого дані, що захищаються конкретним криптографічним алгоритмом (з відповідним розміром ключа), залишаються захищеними від криптоаналітичних атак. Протягом такого періоду алгоритм може використовуватися для реалізації різних криптографічних функцій. При обґрунтуванні та виборі криптографічних алгоритмів спочатку визначають криптографічні послуги, які потрібні для конкретного застосування. Потім, відштовхуючись від значення безпечного часу алгоритму криптографічного перетворення необхідно вибрати алгоритм і розмір ключа, але такими, щоб цього було достатньо для виконання вимог. Потім проектують і створюють систему управління ключами (якщо це потрібно), вибираючи тільки атестовані криптографічні засоби. У міру наближення комплекту криптографічних алгоритмів і розмірів ключів до прогнозованого терміну закінчення їх придатності необхідно обґрунтовувати й вибирати новий комплект алгоритмів(му) і розмірів(ру) ключів.

Нині застосовується багато прикладних інформаційних систем, у яких використовують алгоритми та розміри ключів, які не зазначені в таблиці 10.9. Прийнято, що коли алгоритм і розмір ключа вже не задовольняють вимогам, то будь-яка інформація, захищена з використанням такого алгоритму або розміру ключа, вважається «розкритою (наприклад, більше не конфіденційною, або цілісність і справжність не можуть бути гарантованими). Якщо дані, що потребують захисту, зберігаються, то вони мають бути захищені з використанням затвердженого алгоритму та розміру ключа, що гарантують їх захист протягом безпечного часу (життєвого циклу). При цьому необхідно враховувати, що, наприклад, зашифрована інформація може збиратися й зберігатися несанкціонованими об'єктами (порушниками).

При виборі підходящого криптографічного алгоритму та розміру ключа дуже важливо брати до уваги очікуване значення безпечного часу життєвого циклу даних. Слід враховувати, що криптографічний алгоритм з відповідним розміром ключа використовується як для прямого криптографічного перетворення, так і зворотного. Коли до уваги береться безпечний час життєвого циклу даних, то криптографічний захист не повинний застосовуватися до даних, якщо безпечний час життєвого циклу даних перевищує термін безпечного часу життєвого циклу криптографічного алгоритму. У подальшому період часу, протягом якого може використовуватися алгоритм із заданим розміром ключа, будемо називати періодом використання алгоритму для прямих перетворень (наприклад, відправником). У цілому, вважається, що безпечний час $T_{\text{ітс}}$ інформаційно-телекомунікаційної системи треба визначати як:

$$T_{\text{ітс}} = T_{\text{а}} + T_{\text{д}},$$

де $T_{\text{а}}$ – період використання криптографічного алгоритму, а $T_{\text{д}}$ – необхідний безпечний час даних, що захищаються.

Наприклад, припустимо, що 3TDEA має бути введений в експлуатацію у 2010 р., а безпечний час життя даних може досягати чотирьох років. У таблиці 10.9 зазначено, що 3TDEA має безпечний час життя алгоритму, який досягає 2030 р., але не вище. Однак, у зв'язку з тим, що дані можуть використовуватися протягом чотирьохрічного безпечного часу, період використання алгоритму відправником буде завершуватися у 2026 р., а не у 2030 р. (тобто алгоритм не може використовуватися для захисту даних після 2026 р.). Див. рис. 10.3.

Рис. 10.3. Приклад періоду алгоритму прямого перетворення (відправника)

При розробці та введенні в дію алгоритмів криптографічного захисту рекомендується використовувати найбільш стійкий алгоритм і за можливості більшого розміру ключ. Такий підхід дозволить обійтися без великих матеріально-технічних затрат, які будуть необхідні для заміни алгоритму криптографічного перетворення та/або довжини ключа. Однак вибір деяких алгоритмів або розмірів ключа, що є зайво стійкими або великими, може впливати на ефективність криптографічних перетворень (наприклад, алгоритм може бути недопустимо повільним).

Процес переходу до використання нового алгоритму або розміру ключа повинний бути як можна простішим, наприклад за рахунок вибору інших параметрів, а не вимагати побудови цілої нової криптографічної системи. Важливим є правильне визначення критичності інформації, перш за все з урахуванням періоду життєвого циклу системи. Причому критичність інформації, що повинна бути захищена з використанням нового алгоритму(ів), має оцінюватися з метою визначення мінімальних вимог безпеки для системи. Необхідно подбати про те, щоб не недооцінювати період життя інформаційної системи або критичність інформації, що вимагає захисту. Багато рішень, що були спочатку прийняті як тимчасові рішення, уже вичерпали свої очікувані терміни придатності.

Вибір алгоритму

Нові алгоритми повинні ретельно вибиратися для гарантії, що вони будуть відповідати або перевищувати мінімальні вимоги безпеки системи.