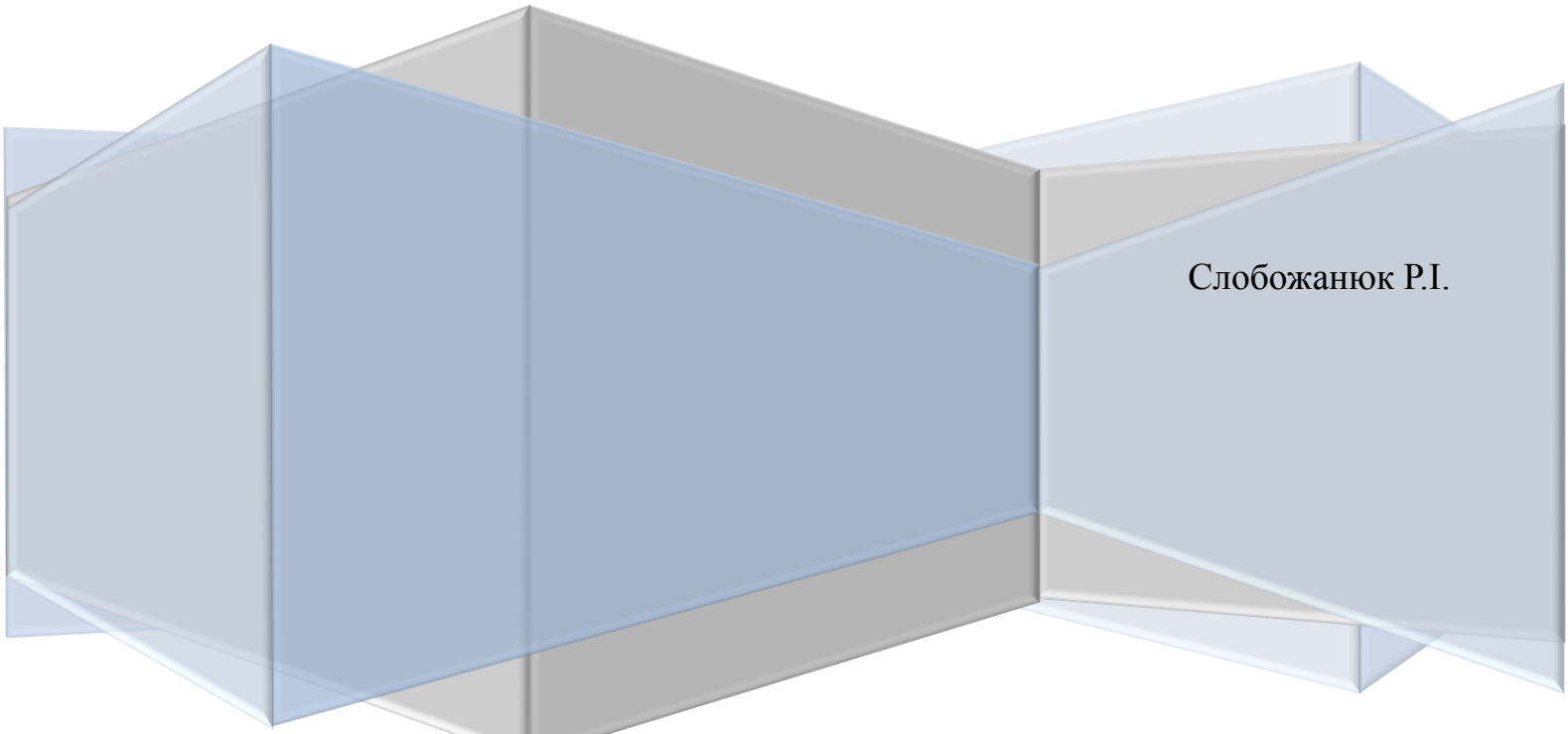
ХДПК

Інформаційна безпека

Конспект лекцій



Слобожанюк Р.І.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ ДЕРЖАВНИЙ ПОЛІТЕХНІЧНИЙ КОЛЕДЖ

Для спеціальності
151 «Автоматизація та комп'ютерно-інтегровані технології»

Конспект лекцій

з навчальної дисципліни «Інформаційна безпека»

ХДПК - 2019 р.

Конспект лекцій з дисципліни «Інформаційна безпека» для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології, спеціалізації» 5.151.2 «Обслуговування пристроїв електрозвязку».

Укладач: Слобожанюк Р.І. – ХДПК, 2019. – 137 с.

Конспект лекцій розглянутий та рекомендований цикловою комісією

«Транспорту та електрозв'язку»

(назва циклової комісії)

Протокол № _____ від "___"_____20____р.

Голова циклової комісії _____ (Руденко А.І.)

(підпис) (прізвище та ініціали)

Схвалено методичною радою Харківського державного політехнічного коледжу

Протокол № _____ від "____"_____2019р.

Голова методичної ради _____(Величко В.О.)

(Підпис) (прізвище та ініціали)

ІНФОРМАЦІЙНИЙ ОБСЯГ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ (лекції)

№ п/п	Форма занять	Обсяг годин	Зміст занять
Модуль 1. Основи захисту інформації			
1.	Лекція 1		Вступ. Основні поняття та визначення в сфері інформаційної безпеки.
			Змістовний модуль 1 Загрози інформаційній безпеці
2.	Лекція 2		Сучасна ситуація у сфері інформаційної безпеки
3.	Лекція 3		Архітектура системи безпеки інформації: основні шляхи витоку інформації та несанкціонованого доступу в каналах телекомунікацій
4.	Лекція 4		Основні підходи до забезпечення інформаційної безпеки в телекомунікаційних мережах
5.	Лекція 5		Структура та задачі органів безпеки інформації в інформаційних системах
6.	Лекція 6		Організаційно-технічні та режимні заходи систем захисту інформації
7.	Лекція 7		Класифікація загроз інформаційної безпеки
8.	Лекція 8		Канали несанкціонованого доступу інформації
9.	Лекція 9		Нормативна і правова база захисту інформації в системах та мережах телекомунікацій України: законодавча, нормативно-методична, наукова, нормативно-правова бази України із забезпечення інформаційної безпеки в системах телекомунікацій
10.	Лекція 10		Стандартизація методів забезпечення та сертифікація компонентів систем телекомунікації за вимогами інформаційної безпеки
Модуль 2. Механізми забезпечення «інформаційної безпеки»			
			Змістовй модуль 1 Ідентифікація та аутинфікація
11.	Лекція 11		Визначення понять «ідентифікація» «аутинфікація» Протоколи аутентифікації, взаємна аутентифікація, одностороння аутентифікація
			Змістовий модуль 2 Криптографія та шифрування.
12.	Лекція 12		Криптографічний захист інформації Теоретичні основи критографії
13.	Лекція 13		Сучасні концепції криптографії
14.	Лекція 14		Класичні методи шифрування
15.	Лекція 15		Принципи криптографічного захисту інформації

16.	Лекція 16		Загальні відомості про блочні шифри Генерування блочних шифрів
17.	Лекція 17		Поточні шифри. Шифри гаммування
			Змістовий модуль 3 Симетричні криптографічні системи
18.	Лекція 18		Класичні симетричні криптосистеми. Криптосистема Хілла. Особливості, принцип організації
19.	Лекція 19		Сучасні симетричні криптосистеми. Стандарт шифрування DES
20.	Лекція 20		**Алгоритм шифрування IDEA**
21.	Лекція 21		Керування ключами криптографії
			Змістовний модуль 4 Асиметричні криптографічні системи
22.	Лекція 22		Концепція криптосистеми з відкритим ключем
23.	Лекція 23		Види електронних підписів в Україні Управління ключами. Використання ЕП
Модуль 3. Засоби захисту від несанкціонованого доступу в системах звязку			
			Змістовий модуль 1. Технічний захист інформації. Загальні поняття та визначення
24.	Лекція 24		Технічний захист інформації в телекомунікаційних системах
25.			**Змістовий модуль 2.** Технічний захист інформації в цирових системах комутації
26.	Лекція 25		Організація та порядок технічного захисту інформації в ЦАТС
27.	Лекція 26		Комплексна система захисту інформації в програмно-керованих АТС
			Змістовий модуль 3. Захист мовної інформації в технологіях безпровідного зв’язку.
28.	Лекція 27		Інформаційна модель безпеки технологій зв'язку
29.	Лекція 28		Забезпечення інформаційної безпеки в мережі стільникового зв’язку стандарті GSM , CDMA
30.	Лекція 29		Забезпечення інформаційної безпеки в системах транкінгового зв’язку TETRA
Разом			

МОДУЛЬ 1. ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Лекція 1

Тема: ВСТУП. Основні поняття та визначення в сфері інформаційної безпеки

Проблема інформаційної безпеки обумовлена зростаючою роллю інформації в суспільному житті. Сучасне суспільство все більше набуває рис інформаційного суспільства. Інформаційна безпека є однією з проблем, з якою зіткнулося сучасне суспільство в процесі масового використання автоматизованих засобів її обробки.

Згідно із Законом України «Про інформацію» у його першій редакції інформація визначалася як «систематизовані, докумен-то-вані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище». У чинній редакції цього Закону це поняття розкрите як «будь-які відо-мості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

Інформаційна безпека - це захищеність інформації і підтримуючої її інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати шкоди власникам або користувачам інформації.

Інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації - це принципово ширше поняття.

Завдання по забезпеченню інформаційної безпеки для різних категорій суб'єктів може істотно різнитися.

Під захистом інформації розуміється комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Захист інформації (ГОСТ 350922-96) - це діяльність, спрямована на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних дій на захищає інформацію.

В дисципліні «Інформаційна безпека» розглядаються загальні питання забезпечення інформаційної безпеки взагалі та в телекомунікаційних системах.

Інформаційна безпека має першорядне значення у зв’язку із значним поширенням атак, яким постійно піддаються як окремі мережі підприємств, так і національні мережі в цілому.

Під час розгляду питань безпеки виходжу з необхідності розгляду цілісного підходу до управління інформаційною безпекою й навчання методам безпеки мереж.

В дисципліні комплексно розглядаються правові, організаційні, криптографічні й технічні питання захисту інформації.

Подано основні визначення, необхідні фахівцеві в галузі інформаційної безпеки, розглядаються різні типи загроз і методи їхній протидії, криптографічний захист інформації, механізм електронного цифрового підпису, формування інфраструктури відкритого ключа, основні радіоканали витоку інформації, питання протидії несанкціонованому зніманню інформації за допомогою закладних пристроїв, методи виявлення й протидії побічним електромагнітним випромінюванням, питання використання спеціальної апаратури для виявлення каналів витоку інформації.

1 Основні терміни та поняття у сфері інформаційної безпеки

Інформація — це відомості про особи, предмети, факти, явища і процеси незалежно від форми їхнього подання.

Інформація, що захищається, — це інформація, що є предметом власності якого-небудь суб'єкта (держави, відомства, групи осіб або окремого громадянина) і підлягає захисту відповідно до вимог правових документів або вимог, які встановлюються власником інформації. До такого типу інформації належить інформація з обмеженим доступом і критична інформація. Саме така інформація, найчастіше, циркулює в телекомунікаційних системах.

Інформаційні відносини в Україні регулюються Законом України про інформацію. Їхніми основними принципами є:

- гарантованість права на інформацію;
- відкритість, доступність інформації й свобода обміну інформацією;
- об'єктивність, вірогідність інформації;
- повнота й точність інформації;
- законність отримання, використання, поширення й зберігання інформації.

Під несанкціонованим доступом до інформації розуміється доступ до інформації з порушенням установлених прав і правил доступу.

Захистом інформації від несанкціонованого доступу є діяльність, спрямована на запобігання отримання інформації, що захищається, зацікавленим суб'єктом з порушенням установлених правовими документами або власником інформації прав або правил доступу до інформації, що захищається. При цьому зацікавленим суб'єктом, що здійснює несанкціонований доступ до інформації, що захищається, може бути держава, громадська організація, група або окремі громадяни.

Захистом інформації від несанкціонованого впливу є діяльність, спрямована на запобігання впливу на інформацію, що захищається, з порушенням установлених прав й (або) правил модифікації, що призводить до її перекручення, знищення, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації. Несанкціонований вплив на інформацію здійснює організований порушник, що переслідує мету руйнування інформації або інформаційної системи.

Захистом інформації від ненавмисного впливу є діяльність, спрямована на запобігання впливу на інформацію, що захищається, в результаті помилкових дій її користувача, збою технічних і програмних засобів інформаційних систем, природних явищ або інших нецілеспрямованих впливів, що призводять до перекручення, знищення, копіювання, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації. Ненавмисний вплив на інформацію має випадковий характер, однак він здатен зруйнувати інформацію або інформаційну систему.

Законодавство України поділяє інформацію на ***відкриту інформацію*** й *інформацію з обмеженим доступом*. У свою чергу, інформацію з обмеженим доступом поділяють на конфіденційну інформацію та державну таємницю.

Конфіденційна інформація — це відомості, які перебувають у володінні, використанні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених для них умов.

Конфіденційну інформацію поділяють на безліч видів таємниць:

службову таємницю, таємницю листування, таємницю телефонних, поштових, телеграфних й інших повідомлень, нотаріальну таємницю, адвокатську таємницю, лікарську таємницю, банківську таємницю тощо.

До інформації, що становить державну таємницю, відносять інформацію, що містить передбачену Законом таємницю, розголошення якої спричинить завдання збитків громадянину, суспільству й державі в цілому. Порядок роботи з державною таємницею та процедура її захисту визначається відповідними державними органами з урахуванням вимог законів України про інформацію й державну таємницю.

Безпека — це стан об'єкта, при якому йому не загрожує небезпека, зберігається його незалежність, надійність, цілісність, є захищеність від небезпек або існуючих загроз. Безпека будь-якого об'єкта свідчить про те, що він здатний розв'язати поставлені перед ним завдання, а у разі виникнення різного роду непередбачених обставин, небезпек або загроз — захиститися від них або відновити свою працездатність.

Метою ***інформаційної безпеки*** є завдання зберегти властивості системи, захистити й гарантувати точність і цілісність інформації та мінімізувати наслідки, які можуть мати місце, якщо інформація буде модифікована або зруйнована. Досягнення мети вимагає обліку всіх подій, у ході яких інформація створюється, модифікується, забезпечується доступ до неї або її поширення за допомогою відкритих мереж.

Інформаційна безпека має надавати гарантію того, що досягаються такі цілі:

- конфіденційність критичної інформації;
- цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка та відображення);
- актуальність (своєчасність відновлення) і доступність інформації (коли вона потрібна авторизованим користувачам);
- облік всіх процесів, пов'язаних з інформацією.

Сутність та зміст понять у сфері інформаційної безпеки

Поняття інформаційної безпеки може розглядатись у широкому та у вузькому розумінні.

Інформаційна безпека (у вузькому розумінні) є необхідною, але невід'ємною складовою інших видів безпеки. Інформаційна безпека – це невід'ємна частина політичної, економічної, військової, соціальної та інших складових національної безпеки.

Інформаційна безпека (у вузькому розумінні) розглядається як одна зі складових економічної безпеки, тому що інформація, яка циркулює на підприємстві має комерційний характер і впливає на економічні показники діяльності підприємства (організації). Інформаційна безпека (у вузькому розумінні) розглядається як інформаційна безпека підприємства (організації) – це стан захищеності інформації підприємства (організації) від дестабілізуючого впливу зовнішніх та внутрішніх загроз. Інформаційна безпека (у широкому розумінні) є самостійним видом безпеки поряд з національною, економічною, військовою, соціальною і політичною.

Інформаційна безпека (у широкому розумінні) розглядається як інформаційна безпека держави – це складова національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз.

Інформаційна безпека інформатизації знайшла юридичний вираз на законодавчому рівні у Законі України „Про Національну програму інформатизації" [2].

Відповідно до цього Закону інформаційну безпеку забезпечують: - комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; - комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; - банк засобів діагностики, локалізації і профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високо надійні криптографічні методи захисту інформації тощо.

В умовах поширення інформаційних впливів справедливе наступне визначення [3]: **„Інформаційна безпека людини, суспільства, держави** – це стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів".

Інформаційна безпека розглядається також як єдність концептуальних, теоретичних і технічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, 7 соціальної, військової, духовної та ін.), а також сфер формування, циркуляції, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління в усіх видах діяльності тощо. В організаційно-управлінському аспекті поняття „інформаційна безпека" розглядається як: стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації.

У книзі [4] пропонується наступне визначення поняття „інформаційна безпека". „Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій і держави". За

конкретних умов середовища функціонування інформації можна формулювати уточненні визначення, що відповідають цим умовам.

Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства) – це суспільні відносини щодо створення і підтримання в належному стані режиму нормального функціонування відповідної автоматизованої (комп‘ютеризованої) інформаційної системи, систем телекомунікацій; комплекс організаційних, правових та інженернотехнологічних (технічних та програмно-математичних) заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних загроз, реалізація яких може порушити або припинити життєдіяльність конкретної соціо - технічної інформаційної системи.

В іншому випадку: **„Інформаційна безпека** – це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати збитку власникам або користувачам інформації і підтримуючій інфраструктурі”.

Поняття „інформаційна безпека” характеризує стан (властивість) інформаційної захищеності людини, суспільства, природи в умовах можливої дії загроз і досягається системою заходів, спрямованих: – на попередження загроз. Попередження загроз – це превентивні заходи для забезпечення інформаційної безпеки в інтересах попередження можливості їхнього виникнення; – на виявлення загроз. Виявлення загроз виражається в систематичному аналізі і контролі можливості появи реальних або потенційних загроз і своєчасних заходів для їхнього попередження; – на локалізацію злочинних дій і вживання заходів по ліквідації загрози або конкретних злочинних дій; – на ліквідацію наслідків загроз і злочинних дій та відновлення статус-кво. У Законі України „Про телекомунікації” під інформаційною безпекою розуміють: „…здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення установленого порядку її маршрутизації” [5].

Як видно з наведених визначень, інформаційна безпека пов’язана із процесом захисту інформації. Тобто, якщо інформація захищена, виходить, що вона в безпеці.

Поняття „захист інформації”.

Під захистом інформації розуміють сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією [6]. Під захистом інформації, у більш широкому сенсі, розуміють комплекс організаційних, правових і технічних заходів для запобігання загрозам інформаційної безпеки й усуненню їхніх наслідків. Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела є загрозою безпеці інформації. Мета та методи захисту інформації відображають її сутність. У цьому розумінні захист інформації ототожнюється з процесом забезпечення інформаційної безпеки, як глобальної проблеми безпечного розвитку світової цивілізації, держав, співдружностей людей, окремої людини, існування природи. Попередження можливих загроз і протиправних дій може бути забезпечене всілякими засобами, починаючи від створення клімату глибоко-усвідомленого відношення співробітників до проблеми безпеки і захисту інформації до створення глибокої, ешелонованої системи захисту фізичними, апаратними, програмними і криптографічними засобами. Попередження загроз можливе і шляхом одержання інформації про протиправні акти, які готуються, плановані розкрадання, підготовчі дії й інші елементи злочинних вчинків. У попередженні загроз важливу роль відіграє інформаційно-аналітична

діяльність служби безпеки на основі глибокого аналізу криміногенного стану й діяльності конкурентів і зловмисників. Виявлення загроз – це дії з визначення конкретних загроз та їхніх джерел, які приносять той або інший вид збитку. До таких дій можна віднести виявлення фактів розкрадання або шахрайства, а також фактів розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів. Виявлення має на меті проведення заходів щодо збирання, нагромадження й аналітичного оброблення відомостей щодо можливої підготовки злочинних вчинків з боку кримінальних структур або конкурентів на ринку виробництва та збуту товарів і продукції. Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози і конкретних злочинних вчинків. Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози. Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань і забезпечити:

– запобігання розголошення і витоку конфіденційної інформації;

– заборону несанкціонованого доступу до джерел конфіденційної інформації;

– збереження цілісності, повноти і доступності інформації;

– дотримання конфіденційності інформації;

– забезпечення авторських прав.

Найбільш загальними принципами захисту будь-якого виду інформації, що охороняється, є:

– захист інформації організує і проводить власник інформації або уповноважені ним особи (юридичні або фізичні);

– захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння і використання на шкоду його інтересам;

– захист інформації здійснюється шляхом проведення комплексу заходів для обмеження доступу до захищеної інформації, що захищається, і створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та її носіїв.

Захищена інформація, яка є державною або комерційною таємницею, як і будь-який інший вид інформації, необхідна для управлінської, науковоробничої та іншої діяльності.

Сьогодні перед захистом інформації ставляться більш широкі задачі: забезпечити безпеку інформації. Це обумовлено низкою обставин, і в першу чергу тим, що все більш широке застосування в накопичуванні й обробленні захищеної інформації, одержують електронно обчислювальні машини (ЕОМ), в яких може відбуватися не тільки витік інформації, але і її руйнування, перекручування, підроблення, блокування й інші втручання в інформацію й інформаційні системи.

Отже, під захистом інформації слід також розуміти забезпечення безпеки інформації і засобів інформації, в яких накопичується, обробляється і зберігається захищена інформація. Таким чином, захист інформації

– це діяльність власника інформації або уповноваженої ним особи з:

– забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією;

– запобігання витоку і втрати інформації;

– збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки;

– збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами.

Таким чином, захист інформації – це діяльність, яка спрямована на забезпечення конфіденційності, цілісності та доступності інформації в процесі одержання, зберігання, оброблення і поширення за допомогою організаційних, правових, технічних та економічних засобів.

Засоби забезпечення збереження та захисту інформації в державній організації, на підприємстві або фірмі відрізняються за своїми масштабами і формами.

Вони залежать від виробничих, фінансових та інших можливостей фірми, від кількості секретів, які вона охороняє та їхньої значимості.

При цьому вибір таких заходів необхідно здійснювати за принципом економічної доцільності, дотримуючись у фінансових розрахунках „золотої середини", оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, можуть викликати втрату певної частки прибутку або призвести до непоправних збитків.

Відсутність у керівників підприємств чіткого уявлення про умови, що сприяють витоку конфіденційної інформації, приводять до її несанкціонованого поширення.

Наявність значної кількості уразливих місць на будь-якому сучасному підприємстві або фірмі, широкий спектр загроз і досить висока технічна оснащеність зловмисників вимагає обґрунтованого вибору спеціальних рішень з захисту інформації.

Основою таких рішень можна вважати:

1. Застосування наукових принципів з забезпечення інформаційної безпеки, що включають у себе: законність, економічну доцільність і прибутковість, самостійність і відповідальність, наукову організацію праці, тісний зв'язок теорії з практикою, спеціалізацію і професіоналізм, програмно-цільове планування, взаємодію і координацію, доступність у поєднанні з необхідною конфіденційністю.

2. Прийняття правових зобов'язань з боку співробітників підприємства по відношенню до збереження довірених їм відомостей (інформації).

3. Створення таких адміністративних умов, за яких виключається можливість крадіжки, розкрадання або перекручування інформації.

4. Правомірне залучення до карної, адміністративної й інших видів відповідальності, які гарантують повне відшкодування збитку від втрати інформації.

5. Проведення діючого контролю і перевірки ефективності планування і реалізації правових форм, методів захисту інформації відповідно до обраної концепції безпеки.

6. Організація договірних зв'язків з державними органами регулювання в галузі захисту інформації.

Здійснюючи комплекс захисних заходів головне – обмежити доступ у ті місця і до тієї техніки, де зосереджена конфіденційна інформація (не забуваючи, звичайно, про можливості і методи дистанційного її одержання).

Зокрема, використання якісних замків, засобів сигналізації, хорошої звукоізоляції стін, дверей, стелі та підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму й ін.) серйозно ускладнять або зроблять безглуздими спроби впровадження спецтехніки.

Лекція 2

Тема: **Сучасна ситуація у сфері інформаційної безпеки**

Роль та місце інформаційної безпеки в інформаційному суспільстві

Інформаційна безпека є однією з важливих складових глобальної безпеки. У процесі глобалізації, в умовах побудови інформаційного суспільства роль інформаційної безпеки посилюється і, навпаки, глобальні процеси впливають на інформаційну безпеку та взаємозв'язану з нею економічну, національну та глобальну.

Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини.

Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів. Особливості необмеженого та неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому.

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності інформаційно-телекомунікаційних мереж. Завдяки стрімкому технологічному прогресу постає ряд життєво важливих питань щодо організації процесів оброблення, зберігання, поширення та захисту інформації в глобальних інформаційно-комунікаційних системах. Бо саме інформаційні технології та розвинена інфраструктура телекомунікацій відіграють сьогодні вирішальну роль у забезпеченні зростання продуктивності виробництва, адміністративного і господарського управління, у розширенні інформаційної взаємодії між людьми, у поширенні масової інформації, у процесі інтелектуалізації суспільства. Інформаційна безпека має важливе значення для того, щоб інформаційні технології могли відповідати очікуванням ділового світу, споживачів і урядів та щоб дійсно надавали всі ті потенційні вигоди, що їх забезпечують інформаційно-комунікаційні технології. Інформаційна безпека в глобальних процесах набуває особливого значення і, внаслідок її тісних взаємовпливів з економічною та національною безпекою, вносить свій значний вклад у глобальну безпеку.

Глобальною безпекою назвемо такий стан глобальних процесів та форм їхньої реалізації за якого забезпечуються: – гармонічне поєднання інтересів народів, націй, держав та інтересів усього людства; – ефективне вирішення завдань, які стоять перед людством та окремими державними, регіональними та місцевими адміністраціями; – усебічний розвиток і забезпечення потреб кожної людини.

Глобальна безпека має фундаментальний характер і може бути досягнута за необхідного забезпечення її складових частин. Складовими частинами глобальної безпеки є: національна,

економічна, інформаційна, технічна, юридична, фізична, соціальна, військова, екологічна, ресурсна, продовольча, енергетична, фінансово-грошова, цінова, демографічна, пожежна, медична, психологічна, психічна, кримінальна безпеки.

Особливості розвитку інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ, комп'ютерні віруси та інше гостро поставили перед суспільством проблеми інформаційної безпеки. Інформаційна безпека повинна здійснюватися комплексно та систематично з використанням повного набору засобів (організаційних, технічних, апаратнопрограмних та ін.) щоб запобігти інформаційному тиску та в цілому будь-якій іншій небезпеці. Зрозуміло, що становлення суспільства нового типу дуже гостро ставить питання інформаційної безпеки простору держави, людини, суспільства, а також створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне одержання, поширення і використання інформації. Це питання неможливо обійти, тим більше, що воно стає дуже актуальним зараз і для нашої країни. Інформаційна безпека є більш вузьким поняттям і розглядається як складова національної безпеки. Інформаційна безпека містить у собі захист інформаційних мереж, ресурсів, програмних засобів, об'єктів інтелектуальної власності й інших нематеріальних активів, включаючи майнові інтереси учасників підприємницької діяльності [1].

В умовах глобалізації посилюється значимість проблем, які пов'язані з інформаційно безпекою, таких як:

– виникнення та зростання кіберзлочинності та кібертероризму;

–виникнення окремих видів інформаційної зброї та ведення глобальних інформаційних війн; – втрата національної культури або злиття її з іншими, вплив культур країн світу та менталітету інших націй;

– стимулювання інформаційно-розвиненими державами „відпливу інтелекту" та капіталів;

– виникнення явищ „інформаційного вибуху", „інформаційного голоду" та „інформаційних війн".

– ускладнення вирішення питань збереження державної, комерційної, службової та персональної таємниці, тому що низький рівень вітчизняних інформаційних технологій обумовив побудову інформаційної інфраструктури України на базі імпортної техніки й технології;

– розвиток телебіометрики й сенсорних мереж у взаємодії людей між собою та навколишнім середовищем.

Інформаційна безпека не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації, вирішення цієї проблеми як складової національної безпеки. Тенденції розвитку сучасного світу характеризуються створенням єдиного глобального інформаційного простору на планеті, отож, проблема інформаційної безпеки стає проблемою колективною, а не окремо взятої країни.

Лекція3

Тема: **Архітектура системи безпеки інформації: основні шляхи витоку інформації та несанкціонірованого доступу в каналах телекомунікацій**

Визначення несанкціонованого доступу

Під НСД слід розуміти доступ до інформації з використанням засобів, включених до складу КС, що порушує встановлені ПРД. Несанкціонований доступ може здійснюватись як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу КС розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

- безпосереднє звертання до об'єктів з метою одержання певного виду доступу;
- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє здійснити НСД;
- впровадження в КС програмних або апаратних механізмів, що порушують структуру і функції КС і дозволяють здійснити НСД.

Під захистом від НСД, звичайно, слід розуміти діяльність, спрямовану на забезпечення додержання ПРД шляхом створення і підтримки в дієздатному стані системи заходів із ахисту інформації. Поняття (термін) захист від НСД є сталим і тому використовується в цьому НД і документах, що на ньому базуються. Проте зміст даного поняття дещо вужчий, ніж коло питань, що розглядаються. Так, політика безпеки КС може містити вимоги щодо забезпечення доступності інформації, які, наприклад, регламентують, що КС має бути стійка до відмов окремих компонентів. Цю вимогу не можна віднести до ПРД, проте її реалізація здійснюється засобами, що входять до складу КЗЗ. Тому система НД щодо захисту інформації в КС від НСД охоплює коло питань, пов'язаних з створенням і підтримкою в дієздатному стані системи заходів, що спрямовані на забезпечення додержання вимог політики безпеки інформації під час її обробки в КС.

Лекція 4

Тема: **Основні підходи до забезпечення інформаційної безпеки в телекомунікаційних мережах**

Захист інформації зазвичай здійснюють за трьома основними напрямками:
правовий, організаційний і *технічний* захист інформації.

До **технічних заходів** можна віднести захист від несанкціонованого доступу до системи шляхом використання спеціальних паролів, шифрування файлів, резервування особливо важливих комп’ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих елементів, контроль

електромагнітного й акустичного стану простору, виявлення й пригнічення технічних каналів витоку інформації, монтаж обладнання виявлення й гасіння пожежі, обладнання виявлення води, застосування конструктивних заходів захисту від розкрадань, саботажу або диверсій, установку резервних систем електроживлення; оснащення приміщень замками, установку сигналізацій тощо.

До **організаційних заходів** належать формування політики безпеки об’єкта, що захищається, охорона об’єкта, ретельний добір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності об’єкта, організацію обслуговування сторонньою організацією або особами, не зацікавленими в прихованні фактів порушення робочих процедур, покладання відповідальності на працівників, вибір місця розташування об’єкта тощо.

До **правових заходів** слід віднести розробку норм, що встановлюють відповідальність за комп’ютерні злочини й злочини в сфері технічного захисту інформації, захист авторських прав, удосконалення карного й цивільного законодавств, а також судочинства.

Властивості інформації з точки зору її захисту

Захист інформації полягає не лише в захисті засобів обробки інформації, а в організації засобів захисту для підтримки певних властивостей інформації. Виявилося, що такими **основними (фундаментальнимиі) властивостями** є конфіденційність, цілісність та доступність (рис.2), адже захист інформації

більшості випадків пов'язаний з комплексним рішенням трьох завдань:

забезпеченням конфіденційності інформації.
забезпеченням цілісності інформації;
забезпеченням доступності інформації.

Властивості інформації	
основні	інші
Конфіденційність. цілісність, доступність	Спостереженість, неспростовність, автентичність, достовірність , адекватність

Рисунок 2 - Види властивостей інформації

Визначення понять конфіденційність, цілісність та доступність дається в Положенні про технічний захист інформації в Україні:

конфіденційність» - властивість інформації бути захищеною від несанкціонованого ознайомлення»;

цілісність» - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення»;

доступність» - властивість інформації бути захищеною від несанкціонованого блокування».

Порушення кожної з трьох складових призводить до порушення інформаційної безпеки в цілому. Так, порушення доступності призводить до відмови в доступі до інформації, порушення цілісності призводить до фальсифікації інформації і, нарешті, порушення конфіденційності призводить до розкриття інформації.На додаток до перерахованих вище основних характеристик безпеки можуть розглядатися також і інші характеристики безпеки. Зокрема, до таких характеристик відносяться:

Спостереженість (accountability) –- забезпечення ідентифікації суб'єкта доступу та реєстрації його дій.

Неспростовність (non-repudiation) - неможливість відмови від авторства

Автентичність (authenticity) - гарантує, що суб'єкт або ресурс ідентичні заявленим.

Достовірність (reliability) - властивість відповідності передбаченому поводженню чи результату.

Адекватність – відповідність створюваного з допомогою отриманої інформації образу реальному об'єкту, процесу, явища тощо

Усі ці види засобів захисту інформації групуються в три основних класи:

Засоби фізичного захисту, що включають системи розмежування доступу, засоби захисту кабельної системи, засоби ідентифікації об’єктів, систем електроживлення, засоби архівації, дискові масиви, системи пригнічення побічних електромагнітних випромінювань, акустичних каналів витоку інформації тощо.

Програмні засоби захисту, у тому числі антивірусні програми, криптографічні засоби захисту інформації, системи розмежування повноважень, програмні засоби контролю доступу.

Адміністративні міри захисту, що включають контроль доступу в приміщення, розробку стратегії безпеки фірми, планів дій у надзвичайних ситуаціях тощо.

У телекомунікаційних системах необхідно застосовувати всі три основні класи засобів захисту інформації!!!.

Під час аналізу безпеки ТКС зазвичай виділяють дві групи проблем: безпека елемента мережі й безпека мережі.

Під елементом мережі розуміється ЕОМ з декількома інтерфейсами введення/виведення інформації й команд управління. До безпеки елемента мережі належать усі проблеми захисту даних, що зберігаються й обробляються в ЕОМ, яка розглядається як автономна система. Ці проблеми розв’язуються засобами операційних систем і додатків, таких як бази даних, а також вбудованими апаратними засобами ЕОМ.

Під безпекою мережі розуміють усі питання, пов’язані із взаємодією елементів мережі: це, насамперед, захист даних під час їх передачі лініями зв’язку й захист від несанкціонованого віддаленого доступу до мережі. І хоча часом проблеми безпеки елемента мережі й безпеки мережі важко відокремити одну від одної, настільки тісно вони пов’язані, очевидно, що безпека мережі має свою специфіку.

Як для елемента мережі, так і для мережі в цілому необхідно забезпечити властивості конфіденційності, цілісності й доступності.

Конфіденційність — гарантія того, що дані (інформація з обмеженим доступом) будуть доступні тільки тим користувачам, яким цей доступ дозволений (цих користувачів називають авторизованими).

Доступність — гарантія того, що авторизовані користувачі завжди одержать доступ до даних.

Цілісність — гарантія збереження правильних значень даних, що забезпечується забороною для неавторизованих користувачів будь-яким чином змінювати, модифікувати, руйнувати або створювати дані.

Ці властивості забезпечуються за рахунок комплексної реалізації служб (сервісів) автентифікації, ідентифікації, авторизації й аудиту.

Розкриємо їх значення, виходячи з необхідності взаємодії об’єктів ТКС. Система управління (підсистема безпеки) у цьому разі виступає як арбітр дій об’єктів.

Автентифікація — це процес доказу об’єктом своєї дійсності системі.

Ідентифікація — це процес визначення прав об’єкта стосовно системи.

Авторизація — це процес доказу дій об’єкта стосовно системи або інших об’єктів.

Аудит — це процес реєстрації й фіксації дій об’єкта(ів) в системі.

У телекомунікаційних системах можуть бути використані такі види автентифікації:

об’єкт може продемонструвати знання якого-небудь загального для сторін секрету: слова (пароля) або факту (дати й місця події, прізвиська людини тощо);

об’єкт може довести, що він володіє унікальним предметом (фізичним ключем: електронною магнітною картою, електронним ключем, смарт-картою й ін.) або файлом;

якщо як об’єкт виступає людина, то він може довести свою ідентичність, використовуючи власні біометричні характеристики, наприклад, малюнок райдужної оболонки ока або відбитки пальців, які попередньо були занесені в базу даних автентифікатора.

Можливі наступні варіанти автентифікації:

локальна автентифікація, яку можна бачити в персональних системах без підключення до мережі. Вся система, включаючи механізм автентифікації й управління доступом, розміщується в межах одного фізичного периметра безпеки. Власник системи й/або користувач ведуть й оновлюють базу автентифікаційних даних у межах цього периметра;

пряма автентифікація, яку можна зустріти в старих серверних системах, що використовуються у локальних обчислювальних мережах (ЛОМ), і в системах з поділом часу (мейнфреймах). Системою можуть віддалено колективно користуватися багато користувачів. Механізми автентифікації й контролю доступу системи розміщуються в межах одного фізичного периметра. Власник веде й підтримує актуальною базу автентифікаційних даних у межах системи;

непряма автентифікація, яку можна зустріти в сучасних мережних серверних системах й яка може бути реалізована, наприклад, через протоколи RADIUS, TACACS, Kerberos і протокол реєстрації в домені безпеки. Система містить кілька точок обслуговування, які вимагають управління доступом і можуть розміщуватися в різних місцях. За необхідності користувачі віддалено звертаються до служб системи. Власник веде й підтримує актуальною одну базу автентифікаційних даних для всієї розподіленої системи;

автономна автентифікація, яку можна зустріти в системах з інфраструктурою відкритого ключа, що містять численні автономні компоненти, які здатні приймати точні рішення щодо управління доступом навіть у тому разі, коли вони не можуть зв’язуватися з іншими системами для одержання авторитетних рішень з автентифікації. Власник погоджується з ризиком того, що такі рішення можуть іноді прийматися з використанням застарілих даних щодо управління доступом або автентифікації, а отже, може відбуватися компрометація підсистеми безпеки.

Засоби ідентифікації й авторизації часто реалізуються в одній підсистемі. Перші дозволяють визначити приналежність того чи іншого ресурсу мережі об’єкта, а другі реалізують механізм причетності, у результаті чого об’єкт не зможе довести, що не робив спроби обігу або впливу на ресурс. Такі засоби контролюють доступ об’єктів до ресурсів системи, надаючи кожному об’єкту саме ті права, які йому були визначені відповідальною особою.

Ідентифікація може відбуватися за різними схемами, залежно від необхідності забезпечення заданого рівня безпеки, швидкості роботи підсистеми безпеки й наявності достатньої кількості системних ресурсів.

Найпоширенішими схемами ідентифікації є:

Використання матриць доступу. Для кожної пари суб'єкт — об'єкт (для системних процесів це об'єкт — об'єкт) у матриці доступу існує частина, у якій задаються права суб'єкта на цей об'єкт. У найпростішому випадку такими правами можуть бути: права на читання, модифікацію й видалення об'єкта, а в більш складних системах їх доповнюють правами на управління й виконання. Цей метод відрізняється більшими накладними витратами на зберігання всього обсягу інформації про права суб'єктів, але дозволяє досить просто визначати, чи дозволений для суб'єкта певний вид доступу до зазначеного об'єкта.

Використання списків доступу. Цей метод є модифікацією підходу з використанням матриці доступу і є економічнішим щодо витрат пам'яті, але відповідно вимагає більше часу на обчислення прав. Залежно від характеру запитів на доступ можуть застосовуватися або непорожні списки прав суб'єктів, або списки об'єктів, доступних для заданого суб'єкта.

Використання міток рівня таємності. Кожному інформаційному об'єкту й суб'єкту видаються мітки рівня й категорії доступу. Рівень — це число, що визначає конфіденційність інформації й ступінь довіри суб'єкту, наприклад: «3» — абсолютно секретно, «2» — секретно, «1» — конфіденційно й «0» — несекретно. Рівень доступу $L(S)$ об'єкта S достатній для доступу до об'єкта O з рівнем таємності $L(O)$, якщо виконується нерівність $L(S) \geq L(O)$. Кожному об'єкту даються мінімально необхідні права, при яких об'єкт не має права доступу до непотрібних для його роботи категорій інформації. Модель не допускає передачу інформації зі зниженням рівня таємності. При агрегації об'єктів агрегату надається мітка, що є об'єднанням декількох категорій об'єктів і найбільший з рівнів їхньої таємності. Найбільш ефективним для складних розподілених систем обробки інформації є саме цей метод. До його недоліків можна віднести складність визначення конкретної множини об'єктів, що мають доступ, а також складніші правила передачі прав об'єктам.

Процедура аудиту доповнює механізм причетності за рахунок протоколювання дій об'єкта в системі та створення протокольних журналів. У журналах фіксуються як спроби доступу до ресурсу, так і вплив на нього й зміна його стану. Для найбільш надійних систем, якими є телекомунікаційні системи, журнали можуть зберігатися протягом багатьох місяців або навіть років.

Лекція 5

Тема: **Структура та задачі органів безпеки інформації в інформаційних системах**

Організація управління інформаційною безпекою в структурі управління мережами телекомунікацій

Для безпосередньої організації роботи із забезпечення інформаційної безпеки (та/або захисту інформації) в структурі управління мережами телекомунікацій має бути створена служба управління інформаційною безпекою, яка повинна забезпечити виконання всього комплексу завдань захисту телекомунікаційних мереж та інформації. Вказаній службі підпорядковуються групи інформаційної безпеки, що створюються на ЦАТС (і/або в структурі місцевої телефонної мережі загального користування), в задачу яких входить комплексне забезпечення інформаційної безпеки. Управління інформаційною безпекою проводиться на усіх

етапах життєвого циклу: планування, створення й експлуатації системи інформаційної безпеки. На стадії технічної експлуатації системи метою процесу управління інформаційною безпекою є оцінювання ефективності створеної системи захисту інформації й вироблення додаткових уточнюючих вимог для дороблляння системи захисту з метою забезпечування її адекватності за зміни умов функціонування: характеристик системи, опрацьовуваної інформації, фізичного середовища, персоналу, призначення системи, політики безпеки тощо. Управління інформаційною безпекою базується на практичних правилах, котрі групуються в такі складові:

1) загальні положення з управління інформаційною безпекою:

- політика безпеки;
- організація захисту;
- класифікація ресурсів та їхній контроль;

2) безпека персоналу, фізична безпека й безпека навколишнього середовища;

3) адміністрування комп'ютерних систем та обчислювальних мереж;

4) управління доступом до систем;

5) розробляння й супроводження інформаційних систем;

6) планування захисту:

- планування безперебійної роботи підприємства;
- виконання вимог.

Завдання управління інформаційною безпекою розв'язуються із застосовуванням засобів контролю.

Ключовими є такі засоби контролю:

- документ про політику інформаційної безпеки;
- розподіл обов'язків щодо забезпечування інформаційної безпеки;
- навчання й підготовка персоналу до підтримування режиму інформаційної безпеки;
- повідомлення про випадки порушування захисту чи інциденти в системі безпеки; - засоби захисту від вірусів;
- процес планування безперебійної роботи підприємства; - контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
- захист документації підприємства;
- захист даних;
- відповідність політиці безпеки.

Реалізація засобів управління безпекою в інформаційній інфраструктурі не повинна заважати іншій виробничій діяльності.

Витрати на систему захисту інформації слід привести у відповідність з цінністю інформації, яка захищається, й інших інформаційних ресурсів, піддаванні ризикові, а також зі збитками, що їх може бути нанесено підприємству через збої в системі захисту. Тому в процесі управління мають оцінюватись ризики порушування безпеки. Для оцінювання ризиків слід: - визначати й аналізувати потенційні загрози, яким піддаються комп'ютерні системи, та їхні вразливості; - розглядати збитки, котрі можуть нанести діяльності підприємства серйозне порушування інформаційної безпеки, з урахуванням можливих наслідків порушування конфіденційності, цілісності й доступності інформації; - розглядати реальну ймовірність такого порушування захисту від суттєвих загроз за наявності засобів контролю.

Оцінка ризику залежить від таких чинників: - характеру виробничої інформації та систем;

- виробничої мети, для якої інформація використовується;

- середовища, в якому система використовується й скеровується;

- захисту, забезпечуваного існуючими засобами контролю. Успішне здійснення системи інформаційної безпеки визначається таким:

- забезпечування безпеки має ґрунтуватися на виробничих цілях і вимогах;

- функції управління безпекою має взяти на себе керівництво підприємства;

- оцінювання ризиків порушування безпеки, загроз і слабкостей інформаційних ресурсів та рівня їхньої захищеності має ґрунтуватися на цінності й важливості цих ресурсів;

- ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;

- вивчання співробітниками політики та стандартів інформаційної безпеки;

- врахування конкретних інформаційних технологій, функцій підприємства та виробничого чи обчислювального середовища.

Згідно зі схемою маршрутизації викликів необхідно передбачити можливість альтернативного виходу до ТМЗК інших операторів, контролювати правильність маршрутизації трафіка, оперативно інформувати НЦУ, інших операторів телекомунікацій взаємо приєднаних мереж стосовно ситуацій, які призвели або можуть призвести до припинення обслуговування трафіка та про надзвичайні ситуації, у тому числі спричинені аваріями, пожежами тощо, використовувати технічні засоби та обладнання телекомунікацій, у тому числі які призначені для обліку обсягів та проведення розрахунків наданих телекомунікаційних послуг, які мають документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій та інформаційної безпеки, дотримуватися технічних вимог та вимог з інформаційної безпеки.

Повноваження та відповідальність суб'єктів взаємовідносин при реалізації задач забезпечення інформаційної безпеки в ЦАТС

Суб'єкти взаємовідносин при реалізації задач інформаційної безпеки в ЦАТС, права та повноваження посадових осіб, відповідальність суб'єктів взаємовідносин і ЦАТС при реалізації задач інформаційної безпеки мають відповідати чинним нормативно-правовим документам. Функції та порядок роботи "Служби захисту інформації" в підрозділах підприємства слід визначати згідно НД ТЗІ 1.4-001-2000 [18]. Права і обов'язки адміністраторів безпеки визначаються наказом та інструкціями, затвердженими керівником підприємства.

Лекція 6
Організаційно-технічні та режимні заходи систем захисту інформації

Для надійного захисту конфіденційної інформації доцільно застосовувати наступні організаційні заходи:

1. Визначення рівнів (категорій) конфіденційності інформації, що захищається.

2. Вибір принципів (локальний, об'єктовий або змішаний), методів і засобів захисту.

3. Установлення порядку оброблення захищеної інформації.

4. Облік просторових факторів:

- уведення контрольованих зон;

- правильний вибір приміщень і розташування об'єктів між собою і щодо межі контрольованої зони.

5. Облік тимчасових факторів:

– обмеження часу оброблення захищеної інформації

– доведення часу оброблення інформації з високим рівнем конфіденційності до вузького кола осіб.

6. Облік фізичних і технічних факторів:

– визначення можливості візуального (або за допомогою технічних засобів) спостереження відображуваної інформації сторонніми особами;

– відключення контрольно-вимірювальної апаратури від інформаційного об’єкта і її знеструмлення;

– максимальне рознесення інформаційних кабелів між собою і щодо провідних конструкцій;

– їхнє перетинання під прямим кутом.

Для блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів і створення системи захисту об’єкта по них необхідно здійснити низку заходів:

- проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і підведенні комунікації;

- виділити ті приміщення, всередині яких циркулює конфіденційна інформація і врахувати технічні засоби використані в них.

Задача забезпечення інформаційної безпеки у телекомунікаційних мережах загального користування (зокрема в телефонних системах та абонентських мережах) має свої особливості.

Важливість цієї задачі посилюється з розширенням використання центрів обробки викликів та центрів надавання послуг з автоматичним чи напівавтоматичним голосовим спілкуванням з клієнтами.

Лекція 7

Класи загроз інформаційній безпеці

1 Загальні положення

В основі організації, планування й здійснення практичних дій щодо забезпечення безпеки є аналіз концепції загрози, оцінка характеру реальних і потенційних внутрішніх/зовнішніх небезпек і загроз, кризових ситуацій, а також інших несприятливих факторів.

Аналіз і виявлення загроз інформаційної безпеки є другою важливою функцією адміністративного рівня забезпечення інформаційної безпеки. Багато в чому вигляд, що розробляється захисту і склад механізмів її реалізації визначається потенційними загрозами, виявленими на цьому етапі. Наприклад, якщо користувачі обчислювальної мережі організації мають доступ в Інтернет, то кількість загроз інформаційній безпеці різко зростає, відповідно, це відбивається на методах і засобах захисту та т. ін.

Загроза інформаційної безпеки - це потенційна можливість порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається атакою на інформаційну систему. Особи, навмисно реалізують загрози, є зловмисниками.

Система реальних і потенційних загроз не є постійною; загрози можуть з’являтися й зникати, наростати й зменшуватися, при цьому змінюватиметься їхня значимість для безпеки.

Найчастіше загроза є наслідком наявності вразливих місць в захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне

програмне забезпечення (на жаль навіть ліцензійне програмне забезпечення не позбавлене вразливостей).

Історія розвитку інформаційних систем показує, що нові вразливі місця з'являються постійно. З такою ж регулярністю, але з невеликим відставанням, з'являються і засоби захисту. Здебільшого кошти захисту з'являються у відповідь на виникаючі загрози, так, наприклад, постійно з'являються виправлення до програмного забезпечення фірми Microsoft, що усувають чергові його вразливі місця і ін. Такий підхід до забезпечення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози і її усуненням. Саме в цей проміжок часу зловмисник може завдати непоправної шкоди інформації.

У зв'язку з цим більш прийнятним є інший спосіб - спосіб упередженого захисту, що полягає в розробці механізмів захисту від можливих, передбачуваних і потенційних загроз.

Відзначимо, що деякі загрози не можна вважати наслідком цілеспрямованих дій шкідливого характеру. Існують загрози, викликані випадковими помилками або техногенними явищами.

Знання можливих загроз інформаційній безпеці, а також уразливих місць системи захисту, необхідно для того, щоб вибрати найбільш економічні і ефективні засоби забезпечення безпеки.

Загрози інформаційної безпеки класифікуються за кількома ознаками:

• за складовими інформаційної безпеки (доступність, цілісність, конфіденційність), проти яких, в першу чергу, спрямовані загрози;

• по компонентам інформаційних систем, на які загрози націлені (дані, програми, апаратура, персонал);

• за характером впливу (випадкові або навмисні, дії природного або техногенного характеру);

• по розташуванню джерела загроз (всередині або поза нашої інформаційної системи).

Відправною точкою при аналізі загроз інформаційної безпеки є визначення складової інформаційної безпеки, яка може бути порушена тією чи іншою загрозою: конфіденційність, цілісність або доступність.

На рис. 1 показано, що всі види загроз, що класифікуються за іншими ознаками, можуть впливати на всі складові інформаційної безпеки.

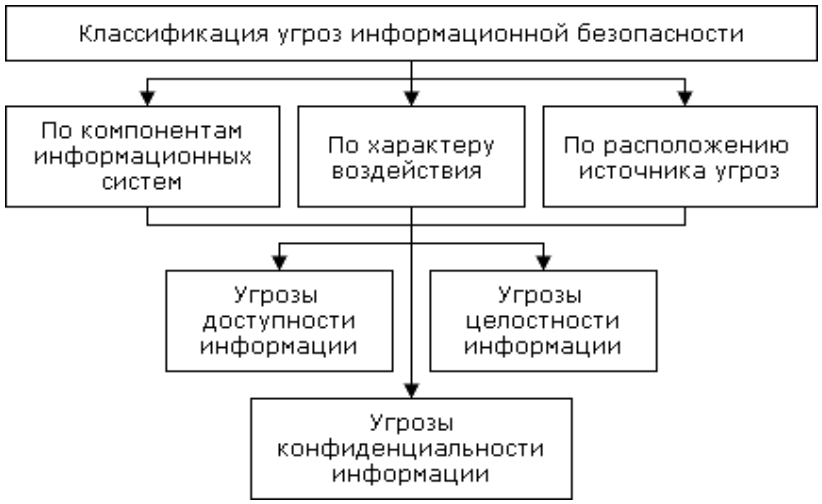


Рисунок 1

Розглянемо загрози за характером впливу.

Досвід проектування, виготовлення і експлуатації інформаційних систем показує, що інформація піддається різним випадковим впливам на всіх етапах життєвого циклу системи.

Причинами випадкових впливів при експлуатації можуть бути:

• аварійні ситуації через стихійне лихо і відключень електроживлення (природні і техногенні впливи);

• відмови і збої апаратури;

• помилки в програмному забезпеченні;

• помилки в роботі персоналу;

• перешкоди в лініях зв'язку через впливів зовнішнього середовища.

Навмисні дії - це цілеспрямовані дії зловмисника. Як зловмисника можуть виступати службовець, відвідувач, конкурент, найманець. Дії порушника можуть бути обумовлені різними мотивами, наприклад:

• невдоволенням службовця службовим становищем;

• цікавістю;

• конкурентною боротьбою;

• ураженим самолюбством і т. ін.

Загрози, що класифікуються за розташуванням джерела загроз, бувають внутрішні і зовнішні.

Зовнішні загрози обумовлені застосуванням обчислювальних мереж і створення на їх основі інформаційних систем.

Основна особливість будь-якої обчислювальної мережі полягає в тому, що її компоненти розподілені в просторі. Зв'язок між вузлами мережі здійснюється фізично за допомогою мережевих ліній і програмно за допомогою механізму повідомлень. При цьому керуючі повідомлення і дані, що пересилаються між вузлами мережі, передаються у вигляді пакетів обміну. Особливість даного виду загроз полягає в тому, що місце розташування зловмисника спочатку невідомо.

Класифікацію загроз подано в табл..1.

Таблиця 1- **Класифікація загроз безпеки**

Класифікаційна ознака	**Класифікаційні групи**
За джерелом погрози	1) внутрішні — джерело на території України; 2) зовнішні — джерело розташоване за кордоном держави
За природою виникнення загроз	1) викликані політикою держави; 2) ініційовані іноземними державами; 3) що надходять від кримінальних структур; 4) що надходять від конкурентів або контрагентів
За ймовірністю реалізації	1) реальні — можуть здійснюватися в будь-який момент часу; 2) потенційні — можуть реалізуватися у разі

	формування певних умов
Стосовно людської діяльності	1) об'єктивні — формуються незалежно від цілеспрямованої діяльності; 2) суб'єктивні — створюються свідомо, наприклад, розвідувальною, підривною й іншою діяльністю, організованою злочинністю
За об'єктом зазіхання	1) на інформацію; 2) на майно; 3) на фінанси; 4) на персонал; 5) на ділове реноме
За можливістю прогнозування	1) що прогнозуються на рівні господарюючого суб'єкта; 2) що не піддаються прогнозу
За наслідками	1) загальні — відбуваються на всій території України або більшості її суб'єктів; 2) локальні — мають вплив на окремі об'єкти
За величиною нанесеного (очікуваного) збитку	1) катастрофічні; 2) значні; 3) що спричиняють труднощі

Загрози для інформації та моделі порушників. Основні загрози інформаційним ресурсам вузла комутації

В інформаційній сфері України відокремлені загрози національній безпеці:

- прояви обмеження свободи слова та доступу громадян до інформації;
- комп’ютерної злочинності та комп’ютерного тероризму;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення невірогідної, неповної або упередженої інформації.

Передумовами можливого витоку інформації, порушення її цілісності, блокування та НСД, безконтрольного та неправомочного доступу до інформації та її використання є:

- комунікаційне обладнання іноземного виробництва, яке використане у мережах зв’язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв’язку та змістом повідомлень, які пересилаються. Використання великої кількості засобів зв’язку іноземного виробництва створює можливість втручання іноземних спецслужб в роботу мереж зв’язку шляхом руйнування програмних засобів в певний момент або створення каналів несанкціонованого впливу на інформацію, а також приводить до зростання залежності операторів зв’язку від закордонних виробників програмно-апаратних засобів зв’язку. В закордонній апаратурі можуть бути “закладки” додаткових, не відображених в технічних

характеристиках режимів роботи. Активізація таких режимів може здійснюватись як випадково, в процесі роботи оператора, так і дистанційно порушником, що приводить до втрати або зміни даних, помилок у програмному забезпеченні або паралельному підключенні до каналів;

- прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних.

Для цього може використовуватись апаратура радіо, радіотехнічної, оптико-електронної, теплової, акустичної, хімічної, магнітометричної та радіаційної розвідок;

- злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

- діяльність громадських формувань, політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб спрямована на одержання переваги у політичній боротьбі та конкуренції;

- розміщення на державних та спільних об'єктах зв'язку технологічного обладнання спільних підприємств та представництв інофірм, що вимагає проведення додаткових заходів із забезпечення вимог ТЗІ;

- зростання зацікавленості іноземних розвідок питаннями промислової, комерційної діяльності, ресурсів в Україні.

- відсутність системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту; - відсутність політики безпеки систем комутації та телекомунікаційних мереж, де б формулювались вимоги щодо захисту від загроз працездатності, підтримання режиму конфіденційності та відсутності несанкціонованого доступу. - нелегальне використання ресурсів операторів для несанкціонованого надання послуг зв'язку, що знижує доходи останніх; - різні фрагменти мережі експлуатуються різними операторами з різними формами власності. Загрози інформаційній безпеці є при забезпеченні:

1) конфіденційності: - крадіжка (копіювання) інформації та засобів її обробки; - утрата (ненавмисна утрата, витік) інформації та засобів її обробки;

2) доступності: - блокування інформації; - знищення інформації та засобів її обробки; 3) цілісності: - модифікація (спотворення) інформації; - заперечення справжності інформації; - нав'язування хибної інформації.

4) спостережності: - блокування; - модифікація інформації; - маскування інформації; 5) порядку маршрутизації трафіка:

- крадіжка трафіка;

- несанкціоноване використання послуг та інформаційних ресурсів телекомунікаційних мереж.

Детально загрози інформаційній безпеці, саме вузлів комутації, а також перелік інформації, яка захищається, наведені в КНД 45-164-2001 [15].

Джерела загроз інформаційній безпеці поділяють на три групи.

1. Обумовлені зловмисними чи випадковими діями суб'єкта (антропогенні джерела загроз).

2. Обумовлені технічними засобами (техногенні джерела загроз). 3. Обумовлені природними стихійними джерелами.

До антропогенних джерел загроз відносять

1. Зовнішні антропогенні джерела загроз:

- кримінальні структури;

- потенційні злочинці та хакери;

- недобросовісні партнери, конкуренти, представники сторонніх організацій, відвідувачі;

- технічний персонал постачальників;

- представники організацій нагляду та аварійних служб; - представники силових структур.

2. Внутрішні антропогенні джерела загроз:

- основний персонал (користувачі-оператори, системні і прикладні програмісти, розробники, оператори баз даних, оператори вводу даних);

- представники служби захисту інформації (системні і мережні адміністратори, адміністратори безпеки);

- керівництво;

- технічний персонал (життєзабезпечення, експлуатації); - допоміжний персонал (прибиральники, охорона);

- співробітники, звільнені з роботи.

Особливу групу внутрішніх антропогенних джерел загроз складають особи з порушеною психікою, впроваджені та завербовані агенти (іноземні агенти, що збирають інформацію, корпоративні розвідники) з числа основного, допоміжного та технічного персоналу, представників служби захисту інформації.

До техногенних джерел загроз відносять

1. Зовнішні техногенні джерела загроз: - засоби службового зв’язку; - мережі інженерних комунікацій (водопостачання, каналізації, вентиляції); - засоби пожежної, охоронної сигналізації; - транспорт;

2. Внутрішні техногенні джерела загроз: - неякісні технічні засоби комутації та обробки інформації; - неякісні програмні засоби управління та обробки інформації; - допоміжні засоби; - інші технічні засоби, що застосовуються в ЦАТС.

Природними зовнішніми джерелами загроз є пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, різні непередбачені обставини, не пояснювані явища, інші форс-мажорні обставини: різні рішення вищих державних органів, забастовки, війни, революції тощо. При складанні окремої моделі порушника орієнтуються на конкретний об’єкт захисту, враховують мотиви дій і соціально-психологічні аспекти порушення, потенційні можливості у доступу до інформаційних ресурсів різних категорій зовнішніх та внутрішніх порушників на різних просторово-часових зрізах об’єкта захисту.

Аспекти, пов'язані із забезпеченням кібербезпеки держави, відображенітаких законах України: Закон України "Про основи національної безпеки України"; Закон України "Про інформацію"; Закон України "Про Державну службу спеціального зв'язку та захисту інформації України"; Закон України "Про державну таємницю"; Закон України "Про захист інформації в інформаційно - телекомунікаційних системах" та інших. Крім того, в межах цієї проблематики чинними є два стратегічних документи: Стратегія національної безпеки України та Доктрина інформаційної безпеки України. Важливе нормативно-стратегічне значення має також ратифікована Верховною Радою України Конвенція про кіберзлочинність. 27 січня 2016 року Президент підписав Указ, яким увів в дію рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України". В документі наголошується, що разом з перевагами сучасного цифрового світу та розвитком інформаційних технологій, нині активно

розповсюджуються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Лекція 8

Тема: **Канали несанкціонованого доступу до інформації**

Одним з найбільш поширених і різноманітних способів впливу на інформаційну систему, що дозволяє нанести шкоди будь-якій зі складових інформаційної безпеки є **несанкціонований доступ (НД)**.

Несанкціонований доступ можливий через помилки в системі захисту, нераціонального вибору засобів захисту, їх некоректної установки і настройки.

Канали НСД класифікуються за компонентами автоматизованих інформаційних систем:

Через людину:

-розкрадання носіїв інформації;

- читання інформації з екрану або клавіатури;

- читання інформації з роздруківки.

Через програму:

- перехоплення паролів;

- розшифровка зашифрованої інформації;

- копіювання інформації з носія.

Через апаратуру:

- підключення спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

- перехоплення побічних електромагнітних випромінювань від апаратури, ліній зв'язку, мереж електроживлення і т.ін.

Модель порушника безпеки. НСД в програмно-керованих АТС

Детальну класифікацію моделей порушників антропогенного типу, їх рівні можливостей, основні способи реалізації загроз для інформації програмно-керованих АТС наведено у НД ТЗІ

Класифікація проводиться за рівнем можливостей, котрий надається їм штатними засобами.

Виокремлено чотири рівні можливостей порушення НСД:

1 (найнижчий рівень можливостей) – запускання програм (задач) із фіксованого набору, котрий реалізує передбачені функції щодо обробки інформації. Це обслуговуючий персонал, котрий забезпечує експлуатацію обладнання ЦАТС. Інженери-електронники ЦАТС, користуючись автоматизованим робочим місцем (АРМ) та комутаційною системою, можуть мати доступ до інформації абонента. Вони мають можливість приєднувати до ЦАТС закладні пристрої.

2 – можливість створювання та запускання власних програм з новими функціями щодо

обробки інформації. Це оператори даного або інших вузлів комутації. Користуючись комплектом або модулем з'єднувальної лінії, вони мають доступ до програмного забезпечення (ПЗ) АРМ, функціонального й спеціалізованого ПЗ та до баз даних. Типові можливості полягають у передаванні сигналів, як передбачених, так непередбачених у відповідних інтерфейсах.

3 – можливість управління роботою обчислювального комплексу, тобто можливість впливу на базове ПЗ ЦАТС та на склад і конфігурацію обладнання. Це оператори ЦАТС. Користуючись АРМ, вони мають доступ до баз даних, ПЗ АРМ, функціонального й спеціалізованого ПЗ та інформації абонентів. Типові можливості такого порушника: формування штатних команд, запускання задач, не задекларованих у технічній документації, несанкціоноване приєднання до інформаційних трактів.

4 – весь обсяг можливостей суб'єктів, здійснюючих проектування, реалізацію та ремонт технічних засобів, до залучення у склад обладнання власних технічних засобів з новими функціями. Це програмісти, котрі беруть участь у розробленні й виготовленні ВК. Користуючись АРМ і пристроями управління, вони здатні впливати на функціональне та спеціалізоване ПЗ і на ПЗ АРМ.

Типові можливості є такі: впровадження програмних закладок, впровадження шкідливих кодів (вірусів), помилки у ПЗ та комутаційній системі.

Якщо на вузлі комутації нема програмних та апаратних закладок, то звичайний абонент мережі практично не має можливості впливати на управляючу систему телефонної станції. Регламентовані для цифрових та аналогових терміналів користувача основні й додаткові послуги не можуть впливати на роботу управляючого комплексу у цілому. Абонент може діяти лише через абонентський комплект. Він здатен активізувати програмне закладення, дістати інформацію інших абонентів через несправності обладнання ЦАТС.

Продовжимо розгляд загроз інформації від зовнішніх, по відношенню до ЦАТС, джерел.

Загрози інформаційній безпеці можуть бути різноманітними і довільного походження за часом, тривалістю, факторами та наслідками.

Зрив роботи ЦАТС можливий при зупинці системи електроживлення або виведенні її з ладу порушником.

Можливе впровадження "вірусу" – мікропрограми, здатної самостійно розмножуватись і поширюватись у мережі.

Пристрої обробки інформації, котрі є складовою частиною цифрового вузла комутації, це ЕОМ зі стандартною архітектурою, для яких можна створювати засоби нападу, віруси тощо.

Можливості стосовно здійснення загроз залежать від місцезнаходження порушника. Якщо порушник перебуває поза межами ЦАТС, то його можливості залежать від того, чи є засоби захисту інформації у системі тарифікації (припускається чи не припускається віддалене приєднання легальних користувачів до системи тарифікації), засоби безпеки при виході на мережу SS-7 та TMN, при приєднанні до Інтернет. Якщо таких засобів захисту нема, то можливі впливи порушника через зовнішні інтерфейси обладнання, системи сигналізації на абонентських та з'єднувальних лініях.

Загрози стосовно захищеності збільшуються при інтеграції у цифрові комплекси нових функцій, а саме:

часткова (приватна) віртуальна мережа (VPN), що забезпечує внутрішній офісний зв'язок та зв'язок з філіалами;

функції білінгу на базі локальної мережі; вихід на глобальну мережу – Інтернет, а також використання на мережі імпортних програмно-апаратних комплексів.

Існує небезпечна загроза крадіжки трафіка при сумісному використанні системи зв'язку різними операторами.

Захист досягається використанням міжмережних екранів, шлюзів по каналам управління, синхронізації та сигналізації, здійснення контролю трафіка і тарифікації.

Загрози інформаційним ресурсам ЦАТС від приєднаних технологічних мереж

У межах контрольованої зони ЦАТС може встановлюватись різноманітне устаткування телекомунікаційних мереж. Частина цього обладнання приєднується безпосередньо до обладнання ЦАТС і може впливати на її роботу. Зокрема, це система сигналізації й синхронізації, система централізованого управління та технічної експлуатації, з'єднувальні та абонентські лінії, системи передавання до АСКР тощо.

Можливі варіанти інформаційного нападу на мережі зв'язку. Мережа зв'язку складається з вузлів комутації та систем передачі і її можна розглядати, як програмну інформаційну систему з безліччю зовнішніх зв'язків.

Розглядають такі загрози:

- загроза атаки через АРМ адміністратора;
- загроза несанкціонованого входу в АРМ адміністратора;
- загроза модифікації системного або програмного забезпечення адміністрування вузла зв'язку;
- загроза зараження файлів комп'ютерними вірусами;
- загроза прослуховування та модифікація трафіка;
- загроза модифікації апаратної частини АРМ, АТС, SS7 і лінійної апаратури (вставка чужого пристрою); - загроза відмови в обслуговуванні;
- загроза атаки через систему віддаленого програмування і діагностики; - загроза атаки через систему сигналізації та управління;
- загроза атаки наведеним сигналом;
- загроза атаки абонентськими лініями; - загроза атаки через мережу електроживлення;
- загроза атаки через системи тарифікації і записи переговорів;

Ці загрози розділяють на загрози на рівні програмного забезпечення, апаратної частини, середовища розробки і середовища експлуатації.

Більшість загроз на системи зв'язку складають атаки на програмному рівні. Тому необхідно відслідковувати можливість входу у систему програмування або управління системами зв'язку. Входи в програмне забезпечення АТС і системи передачі можуть бути легальними і нелегальними. До легальних входів відносяться зв'язок з системою віддаленого програмування і діагностики та з локальною системою програмування і тарифікації. Решта входів - нелегальні. При цьому у сучасних АТС вхід віддаленого програмування може бути заблоковано парольним захистом або фізичним відключенням. В інтелектуальних мережах вказаний вхід функціонує і відключений бути не може. За рівнем небезпечності ці загрози можна розділити на такі основні рівні:

а) найбільш небезпечним є вхід віддаленого програмування та діагностики АТС, який функціонально призначено для безпосереднього втручання в програмне забезпечення систем

зв’язку. Наслідки такого втручання можуть бути будь-якими, навіть до зупинки системи або мережі зв’язку. При цьому неможливо оперативно усунути причину збою системи та усі неполадки, оскільки нема можливості здійснити протоколювання усіх дій зі сторони віддаленого доступу в систему управління

б) вхід локального програмування і тарифікації також небезпечний для програмного забезпечення, але доступ до нього обмежено персоналом станції і безпека може бути забезпечена організаційними заходами. Втручання може бути легко визначене при дотриманні усіх вимог експлуатації: дії обслуговуючого персоналу завжди протоколюються;

в) напад абонентськими і з’єднувальними лініями, а також зі сторони системи сигналізації може бути проведено через активізацію "закладок", що відкривають по кодовому сигналу доступ до ПЗ АТС і систем передачі з вказаних напрямків. Закладки можуть бути створені на програмному та апаратному рівнях;

г) напад наведеним сигналом (наприклад, з космічного об’єкта) може бути здійснено через апаратні «закладки» разом з програмними «закладками». Можуть бути направлені на виведення обладнання з ладу застосуванням потужних електромагнітних імпульсів;

д) може бути "внутрішній" напад, який забезпечено закладкою у ПЗ, що спрацьовує від лічильника, дати або інших внутрішніх факторів. Крім того, практично все існуюче ПЗ систем передачі має обмеження за часом. По закінченні часу підтримки даної версії необхідно або купувати нову або експлуатувати стару на свій страх і ризик.

Загрози, що реалізуються через систему сигналізації.

Застосування сигналізації SS7 дозволяє здійснювати певні функції управління окремими вузлами зв’язку, при якому може бути нанесена значна шкода оператором зв’язку. Системи сигналізації забезпечують передавання різноманітних сигналів управління, в тому числі цифр номера, які через функціональні елементи комутаційної системи надходять для аналізу в управляючий комплекс. В цьому разі можливі різні варіанти використання сигналів управління для активізації програмних закладок, наприклад таких: - використання режиму типу “додаткова послуга”, котра не декларується в документації; - використання абонентського номера чи коду для активації програмної закладки;

- певні короткочасні маніпуляції з абонентською трубкою. Система сигналізації SS7, крім вищезазначених можливостей, потенційно надає додаткові можливості організації НСД.

У складі SS7 є підсистеми забезпечення можливостей транзакцій (TCAP) та прикладних підсистем, котрі організуються на них, такі як підсистема рухомого зв’язку GSM (MAP), підсистема інтелектуальних мереж (INAP), підсистема експлуатації, техобслуговування, адміністрування й управління (OMAP) та інші.

До загроз від застосування SS7 також належать:

- інтерфейси, спеціалізовані для нетелефонних функцій (TCAP, OMAP тощо) системи SS7, можуть бути використані для прихованого введення команди, котра реалізує несанкціонований вплив на ЦАТС;

- в SS7 організовується доступ до мережних баз даних. Виникає загроза їхнього навмисного спотворення, що може спричинити порушення роботи мережі. Для захисту від можливого впливу необхідно здійснювати фільтрацію загальноканальної сигналізації та протоколювання повідомлень.

Загрози, що реалізуються за допомогою системи централізованого управління. Якщо порушник перебуває всередині ЦАТС, то, навіть якщо наявні засоби безпеки при реалізації

систем тарифікації, засоби безпеки при виході на мережу SS7 та TMN, засоби захисту за приєднанні до Інтернету, то він має багато можливостей для здійснення загроз. Порушник з правами оператора УК може здійснювати НСД шляхом формування штатних команд, запускати програми, нерегламентовані в технічній документації.

Порушення доступу відбувається в разі:

- модифікації баз даних (встановлення несанкціонованих режимів технічної експлуатації та видів обслуговування);

- ознайомлення з конфіденційною інформацією баз даних (адресами вхідних та вихідних з'єднань, часом встановлення з'єднання, режимами зв'язку, додатковими використовуваними видами обслуговування);

- зупинки та перезапускання ЦАТС (порушення зв'язку); - заміни ПЗ (нове інстальоване ПЗ може мати програмні закладення та люки).

Основні можливі варіанти захисту при забезпеченні захисту від впливу через систему управління, як самої критичної ланки, це впровадження жорсткого розмежування прав доступу до інформаційних ресурсів, як на фізичному, так і на програмному рівнях, адміністрування і протоколювання усіх операцій.

Найбільш підпадають під загрози ПЗ АРМ, якщо вони функціонують на базі ПЕОМ і використовують для роботи операційну систему Windows чи MS-DOS. Функціональне та спеціалізоване ПЗ, як правило, зашите у постійні запам'ятовувальні пристрої. Проникнення в операційну систему вузла комутації вважається практично неможливим.

Оскільки найгірший результат нападу - це руйнування системи зв'язку в цілому або окремих її фрагментів, то в цифрових АТС і системах цифрової передачі даних SDH, PDH (радіорелейних, кабельних, волоконно-оптичних) найбільш вразливим елементом являється програмне забезпечення, яке піддається нападу в першу чергу. При цьому, захистивши програмне забезпечення від несанкціонованого втручання, з достатньою ймовірністю забезпечується цілісність мережі та її елементів.

Оскільки сучасне обладнання цифрового зв'язку базується на комп'ютерних технологіях, питання забезпечення інформаційної безпеки найбільш ефективніше можуть бути вирішені спеціалістами з обчислювальної техніки, які мають відповідний досвід. Загрози на абонентських та з'єднувальних лініях.

Стосовно абонентських, з'єднувальних та міжстанційних ліній зв'язку виділяють:

- загрози від випадкових дій (впливів) порушників;

- загрози від зловмисних дій порушників;

- загрози безпеці.

Аварії можуть бути викликані впливами техногенного (результаті земляних та будівельних робіт в районах кабельних трас, розбою та зловмисної диверсійної діяльності) чи природного характеру (промерзання та деформація кабелю у зимовий період). Інформаційна безпека підтримується чіткою стандартною плановою організацією ремонтно-відновлювальних робіт та прогнозуванням ресурсів, необхідних для ліквідації наслідків аварії. В лінійних трактах, на їх елементах порушник може успішно здійснювати тривалий практично не виявляємий НСД до інформації за допомогою спеціальних засобів доступу до аналогових і цифрових каналів, здійснювати виведення на запис, прослуховування або ретрансляцію несанкціоновано одержаних даних та мови. Захист в такому разі здійснюється плановим патрулюванням (пішим чи моторизованим) кабельних трас та посиленням контролю в періоди вирішення важливих

задач. Часто застосовують шифрування інформації.

Загрози інформації в цифрових системах передачі

Цифрові системи передавання мають вразливості на фізичному, канальному та мережному рівнях стеку протоколів передавання. На фізичному рівні порушник прагне НСД до інформаційної сфери, як правило, шляхом встановлення спеціалізованого обладнання в канали доступу або в магістральні канали. Можливий НСД через консолі управління або активізацією "закладок", впроваджених в об'єктах цифрових систем передавання.

Закладки можуть бути активізовані за допомогою радіоканалів. Після одержання НСД на фізичному рівні атака порушника може розвиватись на канальному і мережному рівнях стека протоколів. На канальному рівні порушник може виконувати дії на активізацію вразливості відповідних протоколів. Порушник може одержати доступ до інформації, активізувати "закладку" формуванням спеціальних команд в кадрах (комірках, контейнерах) даних. Команди можуть розміщуватись в заголовку, в полі даних, в полі контрольної суми. Небезпечні атаки блокування передавання повідомлень, що можуть бути реалізовані несанкціонованим формуванням прикмет перевантаження, та які викликають масові повтори передачі. На мережному рівні активізуються вразливості протоколів цього рівня. Порушник може отримати НСД до інформації і провести атаки типу блокування передавання, блокування доступу тощо.

Лекція 9

Тема: **Нормативна і правовова база захисту інформації в системах та мережах телекомунікацій України**

Правові аспекти захисту інформації

У сучасному інформаційному суспільстві інформація виступає не тільки як предмет, і як продукт праці. Інформація як продукт має певну цінність. Її втрата наносить збитки власнику інформації. Запобігання і відшкодування таких збитків в суспільстві здійснюється у відповідності до встановлених юридичних норм. Тому базові поняття дисципліни формулюються в технічних термінах, що мають точні юридичні визначення.

Згідно з українським законодавством2, вирішення проблеми *інформаційної безпеки* на рівні *держави* має здійснюватися за допо-могою:

- створення повнофункціональної інформаційної інфраструк-тури держави та забезпечення захисту її критичних елемен-тів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформацій-ній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співро-бітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпе-чення інформаційної безпеки, зокрема захисту інформацій-них ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація

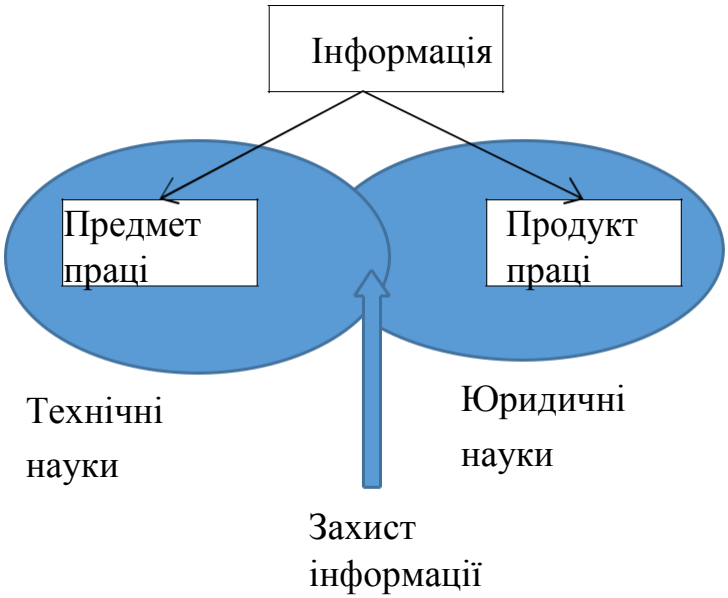


Рисунок 1 - Місцезнаходження поняття «захист інформації»

- .

Вирішення проблеми *інформаційної безпеки* на рівні *держави* має здійснюватися за допомогою:

- законодавчих, нормативно-правових та нормативних актів щодо інформаційної безпеки;
- міжнародними стандартами ISO;
- власними розробками.

Для *реалізації* законодавчих, нормативно-правових та норматив-них актів щодо *інформаційної безпеки* повинна створюватись комп-лексна система захисту інформації (КСЗІ).

Для *реалізації* міжнародних стандартів ISO щодо інформаційної безпеки повинна створюватись система управління інформаційною безпекою (СУІБ).

До *державних органів* забезпечення інформаційної безпеки від-носяться:

- відповідні підрозділи спецслужб держави;
- спеціально уповноважений орган держави з питань захисту інформації: Державна служба спеціального зв'язку та захисту інформації України;
- Національний координаційний центр кібербезпеки;
- Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і обо-рони України.

З 1 липня 2015 року у Державній службі спеціального зв'язку та захисту інформації України розпочав роботу Державний центр кіберзахисту та протидії кіберзагрозам. Його

створено на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв'язку.

До органів забезпечення інформаційної безпеки належать:

- Державне агентство з питань електронного урядування України;
- Державна служба спеціального зв'язку та захисту інформації України;
- Міністерство юстиції України (в частині роботи з електронними цифровими підписами (ЕЦП);
- підрозділ з інформаційного забезпечення органу публічного управління, який серед інших завдань також має займатися створенням і підтриманням систем управління інформаційною безпекою та використовує комплексну систему захисту інформації.

Необхідно також визначити, що у *Стратегії кібербезпеки України*- підкреслено, що мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Також мають бути врегульовані питання щодо обов'язковості вжиття ними захо-дів із забезпечення *захисту інформації* та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберза-хисту. Держава має сприяти залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту

Список законодавчих актів, нормативно-правових актів *(НПА)* та нормативних актів щодо інформаційної безпеки *(стосовно захисту інформації)* в Україні, список не повний *(до нього не входять НПА з обмеженим доступом та деякі НПА)*. Актуальні зміни на сайті Державної служби спеціального зв'язку та захисту інформації України: http://www.dstszi.gov.ua *(Розділ нормативно-правова база)*.

Закони України:

Закон України «Про інформацію» від 02.10.1992 № 2657-XII

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII

Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Постанови КМУ:

Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373

Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні

профілі захищеності оброблюваної інформації від несанкціонованого доступу

НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

Автоматизированные системы. Требования к содержанию документов РД 50-34.698

Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Галузеві стандарти:

Національний банк України

ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)

ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

1. Указ Президента України від 08.07.2009 р. № 514 "Про Доктрину інформаційної безпеки України".

2. Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22.05.98 р. № 505.

3. Закон України "Про основи Lviv Polytechnic National University Institutional Repository альної безпеки України" від 19.06.2003 р. № 964-IV.

4. Закон України "Про інформацію" від 02.10.1992 р. № 2657-XII.

5. Закон України "Про електронний цифровий підпис" від 22.05.2003 р. № 852-IV.

6. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 р. № 80/94-ВР.

7. Закон України "Про Національну систему конфіденційного зв'язку" від 10.01.2002 р. №

Закон України «Про захист інформації в інформаційно телекомунікаційних системах».

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

{Абзац четвертий статті 1 в редакції Закону № 1170-VII від 27.03.2014}

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

володільці інформації;

власники системи;

користувачі;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

{Абзац п'ятий частини першої статті 3 в редакції Закону № 879-VI від 15.01.2009}

{Абзац шостий частини першої статті 3 виключено на підставі Закону № 767-VII від

{Частину другу статті 3 виключено на підставі Закону № 1170-VII від 27.03.2014}

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх

повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

{Частина третя статті 4 із змінами, внесеними згідно із Законом № 1170-VII від

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

{Частина друга статті 8 із змінами, внесеними згідно із Законом № 1170-VII від

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

{Частина друга статті 9 із змінами, внесеними згідно із Законом № 1170-VII від

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

{Частина третя статті 9 із змінами, внесеними згідно із Законом № 879-VI від

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

{Частину другу статті 10 виключено на підставі Закону № 879-VI від 15.01.2009}

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

{Абзац перший частини третьої статті 10 в редакції Закону № 879-VI від 15.01.2009}

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

{Частину третю статті 10 доповнено абзацом згідно із Законом № 1180-VI від

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

{Частина четверта статті 10 із змінами, внесеними згідно із Законом № 879-VI від

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Лекція 10

Тема: **Стандартизація методів забезпечення та сертифікація компоненів систем теелкомунікацій за вимогами інформаційної безпеки**

Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 08.07.2009 р. № 514, визначено реальні та потенційні загрози інформаційній безпеці України, до яких, зокрема, зараховано несанкціонований доступ до інформаційних ресурсів, зокрема

внаслідок використання іноземних інформаційних технологій. Щоб забезпечити інформаційну безпеку України, Адміністрація Держспецзв’язку ініціювала розроблення вітчизняного криптографічного алгоритму блокового симетричного шифру (БСШ). Безумовно, прийняття національного стандарту БСШ сприятиме підвищенню рівня інформаційної безпеки Україн

Серед переваг прийняття національного стандарту – впровадження в Україні сучасного криптографічного БСШ, застосування якого допоможе забезпечити необхідну захищеність інформації та інформаційних ресурсів у частині послуг конфіденційності та цілісності, зокрема обмеженим доступом, а також здійснювати захищену обробку інформації з підвищеною швидкодією в інформаційно-телекомунікаційних системах (ІТС).

МОДУЛЬ2

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Змістовий модуль 1 Ідентифікація та аутинфікація

Лекція 11

Тема: **Визначення понять "ідентифікація" та "аутентифікація". Протоколи аутентифікації, взаємна аутентифікація, одностороння аутентифікація**

План

1 Визначення понять "ідентифікація" та "аутентифікація"

Механізм ідентифікація і аутентифікація користувачів

1 Визначення понять "ідентифікація" та "аутентифікація"

Ідентифікація та аутентифікації застосовуються для обмеження доступу випадкових і незаконних суб'єктів (користувачі, процеси) інформаційних систем до її об'єктів (апаратні, програмні та інформаційні ресурси).

Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що засвідчує його особу, перевірити її справжність і потім надати (або не надати) цьому користувачеві можливість роботи з системою.

Наявність процедур аутентифікації і/або ідентифікації користувачів є обов'язковою умовою будь-якої захищеної системи, оскільки всі механізми захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами інформаційних систем.

Дамо визначення цих понять.

Ідентифікація - присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора_і порівняння його з заданим.

Аутентифікація (встановлення автентичності) - перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора і підтвердження його автентичності. Іншими словами, аутентифікація полягає в перевірці: чи є що підключається суб'єкт тим, за кого він себе видає.

При побудові систем ідентифікації і аутентифікації виникає проблема вибору зони, на основі якого здійснюються процедури ідентифікації і аутентифікації користувача.

В ***якості ідентифікаторів*** зазвичай використовують:

• ***набір символів*** (пароль, секретний ключ, персональний ідентифікатор і т. п.), який користувач запам'ятовує або для їх запам'ятовування використовує спеціальні засоби зберігання (електронні ключі);

• ***фізіологічні параметри людини*** (відбитки пальців, малюнок райдужної оболонки ока і т. т.) або особливості поведінки (особливості роботи на клавіатурі та т. п.).

Біометрична ідентифікація та автентифікація користувача. Процедури ідентифікації та автентифікації користувача можуть базуватися не тільки на секретній інформації, якою володіє користувач (пароль, секретний ключ, персональний ідентифікатор тощо). Останнім часом все більшого розповсюдження набуває біометрична ідентифікація та автентифікація користувачів, яка дозволяє із впевненістю ідентифікувати потенційного користувача шляхом вимірювання фізіологічних параметрів та характеристик людини, а також особливостей його поведінки.

Відмітимо основні переваги біометричних методів ідентифікації та автентифікації користувачів у порівнянні з традиційними:

- високий рівень достовірності ідентифікації за біометричними ознаками у зв’язку з їх унікальністю;
- невіддільність біометричних ознак від дієздатної особи;
- складність фальсифікації біометричних ознак.

В якості біометричних ознак, які можуть бути використані при ідентифікації потенційного користувача, можна виділити наступні :

- узор райдужної оболонки та сітківки ока;
- відбитки пальців;
- геометрична форма руки;
- форма та розміри обличчя;
- особливості голосу;
- біомеханічні характеристики рукописного підпису;
- біомеханічні характеристики „клавіатурного почерку“.

При реєстрації користувач повинен продемонструвати один чи кілька разів свої характерні біометричні ознаки. Ці ознаки (відомі як справжні) реєструються системою як контрольний „образ“ законного користувача. Цей „образ“ користувача зберігається в електронній формі і використовується для перевірки ідентичності кожного, хто видає себе за відповідного законного користувача. Залежно від співпадання чи неспівпадання сукупності виявлених ознак із зареєстрованими в контрольному „образі“, їх власник визнається законним користувачем (при співпаданні) чи не визнається (при неспівпаданні).

Системи ідентифікації за узором райдужної оболонки та сітківки ока можуть бути розділені на два класи:

- системи, які використовують рисунок райдужної оболонки ока;
- системи, які використовують рисунок кров’яних судин сітківки ока.

Оскільки ймовірність повторення даних параметрів рівна 10^{-78}, ці системи є найбільш надійними серед усіх біометричних систем. Такі засоби ідентифікації застосовуються там, де потрібен високий рівень безпеки.

Системи ідентифікації за відбитками пальців є найрозповсюдженішими. Одна з основних причин широкого розповсюдження таких систем полягає в наявності великих банків даних відбитків пальців. Основними користувачами подібних систем в усьому світі є поліція, різноманітні державні та деякі банківські організації.

Системи ідентифікації за геометричною формою руки використовують сканери форми руки, які зазвичай встановлюються на стінах. Слід зазначити, що переважна більшість користувачів віддають перевагу системам саме цього типу, а не описаним вище.

Системи ідентифікації по обличчю та голосу є найбільш доступними у зв'язку з їх дешевизною, оскільки більшість сучасних комп'ютерів легко можна обладнати відео- та аудіозасобами. Системи даного класу широко застосовуються при віддаленій ідентифікації суб'єкту доступу в телекомунікаційних мережах.

Системи ідентифікації особи за динамікою рукописного підпису враховують інтенсивність кожного зусилля підписуючого, частотні характеристики написання кожного елементу підпису та рисунок підпису загалом.

Системи ідентифікації за біомеханічними характеристиками „клавіатурного почерку" базуються на тому, що моменти натиснення та відпускання клавіш при наборі тексту на клавіатурі суттєво відрізняються у різних користувачів. Цей динамічний режим набору („клавіатурний почерк") дозволяє побудувати достатньо надійні засоби ідентифікації. У випадку виявлення зміни клавіатурного почерку користувача йому автоматично забороняється робота на ЕОМ.

Слід відмітити, що застосування біометричних параметрів при ідентифікації суб'єктів доступу автоматизованих систем поки не отримало належного нормативно-правового забезпечення, зокрема у вигляді стандартів. Тому застосування систем біометричної ідентифікації допускається тільки в автоматизованих системах, що обробляють та зберігають персональні дані, які є комерційною та службовою таємницею**.**

Найбільш поширеними простими і звичними є методи аутентифікації, засновані на паролі – конфіденційному ідентифікаторі суб'єктів. В цьому випадку при введенні суб'єктом свого пароля підсистема аутентифікації порівнює його з паролем, що зберігаються в базі еталонних даних в зашифрованому вигляді. У разі збігу паролів підсистема аутентифікації дозволяє доступ до ресурсів системи.

Парольні методи аутентифікації за ступенем змінності паролів діляться на:

методи, які використовують постійні (багаторазово використовувані) паролі;

методи, які використовують одноразові (динамічно змінюються) паролі.

Використання одноразових або динамічно мінливих паролів є більш надійним методом парольного захисту.

Останнім часом набули поширення комбіновані методи ідентифікації і аутентифікації, що вимагають, крім знання пароля, наявність картки (token) - спеціального пристрою, що підтверджує справжність суб'єкта.

Картки поділяють на два типи:

- пасивні (картки з пам'яттю);
- активні (інтелектуальні картки).

Найпоширенішими є пасивні картки з магнітною смугою, які зчитуються спеціальним пристроєм, що має клавіатуру і процесор. При використанні зазначеної картки користувач вводить свій ідентифікаційний номер. У разі його збігу з електронним варіантом, закодованим в картці, користувач отримує доступ до системи. Це дозволяє достовірно встановити особу, яка отримала доступ до системи і виключити несанкціоноване використання картки зловмисником (наприклад, при її втраті). Такий спосіб часто називають двокомпонентною аутентифікацією.

Інтелектуальні картки окрім пам'яті мають власний мікропроцесор. Це дозволяє реалізувати різні варіанти парольних методів захисту, наприклад, багаторазові паролі, динамічно мінливі паролі.

Методи аутентифікації, засновані на вимірі біометричних параметрів людини, забезпечують майже 100% ідентифікацію, вирішуючи проблеми втрати або втрати паролів і особистих ідентифікаторів. Однак ці методи не можна використовувати при ідентифікації процесів або даних (об'єктів даних), вони тільки починають розвиватися, вимагають поки

складного і дорогого обладнання. Це обумовлює їх використання поки тільки на особливо важливих об'єктах.

Прикладами впровадження зазначених методів є системи ідентифікації користувача по малюнку райдужної оболонки ока, по почерку, за тембром голосу і ін.

Новітнім напрямком аутентифікації є доказ достовірності віддаленого користувача за його місцезнаходженням. Даний захисний механізм заснований на використанні системи космічної навігації, типу GPS (Global Positioning System). Користувач, що має апаратуру GPS, багаторазово посилає координати заданих супутників, що знаходяться в зоні прямої видимості. Підсистема аутентифікації, знаючи орбіти супутників, може з точністю до метра визначити місце розташування користувача. Висока надійність аутентифікації визначається тим, що орбіти супутників не завжди стабільні, передбачити які досить важко. Крім того, координати постійно змінюються, що виключає їх перехоплення.

2 Механізм ідентифікація і аутентифікація користувачів

Загальна процедура ідентифікації і аутентифікації користувача при його доступі в захищену інформаційну систему полягає в наступному.

Користувач надає системі свій особистий ідентифікатор (наприклад, вводить пароль або надає палець для сканування відбитку). Далі система порівнює отриманий ідентифікатор з усіма що зберігаються в її базі ідентифікаторами. Якщо результат порівняння успішний, то користувач отримує доступ до системи в рамках встановлених повноважень. У разі негативного результату система повідомляє про помилку і пропонує повторно ввести ідентифікатор. У тих випадках, коли користувач перевищує ліміт можливих повторів введення інформації (обмеження на кількість повторів є обов'язковою умовою для захищених систем) система тимчасово блокується і видається повідомлення про несанкціоновані дії (причому, може бути, і непомітно для користувача).

Якщо в процесі аутентифікації справжність суб'єкта встановлена, то система захисту інформації повинна визначити його повноваження (сукупність прав). Це необхідно для подальшого контролю і розмежування доступу до ресурсів.

В цілому аутентифікація за рівнем інформаційної безпеки ділиться на три категорії:

1. Статична аутентифікація.

2. Стійка аутентифікація.

3. Постійна аутентифікація.

Перша категорія забезпечує захист тільки від несанкціонованих дій в системах, де порушник не може під час сеансу роботи прочитати аутентифікаційну інформацію. Прикладом засобу статичної аутентифікації є традиційні постійні паролі. Їх ефективність переважно залежить від складності вгадування паролів і, власне, від того, наскільки добре вони захищені.

Стійка аутентифікація використовує динамічні дані аутентифікації, що змінюються з кожним сеансом роботи. Реалізаціями стійкої аутентифікації є системи, що використовують одноразові паролі і електронні підписи. Стійка аутентифікація забезпечує захист від атак, де зловмисник може перехопити аутентифікаційну інформацію і використовувати її в наступних сеансах роботи.

Однак стійка аутентифікація не забезпечує захист від активних атак, в ході яких маскується зловмисник може оперативно (протягом сеансу аутентифікації) перехопити, модифікувати і вставити інформацію в потік переданих даних.

Постійна аутентифікація забезпечує ідентифікацію кожного блоку переданих даних, що оберігає їх від несанкціонованої модифікації або вставки. Прикладом реалізації зазначеної категорії аутентифікації є використання алгоритмів генерації електронних підписів для кожного біта інформації, що пересилається.

Висновки по темі

1. Ідентифікація і аутентифікації застосовуються для обмеження доступу випадкових і незаконних суб'єктів (користувачі, процеси) інформаційних систем до її об'єктів (апаратні, програмні та інформаційні ресурси).

2. Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що засвідчує його особу, перевірити її справжність і потім надати (або не надати) цього користувачеві можливість роботи з системою.

Ідентифікація - присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим.

Аутентифікація (встановлення автентичності) - перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора і підтвердження його автентичності.

5. В якості ідентифікаторів в системах аутентифікації зазвичай використовують набір символів (пароль, секретний ключ, персональний ідентифікатор і т. п.), Який користувач запам'ятовує або для їх запам'ятовування використовує спеціальні засоби зберігання (електронні ключі). У системах ідентифікації такими ідентифікаторами є фізіологічні параметри людини (відбитки пальців, малюнок райдужної оболонки ока і т. п.) Або особливості поведінки (особливості роботи на клавіатурі та т. п.).

6. Останнім часом набули поширення комбіновані методи ідентифікації і аутентифікації, що вимагають, крім знання пароля, наявність картки (token) - спеціального пристрою, що підтверджує справжність суб'єкта.

7. Якщо в процесі аутентифікації справжність суб'єкта встановлена, то система захисту інформації повинна визначити його повноваження (сукупність прав). Це необхідно для подальшого контролю і розмежування доступу до ресурсів.

8. У цілому аутентифікація за рівнем інформаційної безпеки ділиться на три категорії: статична аутентифікація, стійка аутентифікація і постійна аутентифікація.

9. Постійна аутентифікація є найбільш надійною, оскільки забезпечує ідентифікацію кожного блоку переданих даних, що оберігає їх від несанкціонованої модифікації або вставки.

Змістовий модуль 2 Криптографія та шифрування

Лекція 12

Тема: **Криптографічний захист інформації. Теоретичні основи криптографії**

1 Теоретичні основи криптографії

Питаннями захисту інформації шляхом її перетворювання, яке виключає можливість прочитування інформації сторонньою особою, займається криптологія (*kryptos* – таємний, *logos* – наука).

Криптологія поділяється на два напрями – *криптографію* й *криптоаналіз*. Цілі цих напрямів є прямо протилежні. Взаємини криптографії й криптоаналізу є очевидні: криптографія – захист, тобто розробляння шифрів, а криптоаналіз – напад, тобто атака на шифри. Однак ці дві

дисципліни є щільно пов'язані, й не існує кваліфікованих криптографів, котрі не володіли б методами криптоаналізу.

Криптографія - це область прикладної математики, основним завданням якої є захист цифрової інформації віднесанкціонованого доступу. захист досягається шляхом перетворення вихідного набору даних ввид, з якого отримання вихідноїі нформаціїнеможлива або важкодосяжним. Останнє означає, для того щоб витягти вихідну інформацію будуть потрібні достатні складні обчислення, які займуть тривалий період часу. Отримання вихідної інформації досягається шляхом застосування спеціальної послідовності вхідних даних званих ключем. Під ключем в даному випадку розуміється легко змінна частина системи, що зберігається в таємному місці і визначає одне з можливих перетворень криптотексту.

Криптографія – це наука про способи перетворювання (шифрування) інформації з метою її захисту від неправочинних користувачів. В перекладі з грецької мови слово криптографія означає тайнопис. Основне призначення криптографії – утаємничити необхідну інформацію. Криптографія надає засоби для захисту інформації і тому є складовою діяльності з забезпечення безпеки інформації.

Існують різні засоби втаємничення інформації:

• Приховування каналу передачі повідомлення.

• Маскування змісту повідомлення з використанням стеганографічних методів.

• Ускладнення можливості перехоплення самого повідомлення противником.

• Інші.

На відміну від перерахованих методів криптографія не «приховує» повідомлення, а перетворює їх у формы, недоступну для розуміння противником. Таке перетворення забезпечується використанням криптографічних систем.

Криптографія – одноліток історії людської мови. Більш того, спочатку писемність власне сама була криптографічною системою, тому що в стародавніх суспільствах нею володіли лише обрані. З широким розповсюдженням писемності криптографія стала формуватися як самостійна наука. Дані про перші способи тайнопису є вельми уривчасті. Припускається, що криптографія була відома в давньому Єгипті й Вавілоні. До нашого часу дійшли свідчення про те, що мистецтво секретного письма використовувалося в давній Греції. Перші насправді вірогідні відомості з описанням методу шифрування належать до періоду зміни старої й нової ери. Криптографія займається пошуком і дослідженням математичних методів перетворювання інформації.

***Сфера інтересів криптоаналіз*у** – дослідження можливості дешифрування інформації без знання ключів.

Криптоаналіз – це наука про методи і способи розкривання шифрів.

Інший підхід захисту інформації від неправочинних користувачів – не приховувати власне факту передавання повідомлення, але зробити його неприступним для сторонніх. Для цього повідомлення має бути записане у такий спосіб, аби з його вмістом не міг ознайомитися ніхто, за винятком самих кореспондентів, – у цьому й полягає суть шифрування. І криптографія виникла власне як практична дисципліна, котра вивчає й розробляє способи шифрування повідомлень.

Об'єктом криптографії є інформація (новини, вміст повідомлень) в перебігу передавання її каналами зв'язку. Слід пам'ятати, що криптографія необхідна лише для інформації, котра потребує захисту. Зазвичай в таких випадках говорять, що інформація містить таємницю, чи є захищуваною, секретною, конфіденційною. Тому, як правило, вивчення криптографії як науки

розпочинають з вивчення властивостей відкритої інформації.

Криптографи надають таке означення: *відкрита інформація* – це невтаємничена (незашифрована) інформація, призначена для передавання каналом зв'язку. Відкрита інформація неодмінно має бути зафіксована на певному матеріальному носії (папері, фотоплівці, перфострічці тощо). У цьому разі її називають відкритим повідомленням. Поняття відкритого повідомлення в криптографічній літературі розуміється подвійно: або це змістовний текст, котрий піддається смисловому читанню, або це текст, котрий підлягає зашифровуванню.

Криптографічна система (криптосистема) – система секретного зв’язку, в якій зміст інформації, що передається, утаємничується за допомогою криптографічних перетворень; при цьому сам факт передачі інформації не приховується.

Криптосистема – сімейство оборотних перетворень, що вибираються за допомогою ключа, які трансформують захищуваний блок інформації в шифрограму і назад.

Безліч послідовностей символів або цифр, які формують вхідні дані і з якими функціонує система безпосередньо при шифруванні, називається алфавітом відкритого тексту, а при дешифрування алфавітом криптотексту [36].

Всі сучасні криптосистеми можна розділити за наступними критеріями [3, с.3]:

1. За методом шифрування даних.
2. За методом передачі ключів.
3. За методом зберігання даних.

Криптосистему можна класифікувати за методом шифрування даних в такий спосіб: якщо фрагмент відкритого тексту (окремі символи або послідовність символів) замінюється на деякий його еквівалент в криптотексті, то відповідна криптосистема ставитися до криптосистемам класу заміни. Якщо букви відкритого тексту при шифруванні лише міняються один з одним місцями, то дана система є прикладом класу шифрів перестановки. Якщо ж до початкового тексту застосовується обидва види перетворень, то дана криптосистема ставитися до класу композиційних шифрів

Криптосистема класифікується як симетрична, якщо при шифруванні, і відправник і одержувач застосовують однаковий кріптоключ до вхідних даних.

В цьому випадку шифр ключ тримається в секреті, так як його наявність дозволяє однозначно декодувати існуючий канал зв'язку і передані повідомлення. Даний тип шифрування називається синхронним так, як і відправник і одержувач чинять однакові дії для передачі інформації.

Прикладами таких криптосистем є блокові шифри, мережі Фейстеля, криптоалгоритм Blowfish, Cobra і багато інших. Їх особливістю є відносна висока швидкість дешифрування, так як на даному етапі немає необхідності у виконанні додаткових дій для перетворення ключа.

У системах з асинхронним шифруванням присутні два ключа: відкритий ключ, який передається у відкритому вигляді по каналу зв'язку, і закритий ключ, який використовується при шифруванні повідомлень на одній стороні цього каналу зв'язку. Перевагами таких систем полягає в тому, що при передачі не потрібно генерувати і обмінюватися ключами між сторонами як в симетричному шифруванні, що збільшує швидкість обміну інформації, а також знижує витрати на зберігання великого обсягу ключів.

Одним з найбільш яскравих прикладів асинхронної криптосистеми є алгоритм RSA. Основною особливістю даної криптосистеми, є досить висока криптостійкість закритого ключа, так як зломщикові знадобилося для початку виявити достатню велику натуральне просте число,

а потім перевіряти всі результаті в кільці розмірності цього числа .

Однак дана криптостійкість вимагає досить великих витрат комп'ютерних ресурсів, таких як процесорний час і пам'ять. У більшості криптосистем, таких як аффінна підстановка Цезаря або криптосистема Хілла, ключ передається в початковому вигляді без будь-яких перетворень. Але іноді розмір ключа може бути занадто великим або для його передачі його по мережі, так як це може різко скоротити мережевий трафік, або для його збереження на зовнішні носії такі як компакт диски або flash карти [36].

Криптографічні перетворення визначаються певним параметром, який називається ключ. Зазвичай ключ є буквеною або числовою послідовністю. Кожне криптографічне перетворення однозначно визначається ключем і описується певним криптографічним алгоритмом.

Криптографічними перетвореннями є:

Шифрування– процес перетворення вихідного тексту (P) в зашифрований текст (C) за допомогою шифруючої функції (E) з секретним ключем шифрування (Ke) у відповідності з обраним алгоритмом шифрування: C=EKe(P).

Розшифрування – обернений шифруванню процес перетворення зашифрованого тексту) в вихідний текст (P) за допомогою функції розшифрування (D) з секретним ключем розшифрування (Kd) у відповідності з обраним алгоритмом шифрування: P=DKd(C).

Сімейство обернених перетворень защифрування і розшифрування називають ***шифром***.

Алгоритми шифрування і розшифрування можуть відрізнятись, відповідно можуть розрізнятись і ключі шифрування і розшифрування. В загальному випадку криптосистема має наступну структуру (рис.1):

Рисунок1 – Структура криптосистеми

Робота криптосистеми може бути описана наступним чином:

1. З джерела ключів вибирається ключі (шифрування Ke і розшифрування Kd) і відправляються по надійним каналам передаючій і приймаючій стороні.

2. До вихідного (або відкритого) повідомлення p, що призначене для передачі, застосовується алгоритм шифрування EKe, внаслідок чого отримується зашифроване повідомлення C=EKe(p).

Зашифроване повідомлення пересилається по каналу для обміну повідомленнями, який не вважається надійним (тобто зашифроване повідомлення може бути перехоплене порушником), приймаючій стороні.

На приймаючій стороні до зашифрованого повідомлення C застосовується обернене

перетворення для отримання вихідного повідомлення p=DKd(C).

В класичній криптографії для шифрування і розшифрування використовувався один і той самий ключ: Ke=Kd=K. Такі криптосистеми отримали назву криптосистем з секретним ключом (secret key cryptosystems); сьогодні їх також називають симетричним криптосистемами

Зауважимо, що алгоритми шифрування і розшифрування E і D відкриті, і секретність вихідного тексту p в даному шифротекста C залежить від таємності ключа K.

Для сучасної криптографії революційним стало усвідомлення того факту, що ключі шифрування і розшифрування можуть не співпадати. Такі криптосистеми отримали назву асиметричних криптосистем (asymmetric cryptosystems).

Оскільки зашифроване повідомлення передається через канал, доступний противнику, можливе його перехоплення і «прочитання» особою, яка не має ключа. В цьому випадку говорять про дешифрування повідомлення. Таким чином, терміни «розшифрування» і «дешифрування» слід розрізняти: при розшифровуванні ключ вважається відомим, тоді як при дешифруванні ключ невідомий. Розшифрування здійснюється так само просто, як і шифрування. Дешифрування є значно складнішою задачею. Рівень складності цієї задачі і визначає здатність протистояти спробам противника заволодіти інформацією, 20 яка захищається. В зв’язку з цим говорять про криптографічну стійкість шифру, розрізняючи більш і менш стійкі.

Наука, що вивчає методи дешифрування, називається **криптоаналізом**.

Галузь знань, що об’єднує криптографію і крипто аналіз, називають **криптологією.**

Вочевидь, що термін "криптографія" далеко відійшов від свого первинного значення – "тайнопис", "таємний лист". Сьогодні це наукова дисципліна, яка поєднує методи захисту інформаційних взаємовпливів різноманітного характеру, які спираються на перетворювання даних за секретними алгоритмами, включаючи алгоритми, котрі використовують секретні параметри. Термін "інформаційний взаємовплив", чи "процес інформаційного взаємовпливу" тут позначає такий процес взаємовпливу двох і більш суб'єктів, основним змістом якого є передавання та/чи опрацьовування інформації.

Приміром, за криптографічну може вважатися будь-яка функція перетворювання даних, секретна сама собою чи залежна від секретного параметра K: M' = f(M), або M' = f(M, K). Перетворювання Mk визначається відповідним алгоритмом і значенням параметра K.

Ефективність зашифровування з метою захисту інформації залежить від зберігання таємниці ключа та криптостійкості шифру.

Більшість засобів захисту інформації базується на використанні криптографічних шифрів та процедур шифрування-розшифровування.

Під ***шифром*** розуміють сукупність оборотних перетворень множини відкритих даних на множину зашифрованих даних, що задаються ключем та алгоритмом криптографічного перетворення.

Ключ – це конкретний секретний стан деяких параметрів алгоритму криптографічного перетворення даних, який забезпечує вибір тільки одного варіанту із усіх можливих для даного алгоритму.

Основною характеристикою шифру є ***криптостійкість***, яка визначає його стійкість до розкриття методами криптоаналізу.

Зазвичай ця характеристика визначається інтервалом часу, який необхідний для розкриття шифру.

Криптостійкістю називається характеристика шифру, котра визначає його стійкість до дешифрування без знання ключа (тобто до криптоаналізу).

Є кілька показників криптостійкості, з-посеред яких:

- кількість усіх можливих ключів;

- середній час, необхідний для криптоаналізу.

Однак, окрім перехоплення й розкриття шифру, неправочинний користувач може намагатися здобути захищувану інформацію багатьма іншими способами, коли криптографія просто неспроможна цю інформацію захистити (приміром, за агентурного способу, тобто за правочинного користувача, схиленого до співробітництва; або неправочинний користувач може намагатися не здобути, а знищити чи змодифікувати в перебігу передавання захищувану інформацію тощо).

Отже, на шляху від одного правочинного користувача до іншого інформацію має бути захищуваною у різноманітні способи від всіляких погроз. Неправочинний користувач прагнутиме відвіднайти найслабшу ланку в цьому ланцюзі, аби з найменшими витратами добутися до інформації. Тому правочинні користувачі мають враховувати "засаду рівнопотужності захисту", тобто всі ланки одного ланцюга має бути захищено однаково.

Не слід забувати ще про одне: про проблему співвідношення ціни інформації, витрат на її захист та витрат на її здобуття.

Перш ніж вдаватися до захисту інформації, варто задати два запитання:

1) чи є вона для неправочинного користувача більш вартісною, аніж вартість атаки?

2) чи є вона для правочинного користувача більш вартісною, аніж вартість захисту?

Саме зазначені міркування і є вирішальними при обиранні придатних засобів захисту: фізичних, стеганографічних, криптографічних тощо.

До шифрів, що використовуються для криптографічного захисту інформації, пред’являється ряд вимог:

- достатня криптостійкість (надійність закриття даних);
- простота процедур шифрування та розшифровування;
- незначна надлишковість інформації за рахунок шифрування:
- нечутливість до незначних помилок шифрування та ін.

В тій чи іншій мірі цим вимогам відповідають:

- шифри перестановок;
- шифри заміни;
- шифри гамування;
- шифри, що базуються на аналітичних перетвореннях даних, що шифруються.

Шифрування перестановкою полягає в тому, що символи шифрованого тексту переставляються за певним правилом в межах деякого блоку цього тексту. При достатній довжині блоку, в межах якого здійснюється перестановка, та складному порядку перестановки, який не повторюється, можна досягнути прийнятної для простих практичних застосувань стійкості шифру.

Шифрування заміною (***підстановкою***) полягає в тому, що символи тексту, який шифрується, замінюються символами того ж чи іншого алфавіту відповідно до заздалегідь обумовленої схеми заміни.

Шифрування гамуванням полягає в тому, що символи шифрованого тексту поєднуються з символами деякої випадкової послідовності, яка називається ***гамою шифру***. Стійкість шифрування визначається в основному довжиною (періодом) гами шрифту. Оскільки за допомогою ЕОМ можна генерувати практично безмежну гаму шифру, то даний спосіб є одним із головних для шифрування інформації в інформаційних системах.

Шифрування аналітичним перетворенням полягає в тому, що шифрований текст перетворюється за деяким аналітичним правилом (формулою). Наприклад, можна використовувати правило множення вектора на матрицю, причому матриця є ключем шифрування, а символами вектора – символи шифрованого тексту. Іншим прикладом може служити використання так званих однонаправлених функцій для побудови криптосистем з відкритим ключем.

Процеси шифрування та розшифровування здійснюються в рамках деякої криптоситеми. Характерною особливістю симетричної криптосистеми є застосування одного і того ж секретного ключа як при шифруванні, так і розшифровуванні повідомлень.

Як відкритий текст, так і шифротекст утворюються із букв, що входять до скінченної множини символів, яка називається алфавітом. При виконанні криптографічних перетворень корисно замінити букви алфавіту цілими числами, що дозволяє спростити виконання необхідних алгебраїчних маніпуляцій. Заміна букв традиційного алфавіту числами дозволяє більш чітко сформулювати основні концепції та прийоми криптографічних перетворень. Хоча в багатьох шифрах, зокрема класичних, напряму використовується звичайний алфавіт

Класифікація алгоритмів шифрування

Перш ніж приступитися до класифікації криптологічних систем слід зробити деякі зауваження. По етапах розвитку можна виділити три періоди розвитку:

перший етап – етап донаукової криптології (до 1949 р.);

другий етап – етап наукової криптології із секретними ключами (з 1949 р. по сімдесяті роки);

третій етап – етап наукової криптології з використанням ЕОМ (із сімдесятих по теперішній час).

Звичайно, такий розподіл достатньо умовний, але воно враховує основні події, що вплинули на розвиток криптології як науки. Якщо в стародавньому світі криптологією займалися як мистецтвом, то після опублікування знаменитої статті К.Шеннона криптологія стала наукою. Прорив у криптоаналізі був зроблений з моменту виникнення ЕОМ. Слід зазначити, що перші досліди такого роду були початі під час другої світової війни. В Англії в 1942 році вступили в стрій кілька спеціалізованих для злому шифрів ЕОМ, спеціально створених для цього Аланом Тюрінгом. Це була перша у світі досить швидкодіюча ЕОМ за назвою "Колос". За допомогою цієї машини англійські криптоаналітики менше ніж за день могли розколоти будь-яку шифровку німецької шифрувальної машини Энігма.

Створення персональних ЕОМ відкрило нову сторінку в криптологія. З однієї сторони різко зросли можливості криптоаналітиків. Це в першу чергу стосується криптоаналізу за допомогою простого перебору. З іншої сторони з'явились практично необмежені можливості у шифрувальників, які, використовуючи можливості ПЕОМ, створювати шифри, що практично не розкриваються.

На першому етапі розвитку криптології існувало два основних типу перетворень відкритих текстів – заміни й перестановки. Шифрів перестановки відомо достатньо велика кількість – це й шифр «скітала», шифруючи таблиці й ін. Головна ідея шифрів перестановки є заміна місця розташування символів відкритого тексту. Шифрів заміни було значне більше, але всі вони будувалися на заміні символу відкритого тексту символом зашифрованого тексту. До таких шифрів належать полібіанський квадрат, шифруючи таблиці, Трисемуса, система

шифрування Віжінера й ін.

На другому етапі передбачалося, що для шифрування й розшифрування використовується один секретний ключ. Дані системи були названі симетричними. Як було сказано вище, основними принципами шифрування стають розсіювання й перемішування. У міру розвитку криптологія в симетричних криптологічгих системах виділяються два головних напрямки шифрування: блокові й потокові шифри. У блокових шифрах відкритий текст розбивається на блоки фіксованої довжини й зазнає шифруванню. Причому кожний блок зашифровується своїм шифром, але алгоритм перемішування залишався однаковим для всіх блоків. На цьому принципі побудовані велика кількість шифрів, включаючи американський стандарт DES і національний стандарт ДЕРЖСТАНДАРТ 28147-89. У блокових шифрах широко використовується перемішування. При використанні потокових шифрів кожний символ відкритого тексту зашифрується незалежно від інших. Головною проблемою створення потокового шифру є створення послідовності, що шифрує. Вимоги до таких послідовностей досить тверді. Як тільки ми починаємо говорити про шифри, перед нами встає проблема їх передачі до одержувача. При використанні потокових шифрів вони можуть вироблятися як на передавальному, так і на прийомному кінцях лінії зв'язку. У цьому випадку постає проблема синхронізації, і шифри можуть бути синхронні і само синхронні.

Слід зазначити той факт, що в цей час практично жоден шифр не є чистим, у тому розумінні, що ставиться до одному з видів. Найчастіше використовується комбінація декількох шифрів.

Наступним більшим класом є асиметричні криптологічні системи або системи з відкритим ключем. Головною ідеєю при створенні цього класу шифрів є генерація двох ключів. Один відкритий ключ поширюється по відкритих каналах зв'язку й використовується при шифруванні повідомлень. На прийомній стороні за допомогою секретного ключа проводиться розшифрування повідомлення. Основою при створенні таких шифрів, як сказано вище, є задачі з важким розв’язком.. У якості таких задач у цей час використовуються задачі факторизації, дискретного логарифмування й методи теорії завадостійкого кодування.

Класифікація алгоритмів шифрування представлено на рис 1.

Існує декілька класифікацій шифрів. Розглянемо деякі з них.

I **По області застосування** розрізняють шифри обмеженого і загального використання.

Стійкість шифрів обмеженого використання грунтується на збереженні в секреті алгоритму криптографічного перетворення в силу його уразливості, малу кількість ключів або відсутності таких (секретні кодові системи).

Стійкість шифрів загального використання грунтується на секретності ключа і складності його підбору потенційним противником.

II. За особливостями алгоритму шифрування шифри загального використання можна розділити на наступні види.

В одноключових системах для шифрування і дешифрування використовується один і той же ключ.

В шифри перестановки всі букви відкритого тексту залишаються в шифрограмі, але змінюють свої позиції. В шифри заміни навпаки, позиції букв в шифрограмі залишаються тими ж, що і у відкритого тексту, але символи відкритого тексту замінюються символами іншого алфавіту. операція «Що виключає АБО» (XOR, додавання по модулю 2).

В адитивних шифри літери алфавіту замінюються числами, до яких потім додаються числа секретної випадкової (псевдовипадкової) числової послідовності (гами), після чого береться залишок від ділення по модулю (операція mod). Якщо вихідне повідомлення і гамма

представляються в бітовому вигляді, то при шифруванні і дешифруванні застосовується логічна

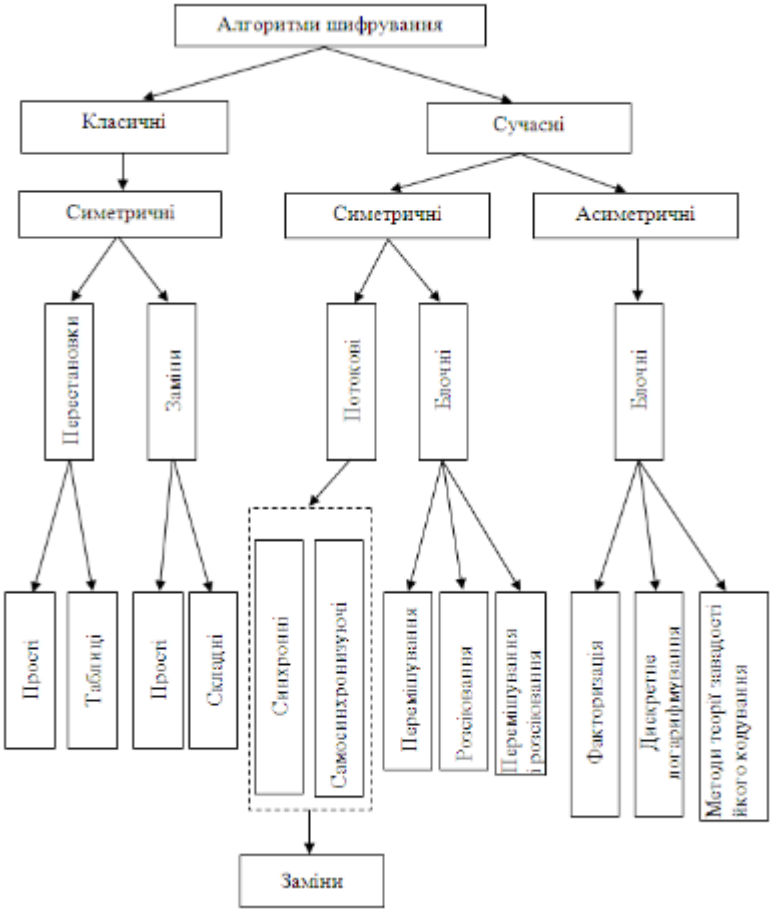


Рисунок 1 - Класифікація алгоритмів шифрування

Квантова криптографія вносить в процес шифрування природну невизначеність квантового світу. Процес відправлення та прийому інформації виконується за допомогою об'єктів квантової механіки (наприклад, за допомогою електронів в електричному струмі або фотонів в лініях волоконно-оптичного зв'язку). Найціннішим властивістю цього виду шифрування є те, що при посилці повідомлення відправляє і приймаюча сторона з досить великою ймовірністю можуть встановити факт перехоплення противником зашифрованого повідомлення.

У двохключового системах для шифрування і дешифрування використовується два скоєно різних ключа. У детермінованих шифри при шифруванні одного і того ж повідомлення одним і тим же ключем завжди буде виходити один і той же шифртекст. В імовірнісних шифри в процедурі шифрування використовується додаткова випадкова величина (число) - в результаті при шифруванні одного і того ж вихідного повідомлення одним і тим же ключем можуть вийти різні шифртекст, які при розшифровці дадуть один і той же результат (вихідне повідомлення).

Комбіновані (складові) методи передбачають використання для шифрування повідомлення відразу декількох методів (наприклад, спочатку заміна символів, а потім їх перестановка).

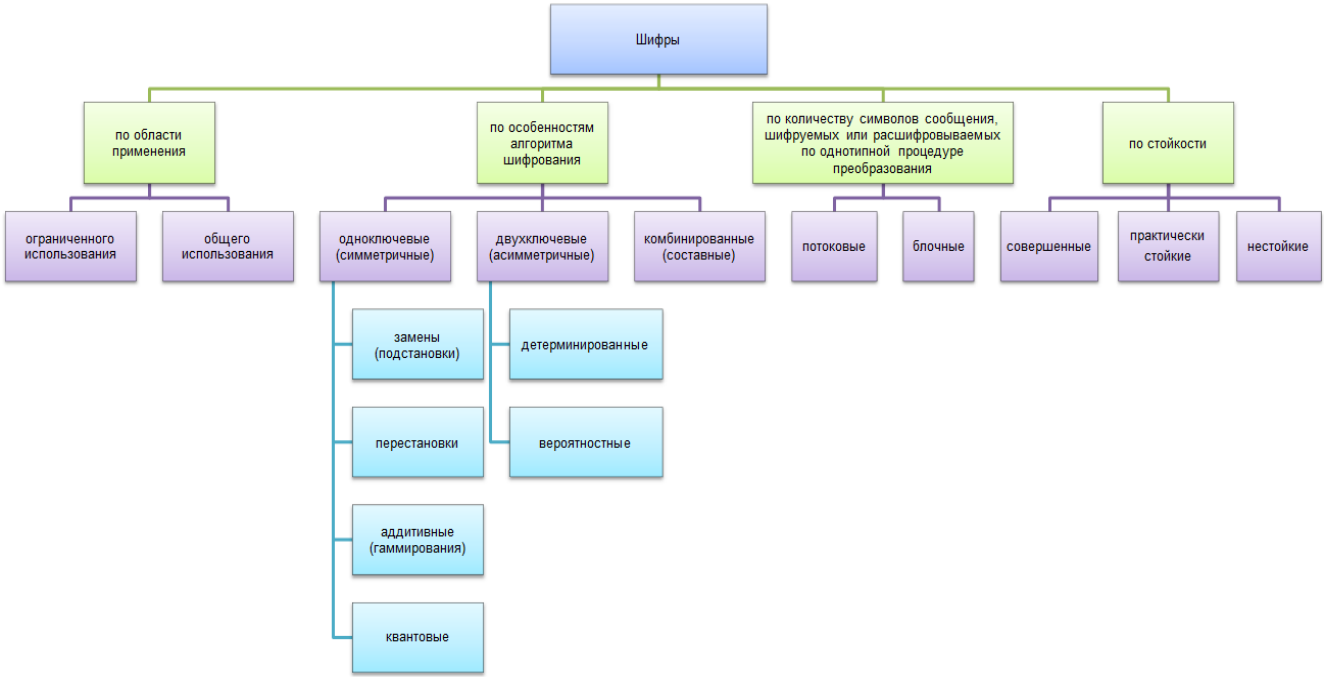


Рисунок 2 - Класіфікація шифрів

III. За кількістю символів повідомлення (або його кодової заміни), шифрованих або розшифровуються за однотипною процедурі перетворення розрізняють**:**

- потокові шифри - процедура перетворення застосовується до окремого символу повідомлення;

- блокові шифри - процедура перетворення застосовується до набору (блоку) символів повідомлення.

Відрізнити потоковий шифр від блокового можна за наступним ознакою - якщо в результаті розбиття вихідного повідомлення на окремі елементарні символи і застосування до них однотипної процедури перетворення отримується шифрограма еквівалентна тій, яка виходить при застосуванні перетворення «як ніби до всього вихідного повідомлення», то шифр потоковий, інакше блоковий.

IV. По стійкості шифри діляться на три групи:

- досконалі (абсолютно стійкі, теоретично стійкі) - шифри, свідомо не піддаються розтину (при правильному використанні). Дешифрування секретного повідомлення призводить до виникнення кількох осмисленим равновероятности відкритим повідомленнями;

- практично (обчислювально, досить) стійкі - шифри, розтин яких за прийнятний час неможливо на сучасному або перспективному рівні обчислювальної техніки. Практична стійкість таких систем базується на теорії складності і оцінюється виключно на якийсь певний момент часу з двох позицій:

- обчислювальна складність повного перебору;

- відомі на даний момент слабкості (уразливості) і їх вплив на обчислювальну складність;

- нестійкі шифри [37,38].

Лекція 13

Тема: **Сучасні концепції криптографії**

Вимоги до криптографічних систем

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, однак їй властиві й переваги: висока продуктивність, простота, захищеність і т.д.. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;

число операції, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення й відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;

число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, повинне мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень) або вимагати неприйнятно високих витрат на ці обчислення;

знання алгоритму шифрування не повинне впливати на надійність захисту;

незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні того самого вихідного тексту;

незначна зміна вихідного тексту повинне приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;

структурні елементи алгоритму шифрування повинні бути незмінними;

додаткові біти, що уводяться в повідомлення в процесі шифрування, повинні бути повністю й надійно сховані в шифрованому тексті;

довжина шифрованого тексту не повинна перевершувати довжину вихідного тексту;

не повинне бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;

будь-який ключ із множини можливих повинен забезпечувати надійний захист інформації;

алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинне вести до якісного погіршення алгоритму шифрування.

Не слід забувати й про такі банальні речі, як гроші. Іншими словами - скільки буде коштувати збиток, який понесе власник інформації, при несанкціонованім її використанні? чи Коштує ця інформація тих вкладень, які необхідно зробити для закриття інформації?

Лекція 14

Тема: **Класичні методи шифрування**

Класичні криптографічні методи діляться на два основних типи:

симетричні (шифрування секретним ключем) і ***асиметричні*** (шифрування відкритим ключем).

У симетричних методах для шифрування і розшифрування використовується один і той же секретний ключ. Найбільш відомим стандартом на симетричне шифрування із закритим ключем є стандарт для обробки інформації в державних установах США DES (Data Encryption Standard). Загальна технологія використання симетричного методу шифрування представлена на рисунку 1

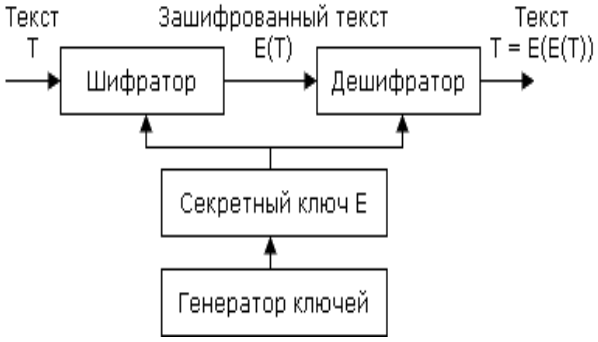


Рисунок 1

Основний недолік цього методу полягає в тому, що ключ повинен бути відомий і відправнику, і одержувачу. Це істотно ускладнює процедуру призначення і розподілу ключів між користувачами. Зазначений недолік послужив причиною розробки методів шифрування з відкритим ключем - асиметричних методів.

Асиметричні методи використовують два взаємопов'язаних ключів: для шифрування і розшифрування. Один ключ є закритим і відомим тільки одержувачу. Його використовують для розшифрування. Другий з ключів є відкритим, тобто він може бути загальнодоступним по мережі і опублікований разом з адресою користувача. Його використовують для виконання шифрування.

Схема функціонування даного типу криптосистеми показана на рис. 2

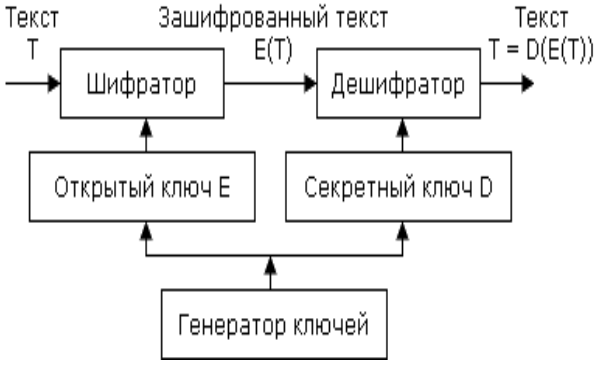


Рисунок 2

В даний час найбільш відомим і надійним є асиметричний алгоритм RSA (Rivest, Shamir, Adleman).

Лекція 16

Загальні відомості про блочні шифри.
Генерування блочних шифрів

Блоковий шифр - це один з видів симетричних криптосистем, що оперує або групами біт фіксованої довжини, або текстовими повідомленнями також фіксованою довжини. Характерна довжина блоку шифрування лежитьв діапазоні 64-256 біт. Якщо довжина вихідного повідомлення, що міститься в блок менше ніж розмірність блоку, то вона доповнюється будь інформацією до необхідної довжини. Ця інформація називається «забруднювачем» або непотрібною інформацією [6]. Блокові шифри є важливими компонентами багатьохсучасних криптосистем і криптографічних протоколів, використовуються для шифрування пакетів для передачі по мережі. До переваг блокових шифрів відносяться схожість алгоритмів шифрування і дешифрування: вони, в більшості випадків, відрізняються тільки порядком дій (при дешифрування послідовність дій прямо обернена а послідовності дій при шифруванні), а також унікальності шифруэмих блоків. Це спрощує створення пристроїв шифрування і створення алгоритмів. Крім можливостей шифрувальних машин блокові шифри можуть бути використані для різних інших цілей: генераторів псевдовипадкових чисел, потокових шифрів, імітовставкі і хеш-функцій.

На даний момент існують 3 найбільш популярний крипто алгоритмів на основі яких стоячи інші блокові криптосистеми – це тітеративні блокові шифри, SP мережі, мережі Фейстеля. У 1971 Хорст Фейстель запатентував два пристрою реалізують різні алгоритми шифрування, названі потім загальним назву «Lucifer». Одне з пристроїв використовувало конструкцію, згодом названу «мережею Фейстеля », яке в майбутньому стало основою для багатьох сучасних крипто алгоритмів таких як Lucifer, Blowfish, KASUMI, RC2, RC5, RC6, TEA і багато інших [36]

Для побудови стійкого шифру, зручного для практичного використання, можна запропонувати такі підходи [35]:

1. Блоковість. Вибираємо довжину ключа меншою за довжину повідомлення, розбиваємо повідомлення на окремі блоки і шифруємо кожний з них (крім, можливо, останнього) шляхом сумування з ключем по модулю два.

2. Режими шифрування. Для збільшення стійкості блокового шифрування можна забезпечити використання при шифруванні кожного наступного блоку результатів шифрування попереднього блоку (наприклад, в якості нового ключа шифрування для блоку). Тоді

зловмисник не зможе розшифрувати блок криптотексту, доки не розшифрує всі попередні блоки.

3. Багатораундовість. Додатково збільшити стійкість блокового шифрування можна з рахунок багаторазового виконання шифрування кожного блоку за умови, що функція шифрування є нелінійним перетворенням.

В блокових алгоритмах вхідна послідовність розбивається на блоки – ділянки певної довжини (найчастіше, по 64 біти). Якщо довжина відкритого тексту виявляється некратною довжині блоку, застосовується операція доповнення (padding) останнього блоку до необхідної довжини, яка полягає у дописуванні необхідної кількості нулів або випадкового набору символів рис. 1).

Рисунок 1 - Представлення даних в блоковому алгоритмі

Криптографічне перетворення в блокових алгоритмах шифрування здійснюється над кожним блоком окремо (Рис..2). Його сутність полягає у застосуванні до блока багаторазово математичного перетворення. Внаслідок цього результуюче перетворення виявляється криптографічно більш сильним, ніж перетворення над окремо взятим блоком. Метою таких перетворень є створення залежності кожного біту блоку шифротексту від кожного біту ключа і кожного біту відкритого тексту:

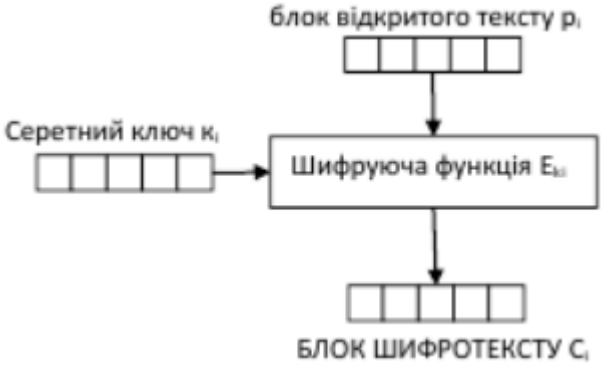


Схема шифрування блоку даних в блоковому алгоритмі

Зашифрований блок може використовуватися для шифрування наступного, в результаті чого кожний блок отримає контекст, що властивий всьому повідомленню (рис. 3). Такі механізми шифрування використовуються для уникнення від деяких атак, заснованих на стиранні або вставки блоків, і визначаються відповідним режимом шифрування.

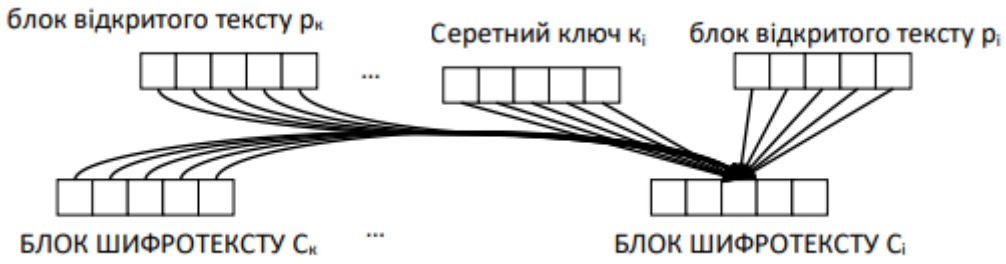


Рисунок 3 -Механізм режимів шифрування [35]

Режим шифрування – метод застосування блокового шифру, в якому для забезпечення вищого рівня криптостійкісті шифрування блоків вхідного повідомлення здійснюється з використання блоків криптотексту. Розрізняють п’ять основних режимів шифрування: блок відкритого тексту

) – режим електронної кодової книги.

) – режим зціплення блоків по криптотексу.

) – режим з оберненим зв’язком по криптотексу.

) – режим з оберненим зв’язком по виходу.

5. CTR (Coutner) – режим з лічильником. Блокові алгоритми шифрування сьогодні є основним засобом криптографічного захисту інформації.

Основні переваги блокових алгоритмів шифрування:

Висока швидкість шифрування/розшифрування.

Висока гарантована стійкість, яка до того ж може бути доведена математично.

Можливість ефективної програмної реалізації [35].

Блочні та потокові шифри.

Проектування алгоритмів шифрування базується на раціональному виборі функцій, що перетворюють вихідні (незашифровані) дані в шифротекст. Ідея застосування такої функції до всього повідомлення реалізується надзвичайно рідко. Практично усі криптографічні методи зв’язані з розбиттям повідомлення на велику кількість фрагментів (чи знаків) фіксованого розміру, кожний з яких шифрується окремо. Такий підхід суттєво спрощує задачу шифрування, оскільки повідомлення зазвичай мають різну довжину.

Розрізняють три основних способи шифрування: поточні шифри, блочні шифри та блочні шифри з оберненим зв’язком. Для класифікації методів шифрування даних слід вибирати деяку кількість характерних ознак, які можна застосувати для встановлення відмінностей між цими методами. Виділяють такі характерні ознаки методів шифрування даних [**Ошибка! Закладка не определена.**]:

- ***Виконання операцій з окремими бітами чи блоками***. Відомо, що для деяких методів шифрування знаком повідомлення, над яким здійснюють операції шифрування, є окремий біт, тоді як інші методи оперують кінцевою множиною біт, яка зазвичай називається блоком.
- ***Залежність чи незалежність функції шифрування від результатів шифрування попередніх частин повідомлення***.

- ***Залежність чи незалежність шифрування окремих знаків від їх розташування в тексті***. В деяких методах знаки шифруються з використанням однієї і тієї ж функції незалежно від їх розміщення в повідомленні, а в інших методах, наприклад при потоковому шифруванні, різні знаки повідомлення шифруються з врахуванням їх розташування в повідомленні. Цю властивість називають позиційною залежністю чи незалежністю шифру.
- ***Симетрія чи асиметрія функції шифрування***. Ця важлива характеристика визначає суттєві відмінності між звичайними симетричними (одноключовими) криптосистемами та асиметричними (двохключовими) криптосистемами з відкритим ключем. Основна відміна між ними полягає в тому, що в асиметричній криптосистемі знання ключа шифрування (чи розшифровування) недостатньо для розкриття відповідного ключа розшифровування (чи шифрування).

У табл. 1 наведено типи криптосистем та їх основні характеристики.

Таблиця 1 -Основні характеристики криптосистем

Тип криптосистеми	Операції над бітами чи блоками	Залежність від попередніх знаків	Позиційна залежність	Наявність симетрії функції шифрування
Потокового шифрування	Біти	Не залежить	Залежить	Симетрична
Блочного шифрування	Блоки	Не залежить	Не залежить	Симетрична чи несиметрична
З оберненим зв'язком від шифротексту	Біти чи блоки	Залежить	Не залежить	Симетрична

Потокове шифрування полягає в тому, що біти відкритого тексту сумуються за модулем 2 з бітами псевдовипадкової послідовності. До переваг потокових шифрів відносяться висока швидкість шифрування, відносна простота реалізації та відсутність розмноження помилок. Недоліком є необхідність передачі інформації синхронізації перед заголовком повідомлення, яка повинна бути прийнята до розшифровування будь-якого повідомлення. Останнє зумовлене тим, що якщо два різних повідомлення шифруються на одному і тому ж ключі, то для розшифровування цих повідомлень потрібна одна і та ж псевдовипадкова послідовність. Таке становище може створити загрозу криптостійкості системи. Тому часто використовують додатковий ключ повідомлення, що вибирається випадково, який передається на початку повідомлення і застосовується для модифікації ключа шифрування. В результаті різні повідомлення будуть шифруватися за допомогою різних послідовностей.

Потокові шифри широко застосовуються для шифрування оцифрованих голосових сигналів та цифрових даних, що потребують оперативної доставки споживачу інформації. До недавнього часу такі застосування були переважаючими для даного методу шифрування. Це зумовлено, зокрема, відносною простотою проектування та реалізації генераторів шифруючих послідовностей. Але найважливішим фактором є відсутність розмноження помилок у потоковому шифрі. Стандартним методом генерування послідовностей для потокового

шифрування є метод, що застосовується у стандарті шифрування DES в режимі оберненого зв'язку по виходу (режим OFB).

При ***блочному шифруванні*** відкритий текст спочатку розбивається на блоки однакової довжини, потім застосовується функція шифрування, яка залежить від ключа, для перетворення блоку відкритого тексту довжиною *m* біт у блок шифротексту такої ж довжини. Перевагою блочного шифрування є те, що кожний біт блоку шифротексту залежить від значень усіх біт відповідного блоку відкритого тексту, і ніякі два блоки відкритого тексту не можуть бути представлені одним і тим же блоком шифротексту. Алгоритм блочного шифрування може використовуватися в різних режимах. Чотири режими шифрування алгоритму DES фактично можуть бути застосовані до будь-якого блочного шифру: режим прямого шифрування чи шифрування з використанням електронної книги кодів ECB (Electronic code book), шифрування зі зчепленням блоків шифротексту CBC (Cipher block chaining), шифрування з оберненим зв'язком по шифротексту CFB (Cipher feedback) та шифрування з оберненим зв'язком по виходу OFB (Output feedback).

Основною перевагою прямого блочного шифрування ECB є те, що в добре спроектованій системі блочного шифрування невеликі зміни в шифротексті викликають великі і непередбачувані зміни у відповідному відкритому тексті і навпаки. Разом з тим застосування блочного шифру в даному режимі має суттєві недоліки. Перший з них полягає в тому, що внаслідок детермінованого характеру шифрування при фіксованій довжині блоку 64 біти можна здійснити криптоаналіз шифротексту „зі словником" в обмеженій формі. Останнє зумовлено тим, що ідентичні блоки відкритого тексту довжиною 64 біт у вихідному повідомленні представляються ідентичними блоками шифротексту, що дозволяє криптоаналітику зробити певні висновки про зміст повідомлення. Другий потенційний недолік цього шифру пов'язаний з розмноженням помилок. Результатом зміни тільки одного біту в прийнятому блоці шифротексту буде неправильне розшифрування усього блоку.

Із-за зазначених недоліків блочні шифри рідко застосовуються у вказаному режимі для шифрування довгих повідомлень. Проте у фінансових закладах, де повідомлення часто складаються з одного чи двох блоків, блочні шифри широко використовують в режимі прямого шифрування. Таке застосування зазвичай зумовлене можливістю частої зміни ключа шифрування, у зв'язку з чим ймовірність шифрування двох ідентичних блоків відкритого тексту на одному і тому ж ключі дуже мала.

Криптосистема з відкритим ключем також є системою блочного шифрування і повинна оперувати блоками великих розмірів. Останнє зумовлено тим, що криптоаналітик знає відкритий ключ шифрування і міг би заздалегідь вирахувати та скласти таблицю відповідності блоків відкритого тексту та шифротексту. Якщо довжина блоків мала, наприклад 30 біт, то кількість можливих варіантів блоків не дуже велика (при довжині 30 біт це $2^{30} \approx 10^9$), і може бути складена повна таблиця, яка дозволяє моментально розшифрувати будь-яке повідомлення з використанням відомого відкритого ключа. Асиметричні криптосистеми з відкритим ключем детально розглядатимуться далі.

Найчастіше блочні шифри застосовуються у системах шифрування з оберненим зв'язком. Системи шифрування з оберненим зв'язком зустрічаються в різних практичних варіантах. Як і при блочному шифруванні, повідомлення розбивають на ряд блоків, що складаються з *m* біт. Для перетворення цих блоків у блоки шифротексту, які також складаються із *m* біт, використовуються спеціальні функції шифрування. Проте, якщо в блочному шифрі

така функція залежить тільки від ключа, то у блочних шифрах з оберненим зв'язком вона залежить як від ключа, так і від одного чи більше попередніх блоків шифротексту.

Практично важливим шифром із оберненим зв'язком є шифр зі зчепленням блоків CBC. В цьому випадку *m* біт попереднього шифротексту сумуються за модулем 2 з наступними *m* бітами відкритого тексту, після чого застосовується алгоритм блочного шифрування під управлінням ключа для отримання наступного блоку шифротексту. Іще один варіант шифру з оберненим зв'язком отримується із стандартного режиму CFB алгоритму DES – із режиму з оберненим зв'язком по шифротексту.

Перевагою криптосистем блочного шифрування з оберненим зв'язком є можливість їх застосування для виявлення маніпуляцій з повідомленнями, які можуть здійснити активні перехоплювачі. При цьому використовується факт розмноження помилок в таких шифрах а також здатність цих систем легко генерувати код автентифікації повідомлення. Тому системи шифрування з оберненим зв'язком використовуються не тільки для шифрування повідомлень, а й для їх автентифікації. Криптосистемам блочного шифрування з оберненим зв'язком властиві деякі недоліки. Головним з них є розмноження помилок, оскільки один помилковий біт при передачі може викликати ряд помилок у розшифрованому тексті. Інший недолік пов'язаний з тим, що розробка і реалізація систем шифрування з оберненим зв'язком часто виявляється складнішою, ніж систем потокового шифрування.

На практиці для шифрування довгих повідомлень застосовують поточні шифри чи шифри з оберненим зв'язком. Вибір конкретного типу шифру залежить від призначення системи та вимог, що до неї висуваються.

Криптосистема з депонуванням ключа. Криптосистема з депонуванням ключа призначена для шифрування користувацького трафіку (наприклад, голосового чи передачі даних) таким чином, щоб сеансові ключі, які використовуються для шифрування та розшифровування трафіку, були доступні при певних надзвичайних ситуаціях третій авторизованій стороні.

По суті, криптосистема з депонуванням ключа реалізує новий метод криптографічного захисту інформації, який забезпечує високий рівень інформаційної безпеки при передачі по відкритих каналах зв'язку і відповідає вимогам національної безпеки. Цей метод базується на застосуванні спеціальної шифруючої/дешифруючої мікросхеми типу Clipper та процедури депонування ключа, яка визначає правила розкриття унікального ключа цієї мікросхеми. Мікросхема Clipper розроблена за технологією TEMPEST, яка перешкоджає зчитуванню інформації за допомогою зовнішніх впливів.

Генерація та запис унікального ключа в мікросхему виконується до вбудовування мікросхеми в кінцевий пристрій. Слід зазначити, що не існує способу, який дозволяє безпосередньо зчитувати цей ключ як під час, так і після завершення технологічного процесу виробництва та програмування даної мікросхеми.

Ключ розділяється на два компоненти, кожний з яких шифрується і потім передається на зберігання довіреним агентам депозитної служби, які представляють собою урядові організації, що забезпечують надійне зберігання компонентів ключа на протязі терміну його дії. Агенти депозитної служби видають ці компоненти ключа тільки за відповідним запитом, підтвердженим судовим рішенням. Отримані компоненти ключа дозволяють службам, які відповідають за національну безпеку, відновити унікальний ключ та виконати розшифровування користувацького трафіку.

Лекція 17

Тема: **Поточні шрифти. Шрифти гамування**

Поточні шрифти

Взагалі, шифри, що вимагають попереднього розподілення відкритого тексту на блоки однокової довжини, і подальше зашифрування кожного з них окремо, називають *блочними шифрами*. У протилежному випадку, мають місце *поточні шифри.* Інакше кажучи, у поточних алгоритмах кожен символ відкритого тексту шифрується незалежно від інших і розшифровується в такий же спосіб.

Поточне шифрування полягає в тому, що біти вихідного тексту додаються за модулем два до псевдовипадкової послідовності (її іноді називають гаммою). Від того, наскільки вироблена гамма буде мати властивість рівноймовірності появи її символів, залежить стійкість поточних алгоритмів шифрування.

До переваг поточнних шифрів слід віднести те, що вони мають високу швидкість шифрування, відносно просто зреалізовуються та при цьму методі шифрування відсутнє розповсюдження похибок. Недоліком є необхідність передавання синхронізуючої інформації раніш повідомлення. Це може створити загрозу криптостійкості системи. Тому використовують додатковий, випадковий ключ повідомлення, який має модифікувати ключі, що шифрують повідомлення.

На практиці цей метод шифрування використовують тоді, коли треба зашифрувати повідомлення великої довжини.

Шифри гаммування

Стійкий спосіб ускладнення числових кодів – гаміювання. Він полягає у перешифровуванні закодованого повідомлення за допомогою деякого ключового числа, яке називається гамою.

Під ***гамуванням*** розуміють процес накладання за певним законом гами щифру на відкриті дані.

Гама шифру – це псевдовипадкова послідовність, вироблена за певним алгоритмом для зашифровування відкритих даних та розшифровування зашифрованих даних. Процес зашифровування полягає в генерації гами шифру і накладання отриманої гами на вихідний відкритий текст відтворюваним способом, наприклад з використанням операції сумування по модулю 2.

Слід зазначити, що перед зашифровуванням відкриті дані розбивають на блоки $T_0^{(i)}$ однакової довжини, зазвичай по 64 біти. Гама шифру виробляється у вигляді послідовності блоків $Г_ш^{(i)}$ аналогічної довжини. Рівняння зашифровування можна записати у вигляді

$$T_ш^{(i)}=Г_ш^{(i)}\oplus T_0^{(i)},\ i=1...M,$$

де $T_ш^{(i)}$ – i-й блок шифротексту; $Г_ш^{(i)}$ – i-й блок гами шифру; $T_0^{(i)}$ – i-й блок відкритого тексту; M – кількість блоків відкритого тексту.

Процес розшифровування зводиться до повторної генерації гами шифру і накладання цієї гами на зашифровані дані. Гама генерується з використанням генератора псевдовипадкового числа. Для того, щоб у відправника і отримувача генерувалася одна і та ж гама, їм потрібно використовувати ідентичні алгоритми генерації псевдовипадкових чисел. Крім того, генератор псевдовипадкових чисел потрібно ініціалізувати початковим 64-бітним значенням, в якості якого дуже часто використовується поточний час шифрування. Останнє приводить до цікавого ефекту, який полягає в тому, що одне і те ж саме повідомлення, зашифроване в різні моменти часу, буде давати зовсім різні шифротексти.

Значення, яким було проініціалізовано генератор псевдовипадкових чисел, відправляється отримувачу разом з масивом зашифрованих даних. Таке значення називають ***синхропосилкою*** або початковим заповнювачем. Слід зазначити, що в якості синхропосилки зазвичай відправляється не саме число, отримане з якогось джерела (наприклад, поточний час), а результат зашифровування цього числа.

Рівняння розшифровування має вигляд:

$$T_0^{(i)}=Г_ш^{(i)}\oplus T_ш^{(i)}.$$

Отриманий цим методом шифротекст є досить складним для розкриття, оскільки ключ є змінним. По суті гама шифру повинна змінюватися випадковим чином для кожного шифрованого блоку. Якщо період гами перевищує довжину всього шифрованого тексту і зловмиснику невідома ніяка частина вихідного тексту, то такий шифр можна розкрити тільки прямим перебором усіх варіантів ключа. В цьому випадку криптостійкість ключа визначається його довжиною.

Генерування непередбачуваних двійкових послідовностей великої довжини є однією з найважливіших проблем класичної криптографії. Для розв’язання цієї проблеми широко використовуються генератори двійкових псевдовипадкових послідовностей. Такі послідовності часто називають гамою шифру або просто гамою (за назвою букви γ грецького алфавіту, яка часто використовується у математичних формулах для позначення випадкових величин).

Зазвичай для генерації послідовності псевдовипадкових чисел використовуються комп’ютерні програми, які, хоча і називаються генераторами випадкових чисел, в дійсності видають детерміновані числові послідовності, які за своїми властивостями дуже подібні на випадкові.

До криптографічно стійкого генератора псевдовипадкової послідовності чисел (гами шифру) ставляться три основні 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 та попередня частина гами;
- генерування гами не повинно викликати великих технічних проблем.

Довжина періоду гами є найважливішою характеристикою генератора псевдовипадкових чисел. По закінченні періоду числа почнуть повторюватися, і їх можна буде передбачити. Потрібна довжина періоду гами визначається мірою конфіденційності даних. Чим довший ключ, тим складніше його підібрати. Довжина періоду гами залежить від вибраного алгоритму отримання псевдовипадкових чисел.

Друга вимога зв'язана з такою проблемою: як можна достовірно впевнитися, що псевдовипадкова гама конкретного генератора є дійсно непередбачуваною? На даний час не існує таких універсальних і перевірених на практиці критеріїв та методик. Щоб гама вважалася непередбачуваною (істинно випадковою), необхідно, щоб її період був дуже великим, а різні комбінації біт певної довжини були рівномірно розподілені по всій її довжині.

Третя вимога обумовлює можливість практичної реалізації генератора програмним чи апаратним шляхом із забезпеченням необхідної швидкодії.

Шифрування за допомогою гами полягає у сумуванні всіх кодованих груп повідомлення з одним і тим самим ключовим числом.

Приклад 1. Результат накладення гами 6413 на кодований текст (одиниці перенесення, що з'являються при додаванні між кодовими групами, опускаються):

Приклад 2. Результат оберненої операції «зняття гами» 6413:

Лекція 18

Тема **Класичні симетричні криптосистеми. Криптосистема Хілла. Особливості, принцип організації**

1 Криптосистема Хілла

Лестером Хіллом було сформульовано алгебричний метод, котрий узагальнює афінне підставляння Цезаря

$$E_{a,b}: \rightarrow \overline{Z}_m \rightarrow \overline{Z}_m;$$
$$E_{a,b}: t \rightarrow E_{\text{а,б}}(t);$$
$$E_{a,b}(t) = at + b \pmod m,$$

де a, b – цілі числа, $0 \le a, b < m$; НСД (найбільший спільний дільник) $(a, m) = 1$, для визначення n-грам

Множина цілих $\overline{Z}_m$, для якої визначено операції додавання, віднімання та множення за модулем m, являє приклад кільця. Кільце являє собою алгебричну систему, в якій визначено операції додавання, віднімання та множення пар елементів.

Нехай $\overline{A}$ є лінійним перетворенням, описуваним квадратною матрицею, причому $\overline{A}: \overline{Z}_m \to \overline{Z}_m$.

Криптосистема, розроблена Хіллом, базується на лінійній алгебрі.

Нехай простори вихідних повідомлень та криптотекстів збігаються і дорівнюють ∑, де ∑ – англійська абетка. Надамо літерам номери відповідно до порядку їхнього слідування в абетці:

Таблиця 2.1 - Відповідність поміж англійською абеткою та множиною цілих

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Всі арифметичні операції виконуються за модулем 26 (кількість літер в абетці). Це означає, що 26 ототожнюється з 0, 27 – з 1, 28 – з 2 і т. д.

Оберемо ціле число $d \geq 2$. Воно зазначає розмірність використовуваних матриць. У процедурі зашифровування набори з d літер вихідного повідомлення зашифровуються разом. Візьмемо $d = 2$.

Нехай тепер A – квадратна $d \times d$ матриця. Елементами A є цілі числа від 0 до 25. Вимагатимемо далі, аби матриця A була невиродженою, тобто існувала обернена матриця A^{-1}. Наприклад,

$$A = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \quad \text{та} \quad A^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}.$$

Нагадаємо, що арифметичні операції провадяться за модулем 26. Це дає, приміром,

$$2 \cdot 17 + 5 \cdot 9 = 79 = 1 + 3 \cdot 26 = 1,$$

тобто, як і мало бути, одиницю на головній діагоналі одиничної матриці.

Зашифровування здійснюється за допомогою рівняння

$$AP = C,$$

де P та C – d-розмірні вектори-стовпці. Більш докладно: кожен набір з d літер вихідного повідомлення визначає вектор P, компонентами якого є номери літер. Врешті, C знову інтерпретується як набір d літер криптотексту.

Наприклад, HELP визначає два вектори:

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad \text{та} \quad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

З рівнянь

$$AP_1 = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = C_1 \quad \text{та} \quad AP_2 = \begin{pmatrix} 0 \\ 19 \end{pmatrix} = C_2$$

дістаємо криптотекст HITE.

Розглянемо тепер сферу діяльності криптоаналітика. Припустімо, що аналітик здогадався, що $d = 2$. Йому потрібно віднайти матрицю A чи, ще краще, обернену матрицю A^{-1}. З цією метою він обирає вихідне повідомлення HELP і довідується, що відповідний криптотекст є HITE. Криптоаналітикові відомо, що

$$A\begin{pmatrix}7\\4\end{pmatrix} = \begin{pmatrix}7\\8\end{pmatrix} \quad \text{та} \quad A\begin{pmatrix}11\\15\end{pmatrix} = \begin{pmatrix}0\\19\end{pmatrix}.$$

Це може бути записано у вигляді

$$A = \begin{pmatrix}7 & 0\\0 & 19\end{pmatrix}\begin{pmatrix}7 & 11\\4 & 15\end{pmatrix}^{-1} = \begin{pmatrix}7 & 0\\8 & 19\end{pmatrix}\begin{pmatrix}19 & 19\\14 & 21\end{pmatrix} = \begin{pmatrix}3 & 3\\2 & 5\end{pmatrix}.$$

Обернена матриця A^{-1} одразу ж обчислюється з матриці A. Після цього який завгодно криптотекст може бути розшифровано за допомогою M^{-1}.

Важливим моментом у цих обчисленнях є існування оберненої матриці до $\begin{pmatrix}7 & 11\\4 & 15\end{pmatrix}$. З іншого боку, наш криптоаналітик обрав вихідне повідомлення HELP, котре породжує матрицю $\begin{pmatrix}7 & 11\\4 & 15\end{pmatrix}$, тобто він здійснює вибір у такий спосіб, аби результуюча матриця мала обернену.

Припустімо тепер, що криптоаналітик працює з іншою початковою постановкою – "відоме є певне вихідне повідомлення". Більш докладно: нехай криптоаналітикові відомо, що CKVOZI – криптотекст, який відповідає вихідному повідомленню SAHARA. Хоча ми маємо тут приклад довшого повідомлення, аніж раніше, однак добуваної з нього інформації є набагато менше.

Насправді, тепер рівняння для повідомлення криптотексту мають вигляд

$$A\begin{pmatrix}18\\0\end{pmatrix} = \begin{pmatrix}2\\10\end{pmatrix}, \quad A\begin{pmatrix}7\\0\end{pmatrix} = \begin{pmatrix}21\\14\end{pmatrix} \quad \text{та} \quad A\begin{pmatrix}17\\0\end{pmatrix} = \begin{pmatrix}25\\8\end{pmatrix}.$$

Не існує оберненої квадратної матриці, котру може бути утворено з трьох векторів-стовпців, які з'являються як коефіцієнти M.

Криптоаналітик виявляє, що кожна обернена квадратна матриця

$$A' = \begin{pmatrix}3 & x\\2 & y\end{pmatrix}$$

може бути базисом криптосистеми, оскільки вона шифрує SAHARA як CKVOZI. Отже, криптоаналітик може зупинитися на матриці

$$A' = \begin{pmatrix}3 & 1\\2 & 1\end{pmatrix},$$

для якої оберненою є матриця

$$(A')^{-1} = \begin{pmatrix} 1 & 25 \\ 24 & 3 \end{pmatrix}.$$

Криптоаналітик є готовий до перехоплення криптотексту. Він дістає текст NAFG й одразу обчислює

$$\begin{pmatrix} 1 & 25 \\ 24 & 3 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \quad \text{та} \quad \begin{pmatrix} 1 & 25 \\ 24 & 3 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 25 \\ 8 \end{pmatrix}.$$

Два вектори-стовпці породжують вихідне повідомлення NAZI. Однак легальний користувач знає оригінальну матрицю A та її обернену матрицю й обчислює

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \quad \text{та} \quad \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 21 \\ 24 \end{pmatrix},$$

що дає вихідне повідомлення NAVY.

Криптоаналітик припустився прикрої помилки, котра могла спричинитися до хибних кроків.

Алгоритм зашифровування в криптосистемі Хілла.

Дано квадратну матрицю виду $\begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$

$$A = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}.$$

1 Обчислюється визначник D матриці A:

$$D = a_{11}a_{22} - a_{12}a_{21} = 3 \cdot 5 - 2 \cdot 3 = 15 - 6 = 9.$$

2 Визначається долучена матриця алгебричних доповнень A^*, складена з алгебричних доповнень до елементів матриці A, причому алгебричне доповнення до елемента a_{ij} перебуває на перетинанні j-того рядка й i-того стовпця.

$$A^* = \begin{pmatrix} A_{11} & A_{21} \\ A_{12} & A_{22} \end{pmatrix}.$$

Під алгебричним доповненням A_{ij} елемента a_{ij} розуміють мінор M_{ij}, домножений на $(-1)^{i+j}$:

$$A_{ij} = (-1)^{i+j} M_{ij},$$

тобто

$$A_{11} = (-1)^{1+1} \cdot M_{11} = (-1)^2 \cdot a_{22} = 1 \cdot 5 = 5;$$
$$A_{12} = (-1)^{2+1} \cdot M_{12} = (-1)^3 \cdot a_{12} = -1 \cdot 2 = -2;$$

$A_{21} = (-1)^{1+2} \cdot M_{21} = (-1)^3 \cdot a_{21} = -1 \cdot 3 = -3;$
$A_{22} = (-1)^{2+2} \cdot M_{22} = (-1)^4 \cdot a_{11} = 1 \cdot 3 = 3.$

Отже, можна записати здобуту матрицю алгебричних доповнень:

$$A^* = \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}.$$

3 Визначається обернена матриця A^{-1}.

За обернену матрицю для A слугуватиме матриця, котра виходить із долученої матриці A^* діленням усіх її елементів на D.

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{D} & \frac{A_{21}}{D} \\ \frac{A_{12}}{D} & \frac{A_{22}}{D} \end{pmatrix} = \begin{pmatrix} \frac{5}{9} & \frac{-3}{9} \\ \frac{-2}{9} & \frac{3}{9} \end{pmatrix}.$$

Перевіримо, чи виконується умова $A \cdot A^{-1} = E$, де E – квадратна одинична матриця.

За правилом перемножування матриць, елемент, який розміщено в i-тому рядку й j-тому стовпці матриці добутку, дорівнює сумі добутків відповідних елементів i-того рядка матриці A та j-того стовпця матриці A^{-1}.

$$A \cdot A^{-1} = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} \frac{5}{9} & \frac{-3}{9} \\ \frac{-2}{9} & \frac{3}{9} \end{pmatrix} = \begin{pmatrix} 3\frac{5}{9} - 3\frac{2}{9} & 3\left(\frac{-3}{9}\right) + 3\frac{3}{9} \\ 2\frac{5}{9} - 5\frac{2}{9} & 2\left(\frac{-3}{9}\right) + 5\frac{3}{9} \end{pmatrix} = \begin{pmatrix} \frac{15-6}{9} & \frac{9-9}{9} \\ \frac{10-10}{9} & \frac{15-6}{9} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Отже, можна дійти висновку, що обернену матрицю знайдено правильно.

4 Зведення оберненої матриці за модулем 26.

$$A^{-1} \bmod 26 = \begin{pmatrix} \frac{5}{9} & \frac{-3}{9} \\ \frac{-2}{9} & \frac{3}{9} \end{pmatrix} \bmod 26 = \begin{pmatrix} \frac{135}{9} & \frac{153}{9} \\ \frac{180}{9} & \frac{81}{9} \end{pmatrix} \bmod 26 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}.$$

Нотатка: число 135 – це результат пушуку числа, яке дає залишок 5 за модулем 26. При цьому виконується додаткова умова – знайдене число повинно ділитися на 9 без залишку. Аналогічно здобуваються числа 153, 180, 81.

5 Зашифровування відкритого повідомлення.

Зашифровування здійснюється за допомогою рівняння $A \cdot P = C$, де A – матриця перетворення; P – вектор, компонентами якого є номери літер відкритого повідомлення відповідно до табл. 1; C – вектор, компонентами якого є номери літер закритого повідомлення відповідно до табл. 1.

Приклад

Зашифруємо слово HELP.

Спочатку розіб'ємо *n*-граму відкритого тексту на біграми. Потім у кожній біграмі відкритого тексту замінимо кожну літеру на її числовий еквівалент відповідно до табл..1.

Вихідне повідомлення HELP визначає два вектори:

$$P_1 = \begin{pmatrix} H \\ E \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad \text{та} \quad P_2 = \begin{pmatrix} L \\ P \end{pmatrix} = \begin{pmatrix} 11 \\ 15 \end{pmatrix};$$

$$C_1 = A \cdot P_1 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \cdot 7 + 3 \cdot 4 \\ 2 \cdot 7 + 5 \cdot 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} 33 \\ 34 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 8 \end{pmatrix};$$

$$C_2 = A \cdot P_2 = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 3 \cdot 11 + 3 \cdot 15 \\ 2 \cdot 11 + 5 \cdot 15 \end{pmatrix} \bmod 26 = \begin{pmatrix} 78 \\ 97 \end{pmatrix} \bmod 26 = \begin{pmatrix} 0 \\ 19 \end{pmatrix}.$$

Отже, здобули послідовність чисел 7, 8, 0, 19.

З табл.2.1 дістаємо криптотекст HIAT.

Процес розшифровування йде за зворотним алгоритмом.

$$P_1 = A^{-1} \cdot C_1 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 15 \cdot 7 + 17 \cdot 8 \\ 20 \cdot 7 + 9 \cdot 8 \end{pmatrix} \bmod 26 = \begin{pmatrix} 241 \\ 212 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix};$$

$$P_2 = A^{-1} \cdot C_2 = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 15 \cdot 0 + 17 \cdot 19 \\ 20 \cdot 0 + 9 \cdot 19 \end{pmatrix} \bmod 26 = \begin{pmatrix} 323 \\ 171 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 15 \end{pmatrix}.$$

Здобута цифрова послідовність 7, 4, 11, 15 відповідно до табл. 2.1 надає можливість відновити вихідний текст: HELP.

Лекція 19

Тема: **Сучасні симетричні криптосистеми. Стандарт шифрування DES**

1 Сучасні симетричні криптосистеми

На думку К.Шеннона, в практичних шифрах необхідно використовувати два загальних принципи: ***розсіювання*** та ***перемішування*** [**Ошибка! Закладка не определена.**].

Розсіювання представляє собою розповсюдження впливу одного знаку відкритого тексту на багато знаків шифротексту, що дозволяє приховати статистичні властивості відкритого тексту.

Перемішування передбачає використання таких шифруючих перетворень, які ускладнюють відновлення взаємозв'язку статистичних властивостей відкритого та шифрованого текстів. Проте шифр повинен не тільки ускладнювати розкриття, а й забезпечувати легкість шифрування та розшифровування при відомому користувачеві секретному ключі.

Розповсюдженим способом досягнення ефектів розсіювання та перемішування є використання ***складового шифру*** – шифру, який реалізований у вигляді деякої послідовності простих шифрів, кожний з яких вносить свій вклад у значне сумарне розсіювання та перемішування. У складових шифрах в якості простих шифрів найчастіше використовуються прості перестановки та підстановки.

При ***перестановці*** просто перемішують символи відкритого тексту, причому конкретний вид перемішування визначається секретним ключем.

При ***підстановці*** кожний символ відкритого тексту заміняють іншим символом з того ж алфавіту, а конкретний вигляд підстановки також визначається секретним ключем. Слід зазначити, що в сучасних блочних шифрах блоки відкритого тексту та шифротексту являють собою двійкові послідовності зазвичай довжиною 64 біти. В принципі кожний блок може набувати 2^{64} значень. Тому підстановки виконуються в надзвичайно великому алфавіті, що містить до $2^{64} \approx 10^{19}$ „символів".

При багаторазовому чергуванні простих перестановок та підстановок, що управляються достатньо довгим секретним ключем, можна отримати дуже стійкий шифр з добрим розсіюванням та перемішуванням. Розглянуті далі симетричні криптоалгоритми побудовані у повній відповідності до вказаної методології.

2 Стандарт шифрування даних DES

Стандарт шифрування даних ***DES*** (***Data Encryption Standard***) опубліковано в 1977 році Національним бюро стандартів США. Стандарт DES призначений для захисту від несанкціонованого доступу до важливої, але не секретної інформації в державних та комерційних організаціях США. Алгоритм, покладений в основу стандарту, розповсюджувався досить швидко, і уже в 1980 році був схвалений Національним інститутом стандартів і технологій США.

До нашого часу DES є найбільш розповсюдженим алгоритмом, що використовується в системах захисту комерційної інформації. Більше того, реалізація алгоритму DES в таких системах вважається ознакою хорошого тону.

Він став першим доступним всім бажаючим офіційним алгоритмом і першим світовим стандартом, що проіснував більше 20. Тому його слід відмітити як найважливішу віху на шляху криптографії від чисто військового використання до широкомасштабного застосування.

Головні риси шифру DES визначаються тим, що він ґрунтується на схемі Фейстеля з такими параметрами:

довжина блоку – 64 біти,

кількість раундів – 16,
розмір ключа – 56 бітів,
розмір кожного з підключів k1, k2, …, k16 – 48 бітів.

Наведемо основні переваги алгоритму DES:

- використовується тільки один ключ довжиною 56 біт;
- зашифрувавши повідомлення за допомогою одного пакету програм, для розшифровування можна використовувати будь-який інший пакет програм, який відповідає стандарту DES;
- відносна простота алгоритму забезпечує високу швидкість обробки;
- достатньо висока стійкість алгоритму.

Спочатку метод, який покладено в основу стандарту DES, було розроблено фірмою IBM для своїх потреб і реалізовано у вигляді системи „Люцифер“.

Система „Люцифер“ базується на комбінуванні методів підстановки та перестановки і складається з послідовності блоків перестановки та підстановки, які чергуються один з одним. У них використовувався ключ довжиною 128 біт, який управляв станом блоків перестановки та підстановки.

Система „Люцифер“ виявилася досить складною для практичної реалізації із-за відносно низької швидкості шифрування (2190 байт/с – програмна реалізація, 96970 байт/с – апаратна реалізація).

Алгоритм DES також використовує комбінацію підстановок та перестановок. DES здійснює шифрування 64-бітових блоків даних за допомогою 64-бітового ключа, в якому значущими є 58 біт (решта 8 біт – перевірочні біти, призначені для контролю на парність).

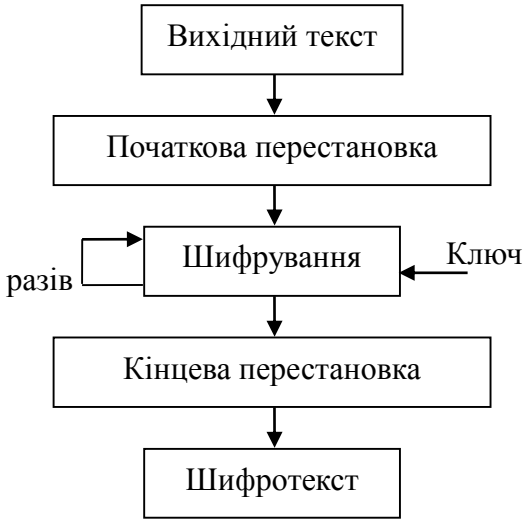


Рисунок 1 - Узагальнена схема шифрування в алгоритмі DES

Дешифрування в DES є операцією, оберненою до шифрування, яка виконується шляхом повторень операцій шифрування в оберненому порядку. Узагальнена схема процесу шифрування в алгоритмі DES представлена на рис. 1. Процес шифрування полягає в початковій перестановці біт 64-бітного блоку, шістнадцяти циклах шифрування та, нарешті, в кінцевій перестановці бітів.

Основні режими роботи алгоритму DES.

Алгоритм DES повністю підходить як для шифрування, так і для автентифікції даних. Він дозволяє безпосередньо перетворювати 64-бітний вхідний відкритий текст у 64-бітний шифрований текст, однак дані рідко обмежуються 64 розрядами. Для того, щоб скористатися алгоритмом DES для розв'язання різноманітних криптографічнихзадач, розроблено 4 робочих режими:

- електронна кодова книжка ECB (Electronic Code Book);
- зчеплення блоків шифру CBC (Cipher Block Chaining);
- обернений зв'язок по шифротексту CFB (Cipher Feed Back);
- обернений зв'язок по виходу OFB (Output Feed Back).

У режимі „***Електронна кодова книжка***" довгий файл розбивають на 64-бітні відрізки (блоки) по 8 байт. Кожний з цих блоків шифрується незалежно з використанням одного і того ж ключа шифрування. Основною перевагою є простота реалізації. Недоліком – відносно слабка стійкість проти кваліфікованих криптоаналітиків. Із-за фіксованого характеру шифрування при обмеженій довжині блоку в 64 біти можливе проведення криптоаналізу зі „словником". Блок такого розміру може повторитися в повідомленні внаслідок великої надлишковості в тексті на звичайній мові. Це приводить до того, що ідентичні блоки відкритого тексту в повідомленні будуть представлені ідентичними блоками шифротексту, що дає криптоаналітику деяку інформацію про зміст повідомлення.

У режимі „***Зчеплення блоків шифру***" вихідний файл M розбивається на 64-бітові блоки: $M=M_1M_2...M_n$. Перший блок M_1 сумується за модулем 2 з 64-бітним початковим вектором IV, який змінюється щоденно і тримається в секреті. Отримана сума потім шифрується з використанням ключа DES, відомого і відправнику і отримувачу інформації. Отриманий 64-бітний шифр C_1 сумується за модулем 2 з другим блоком тексту, результат шифрується і отримується другий 64-бітний шифр C_2, і т.д. Процедура повторюється до того часу, поки не будуть оброблені усі блоки тексту.

Таким чином, для всіх i=1...n (n – кількість блоків) результат шифрування C_i визначається наступним чином:

$$C_i=\mathrm{DES}(M_i \oplus C_{i-1}),$$

де C_0=IV – початкове значення шифру, яке рівне початковому вектору (вектору ініціалізації).

Очевидно, що останній 64-бітний блок шифротексту є функцією секретного ключа, початкового вектора та кожного біту відкритого тексту незалежно від його довжини. Цей блок шифротексту називають ***кодом автентифікації повідомлення*** (КАП).

Код КАП може бути легко перевірений отримувачем, що володіє секретним ключем та початковим вектором шляхом повторення процедури, виконаної відправником. Зловмисник, проте, не може генерувати КАП, який сприймався б отримувачем як справжній, щоб додати його до несправжнього повідомлення, або ж відділити КАП від справжнього повідомлення для його використання зі зміненим чи несправжнім повідомленням.

Перевагою даного режиму є ще й той факт, що він не дозволяє накопичуватися помилкам при передачі. Блок M_i є функцією тільки C_{i-1} та C_i, завдяки чому помилка при передачі приведе до втрати тільки двох блоків вихідного тексту.

Режим „***Обернений зв'язок по шифру***". В цьому режимі розмір блоку може відрізнятися від 64 біт. Файл, який потрібно зашифрувати (розшифрувати), зчитується послідовними

блоками довжиною k біт (k=1...64). Вхідний блок (64-бітний регістр зсуву) спочатку містить вектор ініціалізації, вирівняний по правому краю.

Нехай в результаті розбиття на блоки ми отримали n блоків довжиною k біт кожен (залишок доповнюється нулями чи пропусками). Тоді для довільного i=1...n блок шифротексту

$$C_i=M_i \oplus P_{i-1},$$

де P_{i-1} означає k старших бітів попеерднього зашифрованого блоку.

Оновлення регістру зсуву здійснюється шляхом вилучення його старших k біт та запису C_i в регістр. Відновлення зашифрованих даних також виконується відносно просто: P_{i-1} та C_i вираховуються аналогічним чином і

$$M_i= C_i \oplus P_{i-1}.$$

Для кращого розуміння описаного алгоритму на рис. 2 представлена його структурна схема.

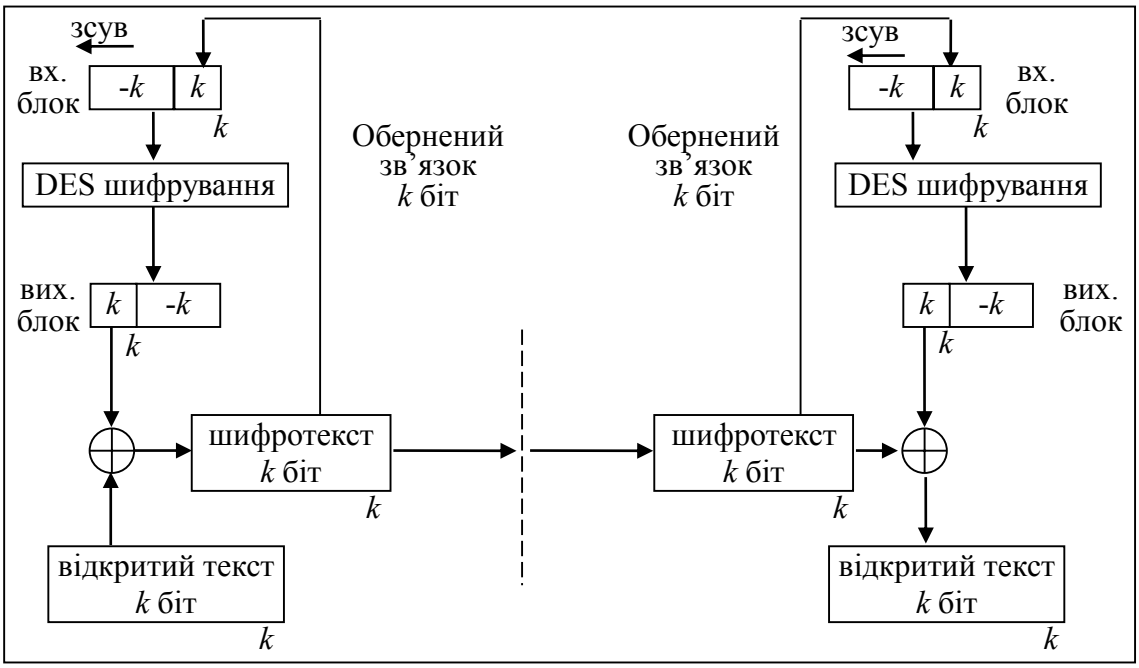


Рисунок 2 - Схема алгоритму DES в режимі оберненого зв'язку по шифротексту

Режим „***Обернений зв'язок по виходу***" використовує змінний розмір блоку та регістр зміщення, що ініціалізується так само, як і в режимі оберненого зв'язку по шифротексту, а саме – вхідний блок спочатку містить вектор ініціалізації IV, вирівняний по правому краю, рис. 3.

При цьому для кожного сеансу шифрування даних необхідно використовувати новий початковий стан регістру, який повинен пересилатися по каналу відкритим текстом. Відмінність від режиму оберненого зв'язку по шифротексту полягає у методі обновлення регістру зміщення. Це здійснюється шляхом відкидання старших k біт та дописування справа P_i.

Галузі застосування алгоритму DES. Кожному з розглянутих режимів (ECB, CBC, CFB, OFB) притаманні свої переваги та недоліки, що зумовлює галузі їх застосування. Режим ECB добре підходить для шифрування ключів; режим CFB, як правило, призначається для

шифрування окремих символів, а режим OFB часто застосовується для шифрування в супутникових системах зв’язку.

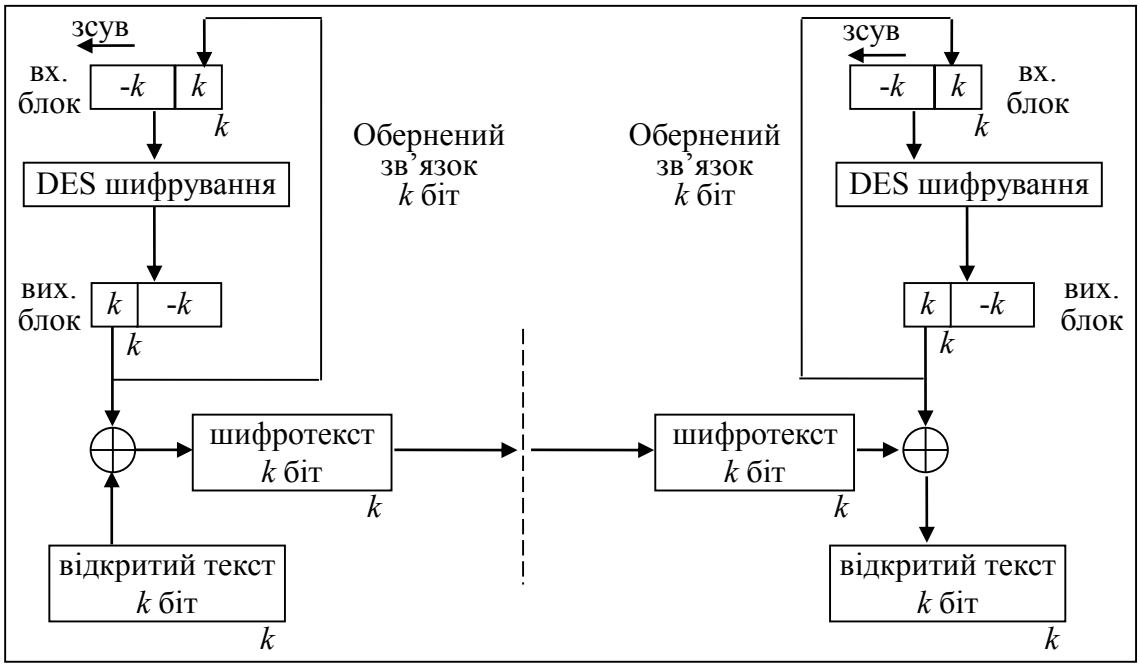


Рисунок 3 - Схема алгоритму DES в режимі оберненого зв’язку по виходу

Режими CBC та CFB ефективні для автентифікації даних. Ці режими дозволяють використовувати алгоритми DES для:

- інтерактивного шифрування при обміні даними між терміналом та головною ЕОМ;
- шифрування криптографічного ключа у практиці автоматизованого розповсюдження ключів;
- шифрування файлів, поштових повідомлень, даних супутників та інших практичних задач.

З самого початку стандарт DES призначався для шифрування та розшифровування даних ЕОМ. Проте його застосування було поширене і на автентифікацію. В системах автоматичної обробки даних людина не в змозі переглянути дані, щоб встановити, чи не внесено в них змін. При величезних об’ємах даних, що опрацьовуються в сучасних інформаційних системах, перегляд даних зайняв би надто багато часу. До того ж надлишковість даних може бути недостатньою для виявлення помилок. Навіть у тих випадках, коли перегляд людиною можливий, дані можуть бути змінені таким чином, що виявити такі зміни людиною буде дуже складно, наприклад „1900 грн.“ може бути змінено на „9100 грн.“. Без додаткової інформації людина при перегляді може легко прийняти змінені дані за істинні. Такі небезпеки можуть існувати навіть при використанні шифрування даних. Тому бажано мати автоматичний засіб виявлення зловмисних та незловмисних змін даних.

Звичайні коди, що виявляють помилки, тут є непридатними, оскільки алгоритм утворення коду відомий і зловмисник може генерувати правильний код після внесення змін у дані. Однак за допомогою алгоритму DES можна генерувати криптографічну контрольну суму, яка може захистити як від випадкових, так і від зловмисних несанкціонованих змін даних. Цей процес описує стандарт для автентифікації даних ЕОМ (FIPS 113).

Суть стандарту полягає в тому, що дані зашифровуються в режимі оберненого зв'язку по шифротексту (режим CFB) чи в режимі зчеплення блоків шифру (режим CBC), в результаті чого отримується кінцевий блок шифру, який представляє собою функцію усіх розрядів відкритого тексту. Після цього повідомлення, що містить відкритий текст, може бути передане разом з розрахованим кінцевим блоком шифру, який виконує роль криптографічної контрольної суми.

Одні і ті ж дані можна захистити, використовуючи як шифрування, так і автентифікацію. Дані захищаються від ознайомлення шифруванням, а зміни виявляються засобами автентифікації. Алгоритм автентифікації можна застосовувати як до відкритого так і до зашифрованого тексту.

Шифрування та автентифікацію застосовують для захисту даних, що зберігаються в ЕОМ. В багатьох операційних системах та прикладних програмах паролі зашифровуються незворотним чином і зберігають в пам'яті ЕОМ. Коли користувач звертається до програми і вводить пароль, останній зашифровується та порівнюється зі значенням, що зберігається в пам'яті. Тільки якщо обидві зашифровані величини співпадають, користувач отримує доступ до комп'ютера. Часто зашифрований пароль генерується за допомогою алгоритму DES, причому ключ береться рівним паролю, а відкритий текст – коду ідентифікації користувача. За допомогою алгоритму DES можна також шифрувати файли для їх надійного зберігання. Одним із найважливіших застосувань алгоритму DES є захист повідомлень електронних платіжних систем при операціях з клієнтами та між банками.

Комбінування блочних алгоритмів. В даний час блочний алгоритм DES вважається відносно безпечним алгоритмом шифрування. Він піддавався ретельному криптоаналізу на протязі більше 20 років і найпрактичнішим способом його зламування є метод перебору усіх варіантів ключа. Ключ DES має довжину 56 біт, у зв'язку з чим існує 2^{56} можливих варіантів такого ключа. Якщо припустити, що суперкомп'ютер зможе перебирати мільйон варіантів ключа за секунду, то знадобиться 2285 років для знаходження правильного ключа. Проте нескладно уявити, що при постійному прогресі можливостей комп'ютерної техніки недалекий той час, коли комп'ютери, здатні виконувати такий перебір за значно менший час, стануть доступними для користувачів.

Тому виникає питання про те, чи не можна використати DES в якості будівельного блоку для створення іншого алгоритму з ключем більшого розміру? В принципі існує багато способів комбінування блочних алгоритмів для отримання нових алгоритмів. Одним з таких способів комбінування є багаторазове шифрування – використання блочного алгоритму декілька разів з різними ключами для шифрування одного і того ж блоку відкритого тексту. Двократне шифрування блоку відкритого тексту одним і тим же ключем не приводить до позитивного результату. При використанні одного і того ж алгоритму таке шифрування не впливає на складність криптоаналітичної атаки повного перебору.

При використанні двократного шифрування блоку відкритого тексту за допомогою двох різних ключів замість 2^n спроб, де n – довжина ключа в бітах, знадобиться 2^{2n} спроб. Зокрема, якщо n=64, то двократно зашифрований блок тексту потребує 2^{128} спроб для знаходження ключа. Проте У. Діффі та М. Хеллман показали на прикладі DES, що використовуючи метод „обміну часу на пам'ять" та криптоаналітичну атаку „зустріч посередині", можна зламати таку систему двократного шифрування за 2^{n+1} спроб [i]. Хоча така атака потребує дуже великого об'єму пам'яті (для алгоритму з 56-бітовим ключем знадобиться 2^{56} 64-бітових блоків чи 10^{17} біт (біля 11368 терабайт) пам'яті).

Більш привабливу ідею запропонував У. Тачмен, суть якої полягає в тому, щоб шифрувати блок відкритого тексту P три рази за допомогою двох ключів K_1 та K_2 [ii]. Процедура шифрування виглядає так:

$$C=E_{K1}(D_{K2}(E_{K1}(P))).$$

Тут блок відкритого тексту P спочатку шифрується ключем K_1, потім розшифровується ключем K_2 і знову зашифровується ключем K_1.

Цей режим іноді називають режимом EDE (encrypt-decrypt-encrypt). Включення в дану схему операції розшифровування D_{K2} дозволяє забезпечити сумісність цієї схеми зі схемою однократного використання алгоритму DES. Якщо в цій схемі вибрати два ключі однаковими, то вона перетворюється в схему однократного використання DES. Процедура розшифровування здійснюється в оберненому порядку:

$$P=D_{K1}(E_{K2}(D_{K1}(C))).$$

Якщо вихідний блочний алгоритм має n-бітний ключ, то схема трьохкратного шифрування має $2n$-бітний ключ. Чергування ключів K_1 та K_2 дозволяє уникнути криптоаналітичної атаки „зустріч посередині". Дана схема наводиться в міжнародних стандартах X9.17 та ISO 8732 в якості засобу покращення характеристик алгоритму DES.

При трьохкратному щифруванні можна застосовувати три різні ключі. При цьому зростає загальна довжина результуючого ключа. Процедури шифрування та розшифровування описуються виразами:

$$C=E_{K3}(D_{K2}(E_{K1}(P)));$$

$$P=D_{K1}(E_{K2}(D_{K3}(C))).$$

Трьохключовий варіант має ще більшу стійкість. Очевидно, що якщо потрібно підвищити безпеку великого парку обладнання, що використовує DES, то значно дешевше переключитися на схеми трьохкратних DES, ніж переходити на інший тип криптосхем.

Лекція 20

Тема: **Алгоритм шифрування даних IDEA**

Теоретичні відомості:

Алгоритм ***IDEA*** (***International Data Encryption Algorithm***) є блочним шифром. Він оперує 64-бітовими блоками відкритого тексту. Цей алгоритм передбачає попереднє розділення вихідної послідовності на *64*-х розрядні блоки, які шифруються за допомогою *128*-и бітового ключа. Безсумнівною перевагою алгоритму IDEA є те, що його ключ має довжину 128 біт. Для шифрування і розшифровування використовується один і той же алгоритм. Алгоритм побудований на основі мережі Фейстеля (рис.1). Алгоритм шифрування зворотний.

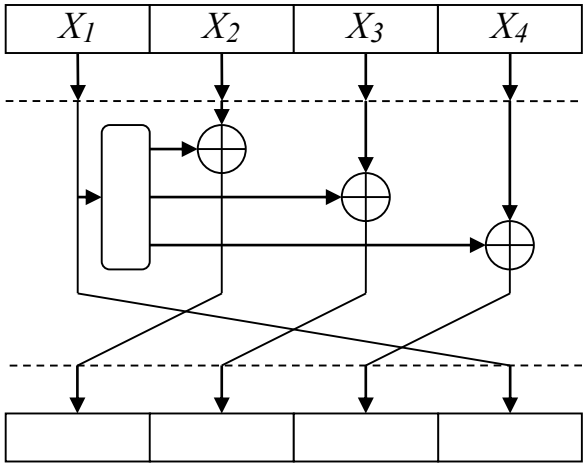


Рисунок 1- Приклад схеми Фейстеля
з чотирма гілками

Перша версія алгоритму IDEA була запропонована в 1990 році С. Лайєм та Дж. Массі. Спочатку алгоритм називався PES (Proposed Encryption Standard). Покращений варіант цього алгоритму, розроблений в 1991 році, отримав назву IPES (Improved Proposed Encryption Standard). В 1992 році назву було змінено на IDEA. Як і більшість інших блочних алгоритмів,

алгоритм IDEA використовує при шифруванні процеси змішування та розсіювання, причому усі процеси легко реалізуються апаратними та програмними засобами.

В алгоритмі IDEA використовуються наступні математичні операції:

– порозрядне сумування за модулем 2 (операція „виключаюче АБО“); операція позначається як $\oplus$;

– додавання беззнакових цілих за модулем 2^{16} (модуль 65536); операція позначається як $\boxplus$;

– множення цілих за модулем $(2^{16}+1)$ (модуль 65537), які розглядаються як беззнакові цілі, за виключенням того, що блок із 16 нулів розглядається як 2^{16}; операція позначається як $\odot$;

Усі операції виконуються над 16-бітними субблоками. Розглянуті три операції несумісні в тому змісті, що:

– ніяка пара з цих трьох операцій не задовольняє асоціативному закону, наприклад $a\boxplus(b\oplus c)\neq(a\boxplus b)\oplus c$;

– ніяка пара з цих трьох операцій не задовольняє дистрибутивному закону, наприклад $a\boxplus(b\odot c)\neq(a\boxplus b)\odot(a\boxplus c)$.

Комбінування цих трьох операцій забезпечує комплексне перетворення входу, суттєво ускладнюючи криптоаналіз IDEA, порівняно з DES, який базується виключно на операції „виключаюче АБО“.

Всі перелічені операції виконуються з *16*-ти бітовими блоками.

Спочатку *64*–х - розрядний блок розбивається на чотири *16*-ти - розрядних підблока X_1, X_2, X_3 та X_4, які є вхідними даними для алгоритма. Усього алгоритм передбачає виконання восьми етапів.

На кожному етапі чотири підблока піддаються операціям додавання (по модулю два), додавання (по модулю 2^{16}) та множення (по модулю $2^{16}+1$) кожен з кожним та з *6*-бітовими *16*-ти ключами.

Кожний етап передбачає виконання наступних операцій:

1. Помножуються X_1 і перший підключ.
2. Виконується додавання за модулем 2^{16} X_2 та другого підключа.
3. Виконується додавання за модулем 2^{16} X_3 та третього підключа.
4. Помножуються X_4 і четвертий підключ.
5. Виконується додавання за модулем два результатів (1) та (3) кроків.
6. Виконується додавання за модулем два результатів (2) та (4) кроків.
7. Помножуються результати кроку (5) та п`ятий підключ.
8. Додавання за модулем 2^{16} результатів (6) та (7) кроків.
9. Помножуються результати кроку (8) та шостий підключ.
10. Виконується додавання за модулем 2^{16} результати (7) та (9) кроків.
11. Виконується додавання за модулем два результатів (1) та (9) кроків.

12. Виконується додавання за модулем два результатів (3) та (9) кроків.
13. Виконується додавання за модулем два результатів (2) та (10) кроків.
14. Виконується додавання за модулем два результатів (4) та (10) кроків.

Вихідом цикла являються чотири підблока, які одержуються як результат виконання останніх чотирьох кроків алгоритма шифрування. Цикл шифрування завершується перестановкою двох внутрішніх блоків (за виключенням останнього цикла). Таким чином, формуються входи для наступного цикла.

По закінченні останнього восьмого цикла, виконується вихідне перетворення:

1. Помноження першого підблока X_1 та першого підключа K_1.
2. Додавання за модулем 2^{16} другого підблока X_2 та другого підключа K_2.
3. Додавання за модулем 2^{16} третього підблока X_3 та третього підключа K_2.
4. Помноження четвертого підблока X_4 та першого підключа K_4.

Отримані після виконання оціх чотирьох операцій результати Y_1, Y_2, Y_3 та Y_4 знову об`єднуються, створюючи шифрблок.

Таким чином: Алгоритм шифрування *IDEA* передбачає використання *52*-х ключів (по шість для кожного із восьми циклів та ще чотирьох для формування вихідного блока). Спочатку *128*-и бітовий ключ розбивають на вісім *16*-ти бітових підключей, шість із яких використовується в першому циклі, а два залишаються для наступного циклу. Потім *128*-и бітовий ключ зсовують на *25* біт вліво та знову ділять на вісім ключей. Перші чотири з них використовують у другому циклі, останні чотири – у третьому циклі. Потім формування наступних ключів виконується аналогічно до завершення алгоритму.

Процес розшифровування супроводжується генерацією ключів в зворотному порядку, причому деякі з них змінюються зворотними величинами.

Алгоритм IDEA може працювати в будь-якому режимі блочного шифру, передбаченому для алгоритму DES. Алгоритм IDEA має ряд переваг, порівняно з алгоритмом DES. Він є значно безпечнішим алгоритму DES, оскільки 128-бітний ключ алгоритму IDEA вдвічі більше ключа DES. Внутрішня структура алгоритму IDEA забезпечує кращу стійкість до криптоаналізу. Існуючі програмні реалізації алгоритму IDEA працюють практично вдвічі швидше реалізацій алгоритму DES. Алгоритм IDEA запатентовано в Європі та США.

Лекція 21

Тема: **Керування криптографічними ключами**

Крім вибору криптографічної системи, найважливішою є проблема керування ключами.

Ключова інформація – це сукупність усіх ключів, які діють в інформаційній системі (ІС).

Якщо не забезспечено надійне керування *ключовою інформацією*, то при її перехопленні, злочинник має необмеженний доступ до всієї інформації.

Керування ключами – це інформаційний процес, який містить в собі три елемента:
генерацію ключів;
накопичування ключів;
розподілення ключів.

Розглянемо, як вони мають реалізовуватися для того, щоб забезпечити безпеку ключової інформації в ІС.

Генерація ключів

Перш за все треба сказати, що не слід використовувати невипадкові ключі, щоб їх було легше запам'ятати.

В ІС використовують спеціальні апаратні та програмні засоби генерування випадкових ключів. Звичайно застосовують давачі псевдовипадкових чисел (ПВЧ). Однак степень випадковості їхньої генерації повинна бути дуже великою. Ідеальними генераторами є пристрої на базі „натуральних" випадкових процесів. В ІС з середніми вимогами щодо захищенності, використовуються програмні генератори ключів, що обчислюють ПВЧ, як функцію від часу та (чи) числа, що вводиться користувачем.

Накопичування ключів

Накопичування ключів - це організація процесу зберження, обліку та вилучання ключів.

Ключ – це самий бажаний об'єкт для злочинника, тому що він дає змогу одержати доступ до конфіденційної інформації. Тому питанням накопичування ключів слід приділяти особливу увагу.

Секретні ключі завжди треба зберігати у зашифровуванному вигляді.

Ключі, які зашифровують ключову інформацію звуться *майстер-ключами*. Треба, щоб майстер-ключі кожен користувач знав напам'ять, та не зберігав їх на яких- небудь носіях.

Дуже важно для забезпечення безпеки інформації, щоб ключова інформація в ІС регулярно змінювалася. При цьому змінюватися повинні, як звичайні ключі, так і майстер-ключі.

Розподілення ключів

Розподілення ключів – найвідповідальніший процес керування ключами. До нього пред'являють наступні вимоги:
Оперативність та точність розподілення
Таємність розподілення ключів.

Розподілення ключів між користувачами зреалізовуються двома методами:
Шляхом побудови одного чи кількох центрів розподілення ключів (ЦРК). Недоліком є те, що в ЦРК відомо кому та які ключі призначені. Це дає змогу читати усі повідомлення, які є в ІС. Це впливає на захист системи від злочинних дій.
Прямой обмін ключами між користувачами ІС.
Тут проблема в тому, щоб ідентифікувати та перевіріти дійсність користувачів.

В обох випадках треба, щоб була гарантована дійсність сеансу зв'язку. Це можна забезпечити двома способами:
Механізм запиту-відповіді. Якщо користувач *A* хоче бути впевненним, що повідомлення, які він одержує від *B*, не є спотворенними, він додає в повідомлення деякий елемент, що є випадковим (запит). При відповіді користувач *B* має виконати деяку операцію з цим елементом (наприклад, додати 1). Це неможна зробити раніше, тому що не відомо яке випадкове число буде в запиті.

Після того, як відповідь, що містить результати дій, одержана, користувач *A* може бути впевненним, що сеанс зв'язку є дійсним. Недоліком цього методу є змога встановлення закономірності між запитом та відповіддю.

Механізм відзначення часу ("часовий штемпель"). Суть є в тому, що фіксується час кожного повідомлення. В цьому разі кожний користувач ІС може знати коли надійшло повідомлення.

В обох випадках слід використовувати шифрування, щоб бути впевненним, що відповідь надіслав не злочинник та штемпель відзначення часу не змінили.

При використанні механізму відзначення часу є проблема припустимого часу інтервалу затримки для підтвердження дійсності сеансу. Повідомлення, що має "часовий штемпель", не може бути отримано миттєво. Крім того, годинники, що є у комп'ютерах передавача та отримувача не можуть бути абсолютно синхронними. Яке запізнювання "часового штемпеля" є припустимим?

Тому в реальних ІС, приміром, в системах платежів кредитних карток використовується саме механізм встановлення дійсності та захисту від підробок. Інтервал відзначення часу складає від однієї до кількох хвилин. Багато відомих способів крадіжок електронниї грошей базується на "вклинюванні" в цей проміжок часу невірних запитів при зніманні грошей.

Для обміну ключами можна використовувати криптосистеми з відкритим ключем за допомогою алгоритму RSA.

Проте дуже ефективним з'явився алгоритм Диффі-Хелмана, який дає змогу двом користувачам, без посередників, обмінюватися ключем, що може потім використовуватися для симетричного шифрування.

Таким чином, керування ключами є зведенням до пошуку такого протоколурозподілення ключів, який забезпечив би:

змогу відмовитися від центру розподілу ключів;

взаємне підтвердження дійсності користувачів;

підтвердження дійсності сеансу за допомогою механізму відзначення часу механизмом, використання для цього програмних чи аппаратних засобів;

використання при обміні ключами миінімального числа повідомлень.

Асиметричні криптосистеми

Лекція 22

Концепція криптосистем з відкритим ключем.

Передумови виникнення асиметричних систем

Традиційні криптографічні системи мають два суттєвих недоліки:

- Проблема розподілення ключів в управління ними. Система з n учасниками вимагає використання n/2 ключів і стільки ж безпечних каналів для їх розповсюдження. При зміні ключа одним з учасників доводиться генерувати і розподіляти (n-1) ключ. А додавання нового учасника вимагає генерування і розподілення n нових ключів.

- Проблема автентифікації. Традиційні криптосистеми не забезпечують потребу користувачів у використанні електронного еквіваленту підпису: будь-яке повідомлення, що відправлене одним з них, може бути відправлене і іншим. Намагання усунути ці недоліки

спонукало дослідників до пошуку криптографічних систем нового типу. Ідея такої системи була опублікована в 1976 р. у піонерській роботі У. Діффі і Д.Хеллмана «Нові напрями в криптографії». Криптографічні системи нового типу отримали назву криптосистем з публічними ключами або асиметричних криптосистем. Наведемо приклади проблем, які вирішуються за допомогою асиметричних систем.

- Проблема зберігання паролів на комп'ютері. Якщо зберігати паролі на магнітному диску, то зловмисник може прочитати їх і використати для несанкціонованого доступу. Тому необхідно організувати зберігання паролів на диску так, щоб унеможливити таке зчитування.

- Проблема радіолокації в ППО. При перетині літаком кордону у нього запитується пароль. Зловмисник може перехопити пароль і використати його для нелегального перетину кордону.

- Проблема віддаленої взаємодії. Так, при взаємодії банка з клієнтом на початку сеансу банк запитує клієнта ім'я і секретний пароль, який при використанні відкритого каналу зв'язку також може бути перехоплений [35]

Ефективними системами криптографічного захисту даних є асиметричні криптосистеми, які також називають криптосистемами з відкритим ключем. В таких системах для зашифровування даних використовується один ключ, а для розшифровування – інший ключ (звідси і назва – асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним. Зрозуміло, що ключ розшифровування не може бути визначеним з ключа зашифровування.

Узагальнена схема асиметричної криптосистеми з відкритим ключем наведена на рис. 1

В цій криптосистемі застосовують два різних ключі: K_B – відкритий ключ відправника A; k_B – секретний ключ отримувача B. Генератор ключів доцільно розміщувати на стороні отримувача B (щоб не пересилати секретний ключ k_B по незахищеному каналу). Значення ключів K_B та k_B залежать від початкового стану генератора ключів. Розкриття секретного ключа k_B за відомим відкритим ключем K_B повинно бути задачею, яку неможливо розв'язати розрахунковими методами.

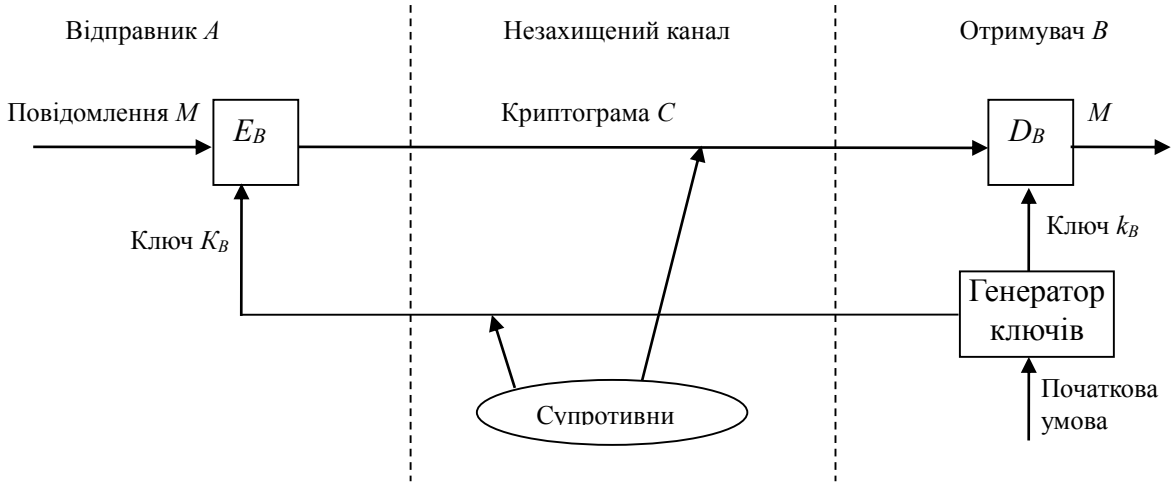


Рисунок 1 - Узагальнена схема асиметричної криптосистеми з відкритим ключем

Наведемо характерні особливості асиметричних криптосистем:

1. Відкритий ключ K_B та криптограма C можуть бути відправлені по незахищеним каналам (супротивнику відомі K_B та C).
2. Алгоритми шифрування та розшифровування

$$E_B: M \to C,$$
$$D_B: C \to M$$

є відкритими.

Захист інформації в асиметричній криптосистемі базується на секретності ключа k_B. У. Діффі та М. Хелман сформулювали вимоги, виконання яких забезпечує безпеку асиметричної криптосистеми:

1. Генерація пари ключів (K_B, k_B) отримувачем B на основі початкової умови повинна бути простою.
2. Відправник A, знаючи відкритий ключ K_B та повідомлення M, може легко генерувати криптограму

$$C = E_{K_B}(M) = E_B(M).$$

3. Отримувач B, використовуючи секретний ключ k_B та криптограму C, може легко відновити вихідне повідомлення

$$M = D_{K_B}(C) = D_B(C) = D_B[E_B(M)].$$

4. Супротивник, знаючи відкртий ключ K_B, при спробі вирахувати секретний ключ k_B наштовхується на нездоланну обчислювальну проблему.
5. Супротивник, знаючи пару (K_B, C), при спробі розшифрувати вихідне повідомлення M наштовхується на нездоланну обчислювальну проблему.

Однонаправлені функції. Концепція асиметричних криптографічних систем з відкритим ключем базується на застосуванні однонаправлених функцій. Неформально однонаправлену функцію можна визначити наступним чином. Нехай X та Y – довільні множини. Функція

$$f: X \to Y$$

є однонаправленою, якщо для всіх $x \in X$ можна легко обчислити функцію

$$y = f(x), \text{ де } y \in Y.$$

І в той же час для більшості $y \in Y$ досить складно отримати значення $x \in X$, таке, що $f(x)=y$ (при цьому вважають, що існує по крайній мірі одне таке значення x). Основним критерієм віднесення функції f до класу однонаправлених функцій є відсутність ефективних алгоритмів оберенного перетворення $Y \to X$.

В якості першого прикладу однонаправленої функції розглянемо цілочисельне множення. Пряма задача – розрахунок добутку двох дуже великих чисел P та Q

$$N = P*Q,$$

є відносно нескладною задачею для ЕОМ.

Обернена задача – факторизація великого цілого числа (знаходження дільників P та Q великого цілого числа $N=P*Q$), є задачею, яку практично неможливо розв'язати засобами сучасних ЕОМ при достатньо великих значеннях N. За сучасними оцінками теорії чисел при цілому $N \approx 2^{664}$ та $P \approx Q$ для факторизації числа N знадобиться біля 10^{23} операцій.

Іншим характерним прикладом однонаправленої функції є модульна експонента з фіксованими основою та модулем. Нехай A та N – цілі числа, такі, що $1 \le A \le N$. Визначимо множину Z_N:

$$Z_N = \{0,1,2,...,N-1\}.$$

Тоді модульна експонента з основою A по модулю N являє собою функцію

$$f_{A,N}: Z_N \to Z_N,$$

$$f_{A,N}(x) = A^x \pmod N,$$

де X – ціле число, $1 \le x \le N-1$.

Існують ефективні алгоритми, які дозволяють досить швидко розрахувати значення функції $f_{A,N}(x)$. Якщо $y = A^x$, то природно записати $x = \log_A(y)$. Тому задачу знаходження функції оберненої до функції $f_{A,N}(x)$ називають задачею знаходження дискретного алгоритму чи задачею дискретного логарифмування. Задача дискретного логарифмування формулюється наступним чином. Для відомих цілих A, N, y знайти ціле число x, таке, що

$$A^x \bmod N = y.$$

Алгоритм розрахунку дискретного логарифму за прийнятний час поки не знайдений. Тому модульна експонента вважається однонаправленою функцією.

За сучасними оцінками теорії чисел при цілих числах $A \approx 2^{664}$ та $N \approx 2^{664}$ розв'язання задачі дискретного логарифмування (знаходження показника степеня x для відомого y) потребує біля 10^{26} операцій – задача має в 1000 раз більшу обчислювальну складність, ніж задача розкладання на множники. При збільшенні довжини чисел різниця в оцінках складності задач зростає. Слід зазначити, що поки не вдалося довести, що не існує ефективного алгоритму обчислення дискретного логарифму за прийнятний час. У зв'язку з цим, модульна експонента віднесена до однонаправлених функцій умовно, що, проте, не заважає з успіхом застосовувати її на практиці.

Другим важливим класом функцій, що використовуються при побудові криптосистем з відкритим ключем, є так звані однонаправлені функції з „таємним ходом". Існує неформальне визначення такої функції: функція

$$f: X \to Y$$

відноситься до класу одннаправлених функцій з „таємним ходом" в тому випадку, якщо вона є однонаправленою і, крім того, можливе ефективне обчислення оберненої функції, якщо відомий „таємний хід" (секретне число, рядок тексту чи інша інформація, що асоціюється з цією функцією). Прикладом такої функції є функція, що використовується в криптосистемі RSA.

Лекція 23

Види електронних підписів в Україні

Закон України від 22 травня 2003 року N 852-IV **«Про електронний цифровий підпис»** встановлює наступні види ЕП:

1 **Простий електронний підпис (ПЕП)**

Створюється за допомогою кодів, паролів та інших інструментів. Ці засоби захисту дозволяють ідентифікувати автора підписаного документа. Важливою властивістю простого електронного підпису є відсутність можливості перевірити

документ на предмет наявності змін з моменту підписання. Прикладом простого електронного підпису є комбінація логіна і пароля.

2 **Посилений некваліфікований електронний підпис (НЕП);**

Створюється з використанням криптографічних засобів і дозволяє визначити не тільки автора документа, але перевірити його на наявність змін. Прості і посилені некваліфіковані підписи замінюють підписаний паперовий документ у випадках, обумовлених законом або за згодою сторін. Наприклад, прості підписи можуть використовувати громадяни для відправки повідомлень органам влади. Посилений підпис також може розглядатися як аналог документа з печаткою.

3 **Посилений кваліфікований електронний підпис (КЕП).**

Раніше видані сертифікати ЕЦП і підписані з їх допомогою документи прирівнюються до кваліфікованих підписів,тобто цей вид підпису найбільш звичний для тих, хто вже користувався ЕЦП. Посилений підпис повинен обов'язково мати сертифікат **акредитованого засвідчуючого центру**. Цей підпис замінює паперові документи у всіх випадках, за винятком тих, коли закон вимагає наявності виключно документа на папері. За допомогою таких підписів ви зможете організувати юридично значущий електронний документообіг з партнерськими компаніями,органами державної влади та позабюджетними фондами.

Алгоритми

Існує кілька схем побудови цифрового підпису:

На основі алгоритмів симетричного шифрування. Дана схема передбачає наявність у системі третьої особи - арбітра, що користується довірою обох сторін. Авторизацією документа є сам факт шифрування його секретним ключем і передача його арбітру.

На основі алгоритмів асиметричного шифрування. На даний момент такі схеми ЕП найбільш поширені і знаходять широке застосування.

Крім цього, існують інші різновиди цифрових підписів (груповий підпис, незаперечний підпис, довірений підпис), які є модифікаціями описаних вище схем. [8] Їх поява обумовлена різноманітністю завдань, що вирішуються за допомогою ЕП.

Використання хеш-функцій

Оскільки документи, які підписували - змінного (і як правило досить великого) обсягу, в схемах ЕП часто підпис ставиться не на сам документ, а на його хеш. Для обчислення хеша використовуються криптографічні хеш-функції, що гарантує виявлення змін документа при перевірці підпису. Хеш-функції не є частиною алгоритмуЕП, тому в схемі може бути використана будь-яка надійна хеш-функція.

Використання хеш-функцій дає наступні переваги:

Обчислювальна складність. Зазвичай хеш цифрового документа робиться у багато разів меншого обсягу,ніж обсяг вихідного документа, і алгоритми обчислення хешу є більш швидкими, ніж алгоритми ЕП. Тому формувати хеш документа і підписувати його виходить набагато швидше, ніж підписувати сам документ.

Сумісність. Більшість алгоритмів оперує з рядками бітів даних, але деякі використовують інші представлення. Хеш-функцію можна використовувати для перетворення довільного вхідного тексту у відповідний формат.

Цілісність. Без використання хеш-функції великий електронний документ в деяких схемах потрібно розділяти на досить малі блоки для застосування ЕП. При верифікації неможливо визначити, чи всі блоки отримані і чи в правильному вони порядку.

Варто зауважити, що використання хеш-функції не обов'язково для електронного підпису, а сама функція не є частиною алгоритму ЕП, тому хеш-функція може використовуватися будь-яка або не використовуватися взагалі.

У більшості ранніх систем ЕП використовувалися функції з секретом, які за своїм призначенням близькі до односторонніх функцій. Такі системи уразливі до атак з використанням відкритого ключа (див. нижче), так як, вибравши довільний цифровий підпис і застосувавши до нього алгоритм верифікації, можна отримати вихідний текст.[9]

Щоб уникнути цього, разом з цифровим підписом використовується хеш-функція, тобто, обчислення підпису здійснюється не щодо самого документа, а щодо його хешу. У цьому випадку в результаті верифікації можна отримати тільки хеш вихідного тексту, отже, якщо використовувана хеш-функція криптографічно стійка, то отримати вихідний текст буде складно, а тому атака такого типу стає неможливою.

Симетрична схема

Симетричні схеми ЕП менш поширені ніж асиметричні, так як після появи концепції цифрового підпису не вдалося реалізувати ефективні алгоритми підпису, засновані на відомих в той час симетричних шифрах. Першими, хто звернув увагу на можливість симетричної схеми цифрового підпису, були основоположники самого поняття ЕП Діффі і Хеллман, які опублікували опис алгоритму підпису одного біта за допомогою блочного шифру.

Асиметричні схеми цифрового підпису спираються на обчислювально складні завдання, складність яких ще не доведена, тому неможливо визначити, чи будуть ці схеми зламані найближчим часом, як це сталося зі схемою, заснованої на задачі про укладання ранця. Також для збільшення криптостійкості потрібно збільшувати довжину ключів, що призводить до необхідності переписування програми, що реалізують асиметричні схеми, і в деяких випадках перепроектовувати апаратуру. Симетричні схеми засновані на добре вивчених блокових шифрах.

У зв'язку з цим симетричні схеми мають такі переваги:

Стійкість симетричних схем ЕП випливає з стійкості використовуваних блокових шифрів, надійність яких також добре вивчена.

Якщо стійкість шифру виявиться недостатньою, його легко можна буде замінити на більш стійкий з мінімальними змінами в реалізації.

Однак у симетричних ЕП є і ряд недоліків:

Потрібно підписувати окремо кожен біт інформації який передається, що призводить до значного збільшення підпису. Підпис може перевищувати повідомлення за розміром на два порядки.

Згенеровані для підпису ключі можуть бути використані тільки один раз, так як після підписування розкривається половина секретного ключа.

Через розглянуті недоліки симетрична схема ЕЦП Діффі-Хелмана не застосовується, а використовується її модифікація, розроблена Березіним і Дорошкевичем, в якій підписується відразу група з декількох біт. Це призводить до зменшення розмірів підпису, але до збільшення обсягу обчислень. Для подолання проблеми «одноразовості» ключів використовується генерація окремих ключів з головного ключа.

Асиметрична схема

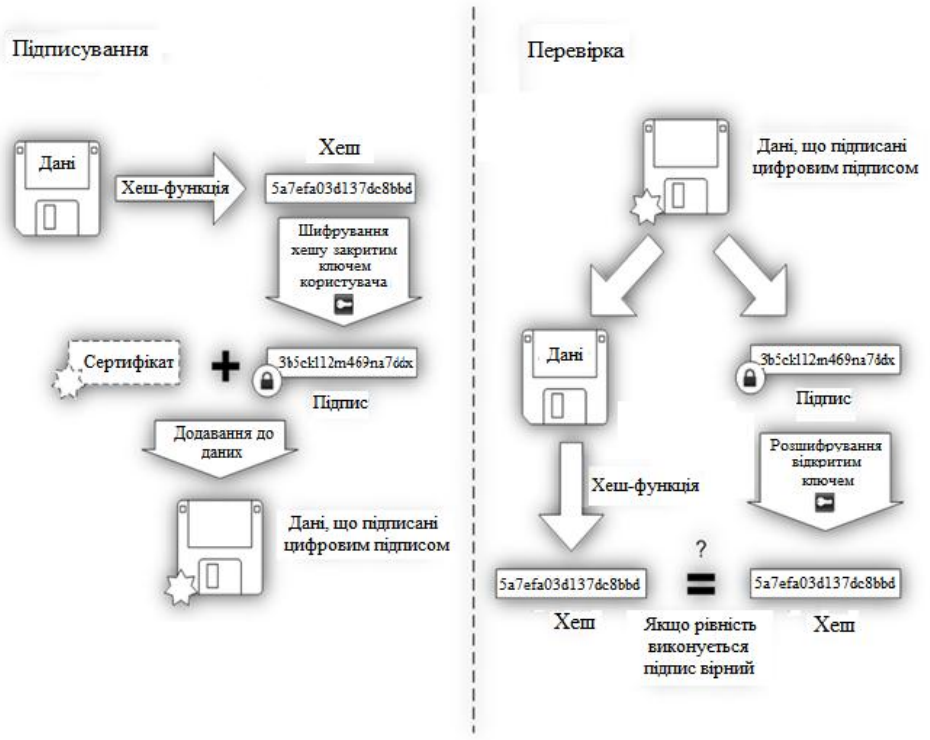


Рисунок 1 - Схема пояснення алгоритмів підпису і перевірки

Асиметричні схеми ЕП відносяться до криптосистем з відкритим ключем.

На відміну від асиметричних алгоритмів шифрування, в яких:

- шифрування проводиться за допомогою відкритого ключа;
- а розшифрування - за допомогою закритого.

У схемах цифрового підпису:

- підписування проводиться із застосуванням закритого ключа,
- а перевірка - із застосуванням відкритого.

Загальновизнана схема цифрового підпису охоплює три процеси

Генерація ключової пари. За допомогою алгоритму генерації ключа рівноймовірним чином з набору можливих закритих ключів вибирається закритий ключ, обчислюється відповідний йому відкритий ключ.

Формування підпису. Для заданого електронного документа за допомогою закритого ключа обчислюється підпис.

Перевірка (верифікація) підпису. Для даних документа та підпису за допомогою відкритого ключа визначається дійсність підпису.

Для того, щоб використання цифрового підпису мало сенс, необхідно виконання двох умов:

Верифікація підпису повинна проводитися відкритим ключем, відповідним саме тому закритому ключу, який використовувався під час підписання.

Без володіння закритим ключем має бути складно обчислювально створити легітимний цифровий підпис.

Слід відрізняти електронний цифровий підпис від коду автентичності

повідомлення (MAC).

Як було сказано вище, щоб застосування ЕП мало сенс, необхідно, щоб обчислення легітимною підпису без знання закритого ключа було складно обчислювальним процесом.

Забезпечення цього у всіх асиметричних алгоритмах цифрового підпису спирається на наступні обчислювальні завдання:

- Завдання дискретного логарифмування (EGSA)

-Завдання факторизації, тобто розкладання числа на прості множники (RSA)

Обчислення теж можуть проводитися двома способами: на базі математичного апарату еліптичних кривих (ГОСТ Р 34.10-2001) і на базі полів Галуа (АДС).

В даний час найшвидші алгоритми дискретного логарифмування і факторизації є субекспоненціальними. Належність самих завдань до класу NP-повних не доведена.

Алгоритми ЕП поділяються на звичайні цифрові підписи і на цифрові підписи з відновленням документа.

При верифікації цифрових підписів з відновленням документа тіло документа відновлюється автоматично, його не потрібно прикріплювати до підпису. Звичайні цифрові підписи вимагають приєднання документа до підпису. Зрозіміло, що всі алгоритми, що підписують хеш документа, відносяться до звичайних ЕП. До ЕП з відновленням документа відноситься, зокрема, RSA.

Схеми електронного підпису можуть бути одноразовими і багаторазовими. В одноразових схемах після перевірки справжності підпису необхідно провести заміну ключів, в багаторазових схемах це робити не потрібно.

Також алгоритми ЕП діляться на детерміновані і імовірнісні.

Детерміновані ЕП при однакових вхідних даних обчислюють однаковий підпис. Реалізація імовірнісних алгоритмів складніша, оскільки вимагає надійне джерело ентропії, але при однакових вхідних даних підписи можуть бути різні, що збільшує криптостійкість. В даний час багато детермінованих схем модифіковані в імовірнісні.

У деяких випадках, таких як потокова передача даних, алгоритми ЕП можуть виявитися занадто повільними. У таких випадках застосовується швидкий цифровий підпис. Прискорення підпису досягається алгоритмами з меншою кількістю модульних обчислень і переходом до принципово інших методів розрахунку.

Перелік алгоритмів ЕП

Асиметричні схеми:

-FDH (FullDomainHash), імовірнісна схема RSA-PSS (ProbabilisticSignatureScheme), схеми стандарту PKCS # 1 і інші схеми, засновані на алгоритмі RSA

-Схема Ель-Гамаля

-Американські стандарти електронного цифрового підпису: DSA, ECDSA(АДС на основі апарату еліптичних кривих)

-Російські стандарти електронного цифрового підпису: ГОСТ Р 34.10-94(на даний час не діє), ГОСТ Р 34.10-2001

- Схема Диффи-Лампорта
- Український стандарт електронного цифрового підпису ДСТУ 4145-2002
- Білоруський стандарт електронного цифрового підпису СТБ 1176.2-99
- Схема Шнорра

Pointcheval-Sternsignaturealgorithm

- Імовірнісна схема підпису Рабина
- СхемаBLS (Boneh-Lynn-Shacham)
- СхемаGMR (Goldwasser-Micali-Rivest)

На основі асиметричних схем створені модифікації цифрового підпису, які відповідають різним вимогам:

-Груповий цифровий підпис
- Незаперечний цифровий підпис
- «Сліпий» цифровий підпис і справедливий «сліпий» підпис
-Конфіденційний цифровий підпис
- Цифровий підпис з доказом підробки
- Довірений цифровий підпис
- Разовий цифровий підпис

Підробка підписів

Аналіз можливостей підробки підписів називається криптоаналіз. Спробу сфальсифікувати підпис або підписаний документ криптоаналітики називають «атака».

Моделі атак та їх можливі результати

У своїй роботі Гольдвассер, Мікалі і Ривест моделі описують Наступні Атак, Які

- ***Атака з використанням відкритого ключа.*** Криптоаналітик володіє тільки відкритим ключем.
- ***Атака на основі відомих повідомлень***. Противник володіє допустимими підписами набору електронних документів, відомих йому, але не обираєїх.
- ***Адаптивна атака на основі вибраних повідомлень.*** Криптоаналітик може отримати підписи електронних документів, які він обирає сам.

Також в роботі описана класифікація можливих результатів атак:

-***Повний злом цифрового підпису.*** Отримання закритого ключа, що означає повний злом алгоритму.

- ***Універсальна підробка цифрового підпису.*** Знаходження алгоритму, аналогічного алгоритму підпису, що дозволяє підробляти підписи для будь-якого електронного документа.

-***Вибіркова підробка цифрового підпису.*** Можливість підробляти підписи для документів, обраних криптоаналітиком.

-***Екзистенціальна підробка цифрового підпису.*** Можливість отримання допустимої підписи для якогось документа, що не обирається криптоаналітиком.

Зрозуміло, що самоюнебезпечною атакою є адаптивна атака на основі обраних повідомлень, і при аналізі алгоритмів ЕП на криптостійкість потрібно розглядати саме її (якщо немає яких-небудь особливих умов).

При безпомилковій реалізації сучасних алгоритмів ЕП отримання закритого ключа алгоритму є практично неможливим завданням через обчислювальну складність завдань, на яких ЕП побудована. Набагато більш ймовірний пошук криптоаналітиком колізій першого і другого роду. Колізія першого роду еквівалентна екзистенціальній підробці, а колізія другого роду - вибірковій. З урахуванням застосування хеш-функцій, знаходження колізій для алгоритму підпису еквівалентно знаходження колізій для самих хеш-функцій.

Зловмисник може спробувати підібрати документ до даного підпису, щоб до нього підходив підпис. Проте в переважній більшості випадків такий документ може бути тільки один. Причина в наступному:

- Документ являє собою осмислений текст.
-Текст документа оформлений за встановленою формою.
- Документи рідко оформляють у вигляді PlainText-файлу, найчастіше в форматі DOC або HTML.

.

—

N
e
w

Якщо у фальшивому наборі байтів і станеться колізія з хешем вихідного документа, то повинні виконатися 3 наступних умови:

- Випадковий набір байтів повинен підійти під складно структурований формат файлу.

- Те, що текстовий редактор прочитає у випадковому наборі байтів, має утворювати текст, оформлений встановленою формою.

- Текст повинен бути осмисленим, грамотним і відповідним темі документа.

Втім, у багатьох структурованих наборах даних можна вставити довільні дані в деякі службові поля, не змінивши вид документа для користувача. Саме цим користуються зловмисники, підробляючи документи.

Можливість такого події також мізерно мала. Можна вважати, що на практиці такого не трапитися навіть з ненадійними хеш-функціями, так як документи зазвичай великого обсягу - кілобайти.

Отримання двох документів з однаковою підписом (колізія другого роду)

Куди більш імовірна атака другого роду. У цьому випадку зловмисник фабрикує два документа з однаковою підписом, і в потрібний момент підміняє один іншим. При використанні надійної хеш-функції така атака повинна бути також складно обчислювальною. Однак ці загрози можуть реалізуватися через слабкість конкретних алгоритмів хешування, підписи, або помилки в їх реалізаціях. Зокрема, таким чином можна провести атаку на SSL-сертифікати і алгоритм хешування MD5.

Соціальні атаки

Соціальні атаки спрямовані не на злом алгоритмів цифрового підпису, а на маніпуляції з відкритим і закритим ключами.

-Зловмисник, який вкрав закритий ключ, може підписати будь-який документ від імені власника ключа.

- Зловмисник може обманом змусити власника підписати будь-який документ, наприклад, використовуючи протокол сліпого підпису.

-Зловмисник може підмінити відкритий ключ власника на свій власний, видаючи себе за нього.

Використання протоколів обміну ключами і захист закритого ключа від несанкціонованого доступу дозволяє знизити небезпеку соціальних атак.

Управління ключами

Управління відкритими ключами

Важливою проблемою всієї криптографії з відкритим ключем, в тому числі і систем ЕП, є управління відкритими ключами. Так як відкритий ключ доступний будь-якому користувачеві, то необхідний механізм перевірки того, що цей ключ належить саме своєму власникові. Необхідно забезпечити доступ будь-якого користувача до справжнього відкритого ключа будь-якого іншого користувача, захистити ці ключі від підміни зловмисником, а також організувати відгук ключа у разі його компрометації.

Завдання захисту ключів від підміни вирішується за допомогою сертифікатів. Сертифікат дозволяє засвідчити укладені в ньому дані про власника і його відкритий ключ підписом будь-якого довіреної особи.

Існують системи сертифікатів двох типів:

- *централізовані;*

- *децентралізовані.*

У децентралізованих системах шляхом перехресного підписування сертифікатів знайомих і довірених людей кожним користувачем будується мережа довіри.

У централізованих системах сертифікатів використовуються центри сертифікації, підтримувані довіреними організаціями.

Центр сертифікації формує закритий ключ і власний сертифікат, формує сертифікати кінцевих користувачів і засвідчує їх автентичність своїм цифровим підписом. Також центр проводить відгук минулих і зкомпроментованих сертифікатів і веде бази виданих та відкликаних сертифікатів. Звернувшись в сертифікаційного центру, можна отримати власний сертифікат відкритого ключа, сертифікат іншого користувача і дізнатися, які ключі відкликані.

Смарт-карта і USB-брелокиeToken

Закритий ключ є найбільш вразливим компонентом всієї криптосистеми цифрового підпису. Зловмисник, який вкрав закритий ключ користувача, може створити дійсний цифровий підпис будь-електронного документа від імені цього користувача. Тому особливу увагу потрібно приділяти способу зберігання закритого ключа. Користувач може зберігати закритий ключ на своєму персональному комп'ютері, захистивши його за допомогою пароля. Однак такий спосіб зберігання має ряд недоліків, зокрема, захищеність ключа повністю залежить від захищеності комп'ютера, і користувач може підписувати документи лише на цьому комп'ютері.

В даний час існують наступні пристрої зберігання закритого ключа :

-Дискети
- Смарт-карти
- USB-брелоки
- Таблетки Touch-Memory

Рисунок 1

Крадіжка або втрата одного з таких пристроїв зберігання може бути легко помічена користувачем, після чого відповідний сертифікат може бути негайно відкликаний.

Найбільш захищений спосіб зберігання закритого ключа - зберігання на смарт-карті. Для того, щоб використовувати смарт-карту, користувачеві необхідно не тільки її мати, але і ввести PIN-код, тобто, виходить двухфакторнааутентифікація. Після цього підписується документ або його хеш передається в карту, її процесор здійснює підписування хешу і передає підпис назад. У процесі формування підпису таким способом не відбувається копіювання закритого ключа, тому весь час існує тільки єдина копія ключа. Крім того, зробити копіювання інформації зі смарт-карти складніше, ніж з інших пристроїв зберігання.

Відповідно до закону «Про електронний підпис», відповідальність за зберігання закритого ключа власник несе сам.

Використання ЕП

В Україні юридично значущий сертифікат електронного підпису видає засвідчуючий центр. Правові умови використання електронного цифрового підпису в електронних документах регламентують Закони України «Про електронний цифровий підпис» та «Про електронні документи та електронний документообіг».

Після становлення ЕП при використанні в електронному документообігу між кредитними організаціями та кредитними бюро активно стала розвиватися інфраструктура електронного документообігу між податковими органами і платниками податків. Почав працювати наказ податків і зборів. Він визначає загальні принципи інформаційного обміну під час подання податкової декларації в електронному вигляді по телекомунікаційних каналах зв'язку.

У законі України «Про електронний цифровий підпис» описані умови використання ЕП, особливості її використання в сферах державного управління та в корпоративній інформаційній системі.

Завдяки ЕП тепер, зокрема, багато компаній України здійснюють свою торгово-закупівельну діяльність в Інтернеті, через системи електронної торгівлі, обмінюючись з контрагентами необхідними документами в електронному вигляді, підписаними ЕП. Це значно спрощує і прискорює проведення конкурсних торгових процедур.

У перспективі громадянам України буде видаватися універсальна електронна карта, в яку вмонтовано посилений кваліфікований електронний підпис.

Лекція 24

Технічний захист інформації в телекомунікаційних мережах

Телекомунікаційні системи як носії інформації складаються з різних засобів електроніки й радіотехніки.

Конструктивно вони виконані з передавальних і приймальних пристроїв, апаратури обробки, реєстрації, зберігання й відображення інформації.

До таких пристроїв можна віднести радіотехнічні й оптико-електронні, інфрачервоні й лазерні, акустичні й гідроакустичні. Всі вони працюють на базі обчислювальної техніки й обслуговують величезну розмаїтість людської діяльності, а отже, можуть бути джерелом витоку конфіденційної інформації. Тому виникає проблема організації безпеки інформації на новому рівні розвитку інформаційного протиборства.

Аналіз походження численних перетворювачів і випромінювачів свідчить про таке:

джерелами небезпечного сигналу є елементи, вузли й провідники технічних засобів забезпечення виробничої й трудової діяльності, а також радіо- й електронна апаратура;

кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;

кожна електронна система, що містить сукупність елементів, вузлів і провідників, має безліч технічних каналів витоку інформації.

З певним ступенем узагальнення безліч радіоканалів витоку інформації можна подати у вигляді структури, наведеної на рис. 1.

Рисунок 1 -Структура радіоканалів витоку інформації

Кожний із цих каналів, залежно від конкретної реалізації елементів, вузлів і виробів у цілому, матиме певний прояв, специфічні характеристики й особливості утворення, пов'язані з умовами розташування й функціонування. Класифікацію радіоканалів витоку інформації походженням, діапазоном випромінювання й середовищем поширення наведено на рис. 2

Під час передачі енергії з каналу в зовнішнє середовище важливу роль відіграє можливість трансформації різних видів енергії. Така трансформація здійснюється за рахунок перебігу різних явищ у фізичних перетворювачах.

Перетворювачем є прилад, що трансформує зміну однієї фізичної величини в зміну іншої. У термінах електроніки перетворювач зазвичай визначається як прилад, що перетворює неелектричну величину в електричний сигнал або навпаки (рис. 12.5.3).

Кожний перетворювач діє на підставі певних фізичних принципів й утворює властивий цим принципам передавальний канал — тобто канал витоку інформації.

Функції приладів й електронних пристроїв можна поділити на два основних види — обробка електричних сигналів і перетворення якого-небудь зовнішнього фізичного впливу в електричні сигнали. У другому випадку основну роль виконують датчики й перетворювачі.

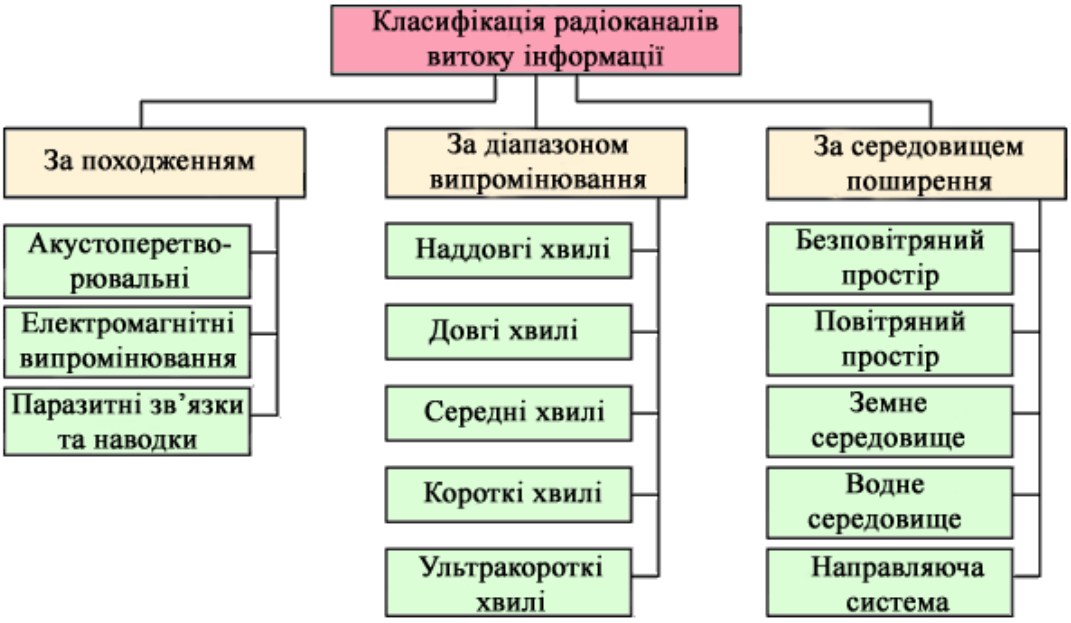


Рисунок 2 - Класифікація радіоканалів витоку інформації

За фізичною природою перетворювачі поділяють на численні групи, серед яких слід

відзначити фотоелектричні, термоелектричні, п’єзоелектричні, електромагнітні й акустоелектричні перетворювачі, які широко використовуються в сучасних системах зв’язку, обробки інформації й управління.

Одними з найнебезпечніших каналів витоку інформації є акустичні канали. Джерелом утворення акустичного каналу витоку інформації є вібруючі, коливні тіла й механізми, такі як голосовий апарат людини, елементи машин, телефонні апарати, звукопідсилювальні системи тощо. Класифікацію акустичних каналів витоку інформації наведено на рис. 4.

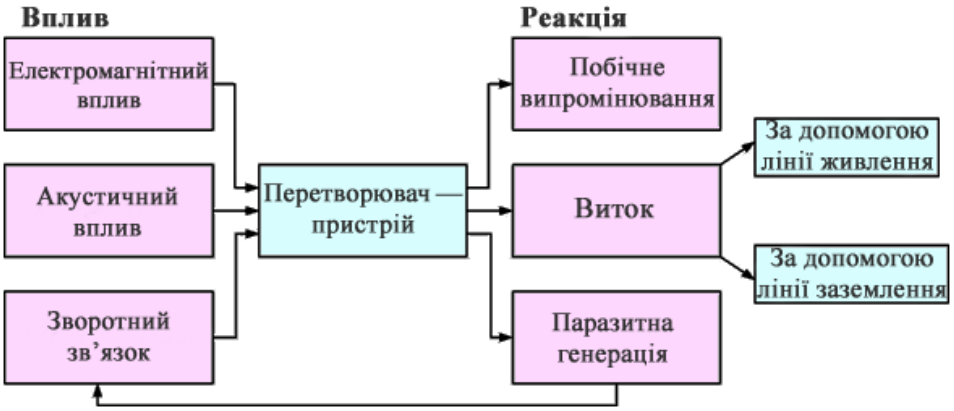


Рисунок 3 - Схема роботи перетворювача

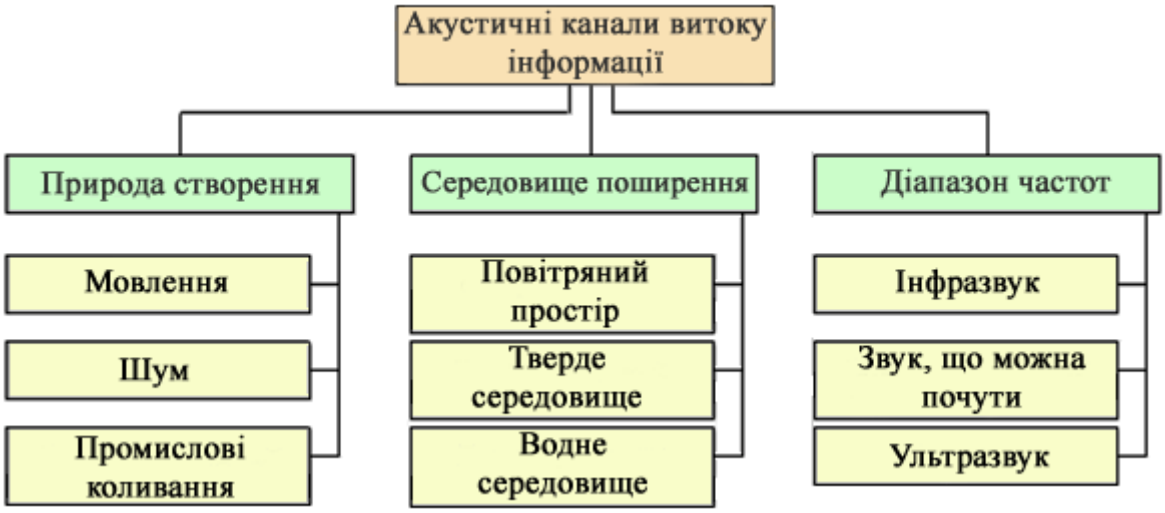


Рисунок 4 - Класифікація акустичних каналів

Акустичні канали витоку інформації утворюються за рахунок:

поширення акустичних коливань у вільному повітряному просторі;

впливу звукових коливань на елементи й конструкції будинків;

впливу звукових коливань на технічні засоби обробки інформації.

Канали формуються за рахунок:

у першому випадку: переговорів на відкритому просторі; відкритих вікон, дверей, кватирок, вентиляційних каналів;

у другому випадку: стін, стель, підлог, вікон, дверей, коробів вентиляційних систем, труб

водопостачання, систем підігріву та кондиціонування тощо;

у третьому випадку: мікрофонного ефекту, акустичної модуляції волоконно-оптичних ліній передачі інформації.

Акустична розвідка здійснюється перехопленням виробничих шумів об’єкта й перехопленням мовленнєвої інформації. В акустичній розвідці використовуються:

пасивні методи перехоплення;

активні методи перехоплення;

контактні методи перехоплення.

За способом застосування технічні засоби знімання акустичної інформації можна класифікувати, як показано на рис. 5

Засоби, що встановлюються заходовими (вимагають фізичного проникнення на об’єкт) методами:

радіозакладки;

закладки з передачею акустичної інформації в інфрачервоному діапазоні;

закладки з передачею інформації за допомогою мережі 220 В;

закладки з передачею акустичної інформації за допомогою телефонної лінії;

диктофони;

провідні мікрофони;

«телефонне вухо».

Засоби, що встановлюються беззаходовими методами:

апаратура, що використовує мікрофонний ефект;

високочастотне нав’язування;

стетоскопи;

лазерні стетоскопи;

спрямовані мікрофони.

Рисунок 5 - Класифікація пристроїв несанкціонованого зняття інформації

Побічні електромагнітні випромінювання (ПЕМВ), що генеруються електромагнітними

пристроями, обумовлені протіканням диференціальних і синфазних струмів. У напівпровідникових пристроях електромагнітне поле, що випромінюється, утворюється при синхронному протіканні диференціальних струмів у контурах двох типів. Один тип контуру формується провідниками друкованої плати або шинами, якими на напівпровідникові прилади подається електроживлення. Площа контуру системи електроживлення приблизно дорівнює добутку відстані між шинами на відстань від найближчої логічної схеми до її розв'язувального конденсатора. Інший тип контуру утворюється при передачі логічних сигналів від одного пристрою до іншого з використанням як лінії зворотного зв'язку шини електроживлення. Лінії передачі даних разом із шинами електроживлення формують динамічні контури, що з'єднують передавальні й приймальні пристрої. Випромінювання, викликане синфазними струмами, обумовлено виникненням спадань напруги в пристрої, що створює синфазну напругу відносно Землі.

Як правило, у цифровому електронному обладнанні здійснюється синхронна робота логічних пристроїв. У результаті при перемиканні кожного логічного пристрою відбувається концентрація енергії у вузькі імпульсні складові, які збігаються за часом, при їх накладенні сумарні рівні випромінювання можуть виявитися вище, ніж може створити кожен з окремих пристроїв.

Значний вплив на рівень ЕМВ, які виникають, чинять характеристики з'єднань із негативною шиною джерела електроживлення або із «землею». Це з'єднання повинне мати дуже низький імпеданс, оскільки й друковані провідники на ВЧ являють собою швидше дроселі, ніж коротко замкнуті лінії.

У багатьох випадках основними джерелами випромінювань виявляються кабелі, якими передається інформація в цифровому вигляді. Такі кабелі можуть розміщуватися всередині пристрою або з'єднувати пристрої між собою.

Застосування заземлювальних перемичок з обплетення кабелю, що характеризуються великими значеннями індуктивності й активного опору для ВЧ перешкод і не забезпечують гарної якості заземлення екрана, приводить до того, що кабель починає діяти як передавальна антена.

Під час проведення аналізу можливості витоку інформації необхідно враховувати такі особливості радіотехнічного каналу витоку інформації із засобів цифрової електронної техніки:

для відновлення інформації окрім знання рівня ПЕМВ потрібно знати їхню структуру;

оскільки інформація в цифрових засобах електронної техніки переноситься послідовностями прямокутних імпульсів, то оптимальним приймачем для перехоплення ПЕМВ є детектор (важливий сам факт наявності сигналу, а відновити сигнал просто, оскільки форма його відома);

не всі ПЕМВ є небезпечними з точки зору реального витоку інформації. Як правило, найбільші рівні відповідають неінформативним випромінюванням (у ПЕМВ найбільший рівень мають випромінювання, що породжуються системою синхронізації);

наявність великого числа паралельно працюючих електричних кіл призводить до того, що інформативні й неінформативні випромінювання можуть перекриватися за діапазоном (взаємна перешкода);

для відновлення інформації смуга пропускання розвідприймача має відповідати смузі частот сигналів, що перехоплюють. Імпульсний характер інформаційних сигналів приводить до різкого збільшення смуги пропускання приймача й, як наслідок, до збільшення рівня власних і

наведених шумів;

періодичне повторення сигналу призводить до збільшення можливої дальності перехоплення;

використання паралельного коду в більшості випадків робить практично неможливим відновлення інформації при перехопленні ПЕМВ.

Важливим питанням технічного захисту об’єктів ТКС є визначення каналів витоку інформації з ЕОМ. Такі канали утворюються як безпосередньо у процесі роботи ЕОМ, так і в режимі очікування. Їхніми джерелами є:

електромагнітні поля;

струми і напруги в провідних системах (електроживлення, заземлення і сполучних ліній);

перевипромінювання інформації, що оброблюється, на частотах паразитної генерації елементів і пристроїв технічних засобів ЕОМ;

перевипромінювання інформації, що оброблюється, на частотах контрольно-вимірювальної апаратури.

Окрім цих каналів, обумовлених походженням процесів, що відбуваються в ЕОМ, й їхніми технічними особливостями, у ЕОМ, що поставляють на ринок, можуть навмисне створюватися додаткові канали витоку інформації. Для утворення таких каналів може використовуватися:

розміщення в ЕОМ закладок для реєстрації мовленнєвого сигналу або інформації, що оброблюється (замасковані під певні електронні блоки);

установка в ЕОМ радіомаяків;

установка закладок, що забезпечують знищення ЕОМ ззовні (схемні рішення);

установка елементної бази, що виходить із ладу.

Навмисне застосування таких конструктивно-схемних рішень призводить до збільшення електромагнітних випромінювань у певній частині спектра.

У групі каналів, у яких основним видом обробки даних є обробка даних апаратурою, можна виділити такі можливі канали витоку:

підключення до ЕОМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів ЕОМ.

Під час перехоплення інформації з ЕОМ використовують схему, наведену на рис. 6.

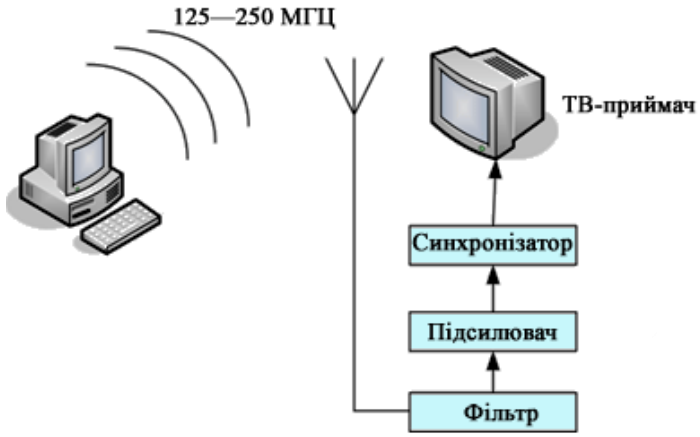


Рисунок 6 - Схема перехоплення інформації з ПЕОМ

Технічний контроль має здійснюватися для таких потенційних каналів витоку інформації:

побічні електромагнітні випромінювання в діапазоні частот від 10 Гц до 100 МГц;

наведення сигналів у лініях електроживлення, заземлення й у лініях зв'язку;

небезпечні сигнали, що утворюються за рахунок електроакустичних перетворень, які можуть відбуватися в спеціальній апаратурі контролю інформації. Ці сигнали мають контролюватися в діапазоні частот від 300 Гц до 3,4 кГц;

канали витоку інформації, що утворюються в результаті впливів високочастотних електромагнітних полів на різні лінії, які розташовані у приміщенні й можуть, таким чином, стать приймальною антеною. У цьому разі перевірка здійснюється в діапазоні частот від 20 кГц до 100 МГц.

Найнебезпечнішим каналом витоку є дисплей, оскільки з погляду захисту інформації він є найслабшою ланкою в системі. Це обумовлено принципами роботи відеоадаптера, що складається зі спеціалізованих схем для генерування електричних сигналів управління апаратною частиною, що забезпечує генерацію зображення.

Протидія в системі технічного захисту інформації має полягати у розробці процедур виявлення каналів витоку інформації, виявленні пристроїв негласного знімання інформації й запобіганні несанкціонованому доступу до інформації.

Пошук пристроїв негласного знімання інформації може відбуватися за допомогою таких методів (рис. 7) і складатися з декількох етапів:

підготовчий етап;

фізичний пошук і візуальний огляд;

виявлення радіозакладних пристроїв;

виявлення технічних засобів з передаванням інформації струмопровідними лініями;

виявлення пристроїв з передаванням інформації інфрачервоним каналом;

перевірка наявності акустичних каналів витоку інформації.

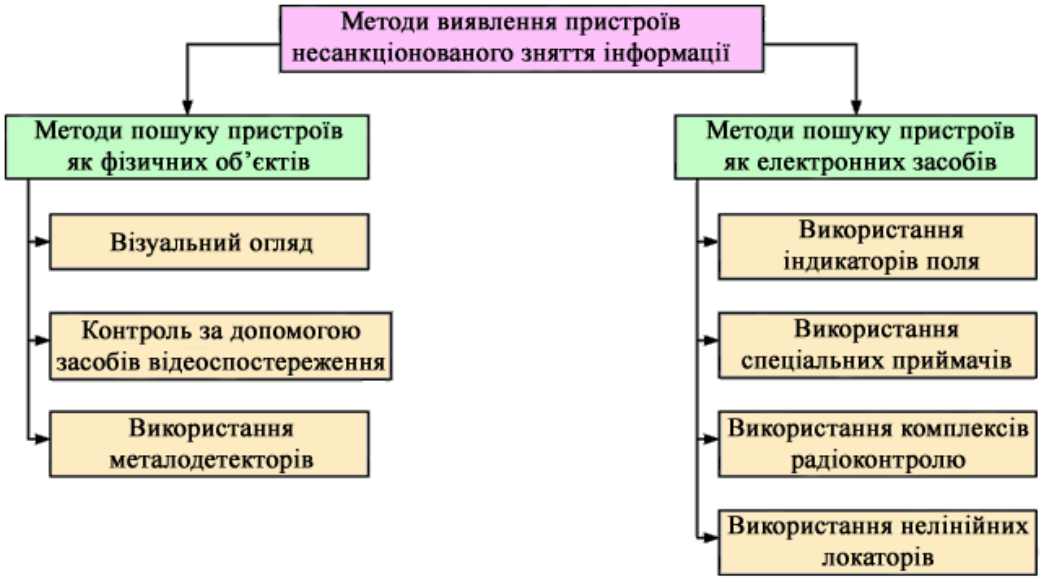


Рисунок 7 - Методи виявлення пристроїв несанкціонованого зняття інформації

Найважливішим є підготовчий етап, оскільки саме тут може бути закладено успіх. Він

містить такі елементи:

1) оцінювання типів і можливого рівня випромінювань технічних засобів, що використовуються;

2) аналіз ступеня небезпеки, що може виходити від своїх співробітників і представників сторонніх організацій;

3) оцінювання можливості доступу сторонніх до приміщення;

4) вивчення історії будинку, у якому планується проводити пошукові заходи;

5) визначення забезпечуваного рівня безпеки відповідно до економічних можливостей і побажаннями замовника, а також фактичною необхідністю в тих чи інших заходах ЗІ;

6) розроблення плану дій для різних ситуацій, які можуть виникнути під час процедур забезпечення ЗІ.

Фізичний пошук і візуальний огляд є важливим елементом виявлення засобів негласного отримання інформації, особливо таких як провідні й волоконно-оптичні мікрофони, пасивні й напівактивні радіозакладні пристрої, дистанційно керовані пристрої, що перебувають у режимі очікування, й інші технічні засоби, які неможливо виявити за допомогою типової апаратури. Візуальний огляд значно спрощується під час використання спеціалізованих засобів.

До сучасних засобів відеоспостереження належать оптико-електронні системи, які умовно можна поділити на дві групи:

ендоскопічна продукція;

доглядові портативні телевізійні або відеопристрої.

Асортимент **ендоскопічної продукції** містить низку волоконно-оптичних фіброскопів, твердих бароскопів, а також відеоскопів, що дозволяють здійснювати огляд важкодоступних місць. Відмінною рисою цих пристроїв є наявність мініатюрного об’єктива, який розміщено на кінці тонкого гнучкого рукава або твердої трубки, які служать і напрямним елементом, і захисною оболонкою для оптоволоконного джгута (рідше багатокомпонентної лінзової системи), призначеного для передачі зображення з виходу об’єктива на окуляр або ПЗК-матрицю.

Доглядові портативні телевізійні системи дозволяють з’єднати переваги високої якості зображення з максимальною зручністю користування пристроями під час огляду. Це досягається шляхом конструктивного об’єднання в єдиному пристрої мініатюрної телевізійної камери, штанги, що регулюється, й телевізійного монітора.

Можна виділити основні сигнальні ознаки наявності радіозакладок у приміщенні:

відносно високий рівень випромінювання, обумовлений необхідністю передачі сигналу за межі контрольованого приміщення. Цей рівень тим вище, чим ближче до пристрою несанкціонованого зняття інформації перебуває апаратура пошуку;

наявність гармонік у випромінюванні радіозакладок, що є наслідком необхідності мінімізації розмірів ЗП, а отже, неможливості забезпечити гарну фільтрацію вихідного сигналу;

поява нового джерела у зазвичай вільному частотному діапазоні. Оператор, що здійснює радіоконтроль, має дуже добре орієнтуватися в загальній радіоелектронній обстановці й знати, які пристрої у яких діапазонах можуть працювати;

використання в окремих радіозакладках спрямованих антен. Це призводить до сильної локалізації випромінювання, тобто істотної нерівномірності його рівня в межах контрольованого об’єкта. На відстанях у декілька метрів цей ефект найкраще виявляється для гармонік основного випромінювання;

особливості поляризації випромінювання радіозакладок. Справа в тому, що під час зміни просторового положення або орієнтації приймальної антени спостерігається зміна рівня всіх джерел. Однак однотипні джерела одного діапазону поводяться приблизно однаково, тоді як сигнал закладки змінюється відмінно від інших;

зміна («розмивання») спектра випромінювань радіомікрофонів під час виникнення яких-небудь шумів у контрольованому приміщенні. Вона виявляється тільки в тому разі, якщо ЗП працює без кодування інформації, що передається;

здатність людини розрізняти акустичні сигнали. Так, якщо закладка працює без маскування, то оператор, що здійснює пошук ЗП, чує шум приміщення або той тестовий сигнал, що сам створив;

алгоритм роботи радіозакладок. Так, найпростіші з них, тобто не обладнані схемами дистанційного включення й VOX, функціонуватимуть безупинно протягом певного часу. Для закладок з VOX характерний переривчастий режим роботи вдень і відсутність передачі сигналу вночі. Пристрої з дистанційним включенням обов'язково мають кілька коротких сеансів протягом дня й майже напевно працюватимуть під час переговорів, важливих з погляду особи, що встановила ЗП.

Цей список ознак не є вичерпним і може бути істотно розширений.

Виявлення закладних пристроїв, що використовують передачу інформації зі струмопровідних ліній здійснюється з використанням спеціальних адаптерів, що дозволяють підключатися до різних ліній, у тому числі й з напругою до 300—400 В. Пошук необхідно здійснювати в частотному діапазоні 50—300 кГц, оскільки з одного боку, на частотах нижче 50 кГц у мережах електроживлення відносно високий рівень впливів від побутової техніки й промислового обладнання, а з іншого боку — на частотах вище 300 кГц існує істотне загасання сигналу в лінії, і, крім того, лінії починають працювати як антени, що випромінюють сигнал у навколишній простір, тому пристрої із частотами передачі 300 кГц і вище будуть виявлені на етапі пошуку радіозакладок.

Найнадійнішим способом виявлення заставних пристроїв з передачею інформації ІЧ-каналом є фізичний пошук. Якщо ж останній нічого не дав, то потрібно використати пошукову техніку зі спеціальними ІЧ-датчиками. Пошук випромінювань від таких заставних пристроїв найкраще здійснювати із зовнішньої сторони будинку. Особлива увага при цьому приділяється вікнам.

Одними з найнебезпечніших є природні канали витоку, такі як поширення звукових коливань назовні через вікна, стіни, водопровідні труби, порожнини в будинку тощо й які вловлюються мікрофонами за межами приміщення, що охороняється. Під час проведення фізичного пошуку обов'язково перевіряються вентиляційні й кабельні канали на можливість прослуховування, а також на наявність у них винесених мікрофонів, з'єднаних проводами зі звукозаписуючою апаратурою. Якщо є потреба, то проводиться повна акустична перевірка контрольованого приміщення.

Для комплексного обстеження приміщень необхідно використати спеціальні програмно-апаратні засоби моніторингу радіотехнічних каналів. Основними пристроями є індикатори (детектори) поля, панорамні приймачі, нелінійні локатори й інші типи пристроїв.

Найпростішими засобами виявлення факту використання радіозакладок є **індикатори**, або **детектори поля**. По суті, це приймачі з дуже низькою чутливістю, тому вони виявляють випромінювання закладних пристроїв на дуже малих відстанях (10—40 см), чим і

забезпечується селекція нелегальних випромінювань на фоні потужних дозволених сигналів. Важлива перевага детекторів — здатність знаходити передавальні пристрої незалежно від модуляції, що застосовується. Основний принцип пошуку полягає у виявленні абсолютного максимуму рівня випромінювання в приміщенні. Добрі індикатори поля постачені частотомірами, акустичними динаміками, мають режим прослуховування й подвійну індикацію рівня сигналу.

Іноді детектори можна використовувати й у так званому **сторожовому режимі**. У цьому разі після повної перевірки приміщення на відсутність заставних пристроїв фіксується рівень поля в певній точці простору (зазвичай це стіл керівника або місце ведення переговорів), і прилад переводиться в сторожовий режим. У разі включення закладки (приблизно до 2 м від детектора) індикатор видає сигнал про підвищення рівня електромагнітного поля. Однак необхідно враховувати той факт, що якщо використовуватиметься радіозакладка з дуже низькими рівнями випромінювання, то детектор швидше за все не зафіксує її активізацію.

Прикладами детекторів поля можуть служити такі пристрої: Cub, Optoelectronics M1, Scout-40, MRA-3, ПІТОН й ін.

Панорамні приймачі дозволяють контролювати великий спектр частот, причому робити це він має або одночасно у всьому діапазоні, або переходячи від значення до значення за гранично малий інтервал часу. Можливості панорамних приймачів значною мірою визначаються методом аналізу частотного діапазону. Від нього повністю залежить і вид структурної схеми приймача. Розрізняють методи паралельного й послідовного аналізу спектра.

При паралельному аналізі всі сигнали, що перебувають у певній смузі частот, що називається смугою огляду, виявляються одночасно. Структурну схему такого приймача наведено на рис. 7.

Тут ВЧ-фільтр *1* формує необхідну смугу огляду, у якій ведеться виявлення сигналів; змішувач *2* виконує лінійне перенесення спектра прийнятого випромінювання в низькочастотну область радіодіапазону; смугові фільтри *3* здійснюють частотний поділ сигналів. Вихідний підсилювач *4* забезпечує необхідний рівень сигналу, достатній для нормальної роботи аналізуючого пристрою *5*.

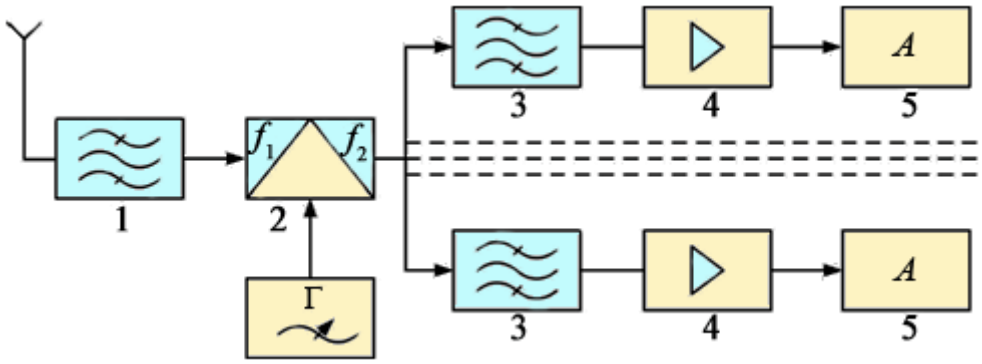


Рисунок 7 - Структурна схема панорамного приймального пристрою з паралельним аналізом спектра сигналів

У радіоприймачі послідовного аналізу, відповідно, здійснюється послідовна зміна частот в

смузі огляду й виявлення сигналу. Спрощену структурну схему пристрою подібного типу показано на рис. 8.

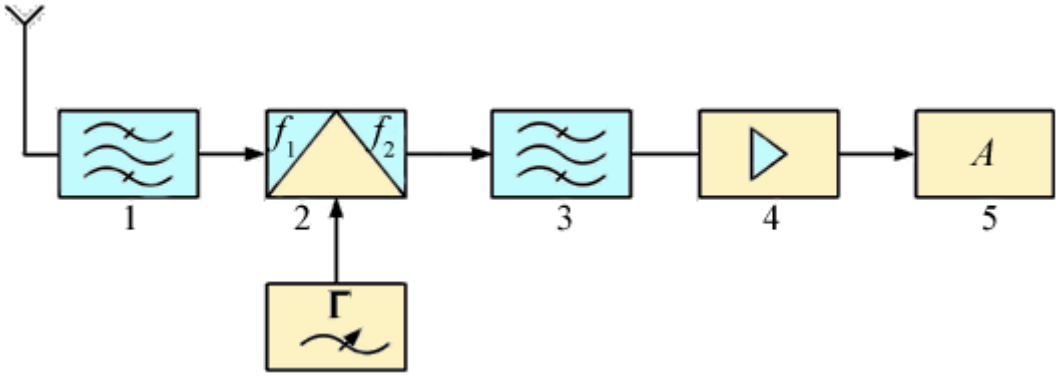


Рисунок 8 - Структурна схема панорамного радіоприймального пристрою з послідовним аналізом спектра сигналів

Тут ВЧ-фільтр *1* має смугу пропускання, що дорівнює смузі огляду, а гетеродин *2* забезпечує перетворення приймача в заданій смузі. Проміжна частота — фіксована. Після селекції фільтром 3 і посилення підсилювачем *4* виявлений сигнал надходить у пристрій *5* для аналізу. При автоматичній зміні частоти приймач ніби «прощупує» (сканує) частотний діапазон, звідси і його повсякденна назва — сканер. Термін не зовсім точний, але досить поширений.

Прикладами приймачів можуть служити AR-8000 і IC-PCR1000.

Подальшим кроком на шляху вдосконалення процедури пошуку ЗП є застосування програмно-апаратних комплексів радіоконтролю й виявлення каналів витоку інформації, оскільки їхні можливості значно ширші, ніж у просто сполучених з ЕОМ сканувальних приймачів. У найбільш загальному вигляді ці можливості полягають у такому:

виявлення випромінювань радіозакладок;

пеленгування радіозакладних пристроїв у реальному часі;

визначення дальності до джерел випромінювання;

аналого-цифрова обробка сигналів з метою визначення їх приналежності до випромінювання радіозакладками;

контроль силових, телефонних, радіотрансляційних та інших мереж;

робота в багатоканальному режимі, що дозволяє контролювати кілька об’єктів одночасно;

постановка прицільних перешкод на частотах випромінювання радіозакладок тощо.

Одним з найскладніших завдань у сфері захисту інформації є пошук ЗП, що не використовують радіоканал для передачі інформації, а також радіозакладок, що перебувають у пасивному (невипромінюючому) стані. Традиційні засоби виявлення такі, як панорамні радіоприймачі, аналізатори спектра або детектори поля, у цьому разі виявляються неефективними. Візуальний огляд також не гарантує виявлення подібних ЗП, оскільки сучасні технології дозволяють виготовляти їх з будь-яким видом камуфляжу, ховати в елементах будівельних конструкцій та інтер’єру.

Саме ця проблема й привела до появи зовсім нового виду пошукового приладу — **радіолокатора нелінійностей** (нелінійного радіолокатора). Своєю назвою він зобов’язаний закладеному фізичному принципу виявлення пристроїв, які проводять зняття інформації, що

полягає у виявленні гармонік зондувального сигналу, які виникають при опроміненні електронних вузлів, що містять нелінійні радіокомпоненти (діоди, транзистори й ін.). До основних характеристик нелінійних радіолокаторів належать: значення робочих частот зондувальних сигналів; режим випромінювання й потужність передавача; форма, геометричні розміри й поляризація антен; точність визначення місця розташування перевипромінювального об'єкта; чутливість приймача; максимальна дальність дії й глибина, на якій можливе виявлення закладки всередині радіопрозорого матеріалу; кількість аналізованих гармонік; розміри, маса й тип електроживлення радіолокатора.

Нелінійні радіолокатори повністю не розв'язують завдання виявлення закладок у приміщенні. Так, наприклад, якщо закладка з дистанційним управлінням установлена в якій-небудь електронній апаратурі (телевізорі, телефонному апарату тощо) і включається тільки під час проведення наради, то вона не може бути виявлена нелінійним локатором при обстеженні приміщення перед переговорами, оскільки сигнал відгуку від неї буде замаскований відгуком від апаратури, у якій вмонтована закладка. Тому в комплекті з локатором завжди має використовуватися панорамний приймач необхідного типу. При цьому досить важливо, щоб контроль несанкціонованого випромінювання в приміщенні здійснювався й під час нарад. При виборі нелінійного радіолокатора слід виходити із завдань, які поставлені перед групою контролю.

У процесі роботи на **відкритих просторах** доцільно використовувати імпульсні локатори великої потужності й найкращої чутливості. Цю ж вимогу висувають і до обстеження в необладнаних приміщеннях, що мають товсті стіни.

Деякі закладні пристрої виконують за МОП-технологією в екранованих корпусах. Тому їхнє виявлення навіть із використанням нелінійних локаторів ускладнено, оскільки рівень перевипроменених сигналів на 2-й і 3-й гармоніках незначний. Для пошуку таких пристроїв можуть використовуватися **металошукачі** (металодетектори).

Захист інформації від витоку по електричному технічному каналу

Захист інформації від витоку по електричному технічному каналу є однією з пріоритетних задач забезпечення інформаційної безпеки. Електричний канал витоку інформації може бути утворений шляхом контактного підключення до сполучних ліній і сторонніх провідників засобів технічної розвідки, або наведення випромінювань на лінії та провідники.

Причинами виникнення електричних каналів витоку інформації можуть бути: наведення електромагнітних випромінювань технічного засобу передавання інформації (ТЗПІ) на з'єднувальні лінії і провідники; просочування інформаційних сигналів у колі електроживлення; витік інформації у колі заземлення ТЗПІ.

Насамперед, основну увагу слід приділити технічним заходам з використанням таких засобів: екранування ТЗПІ і їх сполучних ліній; заземлення ТЗПІ і екранів їх з'єднувальних ліній; установка приладів в мережі електроживлення типу "РІАС 4ЗМ" для створення активної шумової завади зі спектром, аналогічним спектру наведеного сигналу; установка приладу типу «РІАС-4ШЛ» призначеного для активного маскування сигналів в телефонних кабелях; установка спеціальних діелектричних вставок в обплетення кабелів електроживлення та труб; установка автономних або стабілізованих джерел електроживлення; установка загороджувальльного фільтру "РІАС-4 ФМ / 20" який призначений від витоку колами

електроживлення постійного або змінного струму.

Отже, підвищення ефективності захисту інформації від витоку по електричному технічному каналу, досягається шляхом використання спеціальних приладів захисту інформації, які затвердженні державною службою спеціального зв'язку та захисту інформації України, але використання цих засобів під час розроблення комплексів технічного захисту інформації (ТЗІ) на об'єкті інформаційної діяльності (ОІД) не увільняє від необхідності атестації комплексів ТЗІ на ОІД.

Список використаних джерел:

1. Хорев А.А. Техническая защита информации. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с

2. Хорев А.А. Способы и средства защиты информации: учеб. пособие. – М.: МО РФ, 1998. – 316 с.

3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации К.: Юниор, 03. — 504 с.

4. Перелік засобів технічного захисту інформації. [Електронний ресурс] — Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=234237&cat_id=3918

Лекція 25

Організація та порядок технічного захисту інформації в ЦАТС

Для успішної технічної експлуатації КСЗІ на ЦАТС з досягненням заданого рівня захищеності інформаційних ресурсів та рівня гарантій захисту необхідно правильно організувати заходи з ТЗІ на всіх попередніх етапах створення КСЗІ, зокрема на стадіях побудови та здавання в експлуатацію.

Організація ТЗІ на стадії побудови ЦАТС

Заходи та засоби захисту телекомунікаційних мереж та інформації, що циркулює ними, мають застосовуватись на всіх, без винятку, етапах їх життєвого циклу: розробки технічного завдання чи технічних умов на створення, техніко-робочого проектування, будівництва, здавання до експлуатації, власне експлуатації, виведення з експлуатації та утилізації.

При цьому:

- на етапах погодження засобів телекомунікацій, які можуть застосовуватися в телекомунікаційних мережах, одними з критеріїв прийняття рішень є забезпечення надійності та безпеки мереж телекомунікацій;

- розвиток та вдосконалення телекомунікаційних мереж має проводитись з урахуванням технологічної цілісності всіх мереж та їх інформаційної безпеки. Договори на постачання телекомунікаційних засобів та обладнання мають включати в себе вимоги щодо інформаційної безпеки;

- будівництво, реконструкція і модернізація телекомунікаційних мереж не повинні призводити до зниження їх надійності та рівня захищеності.

Проекти будівництва, реконструкції, модернізації телекомунікаційних мереж, та проекти комплексних систем захисту інформації підлягають експертизі в порядку, встановленому

законодавством.

Робоча документація має містити детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію, необхідну для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

На стадії побудови ЦАТС проводиться обстеження цього об'єкта інформаційної діяльності та створюються документи для побудови КСЗІ об'єкта:

- технічне завдання на проектування КСЗІ об'єкта;
- робочий або технічно-робочий проект на створення КСЗІ об'єкта.

Організація ТЗІ на стадії вводу в експлуатацію ЦАТС

При проведенні робіт із введення в дію та оцінки захищеності інформації в телекомунікаційній системі виконуються роботи, передбачені НД ТЗІ 3.7-003- 05 [17], із перевірки КСЗІ на відповідність вимогам нормативних документів з ТЗІ.

При підключенні до об'єктів телекомунікаційних мереж та обладнання інших операторів складаються взаємні вимоги до заходів захисту та порядку захисту інформаційних ресурсів у шлюзових точках підключення інших операторів.

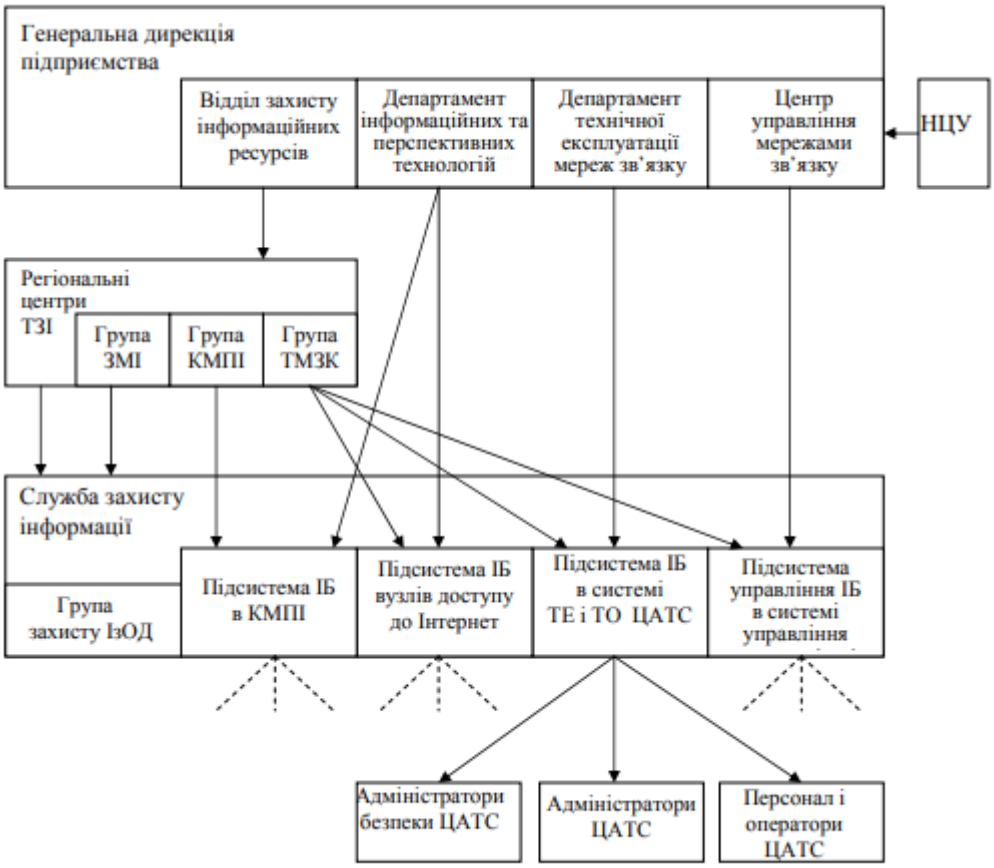
Взаємні вимоги до інформаційної безпеки телекомунікаційних систем оформляються юридично договорами з іншими операторами у порядку, визначеному законодавством.

Організація ТЗІ на етапі технічної експлуатації ЦАТС

Згідно чинної нормативно-правової бази ТЗІ для організації робіт із створення КСЗІ в ЦАТС (чи для групи ЦАТС) створюється служба захисту інформації та призначаються відповідальні особи. Організація та забезпечення діяльності в сфері інформаційної безпеки ЦАТС проводиться не відокремлено, а в тісній взаємодії із всіма службами, які мають відношення до технічної експлуатації телекомунікаційних мереж і, зокрема, ЦАТС.

Схема взаємодії служб наведена на рис. 1

Схемою передбачається функціонування та взаємодія відповідних служб на рівнях Генеральної дирекції, регіональних центрів ТЗІ, філій та безпосередньо в ЦАТС. Розглянемо аспекти організації діяльності, які мають бути сформовані додатково або в складі існуючих. В системі технічної експлуатації і технічного обслуговування (ТЕ і ТО), поряд з підсистемами забезпечення якості, надійності і сталості мереж, створюється підсистема інформаційної безпеки мереж телекомунікацій та ЦАТС. Підсистема виконує такі функції: - створює і забезпечує використання систем моніторингу телекомунікацій, ВОЛЗ та центрів мережі для вирішення комплексного контролю телекомунікацій, виявлення несанкціонованого доступу на фізичному рівні, мережному рівні та на рівні надання послуг, локалізації порушень у найкоротші строки; - створює і підтримує функціонування КСЗІ в ЦАТС у відповідності до державних і галузевих нормативних документів.



Лекція 26

Комплексна система захисту інформації в програмно-керованих АТС

Згідно нормативного документа [8] об'єктом технічного захисту на програмно-керованих АТС, а також на відомчих, корпоративних АТС є конфіденційна, а також відкрита важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих АТС. Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності комплексної системи захисту інформації вимогам із захисту інформації. У цьому розділі розкриваються основні принципи й напрямки забезпечення інформаційної безпеки у відповідності з задачами та функціями ЦАТС, які базуються на нормативно-правових документах України, відповідають вимогам щодо забезпечення конституційних прав людини, проведення заходів із захисту даних споживачів при автоматизованій обробці інформації, захисту засобів телекомунікацій і інформації, що передається телекомунікаційними мережами. Нормативно-правову базу системи захисту інформації в програмнокерованих АТС складають Закони та держстандарти України, комплект НД ТЗІ [9…16] тощо.

Модель цифрового вузла комутації з позицій технічного захисту інформації Для надання послуг якісного, надійного, безпечного телефонного зв'язку має бути сформована надійна захищена інфраструктура ЦАТС та ліній телекомунікацій з використанням доступних та

ефективних засобів і способів інформаційного захисту. Розрізнені заходи щодо інформаційної безпеки, які приймаються при забезпеченні якості послуг, ефективності технічної експлуатації та управління ЦАТС необхідно привести у єдину керовану комплексну систему інформаційної безпеки, яка має забезпечити:

- стійке функціонування ЦАТС та мережі телекомунікацій;

- попередження загроз їхній безпеці; - захист законних інтересів підприємства від протиправних посягань;

- недопущення крадіжки фінансових засобів, розголошення, утрати, спотворення й знищення службової, технологічної, управлінської інформації;

- ефективну виробничу діяльність усіх підрозділів; - підвищення якості наданих послуг та гарантії безпеки майнових прав та інтересів абонентів. Згідно нормативно-правової бази технічний захист інформації спрямований на забезпечення:

- порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, що є об'єктом державної власності та охороняється згідно із законодавством;

- захисту, спрямованому на недопущення блокування інформації, що є державними інформаційними ресурсами, несанкціонованого ознайомлення з нею та/або її модифікації і, в тому числі, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

- захисту від несанкціонованого доступу (НСД) до державних інформаційних ресурсів з боку мереж передачі даних, зокрема, глобальних мереж.

- порядку доступу, цілісності та доступності комерційної та відомчої конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, підприємствах, установах та організаціях;

- захищеності відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює.

Конфіденційність інформації, яка є державним інформаційним ресурсом, під час передавання мережею забезпечує власник автоматизованої системи або оператор мережі передачі даних за договором із власником автоматизованої системи. Заходи щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій, встановлюються власником інформації або розпорядником. Узагальнена модель інфраструктури цифрового вузлу комутації з позицій технічного захисту інформації показана на рис. 1.

Обладнання ЦАТС поділяють на станційну частину, блоки абонентських виносів (БАВ) і мережу абонентських, з'єднувальних та міжстанційних цифрових та аналогових ліній, які є для порушника об'єктами несанкціонованого доступу до них, до інформації, що ними передається, і впливу на їх працездатність. На лініях може бути обладнання, встановлене порушником (ОВП).

Станційна частина виконує функції опорної станції або опорно-транзитної станції і з'єднана з іншими станціями міжстанційними з'єднувальними, а з блоками абонентського виносу – з'єднувальними цифровими лініями Е1 з потрібним числом підсилювальних та регенеративних ділянок. БАВ приєднується до опорної станції, як правило, за інтерфейсом V3.1, V3.2. У якості міжстанційних з'єднувальних ліній можуть використовуватись цифрові канали Е1 з магістральної мережі SDH чи ATM.

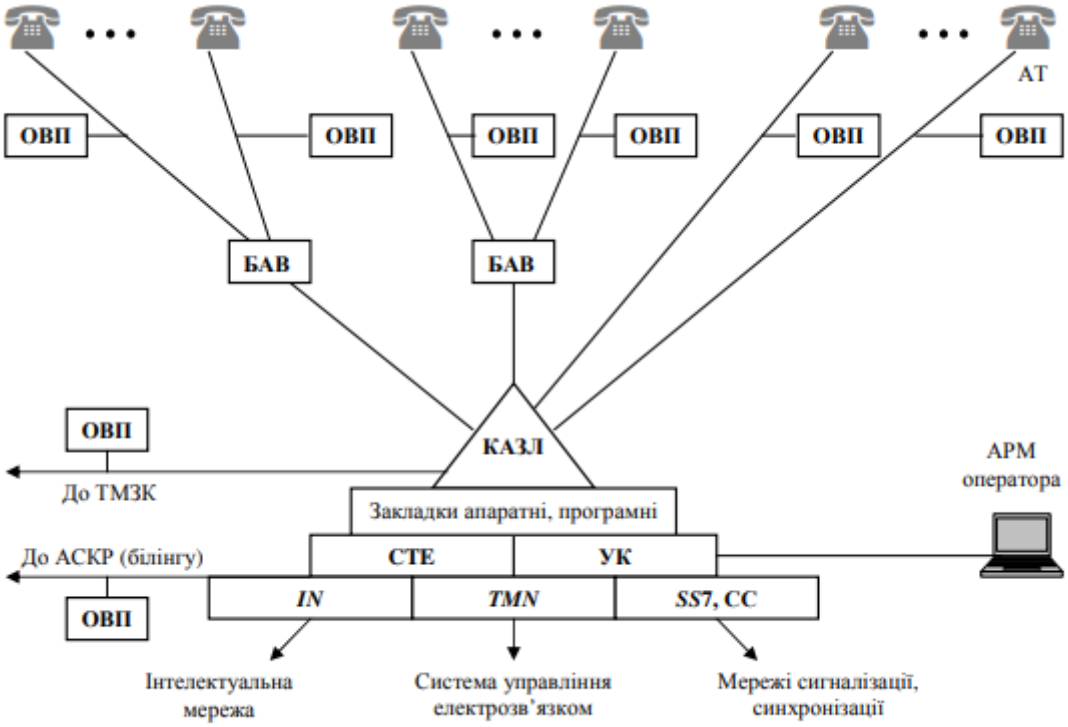


Рисунок 1 - Модель інфраструктури цифрового вузла комутації з позицій захисту інформації

Позначення: АРМ – автоматизоване робоче місце; АСКР – автоматизована система комплексних розрахунків з абонентами; АТ – абонентські термінали; БАВ – блок абонентського виносу; КАЗЛ – підсистема комутації абонентських та з'єднувальних ліній; ОВП - обладнання, встановлене порушниками; СС – система синхронізації; СТЕ – система технічної експлуатації; ТМЗК – телекомунікаційна мережа загального користування; УК – управляючий комплекс; IN - інтелектуальна мережа; TMN - мережа управління телекомунікаціями; SS7 - система сигналізації № 7.

Станційна частина цифрового вузла комутації має у своєму складі:

- підсистему комутації абонентських і з'єднувальних ліній (КАЗЛ);
- управляючий комплекс вузла комутації (УК) з автоматизованими робочими місцями операторів (АРМ оператора);
- підсистему технічної експлуатації (СТЕ) вузла комутації, що дублюється у центрі технічної експлуатації цифрових вузлів комутації, звідки здійснюється віддалений контроль та управління вузлами.

Станційна частина цифрового вузла комутації взаємодіє з наступними технологічними мережами: АСКР – автоматизована система контролю та розрахунків з абонентами для тарифікації наданих телефонних послуг; TMN – мережа управління електрозв'язком для технологічного контролю та адміністративно-бізнесового менеджменту послуг; IN – мережа надання інтелектуальних послуг; SS7 – система сигналізації для управління процесом з'єднання; СС - система синхронізації для отримання опорних тактових частот.

У станційній частині можуть бути виявлені програмні закладки та апаратні закладні пристрої, які виконують не документовані функції і не контролюються системою технічної експлуатації вузла комутації.

Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ наведена на рис. 2 [8].

Схемою виділяються ті елементи станції, які мають безпосереднє відношення до процесів захисту інформації.

Станційне обладнання ЦАТС розміщується на охороняємому об'єкті, де проводиться повний цикл організаційно-технічних заходів з комплексної інформаційної безпеки певного атестованого рівня.

Обладнання програмно - керованих АТС має захищеність базового рівня, яка забезпечується фірмою-виробником даного обладнання.

При встановленні обладнання на мережу рівень захищеності знижується за рахунок можливого впливу на саму систему зі сторони мережі каналами абонентського доступу, сигналізації, синхронізації, тарифікації і системи управління з віддалених терміналів.

Підсистема управління станцією містить у собі:

- спеціалізовані пристрої управління, що реалізують принцип програмного управління і складаються, здебільшого, з процесорів, пристроїв внутрішньої і зовнішньої пам'яті, периферійних пристроїв, спеціалізованих модулів управління сигналізацією, опрацювання викликів, надання послуг і деяких інших програмно-апаратних компонентів, які є характерними для комп'ютерної техніки;

- термінали обслуговування, що приєднані до пристроїв управління через канали технологічного обслуговування АТС і до підсистеми КАЗЛ - через канали інформаційного обслуговування абонентів.

Підсистема КАЗЛ містить у собі пристрої, що реалізують процеси комутації, мультиплексування та концентрації абонентських і міжстанційних з'єднувальних ліній, а також компоненти устаткування абонентських ліній зв'язку - абонентські прикінцеві пристрої, фізичні лінії зв'язку, пристрої мультиплексування абонентських ліній, станційні абонентські комплекти тощо.

На виходах підсистеми управління утворюються в реальному часі потоки технологічних сигналів, за допомогою яких має місце процес управління підсистемою КАЗЛ. З іншого боку, абонентські прикінцеві пристрої мають можливість обмінюватися керуючою інформацією з підсистемою управління станцією через канали управління з'єднаннями й замовлення послуг.

Незалежність підсистем управління станцією і КАЗЛ розуміється в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми управління станцією, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, за передумовою відсутності механізмів реалізації загроз на підсистемі управління з боку підсистеми КАЗЛ і, навпаки, - на підсистемі КАЗЛ з боку підсистеми управління станцією.

Коректність такої декомпозиції структури програмно-керованих АТС обумовлена прийнятими щодо них проектними рішеннями, що не передбачають:

- можливостей штатних впливів на підсистему управління станцією з боку абонентських прикінцевих пристроїв, за винятком можливості запуску абонентом задач із фіксованого набору, що реалізують заздалегідь передбачені функції замовлення абонентом додаткових видів послуг, які надаються станцією;

- можливостей штатних впливів на інформацію в розмовних трактах із боку підсистеми управління станцією, за винятком можливості штатних приєднань до вже встановлених з'єднань (наприклад, із боку телефонного комутатора або абонентських прикінцевих пристроїв у режимі конференц зв'язків), однак з обов'язковим оповіщенням учасників розмови про всі

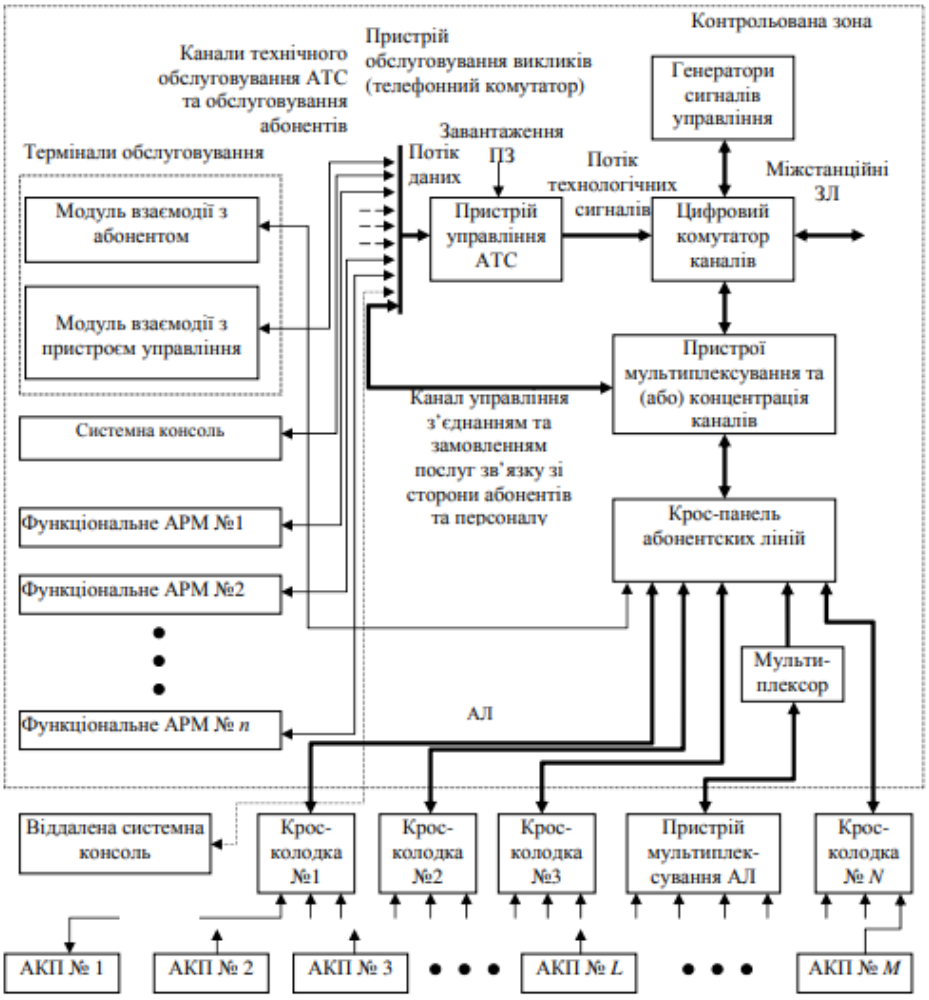


Рисунок 2 - Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ (з НД ТЗІ 1.1-001-99)

Позначення: АКП – абонентські кінцеві прилади (апарати); АЛ – абонентські лінії; АРМ – автоматизоване робоче місце; АТС – автоматична телефонна станція; ЗЛ – з'єднувальні (міжстанційні) лінії; ПЗ – програмне забезпечення; L – поточне число АКП; M – загальна кількість АКП (ємність станції); N – кількість кросових колодок; n – кількість АРМ; контрольована зона – територія, де унеможливлюється присутність сторонніх осіб.

додаткові підключення до їхніх розмовних трактів (зокрема, фоновими тональними сигналами).

Відносність незалежності вищезгаданих підсистем розуміється в тому сенсі, що за певних умов внаслідок помилок або некоректних (зокрема, зловмисних) дій, які були допущені на передексплуатаційних стадіях життєвого циклу АТС (наприклад, при установці програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності АТС, однак,

можливі реалізації загроз на підсистемі управління з боку підсистеми КАЗЛ, і, навпаки, - на підсистемі КАЗЛ з боку підсистеми управління станцією. Далі розглянемо загрози інформації та моделі порушників, які їх здійснюють.

Розглянемо практичний приклад комплексної системи захисту інформації (КСЗІ), яка реалізує функціональний клас послуг безпеки базового рівня (FC-1).

Така КСЗІ базується на штатних засобах захисту інформації й може бути впроваджена у ЦАТС шляхом деякої реорганізації системи технічної експлуатації та додаткових позасистемних засобів захисту.

Основні положення комплексної системи захисту інформації станції

Комплексна система захисту інформації (КСЗІ) створюється згідно пакета НД системи ТЗІ на програмно-керованих АТС загального користування [8…18].

Цифрові комутаційні системи (ЦКС), як правило, оснащуються штатними і, при необхідності, додатковими позаштатними засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), які забезпечують потрібний рівень захищеності інформаційних ресурсів ЦКС, тобто спроможності системи ТЗІ протистояти впливам загроз.

На стадії проектування замовником розробляється підрозділ технічного завдання на будівництво ЦКС за назвою “Вимоги до ТЗІ у ЦКС”, технічний та робочий проекти. На стадії розробки робочого проекту системи ТЗІ у ЦКС виконавцем розробляється КЗМЗ у ЦКС, як взаємопов’язаний набір засобів і механізмів захисту, що реалізують обрану модель захисту.

Модель захисту розробляється на стадії технічного проектування як взаємопов’язаний набір функціональних послуг захисту з необхідними рівнями ефективності і стійкості реалізації цих послуг, за яких забезпечується заданий у технічному завданні рівень захищеності інформаційних ресурсів в ЦКС.

Приклад структури ТЗІ в ЦКС подано на рис. 1, де види забезпечення систем ТЗІ подані з різною глибиною деталізації.

На рисунку 2 є такі позначення: ТС – технологічне середовище; ФПЗ – функціональні послуги захисту. ФПЗ є набором елементарних функцій, виконання яких у середовищі експлуатації ЦКС дозволяє протистояти певній множині загроз для інформації.

Засоби ТЗІ в ЦКС складаються із сукупності фізичних, технічних і програмних підсистем захисту, що функціонують на стадії її експлуатації; системи організаційно-технічних та організаційно-адміністративних заходів; системи ліквідації наслідків реалізованих загроз для інформації на АТС; системи управління засобами ТЗІ.

Підсистеми захисту в ЦКС класифікуються за способами здійснення загроз і в сукупності повинні забезпечувати реалізацію на практиці обраної моделі захисту з необхідними гарантіями. Програмні підсистеми захисту забезпечують реалізацію визначеної номенклатури функціональних послуг захисту. ФПЗ в ЦКС здійснюються за допомогою конкретних засобів і механізмів, що поділяються на штатні та додаткові. Штатні засоби і механізми захисту інформації здебільшого вже закладені в архітектуру сучасних ЦКС або в систему їхньої технічної експлуатації.

Додаткові засоби і механізми захисту розробляються й застосовуються у випадках, коли штатні не забезпечують необхідного рівня захищеності.

Номенклатура штатних ФПЗ складається з функцій захисту:

- від несанкціонованих впливів через штатні засоби доступу;

- від позаштатних впливів через штатні основні або додаткові програмні і/або технічні засоби ЦКС;

- від позаштатних впливів на параметри середовища експлуатації ЦКС;

- від впливів з використанням позаштатних програмними і/або програмнотехнічними засобами на програми, дані і процеси в ЦКС, що встановлені в процесі її експлуатації; від впливів закладних пристроїв і програмних закладок;

- від впливів позаштатними технічними і/або програмно-технічними засобами на елементи устаткування в процесі експлуатації ЦКС; від витоків інформації через канали побічних електромагнітних витоків та наводок (ПЕМВН);

- від витоків інформації через канали побічних акусто-електричних перетворень; від якісної недостатності інформаційно вразливих режимів, функцій і послуг, що надаються ЦКС та від збоїв і відмов у роботі ЦКС;

- від загроз у системах збереження інформації на фізичних носіях.

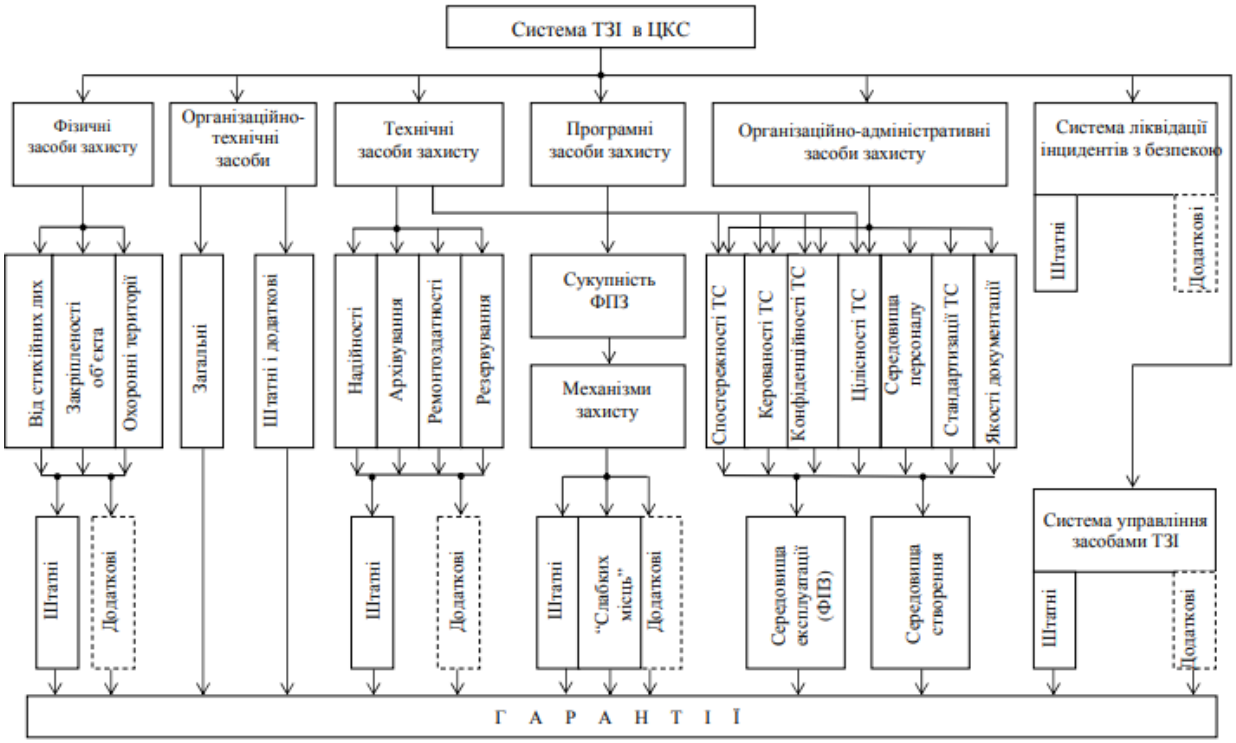


Рисунок 2 – Структура забезпечення системи ТЗІ в ЦКС

Лекція 27

Тема: **Інформаційна модель безепки технологій звязку**

Інформаційна модель захисту даних в технологіях зв'язку: GSM, PSTN, VoIP, ADSL, Wi-

Захист даних в інформаційно-телекомунікаційних системах – один з основних сегментів Національної програми інформатизації та Концепції технічного захисту інформації в Україні.

Триває розвиток нових методів захисту інформації та удосконалення відомих засобів

забезпечення безпеки телекомунікаційних систем.

З метою забезпечення цілісної безпеки структури “система – канал зв’язку– система” розглянемо інформаційну модель захисту даних в технологіях голосової телефонії та передавання даних (рис. 1).

Модель створена на основі принципів системного аналізу – ієрархічності, багатоаспектності, цілісності і характеризує безпеку технологій GSM, PSTN, VoIP, ADSL, Wi-Fi на рівні системи “об’єкт – загроза – захист”.

На основі інформаційної моделі формується комплекс уніфікованих методів і засобів забезпечення безпеки даних в технологіях зв’язку відповідно до нормативного забезпечення.

Технологія GSM: характеристика системи “об’єкт – загроза – захист”.

Технологія GSM (Global System for Mobile Communications) – глобальний цифровий стандарт для мобільного стільникового зв'язку з розділенням частотного каналу за принципом та середнім ступенем безпеки.

Технологія GSM відноситься до мереж 2-го покоління (2G – цифровий стільниковий зв'язок), хоча з 2010 р. умовно знаходилась у фазі 2.75G завдяки численним розширенням. Технологія GSM функціонує в чотирьох частотних діапазонах: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц. Загальна архітектура технології GSM представлена на рис. 2.

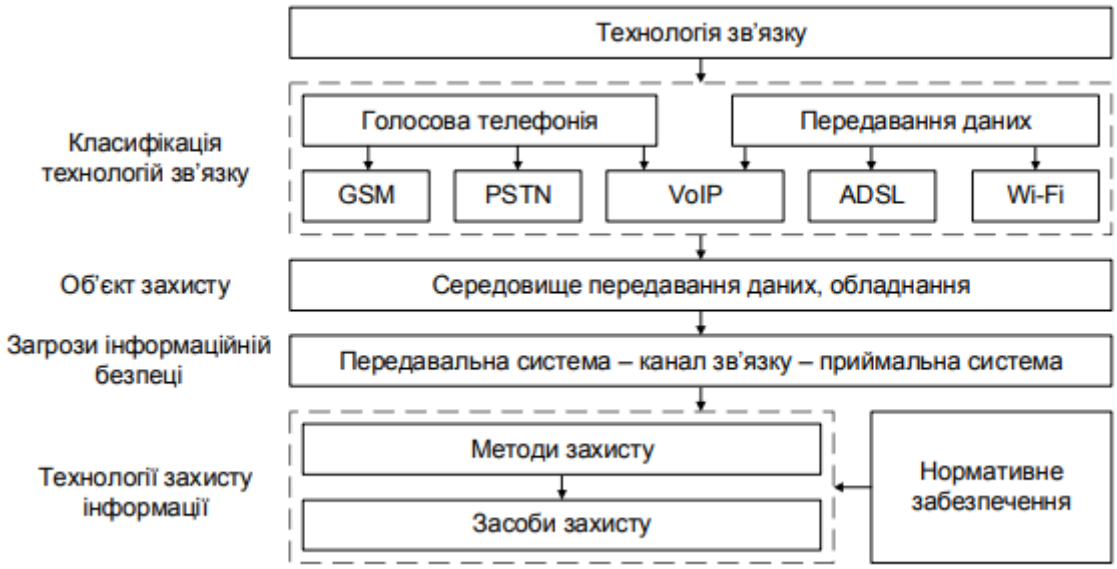


Рисунок 1 - Інформаційна модель захисту даних в технологіях зв'язку

Мобільна станція (МС) із мікропроцесорною картою SIM (Subscriber Identify Modul), в яку занесені унікальні дані для обміну інформацією між абонентами. Контролери базових станцій (КБС) – здійснюють керування базовими станціями (БС) і в подальшому формують з'єднання з центром комутації (ЦК), за допомогою якого можна створити канал передавання даних між двома абонентами. Транскодер (ТР), як проміжна ланка між БС та системою комутації, забезпечує перетворення вихідних сигналів каналу передавання мовного сигналу і даних (64 Кбіт/с) до виду, що відповідає рекомендаціям GSM по радіоінтерфейсу (13 Кбіт/с). В домашньому реєстрі місцезнаходження (ДРМ) зберігається інформація про місцезнаходження будь-якої МС, яка дозволяє центру комутації реалізувати виклик до цієї станції. Загалом ДРМ представляє базу даних (БД), в якій зберігається службова інформація про абонента. Гостьовий реєстр місцезнаходження (ГРМ) – це тимчасова БД абонентів, які знаходяться в зоні дії

відповідного центру комутації.

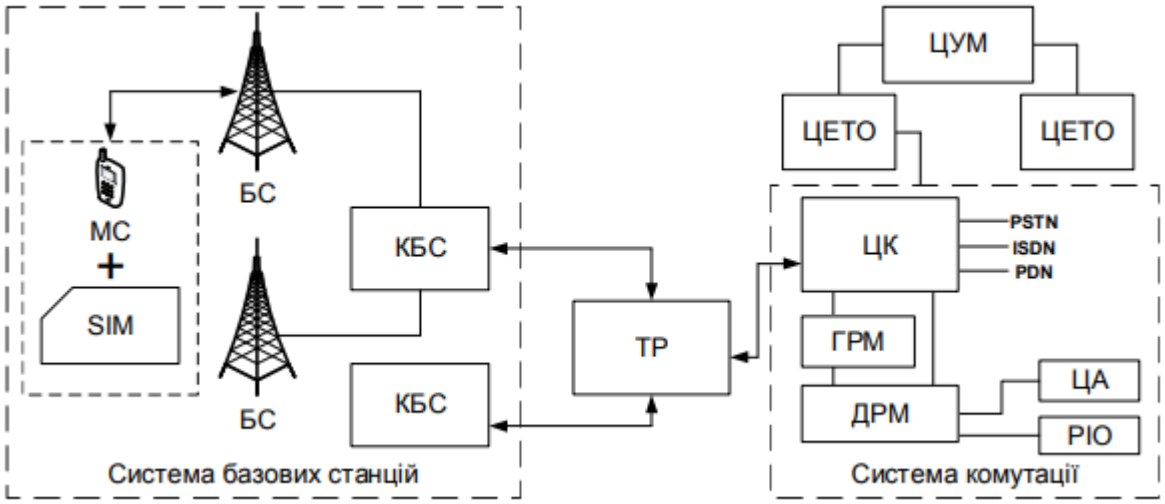


Рисунок 2 - Загальна архітектура технології GSM

У кожного ЦК є лише один гостьовий реєстр місцезнаходження. В ГРМ зберігається та ж інформація. В ГРМ зберігається та ж інформація що і в ДРМ, але лише до того часу допоки МС знаходиться в зоні дії цього ГРМ. Центр автентифікації (ЦА) – це сервіс, за допомогою якого перевіряється право на доступ абонента до мережі, зокрема формуються ключі та алгоритми автентифікації. В ЦА зберігаються: унікальні номери абонента, індивідуальний ключ, алгоритм автентифікації. Реєстр ідентифікації обладнання (РІО) – сервіс, в якому знаходиться централізована БД для підтвердження міжнародного ідентифікаційного номеру МС (IMEI). Центр експлуатації технічного обслуговування (ЦЕТО) – забезпечує контроль і керування іншими компонентами мережі та контроль якості її роботи. Центр управління мережею (ЦУМ) – дозволяє забезпечити раціональне ієрархічне управління мережею GSM та відповідає за експлуатацію і технічне обслуговування. В GSM використовується дві смуги частот: uplink (трансмісія вгору) 890 – 915 МГц, яка призначена для передавання даних від МС до БС; downlink (трансмісія вниз) 935 – 960 МГц відповідно для передавання інформації від БС до МС. Кожна із смуг дозволяє організувати по 124 симплексних канали із частотним рознесенням між каналами до 200 кГц. Враховуючи архітектуру, функціонування та особливості технології GSM розглянемо характеристику системи “об’єкт – загроза – захист” згідно інформаційної моделі (рис. 1) (табл. 1)

Таблиця 1 - Технологія GSM та її характеристика

	Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання	Ефір: Мобільна станція Базові (передавально-приймальні) станції Провідне середовище, або ефір: Контролер базових станцій Транскодер Центр комутації "Домашній" регістр місцезнаходження "Гостьовий" регістр місцезнаходження

		Центр автентифікації Регістр ідентифікації обладнання Центр експлуатації і технічного обслуговування Центр управління мережею
Загрози інформаційній безпеці		Знищення або викривлення логічної структури даних Несанкціоноване отримання інформації та її модифікація Зашумлення каналу зв’язку
Захист інформації: технології	Методи	Шифрування даних в радіоканалі Автентифікація повідомлень Автентифікація користувача Перепризначення TMSI Ідентифікація обладнання
	Засоби	Скремблери Криптофони Інвертори спектру Генератори шуму Змінювачі голосу -карти Шифратори Алгоритми шифрування (A5/1, A5/2, A5/3) Ідентифікаційний номер рухомого терміналу

Технологія PSTN: характеристика системи “об’єкт – загроза – захист”. Технологія PSTN (Public Switched Telephone Network) – це телефонна мережа загального користування (ТМЗК), для доступу до якої використовуються: проводові телефонні апарати, автоматичні телефонні станції (АТС), обладнання передавання даних. Передавання сигналів, налаштування з’єднання, розмова в технології PSTN реалізуються через універсальну лінію зв'язку від АТС джерела до АТС адресата з особливістю встановлення зв’язку між абонентами за умови розмови двох (рис.

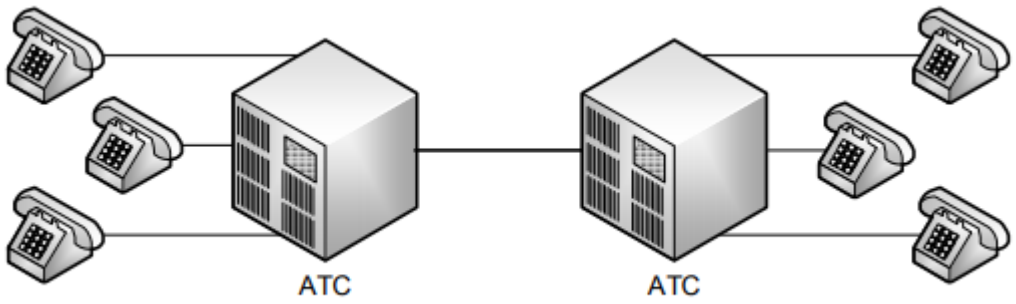


Рисунок 3 - Загальна архітектура технології PSTN

Технологія PSTN нормативно забезпечена стандартами Міжнародного союзу електрозв'язку (ITU-T) і на практиці здебільшого реалізується за зіркоподібною топологією. Поєднання взаємопов'язаних мереж (стандарт Е.163 для ТМЗК) і єдиний міжнародний телекомунікаційний план нумерації (рекомендація Е.164) дозволяють будь-якому абоненту у

глобальному адресному просторі набрати телефонний номер будь-якого іншого абонента. Інформація в мережах такого типу передається зі швидкістю до 33.6 Кб/с. На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології PSTN, враховуючи її особливості (табл. 2)

Таблиця 2 - Технологія PSTN та її характеристика

		Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання		Провідне середовище: Обладнання провайдера – АТС – Комутатори Пристрої клієнти – Телефонні апарати
Загрози інформаційній безпеці		Застосування закладних пристроїв для перехоплення телефонних повідомлень Перехоплення акустичних коливань з пристроїв, які володіють "мікрофонним ефектом" Високочастотне нав'язування Прослуховування приміщень за допомогою виносних мікрофонів Перехоплення побічних електромагнітних сигналів випромінювання і наведень
Захист інформації:\ технології	Методи	Контроль параметрів абонентської телефонної лінії (АТЛ) у робочому стані: – Контроль напруги живлення – Контроль струму короткого замикання – Контроль навантажувальної характеристики – Виявлення сторонніх сигналів Контроль параметрів знеструмлених АТЛ: – Вимірювання опору шлейфа – Вимірювання омічної асиметрії – Вимірювання параметрів імпедансу АТЛ – Контроль вольт-амперної характеристики – Контроль лісажу-характеристики – Контроль перехідної характеристики Послаблення корисного сигналу Фільтрація
	Засоби	Засоби контролю АТЛ: – Сторожові – Пошукові – Універсальні Засоби закриття мовного сигналу: – Скремблери – - Маскувальники – - Вокодери Нелінійні атенюатори Загороджувальні фільтри

Технологія VoIP: система “об’єкт – загроза – захист” Технологія VoIP (Voice over IP) – технологія передавання медіа-даних в режимі реального часу за допомогою системи протоколів

TCP/IP. В технології VoIP аналоговий мовний сигнал від одного абонента дискретизується (кодується), здійснюється компресія та передавання цифровими каналами зв'язку до іншого абонента, де проводиться зворотна операція – декомпресія, декодування і відтворення аналогового сигналу. У випадку, якщо дзвінок надходить на іншу технологію, наприклад PSTN чи GSM, то сигнал проходить через IP-шлюз, який перетворює цифровий (VoIP) сигнал в аналоговий. Для передавання голосу через IPмережу відбувається процедура стискання сигналу спеціальною програмою-кодеком. Це здійснюється для збільшення швидкості передавання даних відповідно для підвищення якості зв'язку. Рівень безпеки передавання мовної інформації підвищує процедура шифрування даних. Зв'язок між двома VoIP-терміналами можливий лише за умови сумісних кодеків. З'єднання двох VoIP-терміналів між собою в мережі забезпечується підтримкою однакового протоколу комутації, наприклад SIP (рис. 4).При передаванні даних в стискання голосового потоку у 8 і більше разів, а деякі з них практично залишають сигнал на рівні імпульсно-кодової модуляції (64 кбіт/с). На основі інформаційної моделі (рис. 1) розглянемо характеристику системи "об'єкт – загроза – захист" для технології VoIP, враховуючи її особливості (табл. 3)

Рисунок 4 - Загальна архітектура технології VoIP

Таблиця 3 - Технологія VoIP та її характеристика

		Характеристики системи "об'єкт-загроза-захист"
Об'єкт: середовище передавання даних, обладнання		Провідне середовище, або ефір: Мережеві пристрої – Маршрутизатор шлюз Пристрої клієнти телефон/ПК з VoIP програмним забезпеченням
Загрози інформаційній безпеці		Відмова в обслуговуванні (DoS) Крадіжка реєстраційних даних і маніпуляція ними Атаки на систему автентифікації Підміна (спуфінг) Caller ID Атаки типу "man in the middle" Атаки типу "Vlan hopping" Спам через Інтернет-телефонію (SPIT) фішинг (Vishing)
Захист інформації: технології	Методи	Ідентифікація/ авторизація користувачів Перевірка обладнання на право доступу до мережі Шифрування даних Забезпечення цілісності

		Контроль авторизованих абонентів Окремий Інтернет-канал для VoIP
	Засоби	Системи виявлення/ запобігання атак Віртуальні приватні мережі Брандмауер VoIP Захищені мережеві протоколи Міжмережеві екрани Системи контролю цілісності

Технологія ADSL: система “об’єкт – загроза – захист” Технологія ADSL (Asymmetric) – технологія широкосмугового доступу, яка забезпечує передавання швидкісного цифрового сигналу звичайною аналоговою телефонною лінією за умови одночасного користування телефоном та Інтернетом. Технологія ADSL відноситься до класу широкосмугових (broadband) та передбачає організацію асиметричного обміну даними (рис. 5).

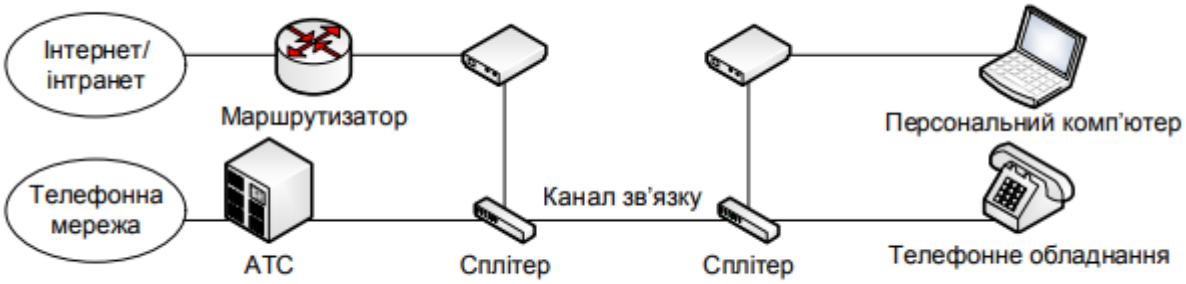


Рисунок 5 - Загальна архітектура технології ADSL

Таблиця 4 - Технологія ADSL та її характеристика

		Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання		провідне середовище: Мережеві пристрої модеми – Сплітери Пристрої клієнти
Загрози інформаційній безпеці		Загрози інформаційній безпеці Відмова в обслуговування (DoS) Крадіжка реєстраційних даних і маніпуляція ними Атаки на систему автентифікації Атаки типу "man in the middle" Несанкціонована модифікація лінії зв'язку
Захист інформації: технології	Методи	Ідентифікація Автентифікація Перевірка обладнання на право доступу до

		мережі Послаблення корисного сигналу Фільтрація
	Засоби	Системи ідентифікації/ автентифікації користувачів Системи виявлення/ запобігання атак Віртуальні приватні мережі Брандмауери; Системи контролю цілісності Нелінійні атенюатори Загороджувальні фільтри

Технологія забезпечує швидкість передавання даних в напрямку абонента – 24 Мбіт/с, від абонента – 3.5 Мбіт/с. В ADSL мовний сигнал передається в частотному діапазоні 0.3 – 3.4 кГц, а інформація в діапазоні 26 кГц – 1104 МГц, який розділений на два піддіапазони: 26 – 138 кГц (для вихідного потоку даних); 138кГц – 1.1МГц (для вхідного). Особливістю технології ADSL є можливість одночасно працювати в Інтернет і розмовляти телефоном. На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології ADSL, враховуючи її особливості (табл. 4). Технологія Wi-Fi: система “об’єкт – загроза – захист” Технологія WI-FI (Wireless Fidelity) – технологія об'єднує декілька протоколів і ґрунтується на системі стандартів IEEE 802.11. На практиці широко використовується протокол IEEE 802.11n, який визначає принцип функціонування безпровідних мереж (рис. 6)

Рисунок 6 - Загальна архітектура технології Wi-Fi

Таблиця 5 - Технологія Wi-Fi та її характеристика

	Характеристики системи "об'єкт-загроза-захист"
Об’єкт: середовище передавання даних, обладнання	Ефір: Базова станція – Маршрутизатор / безпровідна точка доступу Клієнтські пристрої Мобільний пристрій з модулем Wi-Fi Загрози інформаційній безпеці
Загрози інформаційній безпеці	Відмова в обслуговування (DoS) Крадіжка реєстраційних даних і маніпуляція ними Атаки на систему автентифікації Спуфінг Атаки типу "man in the middle" Несанкціоноване отримання інформації та її

		модифікація.
Захист інформації: технології	Методи	Ідентифікація/авторизація користувачів Перевірка обладнання на право доступу до мережі Приховування ідентифікатора мережі Шифрування даних Забезпечення цілісності Обмеження доступу до центрального вузла Контроль авторизованих абонентів
	Засоби	Брандмауери Базові системи автентифікації Протоколи шифрування Модель AAA (Authentication Authorization Accounting) Системи виявлення/запобігання атак Системи приманки Системи контролю цілісності

Функціонування технології Wi-Fi полягає у підключенні мобільного пристрою до точки доступу, роль якої може виконувати як окремий пристрій, так і мобільний, при правильному налаштуванні. Точка доступу розповсюджує свій ідентифікатор (SSID) в ефір за допомогою спеціальних сигналів (“маячків”). На сьогодні в Україні функціонують стандарти: IEEE 802.11a (діапазон частот 5.170 – 5.905 ГГц, максимальна швидкість передавання інформації 54 Мбіт/с), IEEE 802.11b (діапазон частот 2.4 – 2.5 ГГц, максимальна швидкість передавання інформації 11 Мбіт/с), IEEE 802.11g (діапазон частот 2.4 – 2.5 ГГц, максимальна швидкість передавання інформації 54 Мбіт/с), IEEE 802.11n (діапазон частот 2.4 – 2.5 ГГц та 5.170 – 5.905 ГГц, максимальна швидкість передавання інформації 320 Мбіт/с); впроваджується IEEE 802.11ac (максимальна швидкість передавання інформації більше 1Гбіт/с). На основі інформаційної моделі (рис. 1) розглянемо характеристику системи “об’єкт – загроза – захист” для технології Wi-Fi, враховуючи її особливості (табл. 5)

Нормативне забезпечення системи “об’єкт – загроза – захист” для технологій зв’язку На основі інформаційної моделі захисту мовної інформації в ІКТ (рис. 1) розглянемо елементи нормативного забезпечення системи “об’єкт – загроза – захист”, що є основою застосування уніфікованих методів і засобів забезпечення безпеки передавання даних в тракті “система – канал зв’язку – система” (табл. 6).

Таблиця 6 - Нормативне забезпечення захисту мовної інформації в ІКТ

Закони та постанови	Закон України “Про захист інформації в інформаційнотелекомунікаційних системах” від 05.07.1994 №80/94-ВР Постанова Кабінету міністрів “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” від 29.03.2006 № 373. Остання редакція від 13.10.2011
Стандарти	1. Захист інформації. Технічний захист

	інформації. Основні положення: ДСТУ 3396.0-96. – [Чинний від 1997-01-01] – К.: Держстандарт України, 1996 – 20 с. – (Державний стандарт України). 2. 2. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. – [Чинний від 1997-07-01] – К.: Держстандарт України, 1996 – 4с. – (Державний стандарт України). 3. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – [Чинний від 1998-01-01] – К.: Держстандарт України, 1997 – 6 с. – (Державний стандарт України). 4. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, шо ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145-2002. – [Чинний від 2003-07-01]. – К.: Держспоживстандарт України, 2002. – 38 с. – (Національний стандарт України). 5. Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення (ISO/IEC 10118 – 1 : 2000, IDT): ДСТУ ISO/IEC 10118-1:2003. – [Чинний від 2005-01-01]. – К.: Держспоживстандарт України, 2003. – 10 с. – (Національний стандарт України). 6. Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використанням n-бітового блокового шифру (ISO/IEC 10118 – 2 : 2000, IDT): ДСТУ ISO/IEC 10118-2:2003. – [Чинний від 2005-01-01]. – К.: Держспоживстандарт України, 2003. – 24 с. – (Національний стандарт України). 7. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення (ISO/IEC 14888-1:1998, IDT): ДСТУ ISO/IEC 14888-1-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 18 с. – (Національний стандарт України). 8. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми на основі ідентифікаторів (ISO/IEC 14888 – 2 : 1999, ГОТ): ДСТУ ISO/IEC 14888-2-2002. – [Чинний від 2006-10-01]. – К.: Держспоживстандарт України, 2002. – 22 с. – (Національний стандарт України).

	9. Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів (ISO/IEC 14888 – 3 : 1998, IDT): ДСТУ ISO/IEC 14888-3-2002. – [Чинний від 2006-10-]. – К.: Держспоживстандарт України, 2002. – 34 с. – (Національний стандарт України). 10. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий: ГОСТ Р ИСО/МЭК 13335-1-2006. – [Чинний від 2007-06-01]. – М.: Стандартинформ, 2007. – 23 с. – (Межгосударственный стандарт). 11. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.05.1999 №26: НД ТЗІ 2.5-001-99. – [чинний від 1999-07- 01]. – К.: ДСТСЗІ СБ України, 1999 – 56 с. – (Нормативний документ). 12. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.05.1999 №26: НД ТЗІ 2.5-002-99. – [чинний від 1999-07-01]. – К.: ДСТСЗІ СБ України, 1999 – 16 с. – (Нормативний документ). 13. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 06.04.2001 №11: НД ТЗІ 2.3-002-2001 [чинний від 2001-04-10]. – К.: ДСТСЗІ СБ України, 2001 – 11 с. – (Нормативний документ). 14. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. – [Чинний від 2005-11-08]. –

	К.: ДСТСЗІ СБ України, 2005. – 16 с. – (Нормативний документ системи технічного захисту інформації). 15. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – [Чинний від 2010-01-01. – К.: Національний банк України, 2010. – 49 с. – (Галузевий стандарт Україїни). 16. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 – [Чинний від 2010-01-01. – К.: Національний банк України, 2010. – 163 с. – (Галузевий стандарт Україїни).

Список літератури :

1 Закон України “Про Національну програму інформатизації” від 4 лютого 1998 року №74/98- ВР. Остання редакція від 02.12.2012. – [Електронний ресурс]. – Режим доступу:

2 Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 № 1126. Остання редакція від 13.10.2011. – [Електронний ресурс]. – Режим д

3 Щербаков, В. Б. Защита беспроводных телекоммуникационных систем: учеб. пособие / В. Б. Щербаков, А. В. Гармонов, С. А. Ермаков и др. – Воронеж: ФГБОУ ВПО “Воронежский государственный технический университет”, 2013. – 127 с.

4 Рибачек, Н. І. Аналіз захищеності інформаційної системи / Н. І. Рибачек // К.: Національний технічний університет України “Київський політехнічний інститут”: Прикладна математика та комп’ютинг, 2010. – С. 122-125.

5 Дудикевич, В. Б. Захист засобів і каналів телефонного зв’язку: Навчальний посібник / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Л.: Видавництво Львівської політехніки, 2012. – 210 с.

6 Попов, В. И. Основы сотовой связи стандарта GSM / В. И. Попов. – М.: Эко-Трендз, 2005. – 296 с.

. – [Електронний ресурс]. – Режим доступу: http://www.telecomspace.com/ gsm.html.

8 Дудикевич, В. Б. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв’язку / В. Б. Дудикевич, Ю. Р. Гарасим, Г. В. Микитин // Вісник Національного університету “Львівська політехніка”: Автоматика, вимірювання та керування, 2010. – № 665. – С. 18-26.

9 Вайнгартнер, М. Защита голосовых соединений VoIP от прослушивания / М. Вайнгартнер // Журнал сетевых решений/LAN, 2003. – № 12. – [Электронный ресурс]. – Режим доступа: http://www.osp.ru/lan/2003/12/138398.

10 Челнокова, О. ADSL-маршрутизаторы с поддержкой VPN / О. Челнокова // Information Security / Информационная безопасность, 2008. – №2. – С. 32-33.

11 Владимиров, А. А. Wi-фу: "боевые" приемы взлома и защиты беспроводных сетей. Серия "Защита и администрирование" / А. А. Владимиров, К. В. Гавриленко, А. А.

Михайловский. – М.: NT Press, 2005. – 463 с.
12 Гордейчик, С. В. Безопасность безпроводных сетей / С. В. Гордейчик, В. В. Дубровин. – М.: Горячая линия - Телеком, 2008. – 288 с.

Лекція 28

Тема: **Забезпечення інформаційної безпеки в системі стільникового зв'язку стандарту GSM , CDMA**

1 Забезпечення інформаційної безпеки стандарту GSM

При входженні в мережу абонентських станцій (MS) здійснюється їх аутентифікация та ідентифікація.

Процедура аутентифікації закриває несанкціонований доступ до мережі.

Ідентифікація – процедура ототожнення MS, тобто процедура встановлення належності MS до однієї з груп, яким присвоєні певні ознаки. Ця процедура забезпечує виявлення несправних, загублених або вкрадених MS (мобільних телефонів).

Ідея аутентифікації в цифрових СМЗ полягає в шифруванні паролів-ідентифікаторів із використанням квазівипадкових чисел, що періодично передаються на MS з ЦКРЗ, та індивідуального для кожної АС алгоритму шифрування. Таке шифрування виконується на MS і ЦКРЗ, результати шифрування порівнюються.

Аутентифікація вважається закінченою, якщо результати на MS і ЦКРЗ збігаються і MS допускається до обслуговування в мережі.

Аутентифікація у стандарті GSM пов'язана з використанням SIM-карти (модуля ідентифікації абонента). SIM-карта – модуль (типу пластикової картки), що вставляється у відповідне гніздо мобільного телефону (SIM-карта однакова для всіх різновидів стандарту GSM: GSM-900, GSM-1800 і GSM-1900). Модуль містить:

- PIN (Personal Identification Number) – персональний ідентифікаційний номер абонента (PIN-код);
- IMSI (International Mobile Subscriber Identity) – міжнародний ідентифікатор абонента мобільної станції;
- K_i – індивідуальний ключ аутентифікації абонента;
- А3 – індивідуальний алгоритм аутентифікації абонента;
- А8 – алгоритм обчислення ключа шифрування.

Після включення MS із встановленою SIM-картою абонент зобов'язаний, насамперед, зняти блокування останньої – ввести PIN-код, відомий тільки абоненту, що є захистом від несанкціонованого використання SIM-карти, наприклад, під час її втрати. Після трьох невдалих спроб набору PIN-коду SIM-карта блокується. Блокування може бути зняте або набором додаткового коду – персонального коду розблокування PUK (Personal Unblocking Key), або командою з центра комутації.

Коли SIM-карта виймається з MS, вона зберігає всю інформацію, що міститься на ній: персональні ідентифікатори, ключі, шифри і паролі, а також записані абонентом номери

телефонів і повідомлення, і може працювати з іншими MS стандарту GSM. Таким чином, SIM-карта немовби «персоналізує» абонентський апарат MS, у який вона встановлюється.

Процедура аутентифікації зображена на рис.1

АС запрошує доступ до мережі. Регістр аутентифікації (РА) через ЦКРЗ видає випадкове число RAND. АС, отримавши RAND, за допомогою ключа K_i і алгоритму А3 обчислює маркірований відгук SRES (нове число S_1) і передає його в ЦКРЗ, де він порівнюється з тим відгуком, що формується в регістрі аутентифікації. Якщо S_1 і S_2 збігаються, то ЦКРЗ видає дозвіл на доступ АС до мережі.

Ідентифікація обладнання здійснюється в такий спосіб.

ЦКРЗ запитує в АС номер IMEL. Отриманий номер надходить у регістр ідентифікації обладнання (РІО), де є списки обладнання (АС):

- дозволених до використання;
- заборонених до використання;
- несправних.

За результатами аналізу видається інформація про те, до якої групи належить абонент (АС) з отриманим від нього номером IMEL, після чого ЦКРЗ приймає рішення щодо допуску АС до мережі.

Закриття (шифрування) інформації, що передається радіоканалом, здійснюється на БС та АС (застосовуються однакові алгоритми). Для закриття інформації використовується номер циклу доступу та ключ закриття (шифрування) інформації K_C. На БС використовується K_C, а на АС він обчислюється на підставі отриманого випадкового числа RAND і абонентського ключа K_i по алгоритму А8. Алгоритм А8 зберігається в SIM-карті. Отримавши RAND, АС обчислює крім відгуку SRES ключ шифрування K_C (з використанням RAND, K_i та алгоритма А8).

Для встановлення режиму шифрування мережа передає на АС MS команду до переходу у режим шифрування (СМС). Після прийняття цієї команди MS починає шифрування, використовуючи ключ шифрування K_C та алгоритм шифрування А3.

Потік шифрованих бітів передається в мережу і дешифрується перед видачею інформації абоненту.

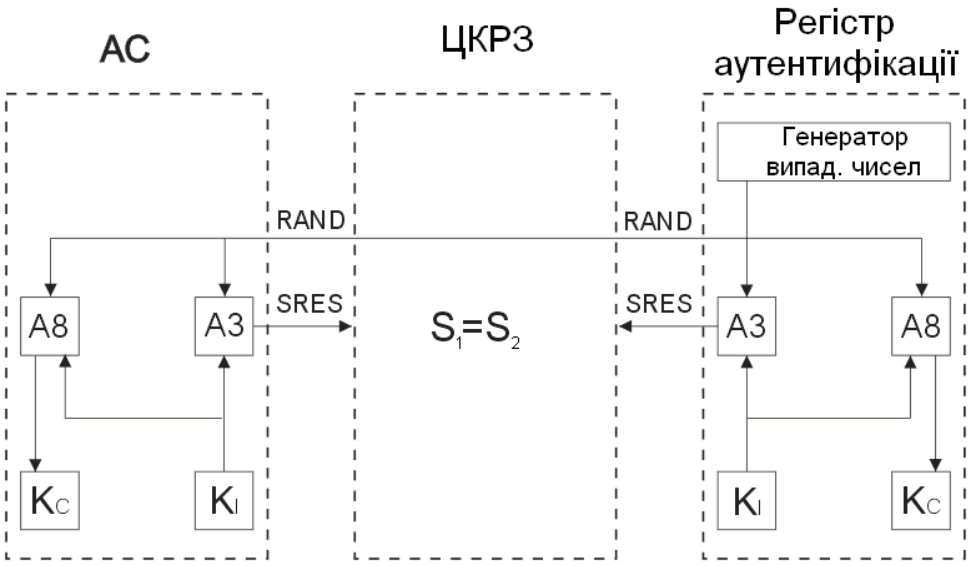


Рисунок 1 – Схема процедур аутентифікації з шифрування у стандарті GSM

2 Безпека абоненської інформації в стандарті CDMA

Безпека абонентської інформації в цьому стандарті базується на чотирьох фундаментальних елементах:

1) функція CAVE (CellularAuthentificationandVoiceEncryption) Н функція перемішування, що використовується в протоколах аутентифікації запит Н відповідь і для генерації ключів,

2) операція XOR Н повторювана маска, накладається на голосові дані для забезпечення безпеки їх передачі,

3) шифр ORYX Н потоковий шифр, призначений для використання в послугах бездротового доступу до даних;

4) шифр CMEA (ControlMessageEncryptionAlgorithm) Н простий блоковий шифр, використовується для шифрування службових повідомлень. Криптографічні протоколи стандарту CDMA грунтуються на 64Нбітному аутентифікаційні ключі AHkey і серійному номері мобільного телефону ESN (ElectronicSerialNumber). Для аутентифікації абонента при реєстрації мобільного телефону в мережі а також подальшої генерації допоміжних ключів, приймають участь в забезпеченні конфіденційності передачі голосових даних і кодованих повідомлень використовується випадкове двійкове число RANDSSD (RandomSharedSecretData), генерованого аутентификационного центром AC (AuthentificationCenter) реєстру власних абонентів HLR (HomeLocationRegister). Ключ AHkey запрограмований в мобільному телефоні а також зберігається в центрі аутентифікації мереж.

Стандартизований алгоритм шифрування CAVE використовується для генерації 128 бітного підключа SSD. Таким чином ключ AHkey, серійний номер ESN і сгенерированное мережею випадкове число RANDSSD подаються на вхід алгоритму CAVE, який в свою чергу генерує допоміжний ключ SSD. Цей ключ складається з двох частин: SSD_A, використовуваний для створення аутентифікаційні цифрового підпису, і SSD_B, використовуваний при генерації ключів для шифрування голосових даних і службових повідомлень. Ключ SSD може бути переданий іншій мережі при роумінгу абонента для забезпечення локальної аутентифікації. Новий SSD може бути згенерований при поверненні абонента в домашню мережу або зміні гостьовий мережі у роумінгу. Мережа генерує і розсилає відкрито в ефір випадкове число RAND, а мобільні пристрої, які реєструються в мережі, використовують його як вхідні дані для алгоритму CAVE, який генерує 18Нбітній цифрового підпису AS (AuthentificationSignature), і посилає його на базову станцію. Цей цифрового підпису звіряється в центрі комутації MSC (MobileservicesSwitchingCenter) з підписом згенерованим самим центром комутації для перевірки легітимності абонента. При цьому випадкове число RAND може бути як однаковим для всіх користувачів, так і заново генеруватися кожен раз, використання конкретного методу визначається оператором. Перший варіант забезпечує дуже швидку аутентифікацію.

Як мобільний телефон так і мережу ведуть 6Нбітові лічильники дзвінків, що забезпечує можливість детектування двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні і в центрі комутації MSC. Секретний ключ

AHkey може бути перепрограмовано при необхідності, але в разі його зміни інформація на мобільному телефоні і в регістрі мережі HLR повинна бути синхронізована. Зміна ключа може бути прошита на заводі, дилером в точці продажу, абонентом через інтерфейс телефону, а також за допомогою спеціального сервісу OTASP (OverTheAirAerviceProvisionig) .Цей сервіс використовує в процесі передачі 512 бітний алгоритм узгодження ключів ДіффіНХелмана, що гарантує достатньо високий рівень безопасності.OTASP забезпечує легкий спосіб зміни ключа AH key мобільного телефону на випадок появи в мережі двійника мобільного телефону, оскільки така зміна автоматично спричинить відключення послуг двійника мобільного телефону і повторне включення послуг легітимного абонента. Таким чином таємність ключа AHkey є практично важливою компонентою безпеки CDMA системи.

Як було вже сказано, для аутентифікації абонента в CDMA мережі використовується допоміжний ключ SSD_A генерований CAVE алгоритмом з A-key, ESN і RANDSSD. Мережа генерує і розсилає відкрито по ефіру випадкове число RAND*, мобільні пристрої, що реєструються в мережі, використовують його як вхідні дані для CAVE алгоритму, що генерує 18- бітну аутентифікаційні цифровий підпис (AUTH_SIGNATURE), і посилає його на базову станцію. Цей цифровий підпис звіряється в центрі комутації (далі згадується як MSC - Mobile services Switching Center) з підписом генерується самим MSC для перевірки легітимності абонента. Число RAND* може бути як одним і тим же для всіх користувачів, так і генеруватися кожен раз нове (використання конкретного методу визначається оператором). Перший випадок забезпечує дуже швидку аутентифікацію.

І мобільний телефон і мережа ведуть 6-бітові лічильники викликів, що забезпечує можливість детектування працюючих двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні і в MSC.

Секретний ключ A-key є перепрограмувальний, у разі його зміни інформація на мобільному телефоні і в HLR/AC повинна бути синхронізована. A-key може бути перепрошитий декількома способами: на заводі, дилером в точці продажу, абонентом через інтерфейс телефону, а також за допомогою OTASP (over the air service provisionig). OTASP передачі використовують 512 бітний алгоритм узгодження ключів Diffie- Hellman'a, що гарантує достатню безпеку. OTASP забезпечує легкий спосіб зміни A-key мобільного телефону на випадок появи в мережі двійника мобільного телефону. Зміна A-key автоматично спричинить відключення послуг двійникові мобільного телефону і повторне включення послуг легітимному абоненту. Таким чином, як можна було помітити, секретність A- key є найважливішою компонентою безпеки CDMA системи.

Процес шифрування інформації абонента в стандарті CDMA

Безпека передачі голосових даних, інформації та службових повідомлень досягається наступним чином. Мобільний телефон

використовує допоміжний подключ SSD_B і CAVE алгоритм для генерації Private Long Code Mask (успадковану від TDMA мереж), 64-бітного підключа CMEA (Cellular Message Encryption Algorithm) key і 32-бітного DATA-key Private Long Code Mask використовується як мобільним телефоном, так і мережею для зміни характеристик Long Code Mask. Цей модифікований Long Code використовується для шифрування голосових даних, що підвищує секретність їх передачі.

Private Long Code Mask не шифрується інформацію, вона просто замінює відомі величини, використовувані в кодуванні CDMA сигналу секретними величинами, відомими

тільки мобільному телефону та мережі. Таким чином підслуховування розмов без знання Private Long Code Mask є надзвичайно складним завданням.

Більше того, мобільний телефон і мережа використовують CMEA і покращений CMEA (E_CMEA) алгоритми для шифрування і дешифрування службових повідомлень при передачі їх по ефіру. Окремий DATA-key і алгоритм шифрування ORYX використовується мобільним телефоном і мережею для шифрування і дешифрування потоку інформації по каналу зв'язку CDMA. рис. ілюструє механізми аутентифікації і шифрування в CDMA мережі.

Анонімність CDMA мереж підтримує призначення мобільному телефону тимчасового ідентифікатора мобільного абонента TMSI (Temporary Mobile Station Identifier) для його представлення в процесі передачі інформації по ефіру між мобільним телефоном і мережею. Ця функція ще більш ускладнює зіставлення даних, що передаються конкретному абоненту.

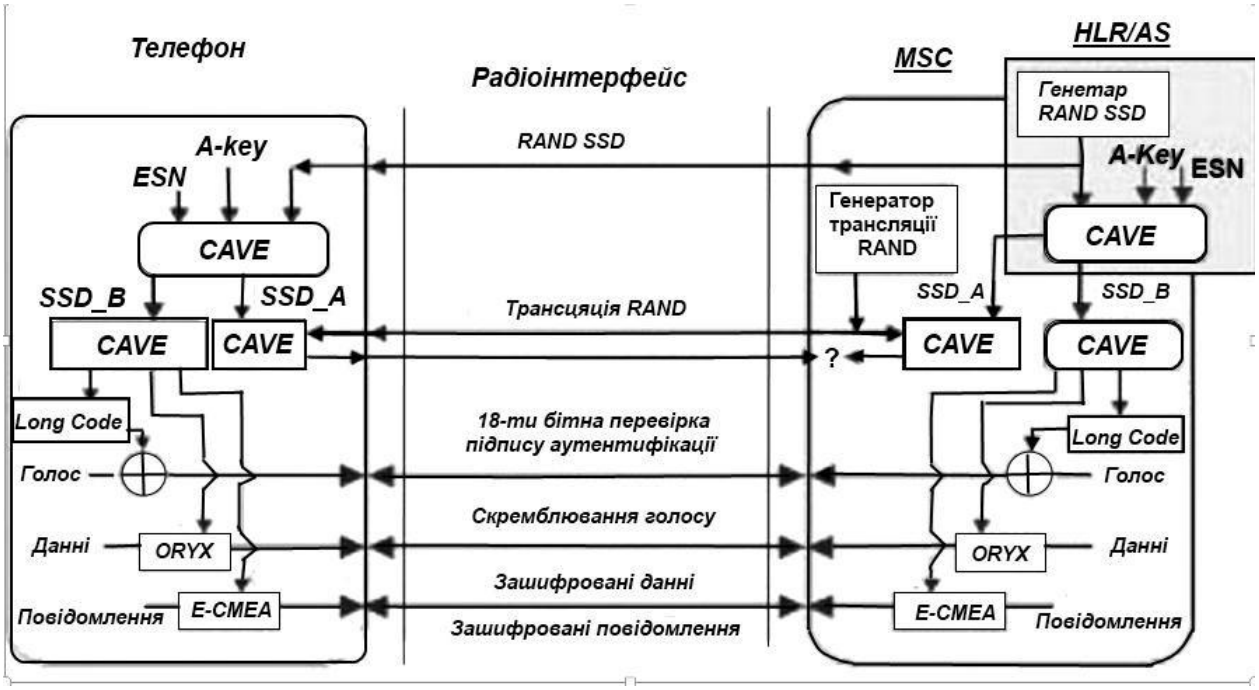


Рисунок 1 - Механізми аутентифікації і шифрування в CDMA мережі

3 Загальний опис захисту інформації GSM

Стільникові системи рухомого зв'язку нового покоління мають можливість прийняти всіх потенційних користувачів, якщо будуть гарантована безпека зв'язку: таємність і аутентифікація. Таємність повинна виключити можливість доступу до інформації в каналах зв'язку будь-кому, крім санкціонованого одержувача. Проблема аутентифікації полягає в тім, щоб перешкодити кому-небудь, крім санкціонованого користувача (відправника), змінити канал, тобто одержувач повинний бути упевнений, що в даний момент він приймає повідомлення від санкціонованого користувача. Основним способом забезпечення таємності є шифрування. Відносно нова концепція - використання шифрування як способу аутентифікації повідомлень.

Аутентифікація повідомлень через шифрування здійснюється за рахунок включення в текст так називаного коду ідентифікації (тобто фіксованого чи залежного від переданих даних

слова, що знають відправник і одержувач, яке вони можуть виділити в процесі передачі). Одержувач розшифровує повідомлення, шляхом порівняння одержує посвідчення, ще прийняті дані є саме даними санкціонованого відправника.

До системи шифрування пред'являються наступні основні вимоги:

1) нелінійні зв'язки між вихідним текстом і зашифрованим текстом;
2) зміна параметрів шифрування в часі.

Якщо алгоритми шифрування відповідають першій вимозі, то, не знаючи ключа виключається можливість змінити код ідентифікації, щоб уникнути виявлення факту несанкціонованого доступу. Друга вимога виключає можливість порушення роботи системи за рахунок відтворення "виявлячем" прийнятого раніше і записаного в пам'яті повідомлення.

Один шлях забезпечення цих вимог - застосування синхронних систем передачі, але при цьому необхідні системи циклової і тактової синхронізації, що в багатьох випадках неприйнятно.

Інший шлях - включення в інформаційну послідовність (кожне повідомлення тимчасових міток так, щоб зашифровані дані були б однозначно з ними зв'язані. Алгоритми шифрування поділяються на два класи [3-5]:

-класичні алгоритми,

- алгоритми з відкритим ключем.

Класичні алгоритми використовують один ключ для шифрування- дешифрування. Алгоритми з відкритим ключем використовують два ключі:

•перший - для переходу від нешифрованого тексту до шифрованого;

•другий - для зворотного переходу від шифрованого до нешифрованого.

Причому знання одного ключа не повинне забезпечити виявлення другого ключа. У цих алгоритмах один із ключів, звичайно використовуваний для шифрування, можна зробити загальним, і тільки ключ, використовуваний для розшифровки, повинний бути засекречений. Ця особливість дуже корисна для зниження складності протоколу й інтеграції структур шифрування в мережах зв'язку.

Алгоритми шифрування з відкритим ключем побудовані на визначенні однобічної функції, тобто деякої функції f такої, що для будь-якого x з її області визначення f (x) легко вираховується, однак практично для усіх y з її області значень перебування x, для якого y=f(x) обчислювано, не здійсненно [3-5]. Тобто, однобічна функція є окремою функцією, що легко розраховується ЕОМ у прийнятному обсязі часу, але час розрахунку зворотної функції в існуючих умовах неприпустимо великий.

Перший алгоритм шифрування з загальним ключем був названий RSA (перші букви прізвищ авторів Rivest, Shamir, Adieman). Алгоритм базується на двох функціях E й D, зв'язаних співвідношенням:

D (E(x) = E (D(x)).

Одна з цих функцій використовується для шифрування повідомлень, інша - для дешифрування.

Таємність алгоритму базується на тому, що знання функції E (чи D) не відкриває легкого способу обчислення E (чи D). Кожен користувач робить загальною функцію E та зберігає в секреті функцію D, тобто для користувача X є відкритий ключ Ex і секретний Dx.

Два користувачі A й B можуть використовувати алгоритм RSA, щоб передати будь-яке

зашифроване повідомлення. Якщо абонент А хоче відправити повідомлення М абоненту В, то він може зробити це в такий спосіб:

-зашифрувати повідомлення М;

-підписати повідомлення М;

-зашифрувати і підписати М.

В першому випадку: А забезпечує перетворення М, використовуючи відкритий ключ 3 = Ев (М) і посилає його абоненту В. В приймає С й обчислює db (c) = db (Ев (М)) = М.

В другому випадку: А підписує М за допомогою обчислення F = Da

(M)

і посилає F абоненту В (ці операції може здійснювати тільки користувач А, якому відомий секретний ключ Da). В одержує F і обчислює Ea (F) = Ea (Da (M)) = M.

В тепер відомо, що повідомлення М дійсне послане користувачем А. В цьому випадку таємність повідомлення М не гарантується, тому що усі можуть здійснити таку ж операцію з використанням загального ключа Еа.

В третьому випадку: А обчислює

F = Da (M) і 3 = Ев (F) = Ев (Da (M);

А посилає С до В. В одержує С та обчислює db (c) = db (Ев (F)) = Da (M); В може тепер легко одержати М, обчисливши Ea (Da (M)) = M.

До операції шифрування і відносимо кожне повідомлення М, яке повинне розділятися на блоки фіксованої довжини, потім кожен блок кодується як сукупність фіксованого числа цифр. RSA кодер оперує такими окремими блоками в кожнім циклі кодування.

Алгоритм шифрування з відкритим ключем RSA забезпечує високий ступінь безпеки передачі мовних повідомлень і рекомендований до використання в цифрових системах рухомого радіозв'язку нового покоління.

У стандарті GSM термін "безпека" розуміється як виключення несанкціонованого використання системи і забезпечення таємності переговорів рухомих абонентів. Визначено наступні механізми безпеки в стандарті GSM :

-аутентифікація;

-таємність передачі даних;

-таємність абонента;

-таємність напрямків з'єднання абонентів.

Захист сигналів керування і даних користувача здійснюється тільки по радіоканалі.

Розглянемо послідовно механізми безпеки в стандарті GSM, загальний склад секретної інформації, а також її розподіл в апаратних засобах GSM системи.

4 Механізми аутентифікації

Для виключення несанкціонованого використання ресурсів в системі зв'язку вводяться і визначаються механізми аутентифікації - посвідчення дійсності абонента. Кожен рухомий абонент на час користування системою зв'язку одержує стандартний модуль дійсності абонента (SIM-карту), що містить:

-міжнародний ідентифікаційний номер рухомого абонента (IMSI);

-свій індивідуальний ключ аутентифікації (Ki);

-алгоритм аутентифікації (А3).

За допомогою закладеної в SIM інформації в результаті взаємного обміну даними між рухомою станцією і мережею здійснюється повний цикл аутентифікації і дозволяється доступ абонента до мережі.

Процедура перевірки мережею дійсності абонента реалізується в такий спосіб. Мережа передає випадковий номер (RAND)) на рухому станцію. Рухома станція визначає значення відгуку (SRES), використовуючи RAND, Ki і алгоритм А3:

SRES = Ki[RAND].

Рухома станція посилає обчислене значення SRES у мережу, що звіряє значення прийнятого SRES зі значенням SRES, обчисленим мережею.Якщо обоє значення збігаються, рухома станція може здійснювати передачу повідомлень. У противному випадку зв'язок переривається, і індикатор рухомої станції повинний показати, що розпізнання не відбулося. Через таємність обчислення SRES відбувається в рамках SIM.

Таємність передачі даних

Для забезпечення таємності переданої по радіоканалі інформації вводиться наступний механізм захисту. Усі конфіденційні повідомлення повинні передаватися в режимі захисту інформації. Алгоритм формування ключів шифрування (А8) зберігається в модулі SIM. Після прийому випадкового номера RAND рухома станція обчислює, крім відгуку SRES, також і ключ шифрування (Кс), використовуючи RAND, Ki і алгоритм А8 (Рис.2).

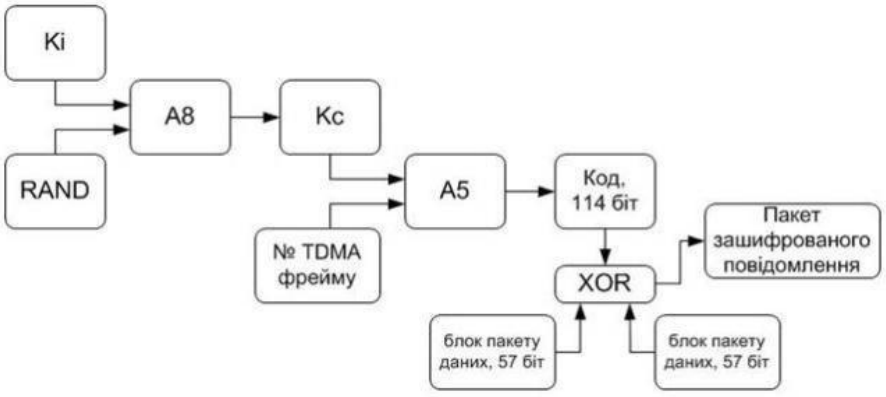


Рисунок 2 - Алгоритм шифрування А8

Ключ шифрування Кс не передається радіоканалом. Як рухома станція, так і мережа обчислюють ключ шифрування, що використовується іншими рухомими абонентами. Черезтаємність, обчислення Кс відбувається в SIM.

Щоб уникнути неправильного формування ключа Кс, БС разом із числом rand посилає МС числову послідовність, що пов'язана з дійсним значенням Кс. Довжина ключа Кс на виході алгоритму А8 дорівнює 64 биткам.

Після обчислення й перевірки ключа Кс БС передає МС команду про перехід у режим шифрування. Мобільна станція, маючи ключ шифрування Кс, приступає до зашифрування й розшифруванню повідомлень. Потік переданих даних шифрується побітно за допомогою алгоритму А5, приведеного на рис. 3.

Алгоритм А5 виводить послідовність, що шифрує, довжиною 114 біт для кожного кадру

окремо. На вхід схеми надходить номер кадру (Nk) довжиною 22 біта й ключ Кс довжиною 64 біта. В обох напрямках з'єднання використаються дві різні послідовності: одна для зашифрування вихідного пакета даних, друга для розшифрування вхідного пакета даних. Номер кадру Nkміняється від пакета до пакета переданих повідомлень, а ключ Кс - при кожному новому сеансі зв'язку.

Процедура шифрування повідомлень у стандарті GSM:

Стандарт GSMпідтримує два варіанти алгоритму А5 (А5/1 - більше криптостойкій алгоритм, А5/2 - менш криптостойкій алгоритм).

Числова послідовність ключа шифрування

Крім випадкового числа RAND мережа посилає рухомої станції числову послідовність ключа шифрування. Це число зв'язане з дійсним значенням Кс і дозволяє уникнути формування неправильного ключа. Число зберігається рухомою станцією і міститься в кожному першому повідомленні, що передане в мережу. Деякі мережі приймають рішення про наявність числової послідовності діючого ключа шифрування у випадку, якщо необхідно приступити до розпізнання, якщо виконується попереднє розпізнання, використовуючи правильний ключ шифрування. У деяких випадках це допущення реально не забезпечується.

Встановлення режиму шифрування

3 – Алгоритм шифрування А5

Для встановлення режиму шифрування мережа передає рухомої станції команду СМС (Ciphering Mode Command) на перехід у режим шифрування. Після одержання команди СМС рухома станція, використовуючи наявний у неї ключ, приступає до шифрування і дешифрування повідомлень. Потік переданих даних шифрується біт за бітом чи потоковим шифром.

Забезпечення таємності абонента

Для виключення визначення (ідентифікації) абонента шляхом перехоплення повідомлень, що передаються по радіоканалу, кожному абоненту системи зв'язку привласнюється "тимчасове посвідчення особи" - тимчасовий міжнародний ідентифікаційний номер користувача (TMSI), що дійсний тільки в межах зони розташування (LA).

В іншій зоні розташування їй привласнюється новий TMSI. Якщо абоненту ще не

привласнений тимчасовий номер (наприклад, при першому включенні рухомої станції), ідентифікація проводиться через міжнародний ідентифікаційний номер (IMSI). Після закінчення процедури аутентифікації і початку режиму шифрування тимчасовий ідентифікаційний номер TMSI передається на рухому станцію тільки в зашифрованому виді.

Цей TMSI буде використовуватися при всіх наступних доступах до системи. Якщо рухома станція переходить у нову область розташування, то її TMSI повинний передаватися разом з ідентифікаційним номером зони (LAI), у якій TMSI був привласнений абоненту.

Забезпечення таємності в процедурі коректування місця розташування: При виконанні процедури коректування місця розташування по каналах керування здійснюється двосторонній обмін між MS і BTS службовими повідомленнями, що містять тимчасові номери абонентів TMSI.

У цьому випадку в радіоканалі необхідно забезпечити таємність перейменування TMSI і їхня приналежність конкретному абоненту.

Розглянемо, як забезпечується таємність у процедурі коректування місця розташування і випадку, коли абонент проводить сеанс зв'язку і при цьому здійснює переміщення з одної зони розташування в іншу.

У цьому випадку рухома станція вже зареєстрована в регістрі переміщення VLR з тимчасовим номером TMSI, що відповідає колишній зоні розташування.При вході в нову зону розташування здійснюється процедура розпізнання, що проводиться по старому, зашифрованому в радіоканалі TMSI, переданому одночасно з найменуванням зони розташування LAI. LAI подає інформацію центру комутації і центру керування про напрямок переміщення рухомої станції і дозволяє запросити колишню зону розташування про статус абонента і її дані, виключивши обмін цими службовими повідомленнями по радіоканалах керування.

Загальний склад секретної інформації та її розподіл в апаратних засобах CSM

Відповідно до розглянутих механізмів безпеки, що діють у стандарті GSM, секретною вважається наступна інформація:

-RAND - випадкове число, використовуване для аутентифікації рухомого абонента;

-значення відгуку - відповідь рухомої станції на отримане випадкове число;

-індивідуальний ключ аутентифікації користувача, використовуваний для обчислення значення відгуку і ключа шифрування;

-ключ шифрування, використовуваний для шифрування/де- шифрування повідомлень, сигналів керування і даних користувача в радіоканалі;

- алгоритм аутентифікації, використовуваний для обчислення значення відгуку з випадкового числа з використанням ключа Кі;
- алгоритм формування ключа шифрування, використовуваний для обчислення ключа Кс із випадкового числа з використанням ключа Кі;

-алгоритм шифрування/дешифрування повідомлень, сигналів керування і даних користувача з використанням ключа Кс;

-номер ключової послідовності шифрування, указує на дійсне число Кс, щоб уникнути використання різних ключів на передавальній і приймальній сторонах;

-тимчасовий міжнародний ідентифікаційний номер користувача.

Висновки:

Розлянувши данний розділ було проведено аналіз методів та алгоритмів захисту абоненьської інформації в мережах стільникового зв’язку стандартів CDMA та GSM. Можемо зробити висновки що з преведених данних стандарт в CDMA принципові підходи до алгоритму захисту інформації абонента знаходяться на більш високому рівні ніж у стандарту GSM.

Лекція 29

Тема: Забезпечення інформаційної безпеки в системах транкінгового зв’язку TETRA

Захист інформації – найважливіший аспект побудови системи TETRA, оскільки однією з основних груп користувачів є служби суспільної безпеки, для яких високий рівень захисту – обов'язкова вимога.

До стандарту увійшли тільки добре перевірені методи захисту, передусім із систем GSM і DECT.

Це механізми аутентифікації мобільного термінала, забезпечення конфіденційності радіоканалу (GSM), а також взаємна аутентифікація термінала з мережею і функції управління ключами кодування (DECT).

Один з основних елементів системи управління захистом – ключові послідовності (ключі). Вони застосовуються під час процедур аутентифікації та шифрування інформації.

Аутентифікаційний ключ використовується для взаємного впізнавання мобільного термінала і базової станції.

Застосовуються три види таких ключів:

- користувальницький аутентифікаційний ключ (UAK) довжиною 128 біт, збережений у пам'яті мобільної станції або Smart-карти;

- аутентифікаційний код, що вводиться користувачем вручну;

- комбінація UAK та ідентифікаційного номера (персонального PIN - коду).

Під час передачі повідомлень захистом від несанкціонованого прослуховування є шифрування. Шифрувальні ключі можна формувати, розподіляти, вибирати і скасовувати при встановленні зв'язку між абонентами. Використовують чотири види шифрувальних ключів:

- виведені ключі застосовуються для двоточкового зв'язку і генеруються під час процедури аутентифікації;

- статичні ключі являють собою набір фіксованих кодових послідовностей (до 32), які можуть використовуватися без попередньої аутентифікації;

- загальний ключ використовується для шифрування при передачі групових викликів, формується з використанням виведеного ключа для кожної мобільної станції, діє у чітко визначеній зоні і періодично змінюється;

- груповий ключ, пов'язаний з певною групою користувачів, генерується системою і передається мобільним станціям заданої групи. Він застосовується для шифрування викликів групи як у початковому вигляді, так і після модифікації за допомогою загального ключа.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. – К.: Кондор, 2004. – 384 с.

2. Закон України „Про Національну програму інформатизації” від 04.02.1998 р. № 74/98-ВР. – Режим доступу:

3. Рубан В.Я. Інформаційна безпека України: сутність та проблеми // Стратегічна панорама. – 1998. – № 3-4. – С. 170.

4. Організація і сучасні методи захисту інформації; За ред. С.А. Дієва та А.Г. Шаваєва – М., 1998. – 52 с.

5. Закон України „Про телекомунікації” від 18.11.03 р. № 1280-IV. – Режим доступу:

6. Закон України „Про захист інформації в автоматизованих системах” від 5.06.1994 р. № 81/94-ВР. – Режим доступу: http://www.dstszi.gov.ua Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – С 12.

8. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – Режим доступу:

9. НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

10. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

11. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

12. НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. – Режим доступу:

13. НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова).

14. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

15. КНД 45-164-2001. Типова модель загроз для формування ресурсів цифрових АТС, що використовуються в мережах електрозв’язку загального користування України. – Режим доступу: http://www.stc.gov.ua

16. ISO/IEC 15408:2000 Части 1 – 3. “Информационные технологии. Общие критерии оценки безопасности информационных технологий (ИТ – безопасности)”, ISO/IEC 13335:1997 «Руководство по управлению ИТ – безопасностью», ИСО/МЭК 17799:2000 “Практические рекомендации по управлению ИТ-безопасностью”.

17. НД ТЗІ 3.7-003-03. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

18. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

19. Домарев В.В. Математические модели систем и процессов защиты информации.Електронний ресурс http://www.domarev.kiev.ua/nauka/. С.56.

20. Кравченко В.П. Система поддержки принятия решений. Електронный ресурс:

21. Черноруцкий И.Г. Методы оптимизации и принятия решений. С.-Пб, 2001, С. 248.

22. Организация планирование и управление предприятиями связи / Е.В. Демина, Е.К. Иодко, Л.И. Майофис, Н.П. Резникова. – М.: Радио и связь, 1990. – 352 с.
23. Котенко М. Центры обработки вызовов // Телеком № 9-10 (27-28)/2000. С.56-63.
24. Гольдштейн Б.С., Зарубин А.А., Потапов А.И. Центры обработки вызовов для органов внутренних дел: учебное пособие // СПбГУТ. – СПб. – 2005. – 52 с.
25. Петренко С. Методические основы защиты информационных активов компании // Режим доступу: – www.infosecurity.ru/ gazeta/content/031104/article03.html.
26. Шварц М. Сети ЭВМ. Анализ и проектирование / Пер. с англ. Под ред. В. А.Жожикашвили – М.: Радио и связь, 1981. – 336 с.
27. Корнышев Ю. Н., Мамонтова Н. П. Задачник по теории телефонных и телеграфных сообщений. − Одесса: ОЭИС, 1974. 139 с.
28. Корявцев П.М. Общий комплекс мер по обеспечению инфрмационной безопасности. Методические рекомендации // Вестник МВД РФ. – М.: 2000. 29. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Режим доступу: zzi.gov.ua/ dstszi/control/uk/publish/article?art_id=40381&cat_id=38835 30. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. – Режим доступу:

31. Бельфер Р. А. Классификация угроз информационной безопасности сетей связи ВСС России (ISDN, IN, UMTS) и методы их количественной оценки // “Электросвязь”, М: – 2002, № 7. – С.14 – 18.
Забезпечення інформаційної безпеки цифрових програмно керованих АТС Інформаційна безпека телефонного зв’язку: навч. посібник / [Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.] За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 168.
Бруce Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Вильямс, 2002. – 816 с.
Венбо Мао. Современная криптография: теория и практика. – М.: Вильямс, 2005. – 768 с.
Д. Г. Сущевский, О. В. Панченко, В. Н. Кугураков СОВРЕМЕННЫЕ КРИПТОСИСТЕМЫ И ИХ ОСОБЕННОСТИ //Вестник технологического университета. 2015. Т.18, №11 с.194-197
https://sites.google.com/site/anisimovkhv/learning/kripto/rabprog
38 https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema3#kriptografia
39 Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, із змінами. – Режим доступу: zakon2.rada.gov.ua/laws/ show/2657-12. – Назва з екрану
Про захист інформації в інформаційно-телекомунікацій-них системах: Закон України від 05.07.1994 р. № 80/94-вр, із змінами. – Режим доступу: zakon5.rada.gov.ua/laws/ show/80/94-вр. – Назва з екрану.
1. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229/99. – Режим доступу: zakon3.rada.gov.ua/laws/show/1229/99. – Назва з екрану.
2. Про затвердження Концепції технічного захисту інформа-ції в Україні: постанова Кабінету Міністрів України від 08.10.1997 р. № 1126, із змінами. – Режим доступу: zakon3. rada.gov.ua/laws/show/1126-97-п. – Назва з екрану.
3. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.
Википедия. Свободная энциклопедия. – [Електронний ресурс]. – http://ru.wikipedia.org/wiki/Triple_DES. Заголовок з екрану. Мова рос., дата цитування: 12.12.2009 р.

Я. М. Стець О. В. Іванченко