УДК 004.056.53

Д. Ю. Гереш

МЕТОДИ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ У ТЕЛЕФОННИХ МЕРЕЖАХ СИСТЕМ БЕЗПЕКИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОСНОВІ СКРЕМБЛЮВАННЯ

Вінницький національний технічний університет

Анотація

Досліджено методи захисту інформації в системах зв'язку від несанкціонованого доступу. Проаналізовано та визначено основні методи скремблювання, що забезпечують найвищий рівень захисту.

Ключові слова: захист інформації, скремблер, системи зв'язку.

Abstract

The methods of information security in communication systems from unauthorized access are investigated. The main scrambling methods that provide the highest level of protection are analyzed and identified.

Keywords: Data protection, scrambler, communication systems.

На сьогодні майже неможливо уявити собі світ без різноманітних систем зв'язку або переоцінити їхній вплив на наше щоденне життя. Це насамперед пов'язане із зручністю даного виду комунікації. Розвиток сучасних систем передачі інформації дозволяє кожний день передавати неймовірну за обсягами кількість інформації. Багато людей використовують мережі передачі даних, як основний засіб зв'язку із своїми діловими партерами чи для вирішення різноманітних важливих питань. Саме в таких випадках з'являється значна ймовірність несанкціонованого доступу до конфіденційної інформації. Тому виникає потреба в організації комплексу заходів з метою запобігання втрати інформації, що циркулює в системі зв'язку [1-2].

При забезпеченні інформаційної безпеки найбільш ефективний захист досягається лише при застосуванні комплексного підходу, який включає такі види захисту: інженерно-технічний, правовий, програмно-технічний, організаційний [3].

Комплексний захист інформації створюється на об'єктах для блокування всіх можливих або найбільш ймовірних загроз безпеці інформації, в якому одним із ключових заходів є програмно-технічний захист інформації [4].

Одним із методів програмно-технічого захисту, який безпосередньо робить перехоплення переданої інформації із лінії зв'язку марною, протягом часу на який інформація залишається важливою, є використання скремблерів.

Скремблер – це пристрій, який призначений для зміни мовної інформації, що передається по лінії зв'язку з подальший її відновленням до початкового стану за допомогою відповідної пари ключів [5].

Класифікація скремблерів відбувається відповідно до систем передачі інформації в яких вони застосовуються. У системах зв'язку відомі два основні методи скремблювання мовних сигналів : аналогове скремблювання і дискретизація мови з наступним шифруванням (цифрове скремблювання). Основними характеристиками аналогових скремблерів, так як, зазвичай, скремблюють телефонні розмови, є якість шифрування, розбірливість сигналу після зворотного перетворення та залишкова розбірливість сигналу після перетворення початкового сигналу [6].

Найперші скремблери, аналогові, представляли собою складні пристрої, що дозволяли провести найпростіші маніпуляції із акустичним сигналом. Аналогові методи скремблювання можуть перетворювати сигнал за трьома параметрами: амплітуді, частоті і часу.

На практиці використання амплітудного перетворення сигналу не застосовується, адже відтворення амплітуди на іншій стороні лінії зв'язку є досить неточним [6].

Частості методи в свою чергу можна розділити додатково на два види: інверсні та смугові. Головний принцип роботи інверсного скремблер полягає у конвертуванні мовного спектру, шляхом перет-

ворення низькочастотних частинок звукового сигналу в високочастотні відрізки і навпаки. Смуговий метод скремблювання перед перетворенням сигналу спочатку ділить спектр на декілька частотних смуг однакової ширини, а далі даний метод здійснює перестановку отриманих спектрів відповідно до ключа системи встановленого заздалегідь. Методи часового скремблювання так як і методи частотного перетворення поділяються на два типи: інверсія сегментів мовного сигналу в часі та перестановка окремих сегментів в часі. Найпростішим методом часового скремблювання є часова інверсія. В даному методі мовний сигнал перед передачею в лінії зв'язку поділяється на суцільний набір рівних між собою сегментів. Під час передачі мовного сигналу відбувається його інверсія відносно середнього сегменту. Скремблер із часовими перестановками здійснює перестановку кожного окремого сегменту в одній суцільній послідовності [7, 8].

В процесі розвитку інформаційно-телекомунікаційних систем широко застосування здобули методи скремблювання з перетворенням аналогового сигналу в цифровий. Дані методи забезпечують значно вищий рівень захищеності мовної інформації в процесі шифрування. Значною перевагою цифрового шифрування є наявність більшої варіативності вибору методу скремблювання. Цифрові скремблери в загальному випадку доцільно поділити на такі, що застосовують в процесі скремблювання – ПВП та криптографічні алгоритми. Цифрові скремблери-ПВП передбачають, що утворений цифровий потік даних, змішується з псевдовипадковою послідовністю, що виробляється ключовим генератором. Використання криптографічних алгоритмів передбачає, що цифрова послідовність параметрів з АЦП подається на вхід шифратора, де піддається перетворенню по одному з криптографічних алгоритмів, а потім надходить через модем в канал зв'язку [9].

Отже, було проаналізовано основні методи захисту мовної інформації від несанкціонованого доступу на основі скремблювання. Беручи до уваги дану інформацію, можна зробити висновок, що цифрові-скремблери є більш гнучкими в плані вибору методу шифрування, забезпечують більший рівень захищеності інформації, а також надають можливість швидкої зміни одного виду шифрування на інший. Тому, для захисту інформації, рекомендовано використовувати цифрові методи шифрування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конахович Г. Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов – К.: "МК-Пресс", 2005. — 288 с, ил.
2. Гайдур Г.І. Фізичні поля як носії інформації: [навчальний посібник] / Г.І. Гайдур, Я.А. Кремнецька, С.В. Морозова:. Київ. Державний університет телекомунікацій. 2019. —170 с.
3. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України. / О.В. Рибальський, В.М. Смаглюк, В.Г. Хахановський – К.: Вид. Національної академії внутріш. справ, 2010. – 255 с.
4. Безбогов, А.А. Методы и средства защиты компьютерной информации : учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.
5. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
6. Сулименко Э.А. Методы скремблирования речевого сигнала / Э.А Сулименко. – 2017. – 5с.
7. Сталенков С.Е., Шулика Е.В. НЕЛК – новая идеология комплексной безопасности. Способы и аппаратура защиты телефонных линий. // Защита информации. Конфидент. – 1998. - №6(24). – 25-30с.
8. Скремблеры [Електронний ресурс]. – Режим доступу: //http://citforum.ru/internet/infsecure/ its2000_15.shtml.
9. Криптографические методы и средства защиты. [Електронний ресурс]. – Режим доступу: // http://pitbot.ru/37.shtml/.
10. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

Гереш Денис Юрійович — студент групи УБ-19м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail:den.heresh@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** — кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця

Heresh D.Y. — student, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnytsia, email : den.heresh@gmail.com

Supervisor: ***Karpinets Vasyl V.*** — Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnitsa National Technical University, Vinnytsia