Прин. №1

ПОГОДЖЕНО
Заступник Голови Держспецзв'язку
_____О.В. Корнейко
"27" 12 2013 р

ЗАТВЕРДЖУЮ
Директор ТОВ «АВТОР»
_____ Татьянін В.В.
"20" 12 2013 р

IP-шифратори
CryptoIP-428, CryptoIP-428/5V, CryptoIP-448, CryptoIP-448/5V

ІНСТРУКЦІЯ
ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ

АЧСА.465653.002 И9

РОЗРОБЛЕНО
Директор департаменту
ТОВ «АВТОР»
_____ Г. Дядік
"20" 12 2013 р

2013

до вх 1953-13Р до вх 2643-Я

АНОТАЦІЯ

IP-шифратори є засобами КЗІ, і виконують функції захисту IP-трафіку віртуальних приватних мереж шляхом забезпечення конфіденційності, автентичності та цілісності пакетів IP-трафику.

IP-шифратори CryptoIP-428, CryptoIP-428/5V, CryptoIP-448, CryptoIP-448/5V призначені для захисту **інформації з обмеженим доступом (крім службової та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.**

Даний документ містить відомості про організаційно-технічні заходи по забезпеченню безпеки експлуатації IP-шифраторів CryptoIP-428, CryptoIP-428/5V (ТУ У 30.0-32248356-014:2008), CryptoIP-448, CryptoIP-448/5V (ТУ У 30.0-32248356-012:2008).

1. Загальні положення

Ця Інструкція визначає організаційно-технічні заходи щодо захисту інформації при організації і експлуатації захищених віртуальних приватніх мереж з використанням IP шифраторів CryptoIP-428, CryptoIP-428/5V (ТУ У 30.0-32248356-014:2008), CryptoIP-448, CryptoIP-448/5V (ТУ У 30.0-32248356-012:2008).

Порушення положень цієї інструкції може привести до втрати конфіденційної інформації.

2. Перелік скорочень.

КД – ключові дані;
КЗІ – криптографічний захист інформації;
НКІ – носій ключової інформації;
ЦГКД – Центр генерації ключових даних;
IP (internet protocol) – інтернет протокол.

Криптоалгоритми та криптопротоколи, які не є національними стандартами, можуть використовуватися для захисту інформації виключно при здійсненні міжнародного обміну або в банківській системі України за відповідним погодженням Національного банку України.

3. Вимоги до організаційного забезпечення безпеки експлуатації IP-шифраторів

3.1. Керівництвом організації, в якій здійснюється експлуатація IP-шифраторів, повинні бути визначені посадові особи, відповідальні за розробку і практичне здійснення заходів щодо забезпечення функціонування і безпеки IP-шифраторів (далі, Адміністратор безпеки).

3.2. Питання забезпечення функціонування і безпеки IP-шифраторів повинні бути відображені в спеціально розроблених, з урахуванням вимог експлуатаційної документації документах, затверджених керівництвом установи, в якій здійснюється експлуатація IP-шифраторів.

3.3. В установі, в якій здійснюється експлуатація IP-шифраторів, повинні бути створені умови, що забезпечують захист НКІ та IP-шифраторів від несанкціонованого фізичного доступу.

3.4. Адміністратором безпеки регулярно повинен проводитися контроль правильності підключення IP-шифраторів до абонентського (незахищеного) устаткування внутрішньої мережі і станційного (захищеного) устаткування зовнішньої мережі. Особливу увагу слід приділяти неприпустимості підключення сторонніх (несанкціонованих) пристроїв до абонентської (незахищеної) частини внутрішньої мережі установи.

3.5. Повинен також проводитися періодичний контроль налаштувань комунікаційного устаткування з метою недопущення появи не передбачених подключений і технічних каналів витоку конфіденційної інформації.

3.6. Адміністратор безпеки повинен:

- знати експлуатаційну і іншу документацію, що входить в комплект поставки IP-шифраторів.
- забезпечувати виконання регламентів роботи з ключовими документами.
- забезпечувати виконання правил поводження з ключовими документами і пристроями; проводити заходи щодо запобігання компрометації КД.
- проводити заходи за фактом компрометації КД, направлені на зменшення можливої шкоди від компрометації.

3.7. Адміністратор безпеки має право:

- перевіряти наявність і стан НКІ, наявність документації, стан і комплектність IP-шифраторів.
- перевіряти виконання режимних заходів і відповідних регламентів співробітниками, допущеними до експлуатації IP-шифраторів.
- проводити всі будь-які інші законні дії, направлені на виконання своїх обов'язків.

4. Вимоги до умов і правил експлуатації IP-шифраторів

4.1. До роботи з IP-шифраторами співробітники допускаються за рішенням керівництва установи, в якій здійснюється його експлуатація.

4.2. До роботи з IP-шифраторами допускаються тільки співробітники, що засвоїли правила його експлуатації, вивчили положення експлуатаційної документації, в тому числі цієї Інструкції.

4.3. Співробітники, які допущені до роботи з IP-шифраторами, повинні мати уявлення про можливі загрози під час її обробки і передачі, про методи і засоби її захисту.

4.4. В процесі експлуатації IP- шифраторів співробітники зобов'язані:

- забезпечити експлуатацію відповідно до вимог експлуатаційної документації на IP-шифратори.
- забезпечити збереження НКІ, цілісність схеми підключень і самих пристроїв захисту.
- не розкривати корпус IP-шифратора, не проводити спроб декомпіляції спеціального програмного забезпечення IP-шифраторів.
- розуміти значення індикації стану IP-шифратора.
- негайно докладати відповідальному за забезпечення безпеки і своєму безпосередньому начальнику про (можливу) компрометацію КД і/або виявлення розкомплектованості IP-шифраторів.

4.5. В процесі експлуатації передача IP-шифраторів та НКІ здійснюється:

- без витягання НКІ з карткоприймача IP-шифратора, якщо IP-шифратор включений, не знаходиться в стані блокування і не відображає помилку доступу до SIM картки (НКІ).
- згідно з заводськими номерами НКІ та IP-шифратора, якщо IP-шифратор вимкнений та в інших випадках.

5. Вимоги до розміщення та порядку допуску в приміщення, в яких установлені засоби КЗІ

5.1. IP-шифратори повинні розміщуватися у приміщеннях, де є умови для забезпечення захисту IP-шифраторів і НКІ від несанкціонованого фізичного доступу, а також контролю штатної схеми їх підключення.

5.2. Порядок допуску в приміщення розташування IP-шифраторів визначається внутрішньою інструкцією, яка розробляється з урахуванням специфіки і умов функціонування конкретної установи, в якій здійснюється експлуатація IP-шифраторів.

6. Порядок забезпечення безпеки засобу КЗІ під час його встановлення, тестування, виведення з експлуатації, ремонту

6.1. Встановлення IP-шифраторів повинен здійснюватися способом, який забезпечує збереження IP-шифраторів і НКІ.

6.2. Забороняється розкриття корпусу IP-шифратора і спроби читання вмісту НКІ на всіх етапах їх життєвого циклу, за винятком періоду ремонту в уповноваженій виробником організації.

6.3. Забороняється розголошення PIN-коду доступу до IP-шифратора.

6.4. Установка і підключення до телекомунікаційної мережі дозволяється тільки для пристроїв, що пройшли процедуру персоналізації в ЦГКД.

6.5. IP-шифратори повинні бути розташовані усередині зони, яка охороняється, так само, як і термінальне устаткування, що захищається, комунікаційне устаткування, сполучні лінії частини мережі, що захищається.

6.6. Тестування IP-шифраторів виконується автоматично після включення живлення протягом 10-15 секунд. Після закінчення тестування слід переконатися у відсутності індикації блокування і індикації інших несправностей, використовуючи інформацію Настанови з експлуатації IP-шифраторів (АЧСА 465653.002 НЕ)

6.7. Ремонту підлягають пристрої, що перейшли в стан блокування або пристрої, які не виконують своїх функцій.

6.8. Перед відправкою на ремонт, дії, не передбачені настановою з експлуатації, не допускаються.

7. Порядок забезпечення безпеки засобу КЗІ під час експлуатації

7.1. У разі порушення функціонування інформаційно-телекомунікаційної системи, IP-шифратори виявляються недоступними для дистанційного контролю з боку адміністратора захищеної мережі, і цей факт повинен бути врахований при плануванні організаційних заходів щодо забезпечення безпеки і збереження устаткування КЗІ.

7.2. Тривалий час непрацюючі або резервні IP-шифратори повинні зберігатися в місцях, що забезпечують надійність їх зберігання.

7.3. У вимкненому стані IP-шифратор зберігає свої настройки протягом всього періоду експлуатації. Виключення і включення живлення приводить до вироблення нового сеансового ключа.

7.4. У разі, коли захищений канал не використовується, а телекомунікаційне з'єднання функціонує, рекомендується залишати IP-шифратор включеним, що дозволяє адміністратору захищеної мережі дистанційно контролювати справність IP-шифратора і готовність захищеного з'єднання до передачі інформації.

8. Заходи у випадку підозри компрометації КД

8.1. Можливість маніпуляцій з шифратором сторонніх осіб, втрата НКІ і/або шифратора, виявлення ознак розкриття IP-шифратора, перехід шифратора в стан блокування повинні розглядатися як події, що викликають підозру компрометації КД.

8.2. У випадку підозрі компрометації КД необхідно негайно повідомити Адміністратора безпеки і безпосереднього начальника.

8.3. Адміністратор безпеки і інші уповноважені посадові особи повинні негайно вжити необхідні заходи по вилученню з експлуатації усіма кореспондентами мережі відкритого ключа відповідного абонента, а також вилученню скомпрометованого НКІ і шифратора.

8.4. Робота захищеної мережі продовжується без обмежень, за винятком кореспондента, щодо КД якого є підозри компрометації.

8.5. За фактом підозри компрометації повинне проводитися адміністративне розслідування. За наслідками розслідування керівник організації ухвалює рішення про перелік заходів по мінімізації наслідків можливої компрометації і заходах по створенню умов, перешкоджаючих компрометації КД.

9. Контроль за виконанням вимог по захисту інформації

9.1. Контроль за станом безпеки використанням IP-шифраторів повинен бути постійним, ефективним та спрямованим перш за все на попередження порушень вимог безпеки.

9.2. Право контролю за станом безпеки експлуатації IP-шифраторів надається уповноваженим особам служби захисту інформації (в тому числі Адміністратору безпеки).

9.3. Виявлені у ході контролю порушення вимог безпеки або передумови до виникнення таких порушень негайно усуваються, аналізуються та здійснюються необхідні заходи щодо подальшого запобігання таких порушень.