УДК 681.384

Новгородський О.В.
Маліновський В.І.

ПІДХОДИ ДО ЗАХИЩЕНОГО ПРОЦЕСУ ПЕРЕДАВАННЯ ДАНИХ У ІНФОРМАЦІЙНИХ КАНАЛАХ ЗВ'ЯЗКУ

Вінницький національний технічний університет

Аннотація. В роботі розглянуто підходи інформаційної безпеки і захищеного передавання даних у оптичних каланах зв'язку, що застосовуються у сучасних приладах і системах, які досить часто використовуються в сучасних розумних системах. Розглядяються основні чинники впливу і фактори кіберзагроз, які проявляються у каналах зв'язку, а також можливості несанкціонованого втручання і зчитування інформації у інформаційних системах та їх наслідки. Розглянуто перспективи розвитку і підходи до методу захищеної передачі даних у оптичних каналах із криптографічним і фізичним захистом у сучасних промислових інтерфейсах і системах для організації безпечного зв'язку і дистанціного керування на промислових об'єктах.

Ключові слова: оптичні і волоконно-оптичні канали, шифрування потоку інформації, інформаційні мережі та системий, Інтернет речей (Internet of Thinks, IoT), захищене середовище.

Abstract. The paper considers aspects and analyses the perspectives of the method of data transmission in modern industrial fiber optic interfaces for the organization of communication on industrial objects. This method allows the transmission of industrial signals for monitoring technological processes and telecontrols with higher quality and high performance.

Keywords: fiber-optic, interface-channel, data stream encoding, data networks and systems, secured environment.

Проблематика галузі та стан сучасних технологій.Сучасні технології і прилади передачі даних високої швидкості і функціональності базуються на оптичних підходах передачі інформації є високоінтелектуальними, відносно добре захищеними і передбачають обмін даними у мережах передачі даних (МПД) у різних архітектурах просмислових систем на різних рівнях ієрархії і в т.ч. на базі глобальної мережі Інтернет. Також сучасні інтелектуальні оптичні технології передавання інформації, а також останні тенденції до впровадження технологій телемоніторингу і телекерування і в т.ч. передачі захищеної інформації дозволяють досить надійно і захищено організувати зв'язок. Але існує проблема росту чинників загроз несанкціонованого зчитування і модифікації. А також перехоплення інформації із цих каналів, що може призвести до втручання та/або перехоплення інформації конфіденційного змісту або втручання чи впровадження (ін'єкцію) шкідливого коду у інформаструктуру сучасних захищених і часом критичних інформаційних систем. Це створює додаткові проблеми безпеки і потенційні ризики порушення функціоналу сучасних інформаційних систем, а також ризики перехоплення і модифікації інформації із каналів зв'язку сучасних інтелектуальних промислових мереж. Таких як Інтернет речей (Internet of Thinks, IoT), промислові оптичні мережі, мережі захищеної передачі даних (МЗПД).

Організовувати високоефективне, комфортне і автоматизоване керування та моніторинг інформаційних процесів і захищену передачі інформації у сучасних захищених процесах і системах через організовані канали віддаленого зв'язку на базі оптичних каналів і мережі Інтернет, що відповідає концепції захищених закритих систем передачі і концепції застосування захищеного Інтернету речей (Internet of Thinks або IoT). Разом з тим, це несе значні ризики від впровадження інформаційних технологій, пов'язані із кібербезпекою та інформаційною безпекою цілісності таких промислових та/або захищених систем і систем IoT. По своїй природі і структурній організації канали і алгоритми і протоколи генерації ключів захищеного каналу RSA (на базі генерації пари ключів шифрування), а також алгоритми і протоколи захищегного з'єднання не завжди дозволяють організувати надійний та захищений зв'язок в промислових і захищених мережах і каналах передачі даних і системах IoT.

Враховуючи високу ступінь наслідків саме для захищених систем і мереж та їх оптичних каналів, як критичних ділянок і необхідності забезпечення стабільного, надійного, захищеного функціоналу і забезпечення повної цілісності даних виникає задача розроблення нових підходів, моделей і методів захищеної і більш стабільної передачі інформації у сучасних закритих систем із можливістю їх нормального ефективного впровадження на практиці і у промисловості. Тому мінімізація і максимально повне виключення і нейтралізація кіберзагроз і витоків інформації із оптичних каналів є важливою задачею у

галузі сучасних інтелектуальних систем і мереж, які мають у своєму складі захищений комунікаційний і «розумний» функціонал і входять у концепцію IoT.

Тренди сучасних років говорять, що основними кіберзагрозами оптичних каналах є:

- *Несанкціоноване перехоплення, втручання на фізичному рівні і спотворення даних;*
- *Генерація та впровадження підмінених сертифікатів захисту шифрування;*
- *влаштовування «ін'єкція» шкідливого коду та сертифікату;*
- *перехопленого (на фізичному) рівні трафіку із супутніх вузлів і дешифрація інформаційних потоків і функціоналу керування системами передачі даних;*
- *таргетовані/цілеспрямовані кібератаки атаки на системи керування каналів зв'язку і вивід їх із ладу та/або порушення функціоналу;*
- *перехоплення керування та/або перехоплення потоків даних моніторингу окремих параметрів (або опосередкованих параметрів інформаційних величин) у каналах зв'язку;*
- *канали передачі Wi-Fi та Bluetooth та кабельні комунікації;*
- *ядро і компоненти вводу-виводу на суміжних мобільних операційних систем пристроїв керування\моніторингу;*
- *втручання в захищені механізми формування VPN/ Proxy та механізми генерації ключів шифрування RSA;*
- *використання мережевих експлойтів і ,,модулів пробиття зв'язку" спрямованих на компоненти управління передачею/шифрування в складі системи та/або каналу передачі даних для порушення штатного його функціоналу - ПЗ/ядра опереаційного притрою/системи, що призводить до порушення/додання/модифікування/зрізання системних програмних функцій ПЗ;*
- *некоректні системні налаштування та/або помилки операціного персоналу;*
- *порушення безпеки пограничних пристроїв та модулів зв'язку у пристрої (маршрутизатори, комутатори, обладнання оптичного/радіозв'язку та інше), у сукупності із - вразливостями проміжних протоколів зв'язку і передачі даних;*
- *порушення механізму втановлення захищеного з'єднання та атаки MITM;*
- *недосконаліть і кіберзагрози опорної архітектури і суміжних пристроїв;*
- *таргетовані віруси і троянські коні, які адаптовані спеціально спрямовані на конкретний програмний чи апаратний системний компонент інфраструктури системи передачі даних (СПД);*
- *недосконаліть апаратної структури і мережевих особливостей і хмарних сервісів;*
- *недосконаліть системних налаштування і мережевих протоколів передачі даних.*

Тренди останніх років і тенденції кіберзагроз свідчать, що за останні роки велика частка до 10-12% загроз перехоплення захищених даних у каналах мереж передачі даних припадає саме на ВОЛЗ (Волоконно-оптичні лінії зв'язку) галузь кінцевих фізичних комунікацій користувачів мережі Інтернет. Серед них перехоплення даних у сфері каналів Інтернету речей складає до 35%, велику доля із якого спрямовано саме на пристрої і комунікаційні канали передачі даних. Можливості сучасних інструментів і апаратно-програмних засобів зчитування та/або прихованого втручання також значно зросли, як зросли і смарт-функції таких систем. В подальшому прогнозується збільшення числа атак на комунікаційну інфраструктуру захищених мереж і систем, в т.ч. й IoT-пристроїв і на сферу IT-інфраструктури передачі даних, охоплюючи при цьому і системи типу "розумний будинок" із окремими компонентами автоматизації і кінцевим функціоналом. У 2020-2021рр. зросли атаки на комунікації та комунікаційні канали і інтерфейси зв'язку мобільних і функціональних пристроїв: Wi-Fi, 3/4/5G, провідні комунікації на базі Ethernet, які активно інтегровані у функціонал сучасних розумних пристроїв, що створюють фактори кіберзагроз для мереж IoT і мереж захищеної передачі інформації. Серед них можна виділити основні:

- *відсутність захищених IPS та VPN/ Proxy та мережевого екрану;*
- *використання експлойтів і ,,пробиття" для порушення штатного функціоналу - ПЗ/ядра опереаційно системи притрою/системи, що призводить до порушення/додання/модифікування/зрізання системних програмних функцій ПЗ та системних помилок стемних;*
- *порушення безпеки пограничних пристроїв та модулів зв'язку у пристрої (маршрутизатори, комутатори, обладнання радіозв'язку та інше);*
- *порушення механізму втановлення захищеного з'єднання та атаки MITM;*
- *недосконаліть і кіберзагрози опорної архітектури і суміжних пристроїв;*
- *віруси, троянські коні і бекдори, які адаптовані спеціально під інфраструктуру мережі;*
- *недосконаліть мережевих і хмарних сервісів, програмних інтерфейсів API і не вірні налаштування.*

Враховуючи це, необхідною є розробка нового методу і засобу захищеної передачі даних для оптичних каналів зв'язку, які можуть використовуватись у критичній інфраструктурі IoT. Такий засіб повинен забезпечували повну безпеку функціоналу і захищену передачу даних та їх обробку для

забезпечення сталості і надійності процесу передачі інформації по оптичним каналам зв’язку. Засіб і метод повинні базуватись на поєднані функціоналу на різних рівнях: апаратного та програмного.

Новгородський О.В. – бакалавр кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Науковий керівник: ***Маліновский Вадим Ігоревич*** – к.т.н.**,** доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Novhorodskyi Oleh — barselour of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Supervisor: ***Malinovskyi Vadym*** — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.