© Odarchenko R., Gnatyuk V., Fediura T., Kobernik A. The development of cyberindidents management system on LTE networks // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 2, p.84-90.

DOI: 10.18372/2225-5036.24.13036

РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ В МЕРЕЖАХ LTE

Роман Одарченко, Віктор Гнатюк, Тетяна Федюра, Анастасія Коберник

Національний авіаційний університет, Україна

ОДАРЧЕНКО Роман Сергійович, к.т.н.

Рік та місце народження: 1988 рік, с. Култук, Слюдянського р-ну Іркутської обл., РФ.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри телекомунікаційних систем з 2012 року.
Наукові інтереси: стільникові мережі зв'язку нового покоління та їх системи безпеки.
Публікації: більше 90 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: odarchenko.r.s@mail.ru

ГНАТЮК Віктор Олександрович, к.т.н.

Рік та місце народження: 1990 рік, м. Нетішин, Хмельницька обл., Україна.
Освіта: Хмельницький національний університет, 2012 рік.
Посада: доцент кафедри телекомунікаційних систем з 2017 року.
Наукові інтереси: інформаційна безпека, управління кіберінцидентами, телекомунікаційні системи та мережі.
Публікації: більше 40 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: viktorgnatyuk@ukr.net

ФЕДЮРА Тетяна Володимирівна

Рік та місце народження: 1997 рік, с. Глажева, Костопільського р-ну, Рівненської обл., Україна.
Освіта: з 2014 року студентка Національного авіаційного університету.
Наукові інтереси: стільникові мережі зв'язку нового покоління та їх системи безпеки, телекомунікаційні системи та мережі.
*E-mail***:** tanyafediura@gmail.com

КОБЕРНИК Анастасія Юріївна

Рік та місце народження: 1997 рік, м. Київ,Україна.
Освіта: з 2014 року студентка Національного авіаційного університету.
Наукові інтереси: стільникові мережі зв'язку нового покоління та їх системи безпеки, телекомунікаційні системи та мережі.
*E-mail***:** kobernika97@gmail.com

Анотація. *Стільникові мережі зв'язку на даному етапі являються одними із найпоширеніших у всьому світі. Останнім технологічним рішенням, яке знайшло широкого поширення, являються мережі LTE. Дані мережі використовуються для передачі голосу, даних, підключення стаціонарних пристроїв, пристроїв Інтер-*

нету речей тощо. Проте із рядом переваг, які надає кожне нове покоління мереж зв'язку, з'являються і нові загрози, зокрема в області забезпечення кібербезпеки. Так виникають нові види атак, кількість пристроїв, з яких вони можуть бути організовані. Тому дуже важливим є розробка нових механізмів забезпечення кібербезпеки в сучасних стільникових мережах, як нададуть гарантії безпечної доставки даних абонентів та пристроїв IoT. Тому було проведено аналіз механізмів забезпечення інформаційної безпеки найпопулярнішого в світі типу мереж LTE. Проведені дослідження показали, що мережі LTE, незважаючи на ряд переваг, мають також недоліки. Насамперед, це вразливість до атак DoS, вірусних атак, атак на додаткові сервіси. Наявність вразливостей та кіберзагроз породжує кіберінциденти, для локалізації та нейтралізації яких необхідні ефективні методи виявлення, ідентифікації, оброблення та розслідування. Щоб виявити та боротися з кіберінцидентами, було створено архітектуру системи управління кіберінцидентами в мережах LTE. В роботі також наведена класифікація кіберінцидентів, розглянута служба реагування на комп'ютерні інциденти (CERT) та параметри звернень до цієї служби. В якості варіанту побудови системи управління кіберінцидентами було досліджено систему netForensics, яка призначена для роботи з гетерогенним середовищем продуктів забезпечення інформаційної безпеки і реалізує безперервний збір, обробку та відображення подій безпеки. Було запропоновано варіант розгортання системи управління кіберінцидентами netForensics в мережі LTE, розглянуто основні елементи мережі LTE та їх взаємодія з netForensics nFX Open Security Platform. Ця система управління кіберінцидентами має широкі можливості щодо роботи в розподіленому режимі, підтримку різних відмовостійких конфігурацій тощо.

Ключові слова: *LTE, кіберінцидент, стільникова мережа, кібератака, 3G/4G/5G, CERT, netForensics.*

Вступ

Архітектура мережі LTE розроблена таким чином, щоб забезпечити підтримку пакетного трафіку з так званою «гладкою» («безшовною», seamless) мобільністю, мінімальними затримками доставки пакетів і високими показниками якості обслуговування [8]. Тому мережі LTE стали однією із ключових технологій, що дозволяють абонентам отримувати, а бізнесу запроваджувати принципово нові сервіси для Інтернету речей (IoT), M2M, V2X тощо.

В цих умовах (ріст абонентської бази, розгортання нових мереж, удосконалення технологічних рішень тощо), не зважаючи на всі існуючі переваги, в LTE є також ряд недоліків, серед яких предметом розгляду даної наукової праці є вразливості від кібератак.

Перша загроза – атаки DoS (Denial of Service) на мережу. Ємність радіоканалу в LTE передбачається велика, але все ж вона має обмеження, а тому може бути повністю вичерпана. Наступним класом загроз є вірусні атаки. Хоча таким атакам піддаються пристрої, а не мережі, LTE надають можливість підвищити швидкість поширення шкідливого програмного забезпечення. Проблеми починаються при установці користувачами додаткових прошивок або при отриманні повного доступу до мобільного пристрою, коли при неправильній конфігурації зловмисникам стають доступні всі ресурси телефону через протокол SSH (Secure SHell). Третя небезпека – атаки на додаткові сервіси. Власне, LTE розроблялося не тільки для забезпечення доступу до Інтернету мобільних користувачів, а радше як платформа для впровадження нових послуг: відео, ігрових і багатьох інших. Ці сервіси також можуть бути уразливі до найрізноманітніших атак - як з Інтернету, так і з боку мобільної мережі. Цілком можливо, що, реалізуючи атаки на один з сервісів (можливо, найменш захищений), зловмисники можуть поширити шкідливе програмне забезпечення вже через клієнтські пристрої. Кібератаки LTE можуть виходити і від сервісів подвійного призначення. Мобільні оператори володіють цінною інформацією абонентів, а отже існує ймовірність того, що вони захочуть її монетизувати. З поширенням інтелектуальних пристроїв число потенційно небезпечних сервісів буде тільки зростати. Злом такого сервісу дозволить зловмисникам отримати доступ до цінної інформації провайдера і побудувати нові схеми вчинення кіберзлочинів і незаконного отримання грошей.

Проаналізувавши вищеокреслені вразливості стільникових мереж LTE, їх архітектуру (відсутність мережевих вузлів, що відповідають за моніторинг кіберінцидентів (КбІ)), можна стверджувати, що створення архітектури центру моніторингу та реагування на кібеінциденти в мережах LTE є дуже актуальною задачею, що дозволить продовжити, так званий довготривалий розвиток даного типу мереж нівелюючи вплив можливих кіберінцидентів.

Аналіз існуючих досліджень

Проблемам стільникових мереж, захисту інформації в них присвятили багато робіт вітчизняні та закордонні вчені: І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк, В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа, С.В. Гладиш. Серед їх праць можна виділити [2, 6, 7], в яких розглядались питання експлуатації центів моніторингу, методи реагування на кіберінциденти в інформаційно-телекомунікаційних мережах (ІТМ). Проте стільникові мережі, хоча і є частиною ІТМ, мають певні особливості (здебільшого мобільність користувачів, хендовер, змінні IP-адреси, роумінг тощо), у зв'язку із чим традиційна архітектура центрів моніторингу та реагування на кіберінциденти повинна бути адаптованою для імлементації до стільникових мереж. У вищерозглянутих же працях зовсім не було приділено уваги моніторингу кіберінцидентів в стільникових мережах, а отже і LTE. Тому *метою даної роботи* є удосконалення традиційної архітектури центру монітоингу та реагування на кіберінциденти для підвищення рівня кіберзахищеності стільникових мереж. Для досягнення поставленої мети були виконані наступні наукові завдання:

– проведено дослідження кіберінцидентів, що можуть виникати у стільникових мережах з метою їх

класифікації та вибору найбільш підходящих механізмів захисту;

– проведено дослідження традиційної архітектури систем реагування на комп'ютерні інциденти з метою визначення слабких місць та напрямків удосконалення для імплементації до архітектури стільникових мереж;

– запропоновано архітектуру системи управління кіберінцидентами в стільникових мережах;

– запропонований варіант реалізації системи управління кіберінциентами на базі обладнання netForensics.

Основна частина дослідження

Під кіберінцидентами розуміють події, що полягатимуть в реалізації певної загрози та порушенні встановленого рівня безпеки стільникових мереж (рис. 1) [1].

Процесом управління інцидентами називають процес реєстрації інформації про стан безпеки та рівноваги телекомунікаційних систем (ТКС), передавання інформації в пункти її накопичення, переробки й аналізу, з узгодженням прийняття рішення та формуванням певного керуючого впливу на об'єкт управління. Інша класифікація таких дій визначає сім основних їх груп, які характеризують передусім способи, що їх використовують зловмисники для здійснення нападу, а саме: перехоплення паролів інших користувачів; «соціальна інженерія»; використання помилок програмного забезпечення (ПЗ) і програмних закладок, а також помилок механізмів ідентифікації користувачів і недосконалості протоколів передавання даних; одержання інформації про користувачів стандартними засобами операційних систем; блокування сервісних функцій системи, що зазнає атаки.

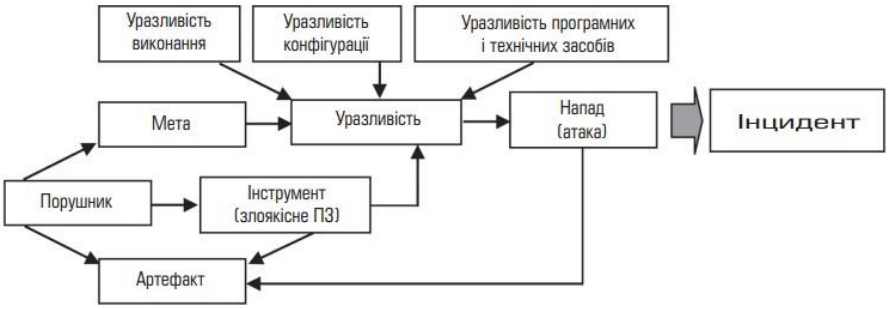

Рис. 1. Діаграма виникнення інцидентів

У Конвенції Ради Європи 2001 року, що спрямована на боротьбу з кіберзлочинністю, йдеться про чотири можливі групи таких дій [2]:

1. Інциденти, що мають на меті завдати шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем і реалізуються через:

– несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, а також до Internet Protocol (IP) протиборчої сторони, здійснений в обхід систем безпеки);

– втручання в дані (протиправна зміна, ушкодження, вилучення, перекручування або блокування комп'ютерних даних і керуючих команд за допомогою кібератак на інформаційні системи, ресурси та мережі державного і військового управління);

– втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розробку та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікацій і зв'язку, на обробку та передавання інформації, на системи захисту IP, систем і мереж, програмно-математичне забезпечення, протоколи передавання даних, алгоритми адресації та маршрутизації);

– незаконне перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних);

– незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

2. Шахрайство та підробка, пов'язані з використанням комп'ютерів:

– підробка документів із застосуванням комп'ютерних засобів (протиправне навмисне внесення, змінювання, вилучення або блокування комп'ютерних даних, що призводить до зниження вірогідності документів);

– шахрайство із застосуванням комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою навмисного протиправного одержання економічної вигоди).

3. Інциденти, пов'язані з розміщенням у мережах протиправної інформації.

4. Інциденти щодо авторських і суміжних прав.

Таким чином, узагальнена модель системи управління кіберінцидентами набирає вигляду[7]:

$$Model\frac{INC}{IKC}=\left(INC,SEC,CRI,KBS,X,Y,S,DMF,AGT,ARS,TRS,IRS,MST,T,SYN\right),$$

де INC — управління інцидентами (внутрішніми та зовнішніми); IKS — інформаційно-комунікаційна система; SEC — мета; CRI — критерії оцінювання стану безпеки; KBS — база знань про внутрішні та зовнішні інциденти; X — вхідні впливи; Y — реакція на внутрішні та зовнішні інциденти; S — стан системи; DMF — функція ухвалення (реагування), що поділяється на два етапи: на першому ухвалюється рішення про включення елемента ARS до набору TRS, а на другому (згідно з результатом виконання першого етапу) — рішення про включення елемента ARS до набору IRS; AGT — множина програмно-

реалізованих мобільних інтелектуальних агентів; ARS — набір ресурсів інформаційної безпеки, які доступні агентам; TRS — тестовий набір ресурсів інформаційної безпеки; IRS — інцидентно-орієнтовані набори ресурсів; MST — стратегія управління інцидентами; T — час; SYN — самоорганізація. Під внутрішнім кіберінцидентом розумітимемо такий інцидент, джерелом якого є порушник, безпосередньо пов'язаний із постраждалою стороною (рис.2).

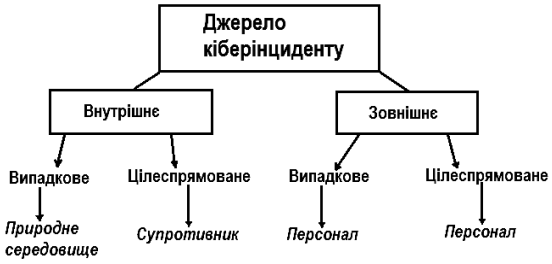

Рис. 2. Класифікація джерел кіберінцидентів

Серед найпоширеніших системних подій такого типу можна виокремити витік конфіденційної інформації; неправомірний доступ до інформації; вилучення інформації; компрометацію інформації; саботаж; шахрайство за допомогою IT; аномальну мережну активність; аномальне поводження бізнес-додатків; використання активів установи в особистих цілях або в шахрайських операціях.

Під зовнішнім кіберінцидентом — інцидент, джерелом якого є порушник, безпосередньо не пов'язаний із постраждалою стороною. До системних подій такого типу належать шахрайство в системах електронного документообігу; атаки типу «відмова в обслуговуванні» (DoS), у тому числі розподілені (DDoS); перехоплення й підміна трафіку; неправомірне використання бренду установи в мережі Інтернет; фішинг; розміщення конфіденційної (провокаційної) інформації в мережі Інтернет; злам або спроба зламу мережних вузлів; сканування порталу установи або мережі, вірусні атаки; неправомірний доступ до конфіденційної інформації; анонімні листи (листи з погрозами) тощо [1].

Слід відмітити, що виникнення всіх вищерозглянутих інцидентів є можливим також і в стільникових мережах, як складовій частині ITC. Проте є багато відмінностей, наприклад, від комп'ютерних мереж. Абоненти стільникових мереж є розподіленими, можуть використовувати різні операційні системи, перебувають в русі, абонентські пристрої є відносно недорогими тощо. Це все породжує нові класи загроз та складнощі при їх виявленні. Тому необхідно провести дослідження традиційних систем реагування на кіберінциденти з метою їх удосконалення та приведення до потреб сучасних стільникових мереж, якими безперечно є мережі LTE.

Архітектура системи реагування на кіберінциденти

Існує єдиний центр для користувачів національних інформаційних систем і сегмента мережі Інтернет для реагування на комп'ютерні інциденти CERT (Computer Emergency Response Team). Ця служба забезпечує збір і аналіз інформації про комп'ютерні інциденти, консультативну та технічну підтримку користувачам у запобіганні загроз комп'ютерної безпеки. CERT займається зниженням рівня загроз інформаційній безпеці для користувачів сегмента мережі Інтернет. У зв'язку з цим CERT сприяє юридичним і фізичним особам при виявленні, попередженні і припиненні протиправної діяльності, що має відношення до мережевих ресурсів сегмента мережі Інтернет. CERT здійснює збір, зберігання і обробку статистичних даних, пов'язаних з поширенням шкідливих програм і мережевих атак. До компетенції служби входить обробка наступних комп'ютерних інцидентів з метою їх виявлення і нейтралізації [3]:

– атаки на вузли мережевої інфраструктури і серверні ресурси, з метою порушення їх працездатності (DoS (Denial of Service) і DDoS) і конфіденційності інформації;

– несанкціонований доступ до інформаційних ресурсів;

– поширення шкідливого програмного забезпечення, небажаної кореспонденції (спам);

– сканування національних інформаційних мереж і хостів;

– підбір та захоплення паролів і іншої аутентифікаційної інформації;

– злом систем захисту інформаційних мереж, в тому числі з використанням шкідливих програм (сніффер, rootkit, keylogger і т.д.).

CERT здійснює [3]:

– моніторинг і виявлення механізмів і інтернет-ресурсів, що порушують законодавство;

– розробку рекомендацій користувачам щодо захисту інтересів особистості, суспільства і держави в інформаційній сфері;

– надання консультативних послуг з питань забезпечення інформаційної безпеки;

– оперативний прийом повідомлень про хакерські атаки.

CERT займається [3]:

– координацією дій підрозділів комп'ютерної безпеки державних органів, операторів зв'язку, а також інших суб'єктів національної інформаційної інфраструктури з питань запобігання правопорушень у сфері використання комп'ютерних та інформаційних технологій;

– збором, аналізом і накопиченням інформації про сучасні загрози комп'ютерної безпеки і про ефективність застосовуваних засобів захисту [3].

Архітектура типової системи управління кіберінцидентами включає в більшості випадків такі

основні компоненти [4, 5, 6]: інтеграційну платформу; апаратно-програмні засоби моніторингу і аудиту; апаратно- програмні засоби захисту інформації; сховище інформації про кіберінциденти; аналітичні інструменти і засоби генерації звітів; засоби управління та користувацькі інтерфейси. Інтеграційна платформа є ядром системи, вона покликана забезпечувати чітку і оперативну координацію та взаємодію осіб, що відповідають за реакцію на події, пов'язані з кіберінцидентами. Апаратно-програмні засоби моніторингу і аудиту – засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування ІКС організації. Вони складають підсистему збору інформації про кіберінциденти. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту. Апаратно-програмні засоби захисту в контексті системи управління кіберінцидентами – засоби, які забезпечують локалізацію інцидентів або зниження збитку. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від кіберінцидентів . Також, в організації повинна бути розроблена та впроваджена система сповіщення про інциденти. Узагальненою метою забезпечення інформаційної безпеки організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих кіберінцидентів. Основною задачею системи управління є усунення інцидентів в гранично стислі терміни. У ході процесу управління інцидентами проводиться виявлення, реєстрація, класифікація і початкова підтримка запитів, а також пошук рішення, його застосування, контроль, інформування і підготовка звітності. Оскільки, як ми вже визначили, інцидентом, в першу чергу, є певна недозволена подія, то вона має бути кимось заборонена. Отже, існує необхідність розробки та затвердження документів, що чітко описують всі дії, які можна виконувати в ІКС і які виконувати заборонено.

Ці всі функції CERT доцільно перенести в площину стільникових мереж, що дозволить операторам стільникового зв'язку не тільки підвищити рівень кібербезпеки та зменшити збитки від потенційно вчинених кіберзлочинів, а й запропонувати, наприклад, великим корпораціям додаткові сервіси забезпечення кібербезпеки.

Розробка архітектури системи управління кіберінцидентами в мережах LTE

Як вже було зазначено раніше, в мережах LTE, як в принципі й інших типах стільникових мереж, навіть 5G, відсутні засоби централізованого управління кіберінцидентами. Тому було прийнято рішення про розробку даного вузла, який пропонується узагальнено називати (можливо буде використовувати для мереж 5G) «Cybersecurity function» (надалі – CSF). Аналізуючи наявний функціонал мережевих вузлів (наприклад HSS, AUC тощо), які мають відношення до забезпечення кібербезпеки в стільникових мережах, було виявлено, що функції, характерні для системи управління кіберінцидентами, відсутні в LTE. Тому нова розроблена функція повинна виконувати наступні операції (таблиця 1).

Опис Cybersecurity function Таблиця 1

Функція	Підфункції
Cybersecurity function (CSF)	– збір усієї можливої інформації про виявлені інциденти в мережі (DIN) – аналіз, виявлення закономірностей та загальних рис, індикація (ADR) – виявлення потенційних та діючих джерел загроз (IST) – обмін здобутою інформацією із іншими мережами, наприклад не-3GPP (IE)

Схема реалізації управління КбІ в стільниковій мережі представлена на рис. 3.

Впровадження системи netForensics в мережу LTE

Як показав проведений аналіз [1,2,7], однією з найбільш підходящих систем управління кіберінцидентами серед присутніх на вітчизняному ринку є програмний продукт для обробки подій – netForensics nFX Open Security Platform [4]. Система netForensics призначена для роботи з гетерогенним середовищем для забезпечення інформаційної безпеки і реалізує безперервний збір, обробку та відображення подій безпеки. Система може працювати на платформах Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну СУБД Oracle. Ця система управління кіберінцидентами має широкі можливості щодо роботи в розподіленому режимі, підтримку різних відмовостійких конфігурацій тощо. Система управління кіберінцидентами netForensics реалізована на базі технології Java за модульним принципом. На рис. 4 зображено розроблену схему впровадження системи netForensics в мережу LTE.

Основними модулями системи є сервер застосунків (реалізує основну логіку обробки подій, представлення даних, взаємодії з користувачами); база даних nF DB (забезпечує зберігання інформації, що надходить до системи); модуль кореляції nF Engine (здійснює кореляцію зібраних даних); модуль автоматизації (здійснює автоматизацію процесів); агенти nF Agent (збирають інформацію безпосередньо з пристроїв). До складу системи також входять засоби щодо написання агентів збору даних з нестандартних систем захисту, засоби формалізації користувацьких правил кореляції і створення звітів.

Агенти nF Agent впроваджуються програмно в Serving Gateway, PDN Gateway, MME, HSS, eNodeB, PCRF та UE. Агенти netForensics збирають повідомлення та сповіщення з керованих пристроїв. За допомогою свого універсального агента можливо розробити підтримку додаткових пристроїв за допомогою стандартної мови на базі XML. Ці агенти є інтерфейсами для розмежування пристроїв безпеки та програм, які нормалізують дані, надаючи кожній події/повідомленню ідентифікатор події netForensics.

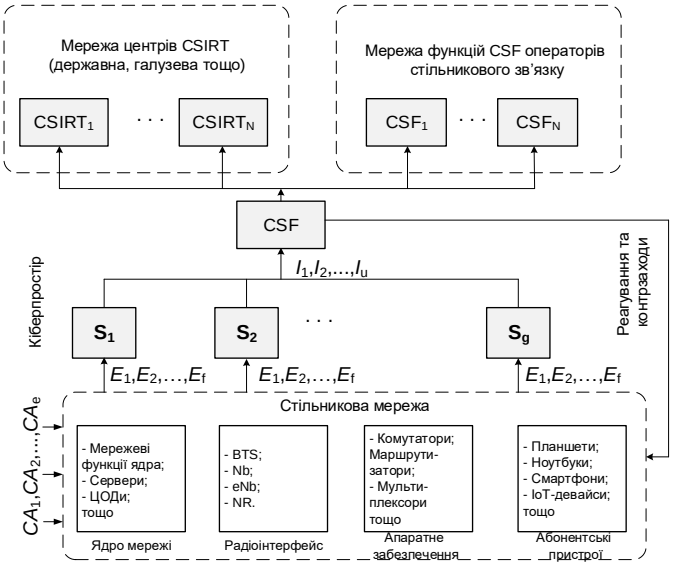

Рис. 3. Схема реалізації роботи системи моніторингу КбІ в стільниковій мережі

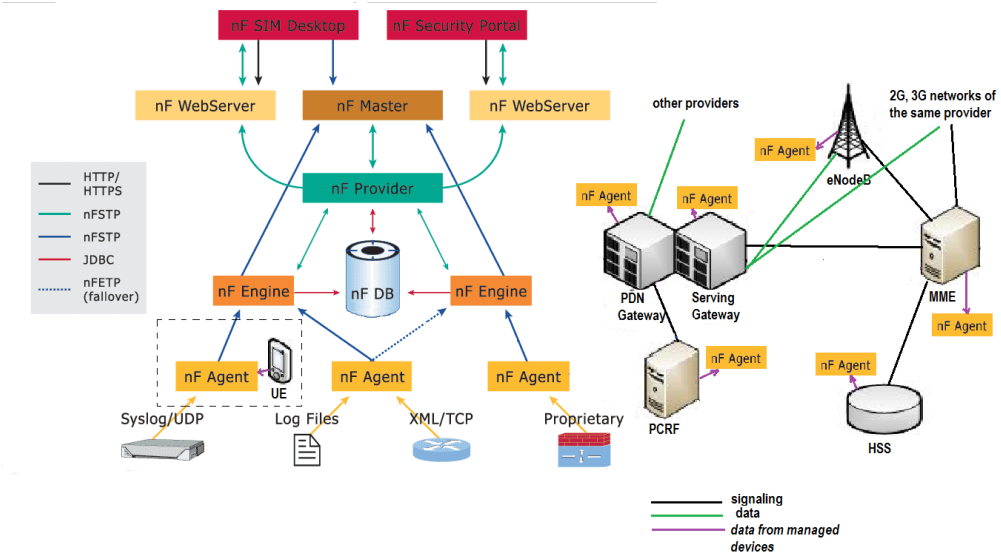

Рис. 4. Система управління кіберінцидентами netForensics в мережі LTE

Це дозволяє nf Engine виконувати аналіз та змістовну кореляцію, а потім, коли необхідно, сповіщати. Всі ці дані розміщуються в базі даних Oracle. База даних подає як спеціальні звіти, так і заплановані звіти, які можна налаштувати через веб-інтерфейс.

Висновки

В роботі було проведено дослідження кіберінцидентів, що можуть виникати у стільникових мережах LTE з метою їх класифікації та вибору найбільш підходящих механізмів захисту. Так як технологія LTE збільшує швидкість поширення шкідливих програм (оскільки сам цей стандарт є високошвидкісним), виникає необхідність створення системи управління кіберінцидентами. Тому було проведено дослідження традиційної архітектури систем реагування на комп'ютерні інциденти з метою визначення слабких місць та напрямків удосконалення для імплементації до архітектури стільникових мереж. Було проведено удосконалення архітектури стільникових мереж зв'язку шляхом введення додаткових безпекових функцій та послідовному зборі інформації про виникнення кіберінцидентів в стільниковій мережі, виявлені типи кібератак, об'єкти та ступінь впливу, реагування на кібератаку та збереження інформації про кіберінцидент в спеціалізовану базу даних. Запропоноване рішення дозволяє в режимі реального часу проводити моніторинг стану забезпечення кібербезпеки та підвищувати її рівень.

Також в роботі був запропонований варіант реалізації системи управління кіберінциентами на базі обладнання netForensics. Як показали проведені дослідження, служба реагування на комп'ютерні інциденти (CERT) та система netForensics знижують рівень загроз інформаційній безпеці в мережах LTE. CERT здійснює збір, зберігання і обробку статистичних даних, пов'язаних з поширенням шкідливих програм і мережевих атак. До компетенції служби входить обробка комп'ютерних інцидентів з метою їх виявлення і нейтралізації. Система netForensics призначена для роботи з гетерогенним середовищем продуктів забезпечення інформаційної безпеки і реалізує безперервний збір, обробку та відображення подій безпеки.

Література

[1] В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. «Інформаційна та кібербезпека: соціотехнічний аспект». К.: ДУТ, 2015. С. 24-30.

[2] В. Гнатюк. «Методи обробки кіберінцидентів в інформаційно-телекомунікаційних системах». 2017.URL:http://dspace.nau.edu.ua/bitstream/NAU/28984/3/diss.pdf.

[3]Служба реагування на комп'ютерні інциденти. URL: http://sts.kz/ru/kzcert.

[4] A Distributed Architecture Delivering Scalability and Performance. URL: http://www.netforen sics. com/architecture.html.

[5] Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. К.: НАНУ 209. С. 149.

[6] В.Г. Кононович, С.В. Гладиш. «Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування». Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник. Одеса : ОНАЗ ім. О.С. Попова, 2009. С. 208.

[7] І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк. «Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій». *Восточноевропейский журнал передовых технологий*. № 2 (56). 2012. С. 18-21.

[8] LTE.Специфика сетей. URL: http://Rohde-schwarz.ru/tech.

УДК 003.26:004.056.55:621.39(045)

Одарченко Р.С., Гнатюк В.А., Федюра Т.В., Коберник А.Ю. Разработка системы управления киберинцидентами в сетях LTE

Аннотация. *Сотовые сети связи на данном этапе являются одними из самых распространенных во всем мире. Последним технологическим решением, которое нашло широкое распространение, являются сети LTE. Данные сети используются для передачи голоса, данных, подключение стационарных устройств, устройств Интернета вещей и тому подобное. Однако с рядом преимуществ, которые предоставляет каждое новое поколение сетей связи, появляются и новые угрозы, в том числе в области обеспечения кибербезопасности. Так возникают новые виды атак, количество устройств, с которых они могут быть организованы. Поэтому очень важным является разработка новых механизмов обеспечения кибербезопасности в современных сотовых сетях, как предоставят гарантии безопасной доставки данных абонентов и устройств IoT. Поэтому был проведен анализ механизмов обеспечения информационной безопасности самого популярного в мире типа сетей LTE. Проведенные исследования показали, что LTE, несмотря на ряд преимуществ, имеет и недостатки. Прежде всего, это уязвимость к атакам DoS (Denial of Service) на сеть, вирусных атакам, атакам на дополнительные сервисы. Наличие уязвимостей и киберугроз порождает киберинциденты, для локализации и нейтрализации которых необходимы эффективные методы обнаружения, идентификации, обработки и расследования. Чтобы выявить и бороться с киберинцидентами, было создано архитектуру центра мониторинга киберинцидентов в сетях LTE. В работе также приведена классификация киберинцидентов, рассмотрена служба реагирования на компьютерные инциденты (CERT) и параметры обращений в эту службу. Было исследовано систему netForensics, которая предназначена для работы с гетерогенной средой продуктов обеспечения информационной безопасности и реализует непрерывный сбор, обработку и отображение событий безопасности. Также был разработан вариант развертывания системы управления киберинцидентами netForensics в сети LTE, рассмотрены основные элементы сети LTE и их взаимодействие с netForensics nFX Open Security Platform. Эта система управления киберинцидентами имеет широкие возможности работы в распределенном режиме, поддержку различных отказоустойчивых конфигураций и тому подобное. Система управления киберинцидентами netForensics реализована на базе технологии Java по модульному принципу.*

Ключевые слова: *LTE, киберинцидент, сотовая сеть, кибератака, 3G/4G/5G, CERT, netForensics.*

Odarchenko R., Gnatyuk V., Fediura T., Kobernik A. The development of cyberindidents management system on LTE networks

Abstract. *Cellular networks at this stage are among the most widespread in the world. The latest technological solution, which has become widespread, are LTE networks. These networks are used to transmit voice, data, connecting stationary devices, Internet devices, etc. However, with a number of advantages provided by each new generation of communication networks, new threats are emerging, including in the field of cybersecurity. So there are new types of attacks, the number of devices from which they can be organized. Therefore, it is very important to develop new mechanisms for providing cybersecurity in modern cellular networks, as it will provide guarantees for the safe delivery of data to subscribers and devices IoT. Therefore, we analyzed the mechanisms of information security in the world's most popular type of LTE networks. Studies have shown that LTE, despite a number of advantages, also has disadvantages. First of all, this is a vulnerability to DoS (Denial of Service) attacks on the network, virus attacks, attacks on additional services. The presence of vulnerabilities and cyber threats generates cyber incidents, which require effective detection, identification, processing and investigation methods for localization and neutralization. In order to detect and combat cyber incidents, the architecture of the cyber incident monitoring center in LTE networks was created. The paper also describes the classification of cyber incidents, examines the Computer Crisis Response Service (CERT), and access control options for this service. The netForensics system, which is designed to work with a heterogeneous information security information security environment and implements a continuous collection, processing and display of security events, was explored. Also developed was the deployment of the NetForensics cyber incident management system on the LTE network, the main elements of the LTE network and their interaction with netForensics nFX Open Security Platform were considered. This cyber incident management system has wide-ranging capabilities in distributed mode, support for various fault-tolerant configurations, and more. NetForensics cyber incident management system is implemented on the basis of Java technology on a modular basis.*

Key words: *LTE, cyber incident, cellular network, cybersecurity, 3G/4G/5G, CERT, netForensics.*

Отримано 20 *червня 2018 року*, затверджено редколегією 20 *липня 2018 року*