тем и технологий Института специальной связи и защиты информации НТУУ «КПИ».
Mokhor Volodymyr, Professor, Doctor of Science in Eng., Head of Academic Department of Cybersecurity and the use of information systems and technologies, Institute of Special Communication and Information Security of NTUU «KPI».

УДК 004.4.056.53:004.43(031)

ОСОБЛИВОСТІ СИСТЕМИ КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ ВЕЛИКОГО РОЗМІРУ

Володимир Луценко, Андрій Балан

Для побудови комплексних систем захисту інформації та інших систем безпеки необхідно проводити аналіз ризиків інформації. При обслуговуванні систем передавання даних великих розмірів в оптичних лініях зв'язку нагляд за даними є складним завданням. Воно вимагає застосування нових апаратних рішень у засобах контролю, нагляду та збору даних, що є вихідною інформаційною базою майбутніх проектів. Розглянутою є проблема використання нових засобів захисту інформації при проектуванні комплексних систем захисту інформації. Головна увага приділяється методам контролю за потоками інформації великого розміру, котрі досяжні атакам кіберзлочинців. Розглядаються питання систем контролю, котрі застосовуються в Україні та за її межами, та мають функціональні властивості що дозволяють здійснювати захист від кібертероризму при їх використанні у якості засобів захисту в рамках проектів комплексних систем захисту (КСЗІ).

Ключові слова: *комплексна система захисту інформації; проект захисту; лінії зв'язку; сітьовий екран; сітьовий комплект.*

Вступ. Згідно Закону України «Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність»», що була ратифікованою 7 вересня 2005 р., в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов`язаних з інформаційно - комп`ютерними системами (ІКС) та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. Необхідність протидії кіберзлочинності визначається фактом підписання цього Закону. Масштабність проблеми може ілюструватися хоча б результатами обговорень на Конференції з питань інформаційної безпеки проведеною 9 грудня 2009 р. Американською торгівельною палатою в Україні, де присутніми були президенти торгівельних палат, посол США, генеральний директор «Майкрософт Україна», українські та зарубіжні фахівці з питань інформаційної безпеки та кіберзлочинності: представники МВС України, Федерального бюро розслідувань (FBI) та інші фахівці. Фахівці одностайні у тому, що безперервне зростання кіберзлочинності пов'язане з тим, що реалізація електронних злочинів, як правило, не є складною (95% фінансове шахрайство та крадіжки; 5% шпіонаж).

З огляду на реальні справи в Україні теза про нескладність реалізації кіберзлочинів має рацію.

Постановка проблеми. З огляду на реальні справи в Україні теза про нескладність реалізації кіберзлочинів має рацію. Такий стан підтримується тим, що не є систематизованими та врегульованими, наприклад, такі питання як:

– централізація відомостей та узгодженість дій з боку дозвольних органів, органів контролю (НКРЗ) та органів слідства про архітектуру та функціонування мереж ВОЛЗ власників «TransTeleCom», «Vympelcom», «RETN», «SMUR», «MTS», «Golden Telecom», «Romtelecom», «PanTel», «T-Com», «Matav», «GTS», «TelKolejowa». Особливо важливими при цьому є відомості щодо мережевого зв'язку з боку Польщі, Білорусі, Росії, Румунії, Молдови, Угорщини, Словаччини, загальні з Україною мережі котрих обслуговуються вищезазначеними власниками;

– фактична складність систематизації даних щодо приватних власників ліній останньої милі;

– встановлення регламенту користування трафіками на фізичних та логічних рівнях від магістралей з віддзеркаленнями на маршрутизатори, а далі на комутатори і до трафіків останньої милі;

– фактичне невиконання вимог Наказу Служби Безпеки УКРАЇНИ та Міністерства Транспорту та зв'язку України від 31.07.2008 № 645/962 про затвердження нормативного документа «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги», що створений відповідно до статті 15 Закону України «Про телекомунікації» (1280-15), статті 5 Указу Президента України від 07.11.2005 N 1556 (1556/2005) «Про додержання прав людини під час проведення оперативно-технічних заходів»;

– невиконання ст.39 Закону України «Про телекомунікації» *(Відомості Верховної Ради України (ВВР), 2004, № 12, ст.155)*, щодо «Обов'язки операторів і провайдерів телекомунікацій»;

– відсутність затвердженого до використання визначеного **єдиного** комплексу технічних засобів для вирішення завдань глобального контролю інформаційних потоків визначеного рівня, аналогічних, наприклад, «СОРМ-1» та «СОРМ-2» (Росія), сумісних з апаратурою власників мереж;

– неадаптованість методології використання трафіків взаємного використання на логічному рівні до завдань контролю над інформаційними потоками.

Зазначені лише головні чинники дієздатності порушень. Проблема полягає у тому, що для безпечного розвитку ІКС в Україні вирішення зазначених питань вимагає більш системного підходу, ніж виключно створення наглядових та каральних структур. Необхідним є створення методики побудови ІКС не стільки в межах повноважень власників мереж та провайдерів, а у регіональних та державних масштабах. При цьому функція наглядовості за користувачами та інформаційними потоками має бути узгодженою з головними засадами діючої методології захисту інформації (ЗІ), котра використовується при створенні систем захисту інформації (СЗІ) на діючих об'єктах інформаційної діяльності (ОІД). Така задача може вирішуватися за рахунок поєднання підходів, направлених на:

– використання або створення дієвої і єдиної для усіх власників ІКС та провайдерів апаратури та систем на її базі щодо контролю за інформаційними потоками у трафіках систем зв'язку;

– здатність виконавців-проектувальників комплексних систем захисту інформації (КСЗІ) враховувати можливості такої апаратури та систем на їх основі при проектуванні захисту ОІД;

– здатність узгодження заходів контролю не тільки з законодавством України, а й інших Держав співкористувачів ІКС.

Метою статті є викладення підходу щодо можливості створення системи контролю за інформаційними потоками з зазначеними властивостями.

Виклад основного матеріалу. Розглянемо питання використання діючих на ринках Європи та України систем, котрі можуть бути функціонально близькими до такої, що розглядається.

Для прикладу, компанія VERNA представляє комплексне рішення RimatriX5 виробництва Rittal для центрів обробки даних (ЦОД). У нашому випадку, позитивним є те, що представленою є практика планування і реалізації інженерної інфраструктури ЦОД. У якості доставника VERNA володіє спеціалізацією Cisco Advanced Security та має досвід будування захищених мультисервісних сіток підприємств на базі продуктів і технологій Cisco. Але проекти, масштабу більш ніж підприємства, окремі банки, поштових служб є недосяжними для такої реалізації.

Такі компанії як ЦЕБИТ, SI BIS, IDC та ін. направляють свою діяльність на методологію забезпечення безпеки бізнесу, що є напрямком поза інтересів правоохоронних органів щодо спостережливості за інформаційними потоками.

Загалом недоліком більшості систем Ethernet є відсутність функцій спостереження в інтересах правоохоронних органів. Справа у тому, що функціональні вузли мереж при своїй розробці і не передбачають такі функції. Тому, найбільш перспективною, мабуть, є така система, котра відповідає функціям систем «СОРМ-2» та розроблювана «СОРМ-3».

Щодо реалізації апаратного комплексу зручно розглянути шлюз мережного комплекту МК LI-J призначений для забезпечення законного перехоплення («Lawful Intercept») телекомунікацій з мережного обладнання – маршрутизаторів Juniper M7i, T640, T1600, Mx480, Mx960 і E320. МК LI-J розроблений у відповідності до ЗТВ «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги» затверджені спільним Наказом Служби безпеки України та Міністерством транспорту та зв'язку України № 645/962 від 31 липня 2008 року. та стандартів ETSI (Європейського Інституту Стандартизації Електрозв'язку).

Перехоплення телекомунікацій здійснюється за допомогою підключення до вузла мережного обладнання через порт. Відбір інформації в сеансах зв'язку за встановленими критеріями, комбінаціями ознак і фільтрами пошуку здійснюється в мережному обладнанні. Інформаційні потоки трафіку відібраних даних поступають на Шлюз мережного комплекту МК LI-J для подальшої обробки та передачі вмісту відібраних об'єктів перехоплення в систему управління системою перехоплення телекомунікацій ЗУСП. Паралельно з передачею вмісту відібраних даних в ЗУСП від МК LI-J потрапляє службова інформація про відібрані сеанси зв'язку.

Основні функції:

– організація інтерфейсу взаємодії з серією маршрутизаторів компанії Juniper;

– формування по командах від ЗУСП ознак перехоплення в мережному обладнанні Juniper;

– взаємодію із системами Авторизації Аутентифікації та Акаунтінгу;

– прийом та обробка повідомлень протоколу Radius;

– прийом/передачу команд управління та контролю між засобами ЗУСП та мережним обладнанням;

– прийом та первинну обробку сеансів зв'язку від мережного обладнання;

– генерування супутньої інформації про відібрані сеанси зв'язку (IRI);

– захист від несанкціонованого доступу до програмних ресурсів системи та інформації, що зберігається в ній;

– дистанційний контроль та конфігурування всіх програмних модулів системи в реальному часу і доступ до відібраної інформації по кодових лініях зв'язку;

– автоматичне протоколювання дій користувачів та підсистем комплексу, за алгоритмами та у формі, які є єдиними та уніфікованими з іншими комплексами, що застосовуються.

– контроль справності каналів обміну інформацією між МК LI-J та ЗУСП. При відсутності зв'язку організовується збереження інформації до моменту відновлення;

Реалізація інтерфейсів функції LI та їх взаємодія з обладнанням Juniper здійснюється при підключення МК LI-J до мережі. Таке підключення МК LI-J здійснюється через порт підключенням до мережного інтерфейсу. Налаштування обладнання Juniper для взаємодії із МК LI-J відбувається одноразово адміністратором обладнання Juniper згідно наданої йому інструкції. Протокольна взаємодія МК LI-J по інтерфейсу **X1**(INI1) із обладнанням Juniper відбувається з використанням протоколу XML, механізмів JUNOScript, Python- та Perl-скриптів.

Для передачі вмісту відібраного сеансу зв'язку (CC) по інтерфейсу **X3**(INI3) з обладнання Juniper до Шлюзу використовуються механізми інкапсуляції, а у випадку, коли використовується віддалене підключення обладнання Juniper до МК LI-J – також механізми тунелювання та шифрування трафіку.Загальна схема взаємодії Шлюзу з обладнанням Juniper та іншим обладнанням оператора зв'язку (провайдера) показана на Рис.1.

X1 – інтерфейс для передачі адміністративної інформації. Генерації супутньої інформації (IRI) здійснюється від двох інтерфейсів X2(INI2):

X2.1 – для отримання всього AAA-трафіку оператора зв'язку. Забезпечується відгалужувачем сигналу, встановленим на каналі зв'язку Juniper – Radius-сервер;

X2.2 – для отримання всієї доступної інформації про клієнта оператора (об'єкта спостереження).

X3 – інтерфейс для передачі змісту сеансів зв'язку.

Шлюз мережного комплекту МК LI-J одночасно може забезпечувати роботу з декількома маршрутизаторами, в тому числі і різних моделей. Передача вмісту відібраних окремих об'єктів перехоплення на віддалені термінали суб'єктів перехоплення відбувається у відповідності до команд управління.

Таким чином, представлений комплекс є загалом, найбільш адаптованим до вирішення поставленої задачі.

Можливості впровадження комплекту широкі. При створенні ОІД інформаційно-телекомунікаційної системи (ІТКС), або обстеженні діючого, рішення про необхідність застосування засобів інформаційного захисту приймається на визначеній стадії створення автоматизованої системи, що дає можливість щодо узгодження етапу побудови системи захисту з відповідним етапом створення КСЗІ [1]. Згідно з функціональною специфікою системи що розглядається, рішення про впровадження системи нагляду має прийматися не раніше п. 2 «Стадії створення АС», а саме на етапі «Розробка концепції АС» [2]. При цьому під функціональною специфікою розуміти необхідно те, що «Визначення й аналіз загроз» як перший етап побудови СЗІ за [3], є відсутнім, оскільки сам факт необхідності впровадження такої

системи вже є визначенням переліку загроз, котрими є загрози, пов'язані з кіберзлочинністю всередині інфраструктури АС, або можливість формування трафіку за межі України. Тоді і «Формування загальних вимог до КСЗІ» за [4] має враховувати те, що при «Обстеженні середовища функціонування ІТКС» за п.6.1.2 згідно [4] виявленим має бути факт функціонування КСЗІ у присутності загалом «ворожої» системи нагляду, що розглядається. Очевидно, що вищим пріоритетом інтересів двох систем, а саме, КСЗІ та системи нагляду, володіє система нагляду. Тоді «Формування завдання на КСЗІ» за п.6.1.3 з [4] логічно вкладається у послідовність стадій створення АС та етапам побудови СЗІ і має враховувати присутність системи нагляду, чого наразі не передбачено при проектуванні КСЗІ.

Тобто, необхідним є доробка методики створення КСЗІ з витікаючою необхідністю ревізії супутніх документів.

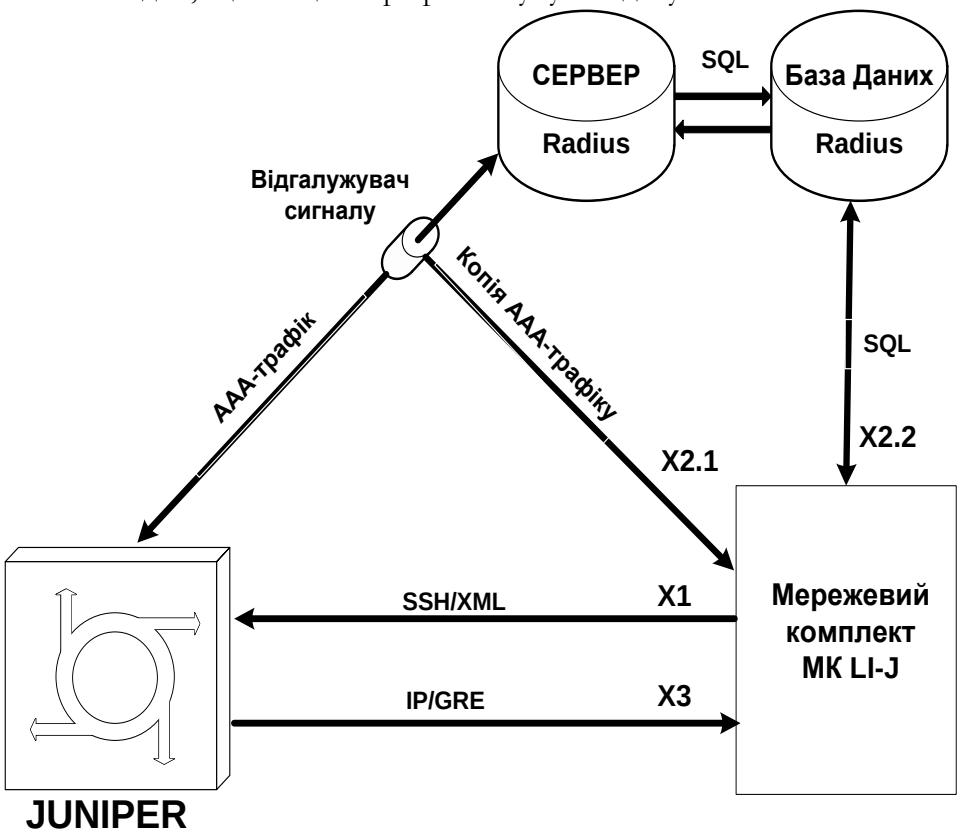

Рис. 1 Загальна схема взаємодії шлюзу мережного комплекту з обладнанням Juniper

Висновки. За такого підходу та при умові розробки відповідних ДСТУ і нормативно-методичної документації з'являється можливість вирішення задачі створення та впровадження системи нагляду на базі мереженого комплекту Juniper.

ЛІТЕРАТУРА

[1]. Луценко В.М. Відповідність етапів побудови систем захисту інформації стадіям створення автоматизованих систем. «Захист інформації», наук. тех. журнал., НАУ, Київ, №3 (52), 2011, С. 52-56.

[2]. ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».

[3]. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення».

[4]. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

REFERENCES

[1]. Lutsenko V. M. Conformity of stages of construction of systems of protection of the information to stages of creation of the automated systems. «Protection of the information», Scientific and technical magazine, National university of aircraft, Kiev, N0 3(52), 2011, p.p. 52-56.

[2]. Standard of Ukraine 34.601-90 «The automated systems. Stages of creation».

[3]. Standard of Ukraine 3396.0-96 «Protection of the information. Technical protection of the information. Stages of creation».

[4]. The normative document of technical protection of the information 3.7-003-05 «The order of work on creation of complex system of protection of the information in information of telecommunication system».

ОСОБЕННОСТИ СИСТЕМ КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ БОЛЬШОГО РАЗМЕРА

Для построения комплексных систем защиты информации и других систем безопасности необходим анализ рисков. При обслуживании систем передачи данных большого размера в оптических линиях связи наблюдение за информацией является сложной задачей. Оно требует применения новых аппаратных решений в средствах контроля и сбора данных, которые являются исходной информационной базой будущих проектов. Рассмотрена проблема использования средств защиты информации при проектировании комплексных систем защиты информации. Главное внимание уделяется методам контроля за потоками информации більшого размера, которые доступны атакам киберпреступников. Рассматриваются вопросы применяемых на рынках Украины и за ее пределами таких систем контроля, функциональные возможности которых позволяют решать задачи защиты от кибертерроризма при их использовании в качестве средств защиты информации в рамках проектов комплексних систем защиты.

Ключевые слова: комплексная система защиты информации; проект защиты; линии связи; сетевой экран; сетевой комплект.

FEATURES OF MONITORING SYSTEMS OF INFORMATION SIZABLE STREAMS

The analysis is necessary for construction of complex systems of protection of the information and other systems of safety to risk. At service of systems of sizable data transmission in optical communication lines supervision over the information is a complicated problem. It demands application of new hardware decisions in means of the control and data gathering which are initial information base of the future projects. The problem of use of new means of protection of the information is considered at designing complex systems of protection of the information. The main attention is given a quality monitoring for streams of the information of the big size, and which are accessible to attacks Cybernetic criminals. Questions used on the markets of Ukraine and behind its limits of such monitoring systems which functionalities allow to solve tasks of protection from Cybernetic terrorism at their use as means of protection of the information within the framework of projects systems of complex of protection are considered.

Index Terms: System of Complex of Protection of the Information; the project of protection; communication lines, the network screen; the network complete set.

Луценко Владимир Николаевич, кандидат технических наук, старший научный сотрудник Академии наук Украины, доцент Физико-технического института НТУУ «КПИ».
E-mail: lutsenkovn@ukr.net
Луценко Володимир Миколайович, кандидат технічних наук, старший науковий співробітник Академії наук України, доцент Фізико-технічного інституту НТУУ «КПІ».
Lutsenko Vladimir, Ph.D., Senior Research Fellow of the Academy of Sciences of Ukraine, Assistant Professor of Physics and Technical Institute of NTU «KPI2.

Балан Андрей Николаевич, аспирант очного отделения Физико-технического института, НТУУ «КПИ».
E-mail: ftzzi@pti.kpi.ua
Балан Андрій Миколайович, аспірант Фізико-технічного інституту, НТУУ «КПІ».
Balan Andrej, the post-graduate student of physicotechnical institute of the «KPI».

УДК 621.372

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СВЧ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ПО ЦЕПИ ЭЛЕКТРОПИТАНИЯ

Валерий Козловский, Роман Лысенко

Для построения фильтрующих устройств СВЧ (сверх высоких частот) с целью предотвращения утечки информации по цепям электропитания необходимо учитывать влияние внешних экранов. Существующие методы синтеза устройств фильтрации основаны на использовании математической модели двухпроводной линии передачи без учёта эффекта экранирования внешней оболочкой. В результате аплитудно-частотная характеристика фильтра отличается от экспериментальной, что приводит к ухудшению фильтрации в полосе заграждения. Предложено использовать в качестве концептуальной математической модели элемента фильтра модель связанной линии передачи. Концептуальная модель позволяет учитывать эффект экранирования внешней оболочки и повышает точность расчета устройств фильтрации цепей электропитания.

Ключевые слова: *связанная линия, восьмиполюсник, четырехполюсник, чётное и нечётное возбуждение, волновое сопротивление.*