ТОМ 16

КІБЕРБЕЗПЕКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 004

Бабяк Є.О., ст. гр. ЗМм-15-1м,
(Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна)

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ МЕТОДУ НЕЧІТКОЇ КЛАСТЕРИЗАЦІЇ ТА ОБЧИСЛЕННЯ ВЗАЄМНОЇ ІНФОРМАЦІЇ

Введение

С развитием Internet-технологий и электронной коммерции с каждым днем появляется все больше угроз безопасности информации. Сегодня организации все чаще используют информацию в бизнес-процессах, для облегчения управленческих решений и ведения бизнеса. Зависимость от информации в бизнес-среде крайне велика, где множество торговых операций осуществляется в электронном виде через Internet. Такая информационная зависимость привела к существенному увеличению влияния уровня безопасности информационных систем на успех, а иногда и просто возможность ведения бизнеса. Поэтому безопасность информационных систем является одним из важнейших вопросов, который привлекает большое внимание со стороны аналитиков, инженеров и других специалистов в области информационно безопасности. Четкой методики количественного расчета величин рисков как не было, так и нет. Это связано в первую очередь с отсутствием достаточного объема статистических данных о вероятности реализации той или иной угрозы. Данная статья предлагает новый метод оценки рисков информационной безопасности, основанный на комбинации вычисления взаимной информации и K-means алгоритма кластеризации. Для того чтобы добиться эффективной оценки уровня рисков информационной безопасности, новый метод определяет количество факторов риска всех данных и зависимость степени безопасности при вычислении взаимной информации. Затем осуществляется поиск оптимального значения для каждой степени риска как центр точек K-means алгоритма кластеризации и используется K-means алгоритм кластеризации для классификации данных.

Оценка рисков информационной безопасности на основе взаимной информации и k-means алгоритма кластеризации

В оценке рисков информационной безопасности основные элементы риска отражаются в активах системы, существующих угрозах и уязвимостях, а также анализ рисков оценивает уровень риска от оценки показателей, таких как частота угрозы, степень тяжести уязвимости, стоимость активов и т. д. Оценочные показатели имеют некоторые свойства значительной двусмысленности и неопределенности, поэтому обычные методы с трудом поддаются измерению. Кроме того, эти оценки показателей и уровней риска являются нелинейными и динамические изменяющимися, поэтом обычные методы так трудно перерабатывать. Новый метод оценки рисков не содержит данных проблем. Во-первых, мы используем метод нечеткой оценки для количественного измерения риска. Во-вторых, рассчитывается значение взаимной информации риска для обозначения зависимости степени риска и уровня риска. Данные были классифицированы по K-means алгоритму с оптимальными взаимными информационными данными в качестве исходных центров кластеров. Этот способ прост и содержит небольшое количество вычислений. Он позволяет избежать проблемы чувствительности к начальному значению, нелинейности и сложности оценки рисков информационной безопасности.

Заключение

Для того чтобы решить проблему оценки рисков информационной безопасности, связанную со сложностью определения оптимальных значений, в данной статье

предложен новый метод оценки рисков информационной безопасности, основанный на вычислении взаимной информации и K-means алгоритме кластеризации, позволяющем эффективно оценивать уровни риска информационной безопасности. Метод определяет степень количественной зависимости между факторами риска и уровнем информационной безопасности с вычислением взаимной информации. На каждом уровне риска, определяются оптимальные точки как начальные центры кластеров по алгоритму K-means, затем алгоритм кластеризации K-means классифицирует данные. Наш метод может динамически регулировать центр кластера в соответствии с результатами кластеризации и вычисление значения взаимной информации. Этот метод легко применять, он имеет меньше вычислений, чем традиционные методы. Метод позволяет предотвратить чувствительность к входным данным, нелинейность, сложность и другие проблемы оценки рисков информационной безопасности. Экспериментальные результаты также показывают превосходность метода.

Перелік посилань

1. Maiwald E. Netwok Secuity: A Begginner’s. The McGraw-Hill Companies, Inc, 2001.

2. ISO/IEC 17799. Information Technology-Code of practic for information security management.2000.

3. MnSCU. Security Risk Assessment-Applied Risk Management Minnesota State Colleges & Universities, 2002, c.7.

4. А. Астахов. Искусство управления рисками. GlobalTrust. 2009.

5. R.L. Winkler, Uncertainty in probabilistic risk assessment, Reliability Engineer- ing and System Safety 54 (2–3) (1996), c. 127–132.

6. Dang Depeng, Meng Zhen. Assessment of information security risk by support vector machine. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2010, 3(38), c.46–49.

УДК 681.3

Віролайнен В.О., студент гр. ЗСм-14-1м,
Науковий керівник: Плец О.О., асистент кафедри БІТ
(Державний ВНЗ "Національний гірничий університет", м. Дніпропетровськ, Україна)

ВРАЗЛИВОСТІ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ ПРИ ЗАСТОСУВАННІ ТЕХНОЛОГІЇ ZIGBEE

За останнє десятиріччя широке поширення одержали бездротові сенсорні мережі (БСМ). Бездротова сенсорна мережа являє собою розподілену систему збору, зберігання і обробки інформації.

БСМ повинна забезпечувати надійну і своєчасну доставку трафіку. В багатьох системах, особливо природних, важко або зовсім неможливо підготувати інфраструктуру для побудови такої мережі. Все ці чинники обумовлюють інтерес дослідників у даній області до розподілених систем збору, доставки та обробки інформації. Існуючі моделі збору інформації в БСМ накладують обмеження на їх використання. В той же час не існує моделі збору, яка може, з деякими обмеженнями, використовуватися для різних за призначенням БСМ.

ZigBee – бездротовий стандарт передачі даних. ZigBee – самоорганізовувані і самовідновлювальні мережі. Це пояснюється тим, що, маючи вбудоване програмне забезпечення, при вмиканні живлення, ZigBee пристрої самостійно знаходять один одного, формуючи мережу. При цьому, якщо будь-який із вузлів виходить з ладу, ZigBee мережі здатні створювати нові маршрути для обміну повідомленнями.

Технологія ZigBee характеризується невеликою швидкістю передачі даних та незначними показниками відстані між вузлами. Проте, при застосуванні у промисловості, ZigBee має певні переваги, а саме:

1. Спрямованість на застосування в системах розподіленого керування із накопиченням інформації з інтелектуальних датчиків, в яких провідними є завдання максимальне зменшення енергоспоживання і ресурсів, які використовуються процесорами;
2. Сприяння утворенню самостійно конфігуруючих мереж зі складною топологією, де маршрут повідомлення визначається кількістю працюючих вузлів та якістю їхнього зв’язку;
3. Забезпечення масштабованості – автоматизоване підключення до роботи вузла або групи вузлів з моменту подачі електропостачання;
4. Завдяки можливості вибору іншого маршруту обміну повідомленнями в разі непередбачених збоїв у роботі вузлів, забезпечується висока надійність мережі;
5. Підтримка вбудованих апаратних механізмів шифрування повідомлень AES-128.

ZigBee заснований на стандарті IEEE 802.15.4-2006 для бездротових персональних мереж, як то бездротові головні телефоні. Специфікація ZigBee створена для того, щоб бути простішою та дешевшою за інші персональні мережі, такі як Bluetooth. ZigBee використовується для мобільних пристроїв, де важливим завданням є багаточасова робота від акумулятора і забезпечення безпеки передачі даних у мережі.

IEEE 802.15.4 – стандарт, який визначає фізичний шар і керування доступом до середовища для бездротових персональних мереж із невеликою швидкості. Архітектура стандарту показана на рисунку 1.

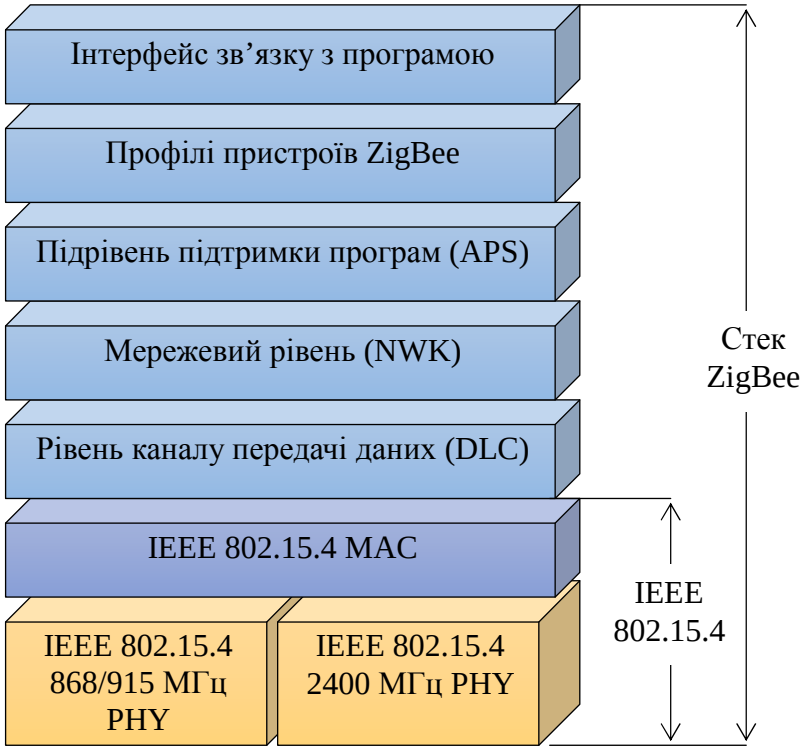

Рисунок 1 – Зв'язок стеку ZigBee із стандартом IEEE 802.15.4

Стек протоколу ZigBee грунтується на стандарті IEEE 802.15.4 і працює на прикладному і мережевому рівні моделі OSI.

При достоїнствах технології ZigBee є і недоліки. А саме:

– недостатньо високий рівень стандартизації і відсутність єдиної програмно-апаратної платформи для розробки складних програм;

– невисока швидкість передачі даних. Велика частина трафіку ZigBee витрачається на передачу пакетів.

Технологія ZigBee розвивається, але головна вразливість цієї технології – дефолтні за замовченням ключі зв'язку потребує вирішення. У гонитві за сумісністю з пристроями інших виробників, низькою ціною і зручністю користувача. Використання дефолтних ключів ставить під загрозу безпеку мережі в цілому. До того ж, сам стандарт ZigBee вельми вільно ставиться до питання безпеки і збереження ключів, тобто безпечна ініціалізація і передача зашифрованих ключів всередині мережі не є достатніми та вразливі. За допомогою простого сніфінга, атакуючий здатний перехопити обмін ключами і проникнути до мережі, використовуючи дефолтний ключ. В результаті пристрої виявляються відкриті для атаки «Людина посередині», а мережа, активний мережевий ключ і всі комунікації всередині мережі будуть скомпрометовані.

До вразливостей технології ZigBee відноситься можливість реалізації DDoS атаки. Головною задачею цієї атаки є доведення до відмови використовуючи метод перебору усіх можливих варіантів ключа.

Перелік посилань

1. Балонин Н.А., Сергеев М.Б. Беспроводные Персональные Сети. [Текст]: Учеб. Пособие, СПбГУАП. СПб., 2012. – 68 с.

2. IEEE 802.15.4 [Електронний ресурс] – Вікіпедія – [Режим доступу] https://ru.wikipedia.org/wiki/IEEE_802.15.4.

3. Проблемы с ZigBee [Електронний ресурс] – [Режим доступу] https://xakep.ru/2015/08/10/zigbee-devices-problems.

УДК 681.3.062

Гончаров С.С., студент гр. ЗСм-14-1м,
Науковий керівник: Масальська Олена Олександрівна, асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ "Національний гірничий університет", м. Дніпропетровськ, Україна)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ САЙТІВ, НАПИСАНИХ ЗА ДОПОМОГОЮ ФРЕЙМВОРКУ DJANGO (PYTHON)

Django (Джанго) – відкритий фреймворк високого рівня для розробки веб-систем, який використовує мову програмування Python як основу. Django реалізований на основі архітектури MVC (Model-View-Controller), що дозволяє досягти високої швидкості написання коду, ефективності його роботи та якісного налагодження програми.[1] Названо його було на честь джазмена Джанго Рейнхардта (відповідно до музичних смаків одного зі засновників проекту).[2]

Відмінні особливості Django:

- будь-який запит обробляється програмно і перенаправляється на свою адресу (url);
- поділ контенту і представлення за допомогою шаблонів;
- не використовується низький рівень баз даних.

Основні атаки, яки можна провести на сайти, створені за допомогою фреймворку Django та методи захисту від подібних атак:

1) XSS атака (англ. CrossSiteScripting – «міжсайтовий скриптінг») – це один з найпоширеніших видів хакерської атаки на прикладному рівні. Метою XSS є вставка в сторінку скриптів, які зазвичай виконуються на стороні клієнта (в браузері користувача), а не на сервері. Суть XSS полягає в наступному: зловмисник впливає на скрипти веб-додатку на стороні клієнта, змінюючи їх виконання. У результаті в сторінку вбудовується скрипт, який буде виконуватися кожного разу при завантаженні сторінки або при певній події.

Захист: Використання шаблонів Django забезпечує захист від більшості XSS атак. За допомогою цих шаблонів екрануються спеціальні символи, які могли б якось вплинути на отриманий HTML. Але незважаючи на те, що екранування може захистити від багатьох видів шкідливого введення, воно не дає стовідсоткового захисту.

Треба фільтрувати дані, які вводяться та виводяться, а також всі поля, які можуть змінюватися користувачами. Сюди відносяться дані, одержувані із запитів GET і POST, а також запити, що повертаються з бази даних.

Також потрібно бути дуже обережним при збереженні HTML в базі даних, особливо якщо цей HTML буде відображений згодом.

Ще одним засобом захисту буде використання заголовка ContentSecurityPolicy, що дозволяє задавати список, до якого заносяться бажані джерела, з яких можна довантажувати різні дані, наприклад, JS, CSS, зображення та ін.

2) CSRF атака (англ. CrossSiteRequestForgery – «міжсайтова підробка запиту») – атака, що дозволяє недобросовісному користувачеві виконувати дії від імені іншого користувача, без відома останнього або його згоди. Вона базується на тому, що коли користувач заходить на сайт, створений зловмисником, від його особи таємно відправляється запит на інший сервер, який здійснює деяку шкідливу операцію.[3]

Захист: По-перше, переконатися, що ніякі GET-запити не виробляють побічні ефекти.

Щодо метода POST, потрібно включити в кожну форму <form>, що відправляється цим методом, приховане секретне поле, значення якого генерується в

кожному сеансі заново. При обробці форми на сервері слід перевірити це поле і вивести виняток, якщо перевірка не пройшла. Так працює система захисту від CSRF-атак в Django.[4]

3) SQL-ін'єкція – атака, яка базується на впровадженні в дані (передані через GET, POST запити або значення Cookie) SQL коду. Якщо сайт вразливий і виконує такі ін'єкції, то зловмисник може робити з базою даних що завгодно.[5]

Захист: Потрібно екранувати все, що формує SQL запит. Використання Django ORM забезпечить правильне екранування сформованого SQL запиту за допомогою відповідного драйвера бази даних.

4) Клікджекінг (англ. Clickjacking) - атака, при якій користувач, здійснюючи клік на спеціально сформованої сторінці зловмисника, насправді клацає по посиланню на абсолютно іншому сайті.

Захист: Розробники браузерів ввели новий заголовок відповіді сервера X-Frame-Options, який дозволяє не відображати сайт, якщо він завантажується с іншого домену через iframe.[6] У Django для додавання цього заголовка є налаштовуємий клас XFrameOptionsMiddleware.

Додаткові поради щодо забезпечення безпеки сайту:

- код сайту не повинен знаходитися на корені веб сервера. В іншому випадку не виключена ймовірність зловмисного або випадкового виконання коду або відображення у текстовому вигляді;
- у тому випадку, якщо передбачено завантаження файлів на сайт, бажано обмежити розмір файлів, що завантажуються на сайт, щоб уникнути DOS атаки. Це робиться в налаштуваннях веб сервера;
- необхідно перевіряти усі файли, що завантажуються на сайт;
- у Django немає обмеження за кількістю спроб автентифікації користувачів. Тому обмежити кількість таких запитів можна за допомогою додатку для Django та налаштувань веб-сервера;
- зберігати в секреті SECRET_KEY;
- також можна обмежити доступ до бази даних та системи кешування за допомогою брандмауеру.

Перелік посилань

1. Что такое Django Framework и для чего он применяется [Електронний ресурс]. – Режим доступу: http://artkiev.com/blog/django-framework.htm.
2. Вікіпедія. Django [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Django
3. Вікіпедія. Межсайтовая подделка запроса [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Межсайтовая_подделка_запроса
4. Защита от атак CSRF Django [Електронний ресурс]. – Режим доступу: http://webdevelop.info/zashhita-ot-atak-csrf-django/
5. SQL инъекции. Проверка, взлом, защита [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/130826/
6. Боремся с Clickjacking [Електронний ресурс]. – Режим доступу: http://prophet.ru/2011/08/fighting-clickjacking/

УДК 621.397.27

Красовська Ю.О., студентка гр. ТКіт-12-1,
Науковий керівник: Магро В.І., доцент кафедри безпеки інформації та телекомунікацій
(*Державний ВНЗ "Національний гірничий університет", м. Дніпропетровськ, Україна*)

ДОСЛІДЖЕННЯ ВІДМІННОСТЕЙ СТАНДАРТІВ ЦИФРОВОГО НАЗЕМНОГО ТЕЛЕБАЧЕННЯ DVB-T і DVB-T2

Вступ

Україна знаходиться на етапі поступової заміни аналогового телебачення цифровим. Але у відомій літературі мало уваги приділяється обговоренню відмінностей між стандартами цифрового телебачення. Дослідження відмінностей таких стандартів допоможе визначитися з доцільністю підключення деякого з них. Розглянемо важливі моменти на прикладі зіставлення стандартів DVB-T і DVB-T2.

Історична довідка

Стандарт DVB-T, прийнятий у 1997 році, завдяки використанню метода OFDM (orthogonal frequency division multiplexing – ортогональне частотне розділення каналів) має достатньо високу завадостійкість, що дозволило забезпечити стійкість до завад від затриманих сигналів, які виникають через віддзеркалення від земного рельєфу та будівель, а також через сигнали віддалених передавачів одночастотної мережі.

На початку 2009 року був розроблений стандарт DVB-T2, який суттєво перевершив стандарт першого покоління за пропускною здатністю та ефективністю використання частотного ресурсу.

Основні переваги DVB-T2

1. Використання технології повороту сигнального сузір'я на певний круговий кут. За рахунок повороту діаграми на точно підібраний кут кожна точка сузір'я набуває унікальних координат (μ1 і μ2), неповторювані іншими точками. Кожна координата точки оброблюється у модуляторі окремо, після чого вони передаються у OFDM сигналі окремо одне від одного. У приймачі μ1 і μ2 знову об'єднуються, формуючи вихідне сузір'я, зміщене по колу. Таким чином, якщо одна несуча або символ загубляться в результаті завад, збережеться інформація про іншу координату, що дозволить відновити символ, хоча і з більш низьким рівнем сигнал/шум (S/N). Лабораторні дослідження показали, що використання повороту сигнального сузір'я дозволяє отримати виграш у відношенні S/N від 4 до 7 дБ.

2. Використання розмірностей FFT 16K і 32K дозволяє передати від 1,7% (16K) до 2,1% (32K) додаткових даних порівняно з режимом 2K.

3. Більш ефективне кодування: LDPC (Low Density Parity Check Codes – завадо захищений код з низькою щільністю перевірок на парність) і код BCH (Bose-Chaudhuri-Hocquenghem – Боуза-Чоудхури-Хоквингема). Використання таких видів кодування дозволяє впритул наблизитися до межі Шеннона та досягти додаткового виграшу у співвідношенні S/N 3-5 дБ.

4. Застосування нових видів кодування та поворот сигнального сузір'я дозволили використовувати модуляцію 256-QAM. Така модуляція переносить 8 біт на символ та дозволяє на 33% збільшити пропускну здатність каналу зв'язку.

5. Ведення додаткового захисного інтервалу 1/128 також дозволяє збільшити пропускну здатність каналу для роботи DVB-T2.

6. На відмінну від системи DVB-T, де кожний дванадцятий модульований елемент є пілот-сигналом, у стандарті другого покоління введені вісім різних варіантів розміщення, які відповідають кожному варіанту відносної тривалості захисного

інтервалу. Динамічний вибір кількості та розміщення пілот-сигналів може використовуватися для пониження необхідного рівня S/N на вході приймача або для покращення синхронізації.

Виграш при використанні системи DVB-T2 складає від 4,6 до 6,2 дБ. Для реалізації такого виграшу можна розглянути два основні варіанти:

- використання модуляції, що забезпечує більшу пропускну здатність каналу. Так, наприклад, замість модуляції 64-QAM, яка зараз використовується для наземного мовлення в багаточастотній мережі у Києві, можна використовувати модуляцію 256-QAM 2/3. При цьому перехід на нову модуляцію зменшить зону обслуговування передавальної станції, а значення пропускної здатності у цьому випадку зросте на 47% - від існуючих 24,13 Мбіт/с до 35,4 Мбіт/с;

- використання такої самої модуляції та швидкості кодування в стандарті DVB-T2 дозволить суттєво збільшити зону впевненого прийому, зберігаючи при цьому існуючу пропускну здатність каналу. Так використання модуляції 64-QAM 2/3 у стандарті DVB-T2 забезпечує виграш у співвідношенні S/N на 5,9 дБ. Для ефективної висоти антени 200 м і потужності передавача 1 кВт зона впевненого прийому збільшиться на 22%, від 45 до 55 км.

Висновки

- Стандарт цифрового наземного телебачення DVB-T2 має суттєві переваги в області мультимедійних мовних служб.

- Завдяки великій кількості системних параметрів, які впливають на конфігурацію мережі, використання стандарту другого покоління дозволяє гнучко адаптуватися під різноманітні вимоги: модель радіоканалу, розмір та конфігурація мережі, види прийому тощо.

- Використання повороту сигнального сузір'я та завадостійких кодів у стандарті DVB-T2 збільшує завадостійкість системи на 4,6 - 6,2 дБ.

- Використання виграшу в співвідношенні S/N забезпечує збільшення пропускної здатності каналу на 30-50% або збільшення зони впевненого прийому на 20-30%.

Перелік посилань

1. Песков С.Н. Рекомендации по внедрению DVB эфирного вещания [Текст] / С.Н. Песков, И.А. Колпаков // Телеспутник, 2007. – № 2. – 32-35 с.

2. Уэллс Н. DVB-T2: Новый стандарт вещания для телевидения высокой точности [Текст] / Н.Уэллс, К.Нокс // Телеспутник, 2008. – №11. – 92 – 95 с.

УДК 004.056

Маковецький І.Ю., студент гр. ЗСм-14-1м,
Науковий керівник: Кручінін О.В., ст. викладач кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ "Національний гірничий університет", м. Дніпропетровськ, Україна)

ПЕРСПЕКТИВА ВИКОРИСТАННЯ ГЕНЕТИКО-ЕПІДЕМІОЛОГІЧНОГО ПІДХОДУ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВРАЗЛИВОСТЕЙ В ІТС

На даний момент існують дуже ефективні методи для виявлення, виявлення та усунення вразливостей програмного забезпечення (ПЗ), і все ж - визначення фактичних ризиків і ймовірності реалізації загроз в значній мірі спирається на думку експертів та евристики. Альтернативним цьому є розробка методів для аналізу ризику системних служб, визначаючи ймовірність того, що система виявиться скомпрометована, а також ризики, пов'язані з наявністю певних налаштувань і конфігурацій. Варто також згадати, що окрім вразливостей ПЗ, в ІТС існують ще вразливості апаратних засобів. Вони зустрічаються не так часто, як вразливості ПЗ, а серед відомих не має актуальних, які б становили загрозу мережі. Крім того - виявити і ліквідувати їх набагато складніше. Саме тому предметом дослідження даної статі є вразливості ПЗ, на які спираються майже усі сучасні атаки.

Генетична епідеміологія має справу з тим, як взаємодіють генотип і фактори навколишнього середовища, збільшуючи або зменшуючи схильність до хвороби. Епідеміологічні дослідження зазвичай проводять за однією з трьох наступних стратегій: типу випадок-контроль, крос-секційного та когортного дослідження. Служби ОС Windows - додатки, автоматично (якщо є відповідне налаштування) запускаються системою при запуску Windows і виконуються в фоновому режимі. Вони мають спільні риси з концепцією демонів в Unix [1]. У цій статті, служби Windows розглядаються спільно з їх аналогами від інших операційних системи, уся множина такого програмного забезпечення умовно позначається як «служби». Використання такого методу в інформаційній безпеці передбачає необхідність заміни ще деяких визначень, а саме: генотип - це комплект служб, встановлених і працюючих в системі; геном - близьке за змістом поняття до генотипу, представляє з себе комплект служб встановлених на комп'ютері без обліку їх кількості; навколишнє середовище – це умови, за якими здійснюється зв'язок з мережею Інтернет та іншими комп'ютерами в мережі (топологія мережі, провайдер і тощо); хвороба – це компрометація системи [2], порушення політики безпеки або отримання несанкціонованого доступу до системи або будь-якої її частини.

Основна ідея полягає в тому, що ймовірність того, що система виявиться скомпрометована конкретною загрозою значною мірою визначається комплектом встановлених і працюючих на ній мережевих служб, тобто - генотипу. Багато різних атак користуються відомими вразливостями в певних мережевих службах, щоб обійти механізми захисту і отримати несанкціонований доступ, а деякі види шкідливого ПЗ можуть самостійно сканувати служби з метою виявлення потенційних цілей, або навіть активно відкривати порти після зараження. Крім того, наявність певних служб у системі може свідчити про те, яким чином використовується ця система, її призначення, що дозволяє оцінити сприйнятливість системи до певних загроз.

Слід зазначити, що наявність вразливості у програмному забезпеченні (наприклад, відкритий порт) ще не означає, що зловмисник може цим скористатися. Для ефективної реалізації атаки, треба виконати деяку послідовність дій, що часто передбачає експлуатацію якоїсь вразливості на кожному з етапів. Це досить добре графічно проілюстровано у науковій праці на тему «графів атаки» [3]. Наприклад, на Рис. 1 зображено граф атаки, де кожна з вершин графа – це якась вразливість, а цифри поряд з нею – критерій важкості реалізації кожного етапу. Кінцем графу буде отримання несанкціонованого доступу до системи або її частини.

Предмет такого дослідження може бути різним – від невеликої моделі мережі, що складається з декількох віртуальних машин – до гігантської корпоративної мережі. Щоб зрозуміти періодичні загрози, з якими стикається велика комп'ютерна мережа, необхідно зібрати журнали загроз системи виявлення вторгнень або системи запобігання вторгнень (СВВ / СЗВ) що захищають обрану мережу. Точність дослідження і результат також багато в чому залежать від обраного методу розпізнавання атак та досвіду самої системи.

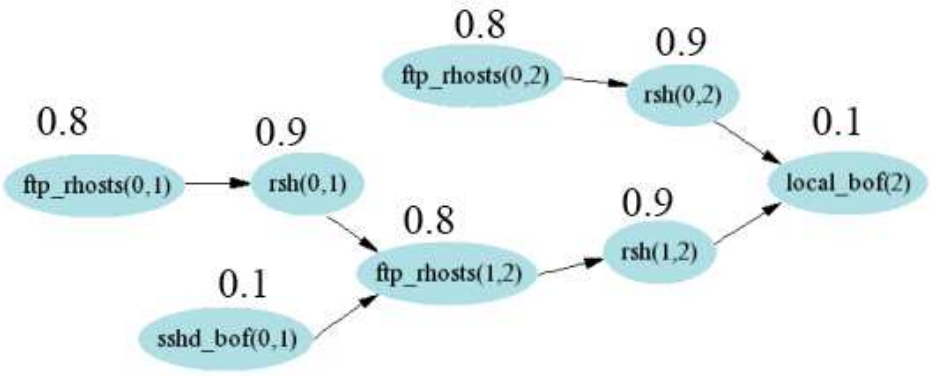

Рисунок 1 – Зразок графу атаки

В одній з наукових робіт на цю тему [4] використовується стратегія типу випадок-контроль, з подальшим дослідженням асоціацій всього генома (Genome-Wide Association Study, GWAS), де комплект усіх просканованих служб прирівнюється до набору мутацій генома, а наявність однієї служби – прирівнюється до наявності однієї алелі (екземпляру) гена. Статистичний зв'язок загроз та служб потім оцінюється шляхом розрахунку статистичної значущості (p-значення) розбіжності між розподілом варіантів для кожного гена в популяції хворих особин і розподілом тих же варіантів гена в популяції здорових особин (контрольної групи). Отримавши статистику, можна побудувати діаграми Манхеттена для кожної загрози, що покаже кореляційну залежність за умови наявності або відсутності служби в системі.

Висновок

Запропонована статистична основа може бути використана, щоб зробити припущення про найбільш актуальні загрози для комп'ютера. Стає можливим створення програмного забезпечення для автоматичної перевірки нових комп'ютерів за наявними статистичними даними загроз. Однак тут слід узяти до уваги оновлення програмного забезпечення - тому як відомі уразливості можуть втратити актуальність, а крім того - можуть з'явитися нові. Що стосується профілактичних заходів на рівні мережі, то цей метод може бути використаний для розробки правил брандмауера з достовірною інформацією про їх потенційний вплив на ймовірність реалізації загроз. Виявляючи всі системи, що мають служби з високим фактором ризику, можна сконцентрувати ресурси на прийнятті суворого контролю над мінімальним їх числом, щоб отримати максимальне зниження частоти реалізації загроз.

Перелік посилань

1. Вікіпедія: вільна загальнодоступна багатомовна універсальна інтернет-енциклопедія [Електрон. Ресурс] / Спосіб доступу: URL: http: //www.wikipedia.org/.

2. НДТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу ДСТСЗІ СБ України, Київ, 1999.

3. Anoop Singhal , Lingyu Wang, Sushil Jajodia Network Security and Risk Analysis Using Attack Graphs [Текст]: Презентація - Concordia University, George Mason University, 2011.

4. Santiago, G., Alexander, K., Albert-László, B. A genetic epidemiology approach to cyber-security [Текст]: Наукова стаття - Center for Complex Network Research, Northeastern University, Boston, MA 02130, USA, 2014.

УДК 004.738.2

Маслов Д.М., студент гр. ЗСм-14-1м
Науковий керівник: Масальська О.О. асистент кафедри БІТ
(Державній ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна)

АНАЛІЗ ЗАГРОЗ МОДЕЛІ КЛІЄНТ-СЕРВЕРНОЇ ВЗАЄМОДІЇ AJAX

Навколишній світ постійно змінюється, постійно прискорюючи темп. Важко знайти людину яка б не чула про Інтернет. З розвитком швидкісних телекомунікаційних систем і мереж практично кожна людина має доступ до глобальної мережі Інтернет. Після вирішення питання комунікації постає питання технологій, які виведуть рівень взаємодії користувача та Веб-ресурсу на якісно новий рівень.

До таких технологій можна віднести модель клієнт-серверної взаємодії AJAX. Дана абревіатура означає асинхронний JavaScript та XML. Головний принцип даної технології полягає у частковому оновленню веб-сторінки. До використання AJAX користувачу доводилось повністю перезавантажувати веб-сторінку, навіть при необхідності оновити незанчну її частину. Розглянемо на прикладі заповнення форми реєстрації користувача на сайті: поле «Логін» повинно бути унікальним, до використання AJAX після заповнення всіх полів форми та відправки її на сервер користувач отримував результат (успішна реєстрація або повідомлення про вже існуючий логін). У разі дублювання логіну користувачу необхідно було знову заповнювати усі поля форми. З використанням моделі AJAX вже під час заповнення наступного поля користувач отримував результат верифікації логіну, таким чином заощаджуючи час. Такий підхід надає можливість заощадити Інтернет-трафік, т.щ. основна частина сторінки вже завантажена (HTML розмітка, рисунки, таблиці стилів тощо). Наступним кроком у розвитку даної моделі є створення SPA веб-додатків, що означає Single page application (односторінковий додаток). Такий додаток складається з однієї веб-сторінки, і може практично не відрізнитися від свого аналогу для персонального комп'ютеру.

Слід розуміти що AJAX – це не технологія і не фреймворк, це модель взаємодії клієнту (веб-браузера) та сервера. Даний підхід реалізується таким стеком технологій: HTML5, CSS, JavaScript, XML, JSON.

Після завантаження сторінки з веб-серверу, браузер на основі коду HTLM розмітки формує DOM модель документа, каскадні таблиці стилів задають правила для графічного оформлення. JavaScript визначає поведінку сторінки. При необхідності динамічного оновлення сторінки JavaScript формує запит та відправляє його на сервер використовуючи об'єкт XMLHttpRequest( ). Даний об'єкт включає в себе методи для роботи з мережевими ресурсами, а саме можливо: надіслати запит, перевірити статус запиту, визначити метод передачі даних (POST, GET), визначити тайм-аут запиту, тощо. Далі сформований запит відправляється на сервер використовуючи загальнопоширені мережеві протоколи (HTTP, HTTPS). Формат відповіді серверу може бути різноманітний, це залежить від складності та архітектурного рішення, наприклад: результат виконання операції, данні у форматі JSON, HTML розмітка, данні у форматі XML. Отримавши відповідь серверу, за допомогою JavaScript динамічно змінюється сторінка сайту з залежності від отриманого результату.

AJAX, як модель взаємодії розкриває широкі можливості перед розробниками та робить більш комфортним роботу з ресурсом для користувача. Проте це ускладнює клієнтську архітектуру, потребує використання більшого стеку технологій, що у свою чергу приводить до зменшення рівня ІБ. Тема інформаційної безпеки надзвичайно актуальна, т.щ. через динамічні форми можуть передаватись персональні данні, номера

кредитних карток та інші цінні данні. До класичних мережевих атак додаються специфічні, які можуть бути проведенні через вразливості характерні моделі AJAX.

До найбільш характерних вразливостей моделі AJAX можно віднести:

1) Підміна прототипу
2) Підміна сесії
3) Сфабриковані запити на інші сайти (Cross-site Request Forgery)
4) Ведення зловмисного коду
5) Недостатня автентифікація клієнта

Атака «Підміна прототипу» базується на властивостях прототипних мов програмування, таких як JavaScript. Головна відмінна прототипного програмування від об'єктно-оріентованого в тому, що в прототипному підході не створюються нові класи. Нові об'єкти створюються клонуванням вже існуючих об'єктів, розширення існуючих об'єктів можна проводити за рахунок перевизначення методів вже існуючих об'єктів. Під час клонування об'єкту з перевизначеними полями, всі його нащадки будуть вміщувати додаткові методи. Наприклад, зловмисник може перевизначити методи об'єкту XMLHttpRequest( ), які відповідають за передачу даних. Така атака залишається абсолютно непомітною для користувача та додатку, але повністю компрометує сесію. Запити користувача відправляються не тільки на легітимний сервер а також на сервер зловмисника.

Атака «Підміна сесії» базується на отриманні контролю над сесією користувача, якщо у зловмисника є можливість помістити свій JS код на сторінку яку буде переглядати користувач. Коли користувач переглядає таку сторінку ідентифікатор його сесії буде перезаписаний та збережений після авторизації. Таким чином у зловмисника може опинитись ідентифікатор користувача, який він використає для доступу під виглядом користувача.

Атака «Cross-site Request Forgery» базується на відправлені AJAX-запиту користувача з сайту зловмисника. Для цього повинні бути виконані деякі умови, а саме сесія користувача залишилась відкритою коли користувач потрапив на сторінку зловмисника. Тоді можливе відправлення запиту з Cookie користувача, для серверу такий запит буде абсолютно легітимним.

Ведення зловмисного коду можливе напряму в AJAX-додаток. Для передачі даних від серверу до клієнта часто використовується формат JSON. Найпростіший спосіб отримання даних із JSON, це його інтерпретація методом eval ( ). Якщо зловмисник знайшов спосіб передати замість JSON відповіді зловмисний код, такий код буде безконтрольно виконаний на стороні клієнта.

Недостатня автентифікація клієнта не являється вразливістю конкретної технології чи мови програмування, це недолік архітектури додатку. Іноді для виконання динамічних запитів серверу не потрібні додаткові ідентифікатори (Cookie, пароль HTTP автентифікації), йому вистачає визначення користувача за IP-адресою. Зловмисник може правильно підібравши час провести запит під виглядом користувача.

У даному аналітичному огляді визначенні основні вразливості моделі взаємодії AJAX, перекриття подібних вразливостей є обов'язковим для збереження основних властивостей інформації.

Перелік посилань

1. Billy Hoffman, Bryan Sullivan. Ajax Security Addison-Wesley [Текст] - 2007
2. Rebecca M. Riordan Head First Ajax O'reilly [Текст] – 2008
3. Дейв Крейн. Ajax в действии. [Текст] Вильямс – М. 2008
4. Інтернет енциклопедія Вікіпедія [Електронний ресурс] – URL: https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D0%B8_AJAX

УДК 004.491

Шевченко Д.І. студент гр. БСіт-12-1
(Державний ВНЗ "Національний гірничий університет", м. Дніпропетровськ, Україна)

НЕЦЕЛЕВЫЕ АТАКИ НА WEB-РЕСУРСЫ

С каждым годом растёт количество атак на веб-ресурсы. Все больше и больше случаев резонансных взломов крупных компаний и сервисов. Это т.н. «целевые атаки», с выбором конкретной жертвы, атака идет на минимальное количество ресурсов с максимальным количеством трудозатрат злоумышленников[1].

Однако, более чем в 90% случаев жертвами атак злоумышленников становятся сайты, попавших «под раздачу» случайно, в результате обезличенных автоматизированных атак, которые называются «нецелевыми». Нецелевая атака на сайт – это попытка получения несанкционированного доступа к веб-ресурсу, при которой злоумышленник не ставит целью взломать конкретный сайт, а атакует сразу сотни или тысячи ресурсов, отобранных по какому-то критерию. Например, сайты, работающие на определенной версии системы управления сайтом. Такого рода атаки бьют по «площадям», стараясь охватить максимальное количество сайтов при минимуме затрат.

Нецелевая атака – это атака, которая проводится фактически «на удачу», а ее жертвами становятся случайные веб-сайты независимо от популярности, размера бизнеса, географии или отрасли. Злоумышленник формирует выборку сайтов по определенным критериям (например, выбираются сайты, работающие на уязвимой версии какого-нибудь плагина для CMS Wordpress), и далее пытается на всех сайтах из списка проэксплуатировать данную уязвимость. При удачной попытке злоумышленник старается извлечь из этого пользу: закрепиться на сайте, добавить еще одного администратора, внедрить вредоносный код или получить необходимую информацию из базы данных.

Как правило злоумышленники в такой ситуации оказываются на два шага впереди владельца сайта: разработчику программного обеспечения необходимо время для устранения уязвимости, а владельцу сайта необходимо установить последнюю версию или обновление.

Фактически, как только сайт попадает в поисковую выдачу, он сразу же становится объектом нецелевых атак. При этом неважно, каков масштаб сайта, сколько у него посетителей, какой индекс цитирования, сколько в день он продает товаров и услуг и к какой тематике относится. Важны только технические характеристики, по которым он может попасть в выборку. Злоумышленники по тем или иным признакам находят потенциально уязвимые сайты и пытаются их использовать.

По статистике примерно 3/4 атак — нецелевые, в 2015 году находится довольно много уязвимостей, которые позволяют злоумышленникам практически «сходу» атаковать сайт:

Во-первых, это простота (доступность) исполнения атак. В настоящее время в открытом доступе находится множество инструментальных средств — различных скриптов, приложений для Windows и Unix- платформ.

Во-вторых, это высокая эффективность и результативность атак (как экономическая, так и техническая). При небольших затратах — иногда практически нулевых — буквально за полчаса можно взломать сотни тысяч сайтов и получить доступ к большому массиву ресурсов. Ну, а моделей монетизации взломанных сайтов сегодня существует довольно много[2].

Как правило, жертвами массовых атак становятся так называемые «среднестатистические сайты», владельцы которых не уделяют внимания вопросам

безопасности и защиты — не обновляют или нерегулярно обновляют программное обеспечение сайта и сервера, используют «слабые» пароли администратора, не меняют настройки по-умолчанию, устанавливают непроверенные версии плагинов и шаблонов.

Сам сайт не интересен злоумышленникам, но они использует его в качестве платформы для атаки на пользователей и распространения вредоносного ПО. Это разрушает одно из больших заблуждений владельцев небольших сайтов — «зачем его ломать, да и кому он нужен». Это заблуждение встречается среди владельцев сайтов, которые пока еще не сталкивались со взломом.

Злоумышленника может интересовать не сам сайт, а ресурс хостинга, с которого, например, можно рассылать спам или на котором можно разместить фишинговую страничку, «ворующую» конфиденциальные данные пользователей. И количество посетителей сайта не играет роли – трафик или не нужен, или может генерироваться другим способом. В ряде случаев злоумышленники используют взломанные сайты как ресурсы для атаки на другие веб-проекты (например, для проведения брут-форс или DOS-атак) или в качестве промежуточного звена для перенаправления посетителей на другие зараженные сайты и страницы, то есть превращают их в звено в т.н. «связке эксплойтов», систем для эксплуатации уязвимостей в браузерах пользователей.

Ежедневно жертвами веб-атак становятся десятки тысяч ничего не подозревающих владельцев сайтов. Однако предотвратить несанкционированное вторжение несложно – для этого достаточно перестать быть владельцем «среднестатистического» веб-ресурса и принять агрессивность веб-среды.

Необходимо проводить процедуры обновления сайта и его компонентов, проверять целостность и вовремя создавать резервные копии, отказаться от использования простых паролей. Если какие-то компоненты или служебные скрипты не используются – удалите их. Также необходимо проводить профилактические мероприятия – аудит безопасности, необходимо периодически проверять свой сайт на наличие уязвимостей. Главное осознать, что безопасность – это не разовая процедура, а непрерывный процесс, которому необходимо уделять постоянное внимание.

Список источников

1. Случайный взлом: зачем ломают низкопосещаемые сайты (Электронный ресурс). Способ доступа: URL: http://security-corp.org/infosecurity/30303-sluchaynyy-vzlom-zachem-lomayut-nizkoposeschaemye-sayty.html

2. Блог компании PENTESTIT / Хабрахабр (Электронный ресурс). Способ доступа: URL: http://habrahabr.ru/company/pentestit/

УДК 004.725.5

Шевченко Д.Д., студент гр. ЗСм-14-1м,
Науковий керівник: Масальська О.О. асистент кафедри БІТ
(Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ, Україна)

ОСНОВИ ОРГАНИЗАЦІЇ РОБОТИ WIFI МЕРЕЖ

За последнее время огромную популярность приобрели беспроводные локальные вычислительные сети. Большое количество домов, офисов, ресторанов, университетов, вокзалов, поездов и других мест общественного пользования оборудуются соответствующей аппаратурой для подключения ноутбуков, персональных компьютеров и телефонов к мировой «паутине». Самое большое преимущество беспроводных сетей заключается в том, что два или более компьютеров могут обмениваться данными и без подключения к Интернету. Главным стандартом беспроводных локальных сетей является стандарт 802.11.

Беспроводные сети данного стандарта могут быть использованы в двух режимах. Первый и самый популярный режим – это режим подключение клиентов, таких как ПК и телефоны, к сети Интернет, либо к внутренней сети какой-либо организации. (рис. 1а) Такой режим, называется инфраструктурным (infrastructure mode), где каждый клиент связывается с точкой доступа (Access Point, AP), которая, в свою очередь, подключена к сети. Пакеты, клиент получает и отправляет через точку доступа. Несколько точек доступа можно соединить вместе, обычно в кабельную сеть, которая называется распределительная система (distribution system), таким образом, создается расширенная сеть 802.11. В данной ситуации клиенты имеют возможность отправлять «кадры» другим клиентам через их точки доступа. Второй режим (рис. 1б), называется произвольной сетью (ad hoc network). Это набор клиентов, не имеющей общую точки доступа, но связанных таким образом, чтобы они могли напрямую отправлять «кадры» друг другу. Исходя из того, что доступ в Интернет на сегодняшний день является практически необходимостью, то произвольный режим объединения в сеть имеет малую популярность.

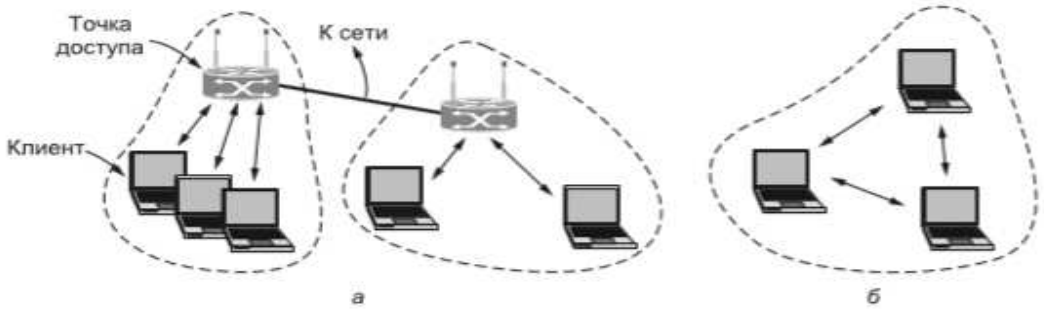

Рисунок 1 – Архитектура сети стандарта 802.11: а – инфраструктурный режим; б – произвольный режим

Однако, несмотря на все преимущества беспроводных сетей, существует ряд проблем безопасности. Так как передача в сетях такого типа является широковещательной, соседние клиенты легко могут получить пакеты информации, которые были предназначены не для них. Для того чтоб избежать такой проблемы, в стандарте применяется схема шифрования WEP (Wired Euivalent Privacy – приватность на уровне проводной связи). Главная идея защиты – создать в беспроводной сети систему безопасности аналогичную проводной. Но, к сожалению, в схеме оказалось

много недостатков, и идея не принесла ожидаемых результатов. Со временем появились новые схемы шифрования, зарегистрированные в стандарте 802.11i, который получил название WPA (WiFi Protected Access), а также более новая версия WPA2, используемая в настоящее время.

Исходя из выбора схемы безопасности, аутентификация обеспечивается по-разному. Если сети 802.11 с открытым доступом, то их может использовать любой клиент. В другом случае для аутентификации требуются параметры учетной записи. Используемая схема, названная WPA2, обеспечивает безопасность как определено стандартом 802.11i. С протоколом WPA2 точка доступа может взаимодействовать с сервером аутентификации, у который имеет имя пользователя и база данных паролей, для того чтобы определить, разрешено ли станции получить доступ к сети. Также может быть сконфигурирован предустановленный ключ (reshared key), который является нестандартным названием сетевого пароля. Несколько кадров с запросом и ответом пересылаются между станцией и точкой доступа, это позволяет станции доказать, что у нее есть «правильные» учетные данные. Для схемы WEP, которая использовалась до WPA, аутентификация с предустановленным ключом выполнялась перед ассоциацией. Однако из-за недостатков конструкции, ее польза не велика, что делает WEP легко взламываемым. [1] Первая демонстрация взлома WEP на практике произошла, когда Адам Стабблефилд был летним стажером в AT&T. [1] Он смог написать программный код и проверить атаку за одну неделю, большая часть которой была потрачена на получение разрешения администрации на покупку карт WIFI, необходимых для эксперимента. Программное обеспечение для взлома паролей WEP на сегодняшний день есть в свободном доступе.

Как уже говорилось ранее, беспроводная передача является широковещательным сигналом. И это значит, что для информации, посланной по беспроводной ЛВС, должна сохраняться конфиденциальность, поэтому информация должна быть зашифрована. Этого можно добиться с помощью службы конфиденциальности (privacy service), которая управляет деталями шифрования и дешифрования. Для WPA2 используется алгоритм шифрования, основанный на AES (Advanced Encryption Standard) американском правительственном стандарте, принятом в 2002 году. Ключи, используемые для шифрования, определяются во время процедуры аутентификации.

Если принять во внимание, все вышеизложенное, то можно сделать ряд выводов относительно беспроводных локальных вычислительных сетей. Это относительно новое и развивающееся направление информационных технологий, беспроводные ЛВС используются не только для обычного обывателя, нуждающегося в просмотре социальных сетей в любой точке города, они также используются в промышленности разного уровня сложности. Но с точки зрения информационной безопасности, даже с таким темпом развития технологий имеется недостаточно надежно система защиты данных сетей.

Перелік посилань

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. [Текст] – СПб: Питер, 2012. – 960 с.: ил.