УДК 004.056.5:621.39
DOI: 10.31673/2412-9070.2023.011320

Я. С. ШАВЛОВСЬКИЙ, аспірант,
Державний університет телекомунікацій, Київ

МОДЕЛЬНА СТРУКТУРА ЗАГРОЗ РЕСУРСАМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИМ МЕРЕЖАМ ЯК БАЗОВОМУ АКТИВУ КРИТИЧНО ВАЖЛИВОГО ОБ'ЄКТА ІНФРАСТРУКТУРИ

Здійснено класифікацію моделей кібератак, спрямованих на комп'ютерні мережі та комплекси і які являють собою найбільшу загрозу. Запропоновано класифікацію, в основу якої покладено основні тенденції практичної реалізації кібератак. Розглядуваний підхід є новим щодо класифікації кібератак на комп'ютерні мережі та комплекси, що обслуговують критично важливі об'єкти інфраструктури, і зважає на десять складових циклу загрози: від комплексного вивчення об'єкта впливу до реалізації кібератаки.

Ключові слова: критично важливий об'єкт інфраструктури; інформаційно-комунікаційна система; класифікація; класифікатор; інформаційно-телекомунікаційна мережа; комп'ютерна мережа; захист інформації; кіберпростір; комп'ютерна кібератака; мережний пристрій.

ВСТУП

Сучасний етап розвитку суспільства визначається підвищенням ролі інформаційного простору, який являє собою сукупність інформації, інформаційної інфраструктури та суб'єктів, що здійснюють збір, формування, поширення та застосування інформації. Під інформаційною безпекою України розуміють стан захищеності її національних інтересів в інформаційному просторі, що визначаються цілісністю збалансованих інтересів особистості, суспільства та держави. До складу щораз більших загроз інформаційній безпеці критично важливого об'єкта інфраструктури належать кібератаки (КА) на комп'ютерні комплекси та на інформаційно-телекомунікаційні мережі (ІТКМ), які є його базовим активом.

Кількість КА на об'єкти критично важливої інфраструктури у 2023 році порівняно з періодом до 2019 року зросла більш ніж учетверо і основним учасником таких КА є рф.

Сучасний вектор КА спрямований на мережу, унаслідок чого контроль ресурсів, злам та дія шкідливого програмного забезпечення (ШПЗ) ІТКМ не з'являється «несподівано з нічого». У багатьох випадках цьому передує тривала та ретельна робота в кіберпросторі: розвідка, пошук уразливості, яку не брали до уваги під час створення ІТКМ та захоплення інформаційних активів [1]. Мінлива топологія загроз, частота появи загроз, складність та цільова властивість КА потребує неперервної еволюції наявної парадигми в політиці інформаційної безпеки.

Для мінімізації збитків, які постають у разі успішної реалізації КА, важливим є перехід до поєднання технологій запобігання, виявлення та реагування на КА. На жаль, на теперішній час аналіз реалізації КА здійснюється за фактом інциденту і вразливість усувається після КА [2].

Велика кількість державних та приватних підприємств мають засоби для виявлення відомих КА, хоча, однак, досвід показує, що вони не завжди рятують від зловмисних мережних вторгнень. Найскладнішим завданням у процесі здійснення захисту конфіденційних інформаційних ресурсів є здатність протидіяти невідомим атакам, які зловмисно створено для обходу наявного захисту, що використовують зміни сигнатур та шаблонів поведінки.

Невід'ємною частиною аналітичної роботи із захисту ІТКМ є розроблення самої повної класифікації КА, які породжують загрози для інформаційних ресурсів.

ОСНОВНА ЧАСТИНА

Аналіз вирішень щодо класифікації кібератак

Багато відомих вирішень щодо класифікації кібератак на комп'ютерні комплекси формуються на основі певних вимог, зокрема:

- взаємовиключність — категорії класифікації не повинні перетинатися і мати схожі значення;
- вичерпність — класифікація має повною мірою розкривати описувану сферу дослідження, максимально охоплювати характеристики розглянутої КА;
- зрозумілість — однозначність та стислість інформації, що надається;
- відсутність двозначності — чіткий поділ запропонованих категорій із чітко вираженою належністю КА до відповідного класифікатора;
- корисність — здатність застосування в сфері інформаційної безпеки узагальнених класифікатором інформації щодо тієї чи іншої КА;

• прийнятність — побудова класифікації на основі аналізу наявної класифікації у сфері дослідження.

Сучасні дослідження щодо класифікації КА варто розділити на дві великі групи. Перша група охоплює розроблення загальних класифікацій за кібератаками на комп'ютерні комплекси, що ґрунтуються на типі кібератаки або на нанесених збитках. Друга група вивчає певні кібератаки, створюючи глибинне уявлення щодо конкретної КА, відповідної вразливості та експлойти, які вона використовує, а також наслідки після вторгнення в інформаційну систему (ІС).

У багатьох класифікаціях акцент робиться або на КА за методами здійснення атак [3-8], або на тенденцію можливих втрат інформаційних активів у разі успішної реалізації КА [9-11].

У [3] здійснено аналіз відомої класифікації кібератак та наведено класифікацію за такими ознаками: мета КА, тип КА, модель 0Sl, операційна система та її характерні вразливості, місце знаходження особи, яка здійснює атаку, тип ІС, сервіс, на який здійснюється КА, наявність зворотного зв'язку, умова реалізації КА, тип впливу, автоматизація, джерело та кількість з'єднань. До недоліків цієї класифікації можна віднести відсутність означень класифікаторів та недостатню увагу щодо характеристик точки впливу, інакше кажучи, на які ключові вузли ІС діє та чи інша кібератака.

В [11] надається більше двадцяти основних типів кібератак, які здійснюють упровадження в інформаційні ресурси енергосистем. Ці типи розділено на чотири базові категорії. Для кожної категорії розглядається своя математична модель. Класифікація надається передусім для інженерного персоналу, який забезпечує системи безпеки сучасних критично важливих об'єктів інфраструктури для ІС енергетичного сектору.

У працях [12-15] автори розглядають п'ять основних класифікаторів: визначення природи та сутності КА, мету кібератаки, вплив кібератаки на інформаційний ресурс, який захищається, та заходи щодо запобігання загрозам та наслідки їх успішної реалізації. Відмінністю стосовно інших класифікаторів є те, що цей класифікатор є розширеним та багатогранним описом змішаних складових мережних атак.

Цікавим класифікаційним підходом є підхід спеціалістів Туніського департаменту інформатики [16], які запропонували гібридну п'ятивимірну модель загроз ІС, котра пов'язує в собі класифікаційні методи, що базуються на техніці кібератак та на впливі загроз. Крім того, даний підхід виявляє можливі джерела реалізації загроз, тип загрози та її мотивацію, план зловмисника та тип впливу.

У статті [17] розглядаються найпоширеніші КА за великим набором класифікаторів, а також пропонуються онтологічні засади для подання класифікації: вона відповідає вимогам корисності, взаємовиключенню пунктів класифікатора, зрозумілості інформації та однозначності. Однак у ній зосереджено увагу переважно на формалізації опису мережних КА, особливостях їх підготовки та реалізації.

У [18] запропоновано класифікацію методів прогнозування та виявлення профілю КА, зокрема метод аналізу логічної топології мережі, метод прихованих марковських моделей, метод на основі fuzzy-технологій, метод на базі графіків мережних атак та статистичні методи аналізу інцидентів. Незважаючи на велику кількість класифікаційних ознак, виокремлені категорії не розглядають такі важливі аспекти, як рівень еталонної моделі взаємодії відкритих систем (EMBBC), мережні пристрої, які передусім піддаються впливу, а також часові характеристики КА.

Класифікацію атак, яка може бути використана для ідентифікації можливих вторгнень у спеціалізовані системи моніторингу та керування даними, наведено в роботах [19; 20]. Класифікатори ідентифікують атаки на основні вузли мережного устаткування, атаки на програмне забезпечення та атаки на стеки протоколів зв'язку, виділені окремо в специфіці SCADA-систем, тобто у сфері застосування диспетчерського контролю, керування та збору даних.

У статті [21] класифікаційні ознаки КА розглядаються як параметри для глибокого машинного навчання систем захисту інформаційних ресурсів, що ґрунтуються на алгоритмічних моделях нейронних мереж.

Отже, аналіз відомих праць у галузі класифікації комп'ютерних атак дає змогу зробити висновки про те, що під час розроблення класифікації КА необхідно керуватися найзагальнішими принципами побудови класифікацій, що сприяють правильному добору оптимальних категорій та критеріїв для подальшої роботи зі створеною класифікацією стосовно різних сфер гарантування інформаційної безпеки. Крім того, під час класифікації КА перевагу слід віддавати загальним та гібридним класифікаторам. Класифікації, які ґрунтуються на обліку збитків, що наносяться інформаційним активам та класифікації, зосередженим на певних типах атак, не здатні достатньо визначити властивості та характеристики кібератак. Класифікації, що розробляються, мають визначати особу, яка здійснює кібератаку, її мету, джерело самої кібератаки, методи поширення кібератаки та наслідки в разі успішної її реалізації. Саме такі класифікації мають велике значення для вибору стратегії захисту, попередження, прогнозування та своєчасного виявлення кібератаки, що зумовлюють протидію її проникнення в ІТКМ. Однак розглянуті підходи не достатньою мірою відповідають усім цим вимогам.

Вузол зв'язку як основна складова ІТКМ та головний об'єкт кібератаки

Схему вузла зв'язку як основної складової ІТКМ зображено на рис. 1. Ця схема має широке застосування в критично важливих галузях, включно із сектором державного керування, банківської сфери, нафтових компаній, промисловим сектором та іншими галузями. Відкритий сегмент вузла зв'язку містить у собі такі базові складові:

- маршрутизатор;
- комутатор;
- корпоративний сервер, на якому працює корпоративний сайт підприємства;
- локальну обчислювальну мережу (ЛОМ) та автоматизовані робочі місця (АРМ) відкритого сегмента;
- засоби IP-телефонії АТС за технологією VoIP, яка спрягається із зовнішніми ресурсами, зокрема міськими та міжміськими телефонними мережами.

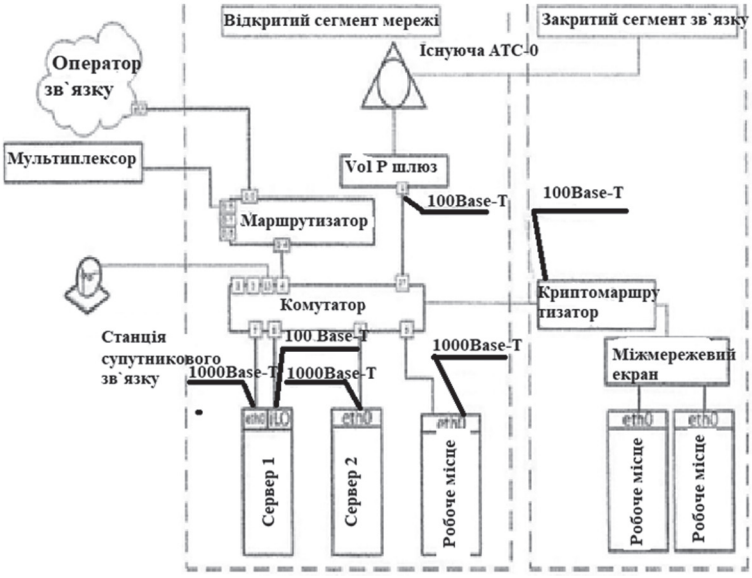

Рис. 1. Вузол зв'язку

Стосовно закритого сегмента вузла, то він містить у собі таке обладнання:

- граничний маршрутизатор або міжмережний екран у разі потреби здійснити маршрут трафіку у зовнішню мережу;
- криптомаршрутизатор;
- комутатор ЛОМ;
- ЛОМ та АРМ закритого сегмента;
- засоби IP-телефонії внутрішньої закритої АТС, яка спряжена із зовнішніми ресурсами, але за умов криптозахисту та передавання трафіку по тунелях віртуальної частини мережі (VPN).

З погляду інформаційної безпеки криптомаршрутизатор і міжмережний екран або граничний маршрутизатор забезпечують криптографічний захист інформації на належному рівні. Однак це не забезпечує гарантованого захисту від кібератак доти, доки підприємство не буде здатним мінімізувати вплив людського фактора. Навіть якщо перевести всі вузли зв'язку в режим тотальної автоматизації, виключивши з процесів, пов'язаних з обслуговуванням ІТКМ, особу, усунути ризики, зумовлені довірчими відносинами, внутрішніми порушниками, апаратними чи програмними закладними засобами й простим невірним настроюванням мережного устаткування, захист не є стовідсотково гарантованим.

Моделі загроз безпеці інформації ресурсам ІТКМ, в яких ураховано десять компонентів циклу загрози, починаючи від комплексного вивчення об'єкта впливу до реалізації кібератаки, а саме виявлення, збирання даних, ексфільтрація, експлуатація, шкідливий код, соціальна інженерія, командування, керування, поширення, приховування, наведено в табл. 1-6.

Модель загроз маршрутизатору

Маршрутизатор є одним із найбільш уразливих складових розглянутого об'єкта, основна причина в тому, що він містить таблицю маршрутизації. Це дає зловмиснику помітну перевагу щодо розвідки корпоративної мережі зсередини. Захопивши маршрутизатор, він може досліджувати мережу стосовно виявлення вразливих сусідів, щоб, скориставшись їхніми системами, здійснити вхід у мережу глибше. Для цього існує багато способів, як це наведено в табл. 1.

Таблиця 1

Рівень EMBBC дорівнює трьом, ІТКМ являє собою маршрутизатор, субелементами ІТКМ є порти мережних служб маршрутизатора, оперативна пам'ять, операційна система, програмне забезпечення та апаратна складова

Розвідка			**Проникнення**			**Виконання**		**Закріплення**	
Виявлення	Збір даних	Ексфільтрація	Експлуатація	Шкідливий код	Соціальна інженерія	Командування	Керування	Поширення	Приховування
Порти мережних служб маршрутизатора									
Сканування мережних сервісів. Виявлення периферійних засобів. Виявлення параметрів конфігурації мережі	Прослуховування мережі	Ексфільтрація через альтернативний протокол. Ексфільтрація через канал керування С2. Ексфільтрація через альтернативне мережеве середовище. Ексфільтрація через альтернативне фізичне середовище	Зовнішні віддалені сервіси. Метод грубої сили або повний перебір		Фішинговий порт. Evil double	SSH FTP	Підімкнення через проксі. Власний криптографічний протокол. Багаторазове здійснення проксі. Багаторазове шифрування. Засоби віддаленого доступу	Прокид портів	Приховування кінцевої адреси з'єднання. Запасні канали. Багатоступеневі канали
Оперативна пам'ять									
Виявлення процесів	Hash-password	Ексфільтрація оперативної пам'яті	Black Mamba						
Операційна система									
Історія команд Bash. Секретні ключі. Виявлення облікових записів. Виявлення файлів у каталогах. Розкриття парольної політики. Виявлення груп доступу. Виявлення інформації про систему	Демпінг облікових даних. Захват вводу. Автоматизований збір	Експлойти для отримання облікових даних. Автоматизована ексфільтрація	Паблік експлойти. 0-день	Black Mamba		TTY	Віддалені сервіси. Зв'язок через мобільні носії	Створення облікових записів	Скриті папки та файли. Port Knocking
Програмне забезпечення									
Секретні ключі	Демпінг облікових даних MITM	Ексфільтрація даних з ПЗ	Паблік експлойти. 0-день	Скриптинг. Пакування софту	Виконання через довірчі утиліти розробників софту		Віддалене копіювання файлів	Упровадження в програмний код	Деобфускація/дешифрування файлів або інформації. Обфускація файлів або інформації
Апаратна складова									
Виявлення файлів із конфігурацією системи	Сканування апартних складових	Ексфільтрація даних про систему	Апаратні закладні засоби, компрометація ланцюга надходжень	malware	Довірчі відносини	Через апаратні закладні засоби	Через malware		Резервний доступ

Усе залежить від самої ситуації та типу пристрою, який здійснює маршрутизацію. Здебільшого існує можливість добору логіна та пароля за допомогою спеціального програмного забезпечення або допоміжного засобу, який має назву Evil double.

За відсутності потенційних потерпілих від кібератак, які здійснюють обмін завдяки маршрутизатору, злодій здатен визначити нові вектори кібератак, спрямованих на поширення та приховування слідів злому.

Оскільки маршрутизатор здійснює обмін інформацією з іншими користувачами мережі, то в разі захвату цього маршрутизатора легко реалізувати кібератаку під назвою «людина всередині» (MITM). Такий процес відбувається через перехоплення трафіку або через відмикнення довільного користувача мережі. Після цього виконують скидання портів або змушують адміністратора ще раз увести облікові дані для їх перехоплення та застосування в іншому вузлі зв'язку мережі.

Модель загроз комутатору

Комутатор являє собою найпростіше обладнання об'єкта ІТКМ. Переважно в нього відсутня таблиця маршрутизації і цей засіб працює на канальному рівні. Способи здійснення загроз комутатору наведено в табл. 2.

Таблиця 2

Рівень EMBBC дорівнює двом, ІТКМ являє собою комутатор, субелементами ІТКМ є порти комутатора та апаратна складова

Розвідка			**Проникнення**			**Виконання**		**Закріплення**	
Виявлення	Збір даних	Ексфільтрація	Експлуатація	Шкідливий код	Соціальна інженерія	Командування	Керування	Поширення	Приховування
Порти комутатора									
Секретні ключі		Ексфільтрація через альтернативний протокол. Ексфільтрація через канал керування C2. Ексфільтрація через альтернативне мережне середовище. Ексфільтрація через альтернативне фізичне середовище	Паблік експлойти. 0-день	DOS-атаки на канальний рівень			Розповсюдження портів	Підмкнення через проксі. Власний криптографічний протокол	Підміна MAC-адреси
Апаратна складова									
Виявлення файлів із конфігурацією системи	Сканування апаратних складових		Апаратні закладні засоби, компрометація ланцюга надходжень		Довірчі відносини			Підміна MAC-адреси	Резервний доступ

Оскільки комутатор є найпростішим засобом, то в табл. 2 відсутнє заповнення колонок, які стосуються операційної системи та програмного забезпечення. Комутатор має вразливості до ARP-атакам, вектор яких спрямовано на прослуховування мережного трафіку і має вразливості до DOS-атакам, вектор яких спрямовано на канали зв'язку. Комутатор варто використовувати для здобуття інформації про елементи мереж користувачів.

Модель загроз серверу

Рівень EMBBC дорівнює трьом, ІТКМ являє собою сервер Windows/Linux, субелементами ІТКМ є порти мережних служб сервера, блок керування сервером бази даних, оперативна пам'ять, операційна система, програмне забезпечення та апаратна складова. Загрози для операційних систем Windows та Linux наведено в табл. 3. Важливим є те, що існує перелік здатності впливу за допомогою відомих експлойтів, які доступні кожному. Однак, зважаючи на те, що сервер міститься всередині мережі, до для здатності його атаки існує три способи з подальшими наслідками.

Спосіб 1. Здійснено захват маршрутизатора, за допомогою якого відбувається атака.

Спосіб 2. На сервері запущено сайт, до якого є доступ із мережі «Інтернет». Це найпоширеніший спосіб.

Спосіб 3. Було здійснено захват сервера зловмисником, але він має права тільки користувача.

Таблиця 3

Рівень EMBBC дорівнює трьом, ITKM являє собою сервер Windows/Linux, субелементами ITKM є порти мережних служб сервера, блок керування сервером, оперативна пам'ять, операційна система, програмне забезпечення та апаратна складова

Розвідка			**Проникнення**			**Виконання**		**Закріплення**	
Виявлення	Збір даних	Ексфільтрація	Експлуатація	Шкідливий код	Соціальна інженерія	Командування	Керування	Поширення	Приховування
Порти мережевих служб сервера									
Сканування мережних сервісів. Виявлення периферійних засобів. Виявлення параметрів конфігурації мережі	Bash History	Ексфільтрація через альтернативний протокол. Ексфільтрація через канал керування C2. Ексфільтрація через альтернативне мережеве середовище. Ексфільтрація через альтернативне фізичне середовище	Зовнішні віддалені сервіси	Black Mamba	Фішинговий порт. Розсилання фішингових e-mail	Розповсюджені порти	Розповсюдження портів	Підімкнення через проксі. Власний криптографічний протокол. Багаторазовий перегляд. Засоби віддаленого доступу	Видалення підімкнень до мережних ресурсів. Приховування кінцевої адреси з'єднання. Запасні канали. Видалення підімкнень до бази даних
Блок керування базами даних									
Секретний ключ. Виявлення витоку записів. Виявлення загальних мережних ресурсів	Перехоплення шляху. Дампінг витоку даних	Експлойти для отримання облікових даних	Видалений сеанс. DCShadow. Метод грубої сили або повний перебір		SQL Injection	SQL	Протоколи керування базами даних	Виконання за допомогою локального виконання задач	Видалення підімкнень до бази даних
Оперативна пам'ять									
Виявлення процесів	Дампінг облікових даних. Захват вводу		GWM-ін'єкції. Читання файлів за допомогою логічного зсуву файлової системи Process Doppelganging				Cold boot attack Уразливість Bolnannare		
Операційна система									
Bash History. Таємні ключі. Виявлення облікових записів. Виявлення файлів та каталогів. Розкриття парольної політики. Виявлення груп доступу. Виявлення інформації про систему. Виявлення мережних підімкнень	Дампінг облікових даних. Облікові данні в реєстрі. Автоматизований збір. Данні зі сховища інформації	Експлойти для отримання облікових даних. Форсована автентифікація. Отруєння LLMNR/NBT-NS. Kerberjasting DLL-бібліотеки фільтрів паролей. Автоматизована ексфільтрація	Зовнішні видалені сервіси. Виконання за допомогою експлойтів. Windows Remote Management. Апаратні закладні засоби. Дистанційний сеанс. Модифікація файлів -/.bash_profile та -/bashrc. Перехоплення викликів функції Windows APL. Виконання через загрузки модулів Windows. Драйвери LSASS	Виконання за допомогою стороннього програмного забезпечення адміністрування мережі		Windows Remote Management	Протокол віддаленого робочого місця. Віддалені сервіси. Зв'язок через зовнішні носії	Виконання за допомогою локального планування задач. Створення облікових записів. Logon-скрипти. Нові служби. Автоматичний запуск за допомогою ключа Plun. Keys та папки «Автозавантаження». Windows Helper DLL	Скриті файли та папки. Port Knocking. Вимкнення засобів захисту. Змінна HISTCONTROL Маскарадінг

Закінчення таблиці 3

Розвідка			**Проникнення**			**Виконання**		**Закріплення**	
Виявлення	Збір даних	Ексфільтрація	Експлуатація	Шкідливий код	Соціальна інженерія	Командування	Керування	Поширення	Приховування
Операційна система									
Виявлення системних сервісів			Mshta. Regsvcs/Regasm. Regsvt 32. Rundll32. Windows Manegement Instrumantation. CMSTP. Модифікація ключів AppCert DLLs					Проксі-виконання коду через підписані операції	
Програмне забезпечення									
Таємні ключі. Виявлення програмних засобів забезпечення безпеки	Дампінг облікових даних. Перехоплення двофакторної автентифікації	Експлойти для отримання даних	Експлойти публічних застосунків. Виконання через підписані сценарії. Виконання за допомогою стороннього програмного забезпечення для адміністрування мережі	Скритинг. Web shell. Встановлення софту. Загальний доступ Webroot	Виконання через довірчі утилити розробників софту		Дистанційне копіювання файлів	Рукити	Дешифрування файлів або інформації. Обфускація файлів або інформації. Пробіл після ім'я файлу. Вебсервіс
Апаратна складова									
Таємні ключі			Апаратні закладні засоби. Компрометація ланцюгів постачання	Гіпервізор	Довірчі відносини	Rootkit	Буткити		Резервний доступ

Модель загроз криптомаршрутизатору

Рівень EMBBC дорівнює чотирьом, ІТКМ являє собою маршрутизатор криптографічного захисту, субелементом ІТКМ є апаратна складова.

Варто зазначити, що маршрутизатор криптографічного захисту має власну операційну систему, до якої є тільки обмежений доступ. Завдяки тому, що про нього відсутня інформація, то здійснити опис атаки та виявити вразливості в його протоколах функціонування є достатньо складною задачею. Одним із слабких місць такого маршрутизатора є некоректне настроювання протоколу IPsec, що може призвести до подальшого розшифрування інформації за наявності ключів шифрування від іншого протоколу, який працює паралельно з IPsec. Крім того, за відсутності рекомендацій щодо налаштування правил фільтрації або за наявності критичних помилок у налаштуваннях фільтрів існує можливість реалізації DoS-атак, спрямованих на порушення роботи маршрутизатора. Слабкими місцями маршрутизатора криптографічного захисту є довірче відношення, внутрішній порушник та апаратні закладні пристрої.

Модель загроз міжмережному екрану

Головною функцією міжмережного екрану (*firewallFW*) є захист внутрішньої мережі користувача підприємства в складі мереж (інтернет) стику протоколів TCP/IP від випадкового або навмисного впливу із зовнішньої мережі. *Firewall* приєднується між зовнішньою мережею та внутрішньою мережею, яка потребує захисту.

Загрози міжмережному екрану аналогічні загрозам серверу (див. табл. 3).

Процес міжмережного екранування являє собою сукупність багатофакторних перевірок дейтаграм за їх автентифікації відповідно до політики інформаційної безпеки. Слід зауважити, що *Firewall*

виконує певну кількість фіскально-контрольних функцій, зокрема IP-фільтрацію, NAT-оброблення, тунелювання, прокси-сервер, реєстрацію подій. Отже, *Firewall* — це набір інструментів для запобігання загрозам внутрішній локальній мережі та забезпечення її захисту.

Моделі загроз робочому місцю

Робочим місцем є кінцевий вузол мережі, на який зловмисник легко може здійснити атаку. Загрози робочому місцю аналогічні загрозам серверу, що наведено в табл. 3.

У разі, коли зловмисник не здатен здійснити проникнення в закритий сегмент мережі, він здійснює закріплення на автоматизованому робочому місці відкритого сегмента. Це дає йому можливість легко здійснити захват даних користувачів, серед яких із великою ймовірністю можуть бути паролі адміністраторів мережі, які зі свого боку можуть підійти до елементів ІТКС закритого сегмента.

Висновки

Розглянуті в статті класифікації комп'ютерних атак є основою для дослідження властивостей самих атак та засобів протидії їм. Однак запропоновані класифікації узагальнюють атаки для мереж зв'язку загального користування, зокрема інтернету, і при цьому не є достатньо інформативними для мереж критичної інфраструктури, в яких наявні особливості захищеної реалізації.

Було здійснено декомпозицію моделі впливу кібератаки на ІТКС, розробленої на базі аналізу відповідності між основними характеристиками елементів ІТКС, особливостями їх застосування та особливостями реалізації кібератак. Розглядувана модель являє собою систематизований перелік кібератак, спрямованих як на програмне забезпечення елементів ІТКС, так і на елементи, що забезпечують функціонування ІТКС.

Аналіз моделі, яку було запропоновано, дає можливість стверджувати, що комп'ютерні атаки є універсальними і здатні бути націлені на довільний елемент ІТКС, а їх вплив має зв'язок із навмисним пошкодженням програмного забезпечення та інформації. Найбільший вектор впливу кібератак направлено на сервери, робоче місце та міжмережні екрани.

Список використаної літератури

1. ***Paulauskas N., Garsva E.*** *Computer system attack classification // Electronics and Electrical Engineering.*

2. ***Jang Wei., Zhi-Hong Tian, Xiang Cui.*** *DMAT: a new network and computer attack classification // Journal of Engineering Science and Technology Review. 2013. №6(5). P. 101–106.*

3. ***AVOIDIT:*** *a cyber attack taxonomy / C. Simmons, C. Ellis, S. Shiva [et al.] // Department of Computer Science University of Memphis, TN, USA. URL:*

http://www.teraits.com/pitagoras/marcio/segapp/CyberAttackTaxonomy_IEEE_Mag.pdf.

4. ***Joinia Mouna, Latifa Ben Arfa Rabaia, Anis Ben Aissab.*** *Classification of security threats in information systems // 5-th International Conference on Ambient Systems, Networks and Technologie (ANT-2014).*

5. ***A computer*** *network attack taxonomy and ontology / R. van Heerden, B. Irwin, ID Burke, L. Leenen // International Journal of Cyber Warfare and Terrorism.*

6. ***Common*** *cyber attacks reducing the impact. URL:*

https://www.ncsc.gov.uk/guidance/white -papers/common-cyber-attacks-reducing-impact (дата звернення 10.04.20).

7. ***Ioannis A., Nurse J. R. C., Goldsmith M.*** *A taxonomy of cyber-harms defining the impacts of cyber-attacks and understanding how they propagate // Journal of Cybersecurity.*

8. ***Pienta D., Johnston A. C.*** *A taxonomy of phishing attack types spanning economic, temporal, breadth, and target boundaries // Association for information Systems AIS Electronic Library.*

9. ***Cybersecurity*** *Incident Taxonomy NIS Cooparation Group // CG Publication, 04/2018.*

10. ***Applegate S. D., Stavrou A.*** *Towards a cyber conflict taxonomy // 5th International Conference of Cyber Conflict, 2013.*

11. ***Harry C., Gallagher N.*** *Classifying cyber events a proposed taxonomy // CISSM Working Paper, 2018.*

12. ***Aruna M., Gayathri K., Inbavalli M.*** *Network security and types of attacks in network security // IOSR Journal of Engineering (IOSRJEN).*

13. ***Cyber*** *risk definition and classification for financial risk management / F. Curti, J. Gerlach, S. Kazzinik [et al.] // Federal Reserve Bank of Richmond.*

14. ***Basumallik S.*** *A taxonomy of data attacks in power systems // Systems and Control. Pub. Date: 2020-02-25. URL:*

https://www.x-mol.com/paper/1232734050568916992.

*15. **Cyber** attack taxonomy for digital environment in nuclear power plants / S. Kim, G. Heo, E. Zio [et al.] // ELSEVIER Nuclear Engineering and Technology. 50(2020)/ P. 995–1001.*

*16. **Douad M. A., Dahmani Y.** ARTT taxonomy and cyber-attack framework // 2015 First International Conference on New Technologies of information and Communication (NTIC).*

*17. **Zhu Bonnie, Anthony Joseph, Shankar Sastru.** A taxonomy of cyber attacks on SCADA systems // 2011 International Conference on Internet of Thigs and 4th International Conference on Cyber, Physical and Social Computing.*

*18. **A novel** approach for network attack classification / Md Mehedi Hassan Onik, Nasr AL-Zaben, Hung Ohan Hoo, Chul-Soo Kim // Annals of Emerging Technologies in Computing (AETiC). 2018. Vol. 2. No. 2.*

*19. **A Cyber** – Kill-Chain based taxonomy of crypto-ransomware features / T. Dargahi, All Dehghantanha, Pooneh Nikkhah Bahrami [et al.] // Journal of Computer Virology and Hacking Techniques. 2019. №5. P. 277–305.*

*20. **A taxonomy** and survey of attacks against machine learning / N. Pitropakis, E. Panaousis, Th. Giannetsos [et al.] // ELSEVIER Computers Scuence Review. 2019.*

*21. **Chapman lan M., Sylvain P. Leblanc, A. Partington.** Taxonomy of cyber attacks and simulation of their effects // 2011 Spring Simulation Multi-Conference, SpringSim 11.*

Ya. S. Shavlovskyi

MODEL STRUCTURE OF THREATS TO RESOURCES OF INFORMATION AND TELECOMMUNICATION NETWORKS AS A BASIC ASSET OF A CRITICALLY IMPORTANT INFRASTRUCTURE FACILITY

The paper classifies the models of cyberattacks aimed at computer networks and complexes and which represent the greatest threat. A classification based on the main trends in the practical implementation of cyberattacks is proposed. This approach is new for the classification of cyberattacks on computer networks and complexes that serve critical infrastructure objects and takes into account ten components of the threat cycle: from a comprehensive study of the object of influence to the implementation of a cyberattack.

Keywords: critical infrastructure object; information and communication system; classification; classifier; information and telecommunication network; computer network; information protection; cyberspace; computer cyberattack; network device.