УДК 004.7.056

[0000-0003-1952-6144] **П. В. Ступень**, *к.т.н, доцент,*
e-mail: stek2000@gmail.com
[0000-0001-5947-2924] **К. В. Дікусар**, *старший викладач,*
e-mail: semuella@gmail.com
А. А. Рябой, *магістр,*
e-mail: atasylle@gmail.com
Одеський національний політехнічний університет
пр. Шевченка, 1, м. Одеса, 65044, Україна

МОДЕЛЮВАННЯ ХАРАКТЕРИСТИК ОБЛАДНАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ У РАКУРСІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дослідження присвячене розвитку моделей аналізу та оцінюванню ризиків інформаційної безпеки в комп'ютерних мережах, які використовуються при розробці систем захисту інформаційних ресурсів підприємств та при аудиті рівня захисту інформаційних систем, які вже функціонують, розробленню сімейства моделей безпеки комунікаційного обладнання комп'ютерних мереж.

Розроблені алгоритми та моделі були реалізовані в системі аналізу та виправлення порушень інформаційної безпеки, використання якої дало можливість скоротити час виправлення наслідків таких порушень.

Виявлено основні елементи порушень, які описуються інформаційною структурою та роблять вплив на діяльність інформаційних систем. Визначено, що більшість подій інформаційної безпеки пов'язані з комунікаційним обладнанням комп'ютерних мереж, на основі яких функціонують інформаційні системи.

Подальші дослідження були спрямовані на пошук та розробку моделей безпеки комунікаційних рівнів функціонування комп'ютерних мереж та системи виправлення порушень інформаційної безпеки. Для реалізації запропонованих алгоритмів розроблено ряд моделей, які описують характеристики мережного обладнання з позиції безпеки.

Ключові слова: *інформаційна безпека, комп'ютерна мережа, комунікаційне обладнання, модель безпеки, порушення безпеки, комутація, тунелювання.*

Вступ. За останні роки зловмисна активність у глобальній мережі постійно підвищується, складність атак на інформаційні системи зростає з дуже великою швидкістю, зростають складність та різноманіття вірусних програм, які використовуються для отримання фінансової вигоди або нищення інформації [1, 2]. В процесі функціонування інформаційних систем та комп'ютерних мереж адміністраторам необхідно впроваджувати багато моделей інформаційної безпеки, таких як: аналіз ризиків, аналіз та розслідування фактів порушення безпеки. Проте ці заходи часто ігноруються IT-спеціалістами. Набагато частіше спеціалісти з інформаційної безпеки стикаються з необхідністю обробляти факти порушень, які вже сталися.

Однією з причин існуючого стану речей є відсутність надійних комплексних методів, які дають змогу в автоматичному режимі протидіяти порушенням безпеки [3-6]. Велика кількість процесів та протоколів інформаційного захисту виконуються інженерами з інформаційної безпеки в ручному режимі, з використанням окремих утиліт, або сценаріїв захисту власної розробки, що потребує багато часу і перешкоджає оперативному вирішенню виникаючих проблем, що в багатьох випадках призводить до фінансових втрат підприємств і організацій. Також більшість процесів виправлення наслідків фактів порушення мережевої безпеки ґрунтується на власному досвіді адміністраторів, що обмежує коло можливих сценаріїв їх виправлення. Таким чином, розробка методів аналізу інформаційних систем та моделей виправлення порушень у контексті автоматичної обробки рутинних операцій з виявлення проблем у системі та їх вирішення є дуже необхідною.

Аналіз останніх досліджень. У сучасних інформаційних системах та мережах для опису процедури управління подіями порушення безпеки використовується класична

DOI: 10.24025/2306-4412.4.2019.184017

модель безперервного поліпшення процесів, що отримала назву від циклу Шухарта–Демінга, – модель PDCA (Плануй, Plan – Виконуй, Do – Перевіряй, Check – Дій, Act). Стандарт ISO 27001 описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. У багатьох великих компаніях впроваджена служба підтримки Service Desk, в обов'язки якої входить управління інцидентами в галузі інформаційних технологій. Процедура управління IT-інцидентами регулюється стандартом ISO IEC 20000: 2005.

Аналіз сучасного стану систем управління інформаційною безпекою показав, що існуюча безліч і різноманіття способів інформаційних атак не дають можливості пов'язати їх єдиними критеріями та показниками оцінювання, що значно ускладнює аналіз фактів подій порушення, їх класифікацію, реєстрацію, розслідування та адекватну і швидку реакцію на них [7, 8].

Метою роботи є скорочення часу реакції на виникнення порушення інформаційної безпеки та автоматизація даних операцій за рахунок розробки моделей безпеки основних рівнів функціонування комп'ютерних мереж.

Виклад основного матеріалу. Виходячи зі структури порушення, а саме впливу вразливостей та пов'язаних з ним сценаріїв загроз, зроблено висновок, що для реалізації сценаріїв виправлення причин виникнення порушень інформаційної безпеки необхідно врахувати такі фактори [9, 10]:

- кількість та типи мережного обладнання, яке функціонує в інфраструктурі системи;
- особливості програмного забезпечення, яке функціонує у складі системи;
- наявність механізмів інформаційного захисту інформації в системі;
- можливість централізованого керування відмовами у системі.

З урахуванням цих факторів, представлено основні класи сценаріїв, які необхідні для виправлення фактів порушення безпеки інформаційної системи або мережі. При цьому за певними ознаками можна виділити два класи сценаріїв – сценарії виправлення в мережі (рисунок 1) та сценарії виправлення додатків. Сценарії, пов'язані з порушеннями безпеки у мережі, можна розділити на такі типи:

- вирішення проблем комутації;
- вирішення проблем маршрутизації;
- вирішення проблем тунелювання;
- вирішення проблем фільтрації;
- вирішення проблем виявлення.

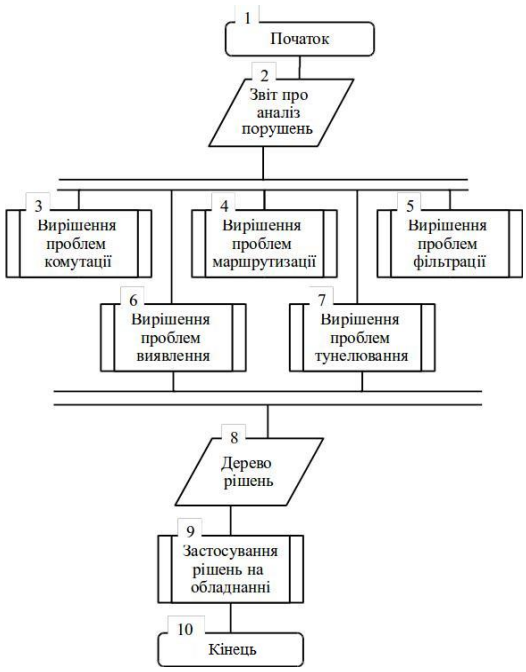

Рисунок 1 – Алгоритм виправлення порушень мережевої безпеки на рівні мережного обладнання

Процес складається з шести процедур, які передбачають втручання в роботу мережного обладнання.

Блок 3 описує вирішення проблем на рівні комутації. Враховуючи, що це основний рівень для корпоративних мереж, більшість проблем виявляється також на ньому. Основними операціями тут є аналіз налаштувань віртуальних мереж, таблиці ARP протоколу, таблиць MAC-адрес, механізмів протоколу STP та PortSecurity. Система аналізує інформацію про порушення та приймає рішення про необхідність внесення коректив у налаштування комутаторів.

Блок 4 описує вирішення проблем на рівні маршрутизації. Якщо мережна інфраструктура організації настільки велика, що необхідно використання підмережі маршрутизаторів, виникає необхідність здійснювати їх контроль. Основними методами маршрутизації всередині мережі є Router-on-a-stick для віртуальних мереж та статичні маршрути між підмережами. Це достатньо прості налаштування і потребують втручання у налаштування інтерфейсів та роботу статичного маршруту.

DOI: 10.24025/2306-4412.4.2019.184017

Блок 5 описує вирішення проблем фільтрації. При виявленні порушень, пов'язаних з помилками при фільтрації трафіку, необхідно використовувати сценарії, які виправляють програмні та апаратні міжмережеві екрани, проксі-сервери та списки доступу.

Блок 6 описує вирішення проблем з виявленням вторгнень. Якщо в системі використовується система виявлення вторгнень, можливі порушення, пов'язані з помилками першого та другого роду в роботі цих систем. При цьому необхідно втручання в сигнатури цієї системи або перенавчання системи за новими правилами функціонування трафіку.

Блок 7 описує вирішення проблем тунелювання. При використанні тунелів для підключення віддалених офісів та працівників виникають порушення, пов'язані з несанкціонованим доступом до ресурсів іншими особами. При цьому необхідні сценарії, які передбачають переналаштування або ліквідацію тунелю для підвищення безпеки системи.

В результаті виконання цих процедур формується загальне дерево рішень для конкретного порушення, яке надходить до виконавчої процедури алгоритму (блок 9). В цьому блоці виконуються сценарії адміністраторів, які автоматично, або напівавтоматично виконують зміни налаштувань мережного обладнання, згідно з представленим рішенням.

Для реалізації алгоритму було розроблено ряд моделей, які описують характеристики мережного обладнання у ракурсі безпеки:

- модель безпеки комутації;
- модель безпеки тунелювання;
- модель безпеки екранування;
- модель безпеки маршрутизації;
- модель безпеки виявлення вторгнень.

Комутація в комп'ютерних мережах реалізована комутаторами другого та третього рівнів [11]. Відповідно, розроблена модель описує характеристики комутатора, які впливають на рівень безпеки та надійності інфраструктури мережі. В загальному рівні модель описується наступним чином:

$$K = \{M, \{TS\},\{PS\}\}, \quad (1),$$

де M – параметр з діапазону [0..2], який характеризує рівень ієрархії комутатора в мережі. 0 – рівень доступу, 1 – рівень розподілу, 2 – рівень ядра; {TS} = {{Tpv}, {TPG}} – множина параметрів використання захисту від петель, де {Tpv} – множина параметрів для кожної віртуальної мережі, {TPG} – множина параметрів для кожної фізичної групи комутаторів; {PS} = {{PMAC}, {PVL}, {PARP}} – множина параметрів використання технології захисту портів комутатора, де {PMAC} – множина параметрів вивчення MAC-адрес, {PVL} – множина параметрів налаштувань реакції на зміну в параметрах {PMAC}, {PARP} – множина таблиць MAC-адрес комутаторів.

Використання цієї моделі дає можливість аналізувати стан системи комутації в мережі та приймати рішення щодо змін в роботі алгоритмів комутації. Для цього необхідно використання централізованої системи, яка побудована на основі протоколу SNMP, або спеціальних сценаріїв, які дають змогу автоматично виконувати команди програмної оболонки комутаторів.

При розгортанні тунелів VPN в комп'ютерних мережах необхідно враховувати особливості кінцевих пристроїв, а саме: зі сторони ресурсів інформаційної системи встановлений спеціальний шлюз, або маршрутизатор з підтримкою відповідних функцій; зі сторони клієнта встановлене спеціалізоване програмне забезпечення; зі сторони інших мереж встановлений спеціальний шлюз, або маршрутизатор [12].

Враховуючи, що в контексті дослідження розглядаються порушення безпеки в основній мережі, розроблена модель описує безпеку шлюзової частини розгорнутого VPN тунелю.

Представлена модель характеризує основні параметри тунелю і виглядає наступним чином:

$$VTUN = \{\{VP\}, \{VTR\}, \{VNET\}\}, \quad (2)$$

де {VP} – тип тунельного протоколу, 0 – IPSec, 1 – GRE, 2 – SSL, 3 – L2TP, 4 – PPP; {VTR} – тип транспорту між мережами, 0 – режим транспорту, 1 – режим тунелю; {VNET} – тип з'єднання з кінцевою точкою, 0 – Site-to-Site, 1 – Remote access.

Множина цих параметрів для кожного шлюзу дає можливість аналізувати типові сценарії розгортання захищених тунелів та вносити зміни у відповідні характеристики функціонування пристрою.

Зміни вносяться за рахунок спеціальних сценаріїв, які оперують налаштуваннями обладнання на рівні командного рядку операційної системи шлюзу.

DOI: 10.24025/2306-4412.4.2019.184017

На рівні екранування трафіку необхідно враховувати, на якому рівні моделі TCP/IP виконується фільтрація трафіку [13]. Враховуючи стандартні типи мережних екранів, модель може бути представлена наступним чином:

$$FW = \{\{LY, FT\}, \{FVL\}\}, \quad (3)$$

де: LY – рівень фільтрації, 0 – канальний рівень, 1 – мережний рівень, 2 – рівень додатків; FT = {FMAC, FACL, FPR, FST, FIDS} – множина типів фільтрації трафіку, FMAC – наявність фільтрації MAC адрес, FACL – наявність пакетної фільтрації, FPR – використання проксі-сервера, FST – використання фільтрації на основі стану, FIDS – параметри розширення функцій фільтрації (модель безпеки вторгнень); {FVL} = {FD, FS, FA} – множина запланованих реакцій на події, FD – скид пакетів, FS – журналювання події, FA – повідомлення про подію.

Параметри типів фільтрації та реакцій на подію можуть комбінуватися всередині відповідної множини або становити порожню множину. Множина реакцій на події є одним із вхідних параметрів для аналізу рішень порушень безпеки.

Вирішення проблем екранування нині не може бути повністю автоматизованим процесом. Це пов'язано з тим, що втручання в фільтрацію трафіку в окремих випадках вимагає внесення часткових або повних змін у правила фільтрації, порядку виконання таких правил та їх видалення [14]. Проте можливе використання сценарних підходів, які дають можливість виконувати передумовлені дії за правилами в разі виникнення відповідного інциденту.

Модель безпеки виявлення вторгнення передбачає використання сумісної моделі з моделлю екранування, а саме розширює параметр фільтрації на основі стану. Це обумовлено тим, що системи виявлення вторгнень безпосередньо виконують контроль вхідного/вихідного трафіку мережи. Системи виявлення вторгнень у реальних системах завжди співпрацюють з системами фільтрації і дають відповідні команди корегування фільтрації трафіку. Тому представлена модель розширює модель фільтрації трафіку наступним чином:

$$FIDS = \{FTIDS, FSIDS\}. \quad (4)$$

У цій моделі параметри описують тип системи виявлення вторгнення і тип виявлення вторгнення.

Тип системи визначає два варіанти: 0 – локальна система, 1 – мережна система. В разі локальної системи виявлення необхідно асоціювати її з конкретним обладнанням мережі (комутатори, маршрутизатори, сервери тощо).

Тип виявлення включає два варіанти. 0 – сигнатурний метод виявлення, 1 – метод виявлення аномалій.

Модель безпеки маршрутизації необхідна, коли сегментація мережі приводить до необхідності використання відповідного обладнання. Для малих мереж з кількістю маршрутизаторів до трьох штук ця модель не використовується:

$$M = \{MR, MR, MH, MU\}, \quad (5)$$

де MR – тип маршрутизації, 0 – статична, 1 – динамічна, 2 – між віртуальними мережами; MR – тип протоколу динамічної маршрутизації, 0 – OSPF, 1 – EIGRP, 2 – RIP, 3 – BGP; MH – наявність (0) або відсутність (1) шифрування даних; MU – тип оновлення інформації, 0 – передача повної таблиці маршрутизації, 1 – часткова передача таблиці маршрутизації.

У разі використання статичної маршрутизації та маршрутизації між віртуальними мережами усі інші параметри не враховуються при аналізі, тому що маршрутна інформація не розповсюджується в мережі [15].

Виправлення проблем маршрутизації полягає у виконанні аналізу лістингу параметрів маршрутизатора, таких як час оновлення, час обміну контрольними пакетами, встановлення відношень сусідства та ін.

Для оцінювання ефективності розробленої системи було проведено порівняльні оцінні розрахунки, а також систему було випробувано в корпоративному секторі інформаційних систем.

Оцінювання проводилося в двох напрямах: 1. Виправлення реальних інцидентів (рисунок 2), які виникали під час спостереження; 2. Виправлення штучних інцидентів (рисунок 3), які генерувались як тестові події.

DOI: 10.24025/2306-4412.4.2019.184017

Рисунок 2 – Час виправлення реальних інцидентів системи

В результаті проведених дослідницьких заходів було отримано наступні дані:

- кількість інцидентів, які було виправлено;
- кількість реальних інцидентів;
- кількість тестових інцидентів;
- час, витрачений на виправлення інцидентів з використанням розробленої системи та без неї.

Рисунок 3 – Час виправлення штучних інцидентів

В результаті оцінених розрахунків було отримано наступні результати:

1. Кількість виправлених інцидентів з використанням системи майже збігається з виправленими інцидентами без використання системи. Без використання системи за аналогічний період часу було виправлено на чотири інциденти менше;

2. Час виправлення реальних інцидентів з використанням розробленої системи скоротився на 27,4 % порівняно з виправленням без використання системи;

3. Час виправлення штучних інцидентів з використанням розробленої системи є меншим на 33,9 % порівняно з виправленням без використання системи.

Для достовірності оцінок сценаріїв виправлення було проаналізовано однакову кількість інцидентів у ході однакового проміжку часу. Це обумовлює той факт, що кількість вирішених інцидентів не збігається. Однак реально всі інциденти були вирішені, що свідчить про те, що система в автоматичному режимі здатна виправляти основні типи інцидентів безпеки

Висновок. Використання вищенаведених моделей у системі виправлення наслідків порушень інформаційної безпеки дало можливість повністю або частково автоматизувати реакцію на події безпеки, які виникають в інформаційних системах. Розроблені моделі дають можливість врахувати особливості інформаційної системи, характер сценаріїв загроз та особливості мережного обладнання. Проведені випробовування показали, що розроблена на основі моделей система дає змогу вирішувати більшість виявлених порушень без суттєвого втручання адміністраторів та суттєво зменшує час самого виправлення порушення. Реальні події порушення інформаційної безпеки, які були більшою мірою пов’язані з вірусами та помилками, були вирішені майже на 30 % швидше; тестові порушення, які складалися зі штучної DoS атаки та помилок на обладнанні, вирішувалися на 34 % швидше.

Список літератури

[1] Д. О. Сікорський, "Аналіз принципів побудови моделей інформаційної безпеки в корпоративних інформаційних системах", *Ефективна економіка*, № 8, серпень, 2015. [Електронний ресурс]. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=4257

[2] М. О. Мельник, Г. Д. Нікітин, та К. О. Мезенцева, "Аналіз побудови моделі політики інформаційної безпеки підприємства", *Системи обробки інформації*, № 2 (148), с. 126-128, 2017.

[3] О. К. Юдін, та С. С. Бучик, "Концептуальна модель інформаційної безпеки державних інформаційних ресурсів", *Наукоємні технології*, № 4 (24), 2014.

[4] А. В. Потий, "Формальная модель процесса защиты информации", *Радіоелектроніка і комп'ютерні системи*, № 5, с. 128-133, 2006.

[5] С. Н. Ильяшенко, "Составляющие экономической безопасности предприятия и подходы к их оценке", *Актуальні проблеми економіки*, № 3, с. 12-19, 2003.

[6] Н. Кабірова, "Мовчання ягнят: як примусити персонал зберігати секрети фірми",

DOI: 10.24025/2306-4412.4.2019.184017

Галицькі контракти, № 45, с. 34-36, 2004.
[7] А. Кремер, "Информационная безопасность как важный фактор эффективного управления компанией", *Управление компанией*, № 9, с. 55-56, 2003.
[8] О. М. Косогов, та А. О. Сірик, "Моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків", *Сучасні інформаційні технології у сфері безпеки та оборони*, № 2 (26), 2016.
[9] В. А. Герасименко, *Защита информации в автоматизированных системах обработки данных*, 1-е изд. Москва: *Энергоатомиздат*, 2010.
[10] Л. К. Бабенко, и Е. А. Ищукова, *Современные алгоритмы блочного шифрования и методы их анализа*. Москва: Гелиос АРВ, 2006.
[11] В. А. Галатенко, *Информационная безопасность*. Москва: Финансы и статистика, 2008.
[12] И. Р. Конеев, и А. В. Беляев, *Информационная безопасность предприятия*. Санкт-Петербург: БХВ-Петербург, 2003.
[13] А. А. Мелюк, С. В. Пазизин, и Н. С. Погожин, *Введение в защиту информации в автоматизированных системах*. Москва: Горячая линия – Телеком, 2001.
[14] Т. Оглтри, *Практическое применение межсетевых экранов*. Москва: ДМК Пресс, 2001.
[15] А. В. Соколов, и О. М. Степанюк, *Защита от компьютерного терроризма:* справ. пособ. Санкт-Петербург: БХВ-Петербург, Арлит, 2002.

References

[1] D. O. Sikorsky, "The analysis of the principles of building information security models in corporate information systems", *Efektyvna ekonomika*. no. 8, August, 2015. [Online]. Available: http://www.economy.nayka.com.ua/?op=1&z=4257
[2] M. O. Melnyk, G. D. Nikitin, and K. O. Mezentseva, "Analysis of building a model of enterprise information security policy", *Systemy obrobky informatsii*, no. 2 (148), pp. 126-128, 2017 [in Ukrainian].
[3] O. K. Yudin, and S. S. Buchik, "Conceptual model of information security of state information resources", *Naukoiemni tekhnolohii*, no. 4 (24), 2014 [in Ukrainian].
[4] V. Potiy, "Formal model of information security process", *Radioelektronika i kompiuterni systemy*, no. 5, pp. 128-133, 2006 [in Russian].
[5] S. N. Ilyashenko, "Components of economic security of an enterprise and approaches to their assessment", *Aktualni problemy ekonomiky*, no. 3, pp. 12-19, 2003 [in Russian].
[6] N. Kabirova, "Silence of lambs: how to make the staff keep the firm's secrets", *Halytski kontrakty*, no. 45, pp. 34-36, 2004 [in Ukrainian].
[7] Kremer, "Information security as an important factor in the effective management of a company", *Upravleniye kompaniyei*, no. 9, pp. 55-56, 2003 [in Russian].
[8] O. M. Kosogov, and A. O. Sirik, "Modeling of the process of information security assessment based on expert findings", *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, no. 2 (26), 2016 [in Ukrainian].
[9] V. A. Gerasimenko, *Information security in automated data processing systems*, 1st ed. Moscow: Energoatomizdat, 2010 [in Russian].
[10] L. K. Babenko, and E. A. Ischukova, *Modern block cipher algorithms and methods for their analysis.* Moscow: Gelios ARV, 2006 [in Russian].
[11] V. A. Galatenko, *Information security.* Moscow, Financy i statistika, 2008 [in Russian].
[12] R. Koneev, and A. V. Belyaev, *Information security of an enterprise*, St. Petersburg: BHV-Peterburg, 2003 [in Russian].
[13] A. Melyuk, S. V. Pazizin, and N. S. Pogozhin, *Introduction to the protection of information in automated systems*, Moscow: Goryachaya liniya – Telekom, 2001 [in Russian].
[14] T. Ogltree, *Practical application of firewalls*, Moscow: DMK Press, 2001 [in Russian].
[15] V. Sokolov, and O. M. Stepanyuk, *Protection against computer terrorism:* reference manual, St. Petersburg: BHV-Peterburg, Arlit, 2002 [in Russian].

DOI: 10.24025/2306-4412.4.2019.184017

P. V. Stupen, *Ph. D., associate professor,*
e-mail: stek2000@gmail.com
K. V. Dikusar, *senior lecturer,*
e-mail: semuella@gmail.com
A. A. Ryaboy, *master*
e-mail: atasylle@gmail.com
Odesa National Polytechnic University
Shevchenko ave., 1, Odesa, 65044, Ukraine

MODELING OF FEATURES OF COMPUTER NETWORK EQUIPMENT FROM THE PERSPECTIVE OF INFORMATION SECURITY

The study focuses on the development of models for analyzing and assessing information security risks in computer networks that are used in the development of enterprise information security systems and in auditing the level of protection of already existing information systems, the development of a family of security models of computer network communications equipment.

The developed algorithms and models have been implemented in the system of analysis and correction of information security violations, the use of which has allowed to reduce the time of correction of the consequences of such violations.

The basic elements of violations, which are described by the information structure and determine the influence on the activity of information systems, are revealed. It is determined that most information security events are related to the communication equipment of the computer networks on which the information systems operate.

Further research has been aimed at finding and developing security models for communication levels of operation of computer networks and a system for correcting information security violations.

To implement the algorithm, a number of models, that describe the characteristics of network equipment in the security perspective, have been developed. The model of switch security describes the switch characteristics that affect the security and reliability of the network infrastructure. The tunneling security model reflects the security of the gateway portion of the deployed VPN tunnel. The intrusion detection security model involves the use of a compatible model with the shielding model, namely extending the state-based filtering parameter. The routing security model considers the types and protocols of routing.

The use of models in the correcting system of the consequences of information security violations has made it possible to fully or partially automate the response to security events occurring in information systems. The developed models allow to take into account the peculiarities of the information system, the nature of the threat scenarios and the features of the network equipment.

Keywords: *information security, computer network, communication equipment, security model, security violation, switching, tunneling.*

DOI: 10.24025/2306-4412.4.2019.184017