УДК 004.056
DOI: 10.31673/2409-7292.2021.020304

Волков М.В., Шаповаленко О.Д.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННОЇ ПОШТИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВІД СПАМУ

Проведено дослідження впливу спам повідомлень та сучасних загроз щодо процесу обміну електронної пошти корпоративної інформаційної системи. Досліджено роль спаму та його вплив у корпоративних інформаційних системах. Досліджено особливості напрямів протидії та технології забезпечення захисту електронної пошти від спаму. На основі досліджень проведених в роботі розроблено рекомендації щодо удосконалення захищеного обміну електронної пошти корпоративної інформаційної системи.

Ключові слова: електронна пошта, спам, захист, інформаційна система.

Вступ

Сучасна кібербезпека стає все менш означеною з більшою складністю та можливостями для обміну та передачі інформації, розвитку електронного урядування, ведення онлайн-бізнесу, надання мобільних та бездротових послуг. Інформаційне та комунікаційне середовище є відкритим для все більшого числа ризиків і загроз, які можуть мати негативні наслідки для фізичних та юридичних осіб. Розповсюдження шкідливого програмного забезпечення є однією з найбільш небезпечних загроз, що впливає на безпеку даних у сучасному кіберсередовищі і може втручатися у весь бізнес.

Постановка проблеми

Щоб захистити свій бізнес, компанії почали впроваджувати захисну-програмну базу, яка блокує, а також фільтрує всі можливі форми небажаних листів. Захисні програми інтегровані із системою електронної пошти та Інтернет-провайдерами щоб миттєво відмовляти та фільтрувати спам-повідомлення. Кібератаки мають місце, коли хакери надсилають зашифровані електронні листи із вбудованим вірусом або шкідливим програмним забезпеченням, прикріпленим до нього. З іншого боку, користувачі не знають про зміст шкідливих програм, який додається до електронного листа, у формі вкладення або посилання.

Компанії можуть запобігти потраплянню електронної пошти зі спамом до поштової скриньки користувача, використовуючи спам-фільтри. Впровадження захисту від спаму може додатково допомогти у визначенні спаму, який був розпізнаний, ізольований та миттєво видалений. Сьогодні це вважається перевагою для бізнесу, оскільки відновлювати наслідки стає набагато складніше більшості спам-інфекцій. Інвестування в протидію від спама може усунути спам-повідомлення з самого початку, перш ніж викликати будь-які проблеми з безпекою.

Мета дослідження – виявлення особливостей побудови та використання методів і засобів захисту електронної пошти корпоративної інформаційної системи від спаму.

Основними завданнями дослідження, спрямованими на досягнення поставленої мети, є:

проаналізувати актуальність спам атак, класифікацію загроз та вектори його атак у кібернетичному просторі;

провести досконалий аналіз особливостей сучасних напрямів протидії спаму і використання ефективних засобів захисту електронної пошти;

розробити методичні рекомендації щодо побудови та використання сучасних методів засобів захисту корпоративної електронної пошти;

Статистика кібер атак у другому кварталі 2020 року.

Згубність спамових розсилок полягає в тому, що спамеру це практично нічого не коштує, зате вони дорого обходяться усім іншим, приміром, одержувачеві спаму або його провайдерові. Велика кількість рекламної кореспонденції може привести до перенавантаження на канали і поштові сервери провайдера, через що звичайна пошта, яку, можливо, дуже чекають одержувачі, проходитиме значно медленее. За все розплачується

одержувач спаму, що оплачує своєму провайдерові час в Мережі, що витрачається на отримання незапрошеної кореспонденції з поштового сервера.

Окрім безпосередніх витрат, відділення непрошеної інформації від потрібної та її видалення вимагає тимчасових витрат, що також дуже незручно, особливо для активних людей - у них на це нерідко йде багато часу. Та і втратити в потоці непотрібних повідомлень одне дійсно важливе - це теж часто дуже невигідно. До того ж, спам часто використовується спільно з різними вірусними технологіями.Очевидно, що спам не можна ігнорувати.

Спам – це масова анонімна незапрошена розсилка поштових повідомлень користувачам, причому немає різниці, чи комерційна це реклама або просто корисна на думку посилача інформація. Слід відрізняти спам від легальних поштових розсилок, які, хоча і багато в чому повторюють багато рис спаму, є запрошеними користувачем і повинні доставлятися йому. Спам в сучасному Інтернеті є негожим зайняттям, і в законодавстві низки країн передбачені ті або інші види відповідальності за подібного роду діяльність.

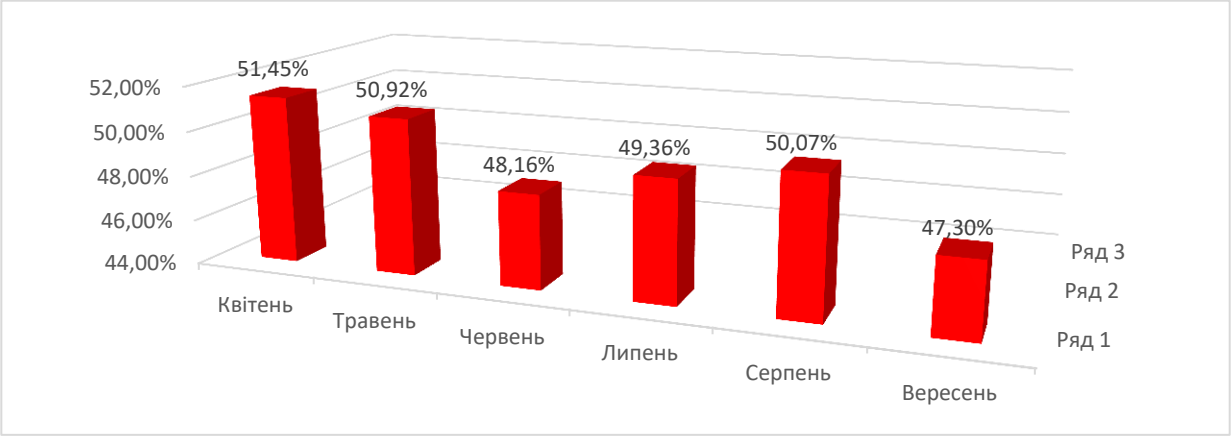

Рис.1. Частка спаму в світовому поштовому трафіку, Q2 2020 року – Q3 2020 рр.

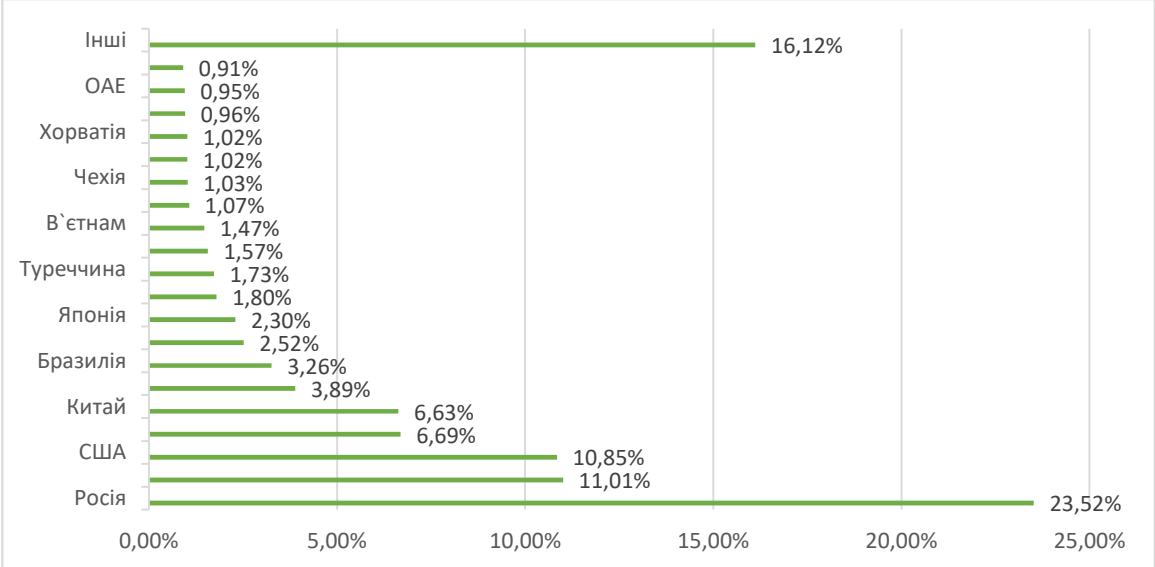

Рис. 2. Країни - джерела спаму в світі, Q3 2020 рр

У третьому кварталі 2020 року найбільша частка спаму була зафіксована в квітні - 51,45%. Середня частка спаму в світовому поштовому трафіку склала 48,91%, що на 1,27 п.п нижче за показник попереднього звітного періоду. Перші п'ять місць серед країн, що лідирують за кількістю вихідного спаму, розділили ті ж учасники, що і в першому кварталі 2020 року. Попереду всіх, як і раніше, Росія (18,52%), а на другому місці Німеччина

(11,94%), яка змістила США (10,65%) з другої на третю позицію. Четверте і п'яте місця, як і в минулому звітному періоді, займають Франція (7,06%) і Китай (7,02%). Шосте місце дісталося Нідерландам (4,21%), за ними з невеликим відривом один від одного слідують Бразилія (2,91%), Туреччина (2,89%), Іспанія (2,83%), а замикає десятку Японія, чия частка становить 2,42%.

Всього за третій квартал 2020 року, наші захисні рішення виявили 51 025 889 шкідливих поштових вкладень, що на 8 мільйонів більше показника минулого звітного періоду.

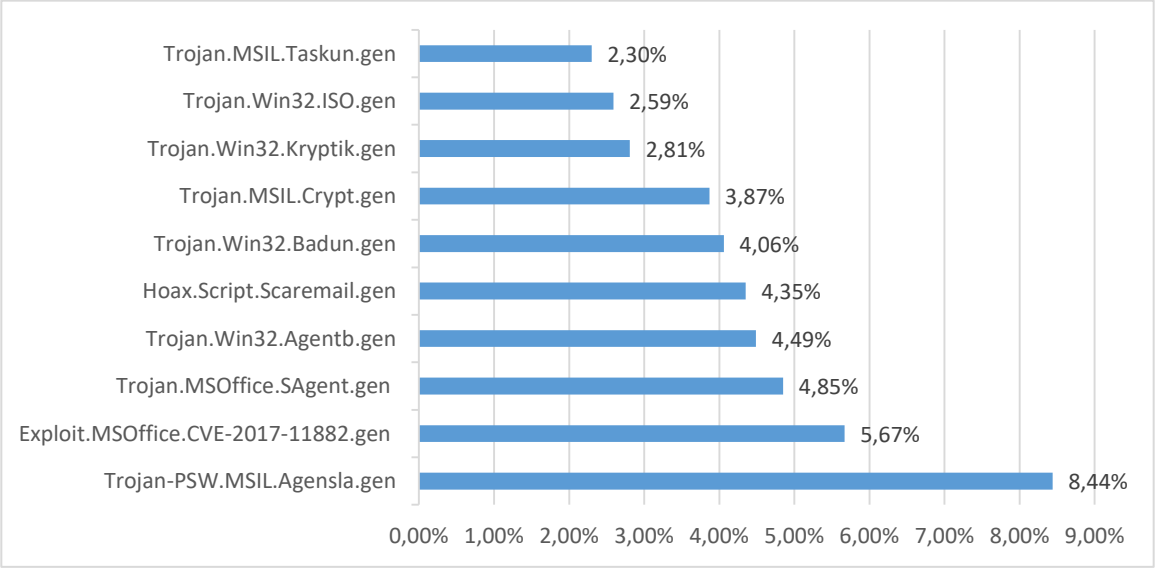

Рис. 3. TOP 10 шкідливих вкладень в поштовому трафіку, Q2 2020 рр.

Аналіз методів розпізнавання спаму

Метод "чорного", "білого" і "сірого" списків. Базою методу є аналіз зворотного IP-адресу відправника листа. Всі листи, відправлені з IP-адрес, занесених до "чорного списку", знешкоджуються ще на поштовому сервері, так і не досягаючи кінцевого користувача. Адреса вноситься в "чорний список" на підставі того, що лист що прийшов з цієї адреси є спамом. З адресатами з "білого списку" дозволений обмін поштовими повідомленнями. У разі, коли IP-адреса листа не присутній ні в "чорному" ні в "білому" списку, то відправнику автоматично висилається запит на авторизацію, а IP-адреса заноситися в тимчасовий "сірий" список. Якщо після закінчення певного терміну підтвердження "надійності" від невідомого адресанта не надходить, то його адреса вноситься в "чорний список", а повідомлення видаляються. Основний недолік даного методу полягає в тому, що IP-адреса не обов'язково є джерелом спаму. Наприклад, спам може прийти з динамічного IP-адреса, або розсилка спаму може проводиться без санкції власника IP-адреси. Таким чином, з високою ймовірністю в "чорний" список можуть потрапити адреси ні в чому не винних користувачів.

Метод листів-підтверджень. Метод базується на тому, що оскільки спам-розсилки відбуваються автоматично, по багатьом мільйонам адрес, а адреса відправника - у більшості випадків - підроблена, то підтвердження від справжнього спамера отримати не вдасться. Однак застосування даного методу різко знижує оперативність доставки листів, у багатьох випадках спам відправляється з реальних IP-адрес, а сучасне програмне забезпечення спамерів може генерувати підтвердження відправки листів.

Метод розпізнавання спаму за ключовими словами, які визначаються користувачем у вигляді деяких правил. Даний метод не отримав широкого поширення через складність і трудомісткість формування зазначених правил.

Метод байєсівської фільтрації. Кожному зустрічається в електронному листуванні слову (або HTML-тегом) присвоюється два значення: ймовірність його наявності в спам (z) і

ймовірність його присутності в листах, дозволених для проходження (1-z). Кожному новому листу за допомогою формули Байеса виставляється оцінка (Z):

$$Z = A/(A+B), \quad (1)$$

де

$$A = z_1 \times z_2 \times \ldots \times z_i \times \ldots \times z_n, \quad (2)$$

$$B = (1-z_1) \times (1-z_2) \times \ldots \times (1-z_i) \times \ldots \times (1-z_n), \quad (3)$$

zi - спам-оцінка кожного слова, що входить в лист.

Якщо отримана оцінка менше деякого заздалегідь визначеного граничного значення, то лист трактується як спам. Очевидно, що ефективність даного методу багато в чому залежить від правильності розрахунку спам-оцінок слів які входять до листа. Для цього необхідно провести статистичний аналіз як спаму, так і звичайних листів одержуваних кожним користувачем.

Таким чином, метод байєсівської фільтрації передбачає деяке запізнювання, пов'язане з накопиченням кожним користувачем достатнього обсягу статистичного матеріалу (архіву листів). Ще одним недоліком методу є пропуск спаму, якщо в листі щодо мало слів з високою спам-оцінкою. Відзначимо, що ця обставина використовується спамерами як для обходу, так і для компрометації фільтрів. Наприклад, лист, що складається з набору нейтральних слів не розпізнає як спам.

У більшості сучасних антиспамових систем реалізовані комплексні методи захисту, які по завіренням їх розробників можуть фільтрувати до 98% спаму. Однак час реакції на новий вид спам-листів найбільших поштових служб інтернету становить не більше 20-30 хв.

Запропонована структура домена антиспамової обробки

Компоненти цієї системи включають в себе об'єкт антиспамової обробки, підоб'єкти антиспамової обробки, сервери електронної пошти та клієнтів електронної пошти. Ці компоненти можуть зв'язуватися один з одним за допомогою загальнодоступних протоколів передачі повідомлень.

DNS	Domain Name Server	Система найменувань доменів
E-mail	Electronic mail	Електронна пошта
ESMTP	Extended Simple Mail Transfer Protocol	Розширений простий протокол передачі електронної пошти
FTP	File Transfer Protocol	Протокол передачі файлів
HTTP	Hypertext Transfer Protocol	Протокол передачі гіпертексту
IMAP4	Internet Message Access Protocol v4	Протокол доступу до повідомлень інтернету, версія 4
IP	Internet Protocol	протокол Інтернет
POP3	Post Office Protocol v3	Поштовий протокол, версія 3
RBL	The term is commonly used to describe Real-time Blacklist.	Цей термін зазвичай використовується для опису "чорного списку" в реальному масштабі часу.
SASL	Simple Authentication and Security Layer	Рівень простий аутентифікації і безпеки
SMTP	Simple Mail Transfer Protocol	Простий протокол передачі електронної пошти
URL	Uniform Resource Locator	Уніфікований покажчик ресурсу

Об'єкт антиспамової обробки отримує повідомлення від під об'єктів антиспамової обробки і приносить їм нові правила. Під об'єкти антиспамової обробки повинні перевіряти період дії правил, що надходять від об'єкта антиспамової обробки, і вносити в них поліпшення. Клієнт електронної пошти є об'єктом, з яким безпосередньо взаємодіють користувачі. Сервер електронної пошти здійснює доставку електронної пошти в мережі електрозв'язку на базі IP. Клієнт електронної пошти направляє скарги подоб'екти антиспамової обробки. У конкретних ситуаціях клієнт електронної пошти може подати скаргу безпосередньо об'єкту антиспамової обробки верхнього рівня.

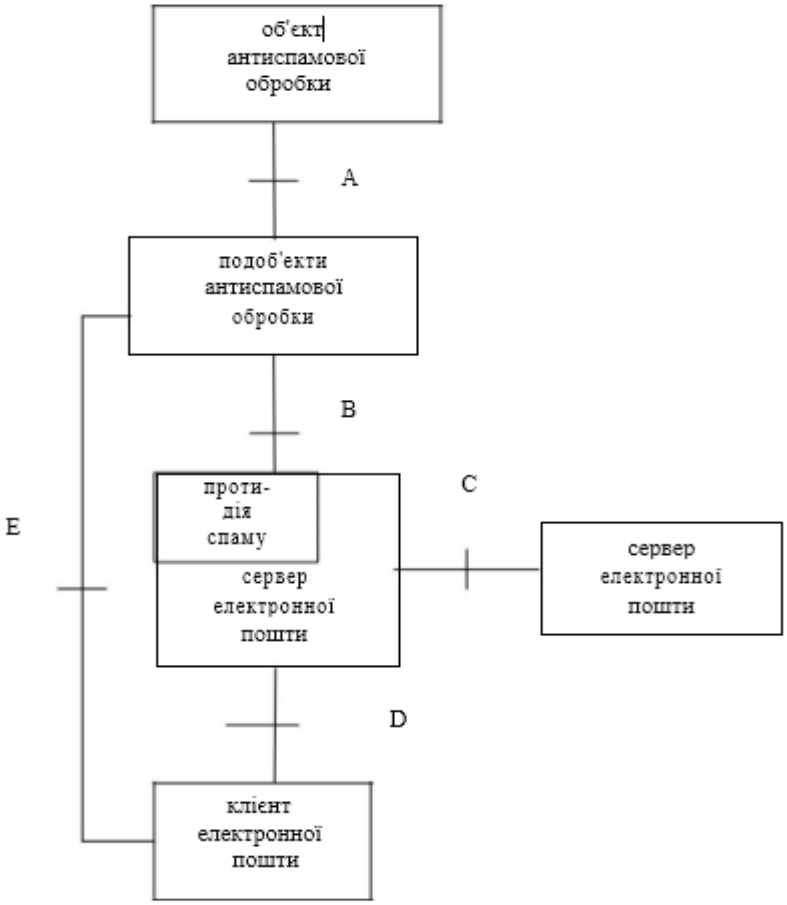

Рис. 4. - Еталонна модель

Інтерфейс A знаходиться між об'єктом антиспамової обробки і під об'єкти антиспамової обробки. Повідомлення про скарги і правила, що стосуються протидії спаму, передаються через інтерфейс A. Правила можуть являти собою складні правила, наприклад "джерело IP + URL". Інтерфейс A повинен підтримувати протоколи FTP і HTTP.

Інтерфейс B знаходиться між під об'єкти антиспамової обробки і сервером електронної пошти. Він використовується для передачі повідомлень про скарги, а також правил. Аналогічним чином, правила можуть являти собою складні правила, наприклад "джерело IP + URL". Інтерфейс B повинен підтримувати протоколи FTP і HTTP. У конкретних ситуаціях сервер електронної пошти може безпосередньо зв'язуватися з об'єктом антиспамової обробки верхнього рівня.

Інтерфейс C знаходиться між серверами електронної пошти, через які передаються повідомлення з використанням SMTP.

Інтерфейс D знаходиться між сервером електронної пошти і клієнтом електронної пошти. Для передачі електронної пошти можуть використовуватися різні протоколи, наприклад POP3, IMAP4.

Інтерфейс E знаходиться між клієнтом електронної пошти і під об'єктом антиспамової обробки. Клієнт електронної пошти може направляти скарги під об'єкту антиспамової обробки.

Функції домену антиспамової обробки

Функції клієнта електронної пошти

• Крім виконання загальних функцій передачі електронних повідомлень, клієнт електронної пошти забезпечує механізм, що допомагає користувачам надсилати скарги про спамові інформації об'єкту антиспамової обробки. Одержувачам електронної пошти потрібно визначити, чи є та чи інша електронне повідомлення спамом, виходячи з його змісту, назви або адреси.

• Клієнт електронної пошти може завантажувати правила, фільтруючі спам, автоматично з об'єкта антиспамової обробки. Правила фільтрації встановлюються згідно з повідомленнями про скарги, що надходять від клієнтів електронної пошти. Вони включають граничний розмір одного електронного повідомлення, кількість електронних повідомлень, що направляються за певний період часу, ключові слова в основному тексті електронних повідомлень і т. д.

• Клієнт електронної пошти може переслати спам, що розсилається по електронній пошті, об'єкту антиспамової обробки для подальшої обробки або видалення деяких правил фільтрації, що викликають помилкове спрацьовування. Об'єкт антиспамової обробки може негайно оновити правила фільтрації відповідно до вимог або скаргами від клієнта електронної пошти.

• Клієнт електронної пошти може безпосередньо відфільтрувати спам, що розсилається по електронній пошті. Зазвичай одержувачі повинні знати про результати фільтрації, з тим щоб не допустити виникнення проблеми помилкового спрацьовування.

Функції сервера електронної пошти.

• Здійснюючи загальні функції передачі електронної пошти, сервер електронної пошти виконує свої звичайні дії з обміну електронною поштою з іншим сервером електронної пошти або з відправлення та одержання електронної пошти між клієнтами електронної пошти; в той же час сервер електронної пошти повинен заборонити функцію відкритої ретрансляції, з тим щоб спамери не змогли змусити його передати спам-повідомлення іншого сервера електронної пошти.

• Будь-який абонент повинен пройти перевірку, перш ніж він направить електронне повідомлення через сервер електронної пошти. Різні системи електронної пошти можуть використовувати різні механізми перевірки. Перевірка проводиться між сервером електронної пошти і клієнтом електронної пошти.

• Будь-який постачальник послуг електронної пошти може вести "чорний список" спамерів, в якому міститься деяка інформація про спамерів (наприклад, найменування хоста, найменування домену або адресу електронної пошти). Сервер електронної пошти відмовляється отримувати електронні повідомлення, які виходять від цих спамерів.

• Сервер електронної пошти може повернути команду перевірки джерела, який вказаний в інформації про відправника електронного повідомлення.

• Деякі команди SMTP можуть використовуватися спамерами, для того щоб вгадати дійсну обліковий запис сервера електронної пошти. Сервер електронної пошти забороняє ці команди, наприклад EXPN і VRFY.

• Деякі види електронних повідомлень рекламного та пропагандистського характеру направляються без надання будь б то не було інформації про відправника. Сервер електронної пошти повинен автоматично додати посилання HTTP в текст електронного повідомлення.

• Сервери електронної пошти виявляють спам-повідомлення за допомогою антиспамових технологій, повідомляють про спам подоб'екти антиспамової обробки і завантажують з нього правила фільтрації.

• У разі виявлення спаму сервер електронної пошти повинен здійснити резервне копіювання вихідного спаму, що включає щонайменше заголовок електронної пошти джерела, і представити його в фільтр.

• Сервер електронної пошти повинен надавати інформацію системного журналу і свої статистичні дані, які періодично копіюються, і передавати їх подоб'екти антиспамової обробки.

• Сервер електронної пошти повертає інший номер стану відповідно до іншими правилами.

• Сервер електронної пошти може обмежити обсяг трафіку, що направляється конкретним абонентом електронної пошти.

Функції об'єкта антиспамової обробки

• Обмін правилами фільтрації з іншими об'єктами антиспамової обробки. Для передачі інформації можуть використовуватися різні протоколи, наприклад FTP і HTTP.

• Зберігання вихідної інформації про спам-повідомленнях, отриманих від абонентів, і об'єкта антиспамової обробки.

• Широкомовна передача правил фільтрації подоб'екти антиспамової обробки і попередження їх про небезпечні електронних повідомленнях.

• Об'єкт антиспамової обробки повинен керувати правилами фільтрації і підтримувати їх. Ці правила можуть бути отримані через веб-сайт для:

• Отримання повідомлень від абонентів і подоб'ектов антиспамової обробки;

• Широкомовної передачі достовірної інформації, в тому числі інформації, що стосується контролю і управління.

Висновки

Провівши аналіз можна зробити висновок, що для захисту електронної пошти від спаму і фішингу звичайних, теоретичних правил безпеки (перевірка листів,навчання працівників) недостатньо. Для максимального захисту даних необхідно звертатися за допомогою спеціалізованого програмного забезпечення, наприклад, антивірусів. Але, крім поштового аккаунта співробітника, атаці може бути підданий поштовий сервер і в цьому випадку антивіруса недостатньо. Це може вивести з ладу сервіс або додаток, яке вимагає підтвердження реєстрації електронною поштою, портал, будь-який веб-ресурс, який використовує механізм поштової комунікації з клієнтами.

Теоретична цінність даної роботи полягає в тому, що її можливо використовувати у якості методичного матеріалу по темі побудови систем захисту у корпоративній інформаційній системі від спам повідомлень та сучасних загроз. Практична значимість даної роботи полягає в тому, що її результатами можуть скористатися системні адміністратори та адміністратори безпеки при розробці та настроюванні систем захисту інформації від спаму.

Перелік посилань

1. Закірова С. Законодавче антиспам-регулювання у контексті стандартів захисту персональних даних: українські кроки і світова практика. Громадська думка про правотворення. 2021. № 3 (208). С. 4–13. URL: http://nbuviap.gov.ua/images/dumka/2021/3.pdf.

2. Посикалюк О. О. Захист особистих немайнових прав споживачів телекомунікаційних послуг від спаму / Посикалюк О. О. // Стратегія модернізації приватного права в сучасних умовах : збірник наукових праць / за ред. В. І. Короля, Ю. В. Білоусова ; НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України. — К.-Хмельницький : Хмельницький університет управління та права, 2013. — С. 133 – 143.

3. Захист інформації в комп'ютерних системах та мережах / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с..

Надійшла: 23.03.2021 Рецензент: д.т.н., професор Савченко В.А.