ВСТУП

Сьогодні, з повсюдним розвитком інтернету, електронна пошта зайняла досить важливе місце в бізнес-процесах, як підприємства малого бізнесу, так і у великих компаніях, що закономірно призвели до появи поняття - корпоративна пошта.

Корпоративна пошта - незамінний помічник для бізнесу та організації : вона допомагає залучати клієнтів, вести переписку з контрагентами і партнерами, моментально обмінюватися важливими документами, макетами та іншими файлами, гарантує своєчасне отримання важливої інформації, виконує функцію автовідповідача. Корпоративна пошта дозволяє відокремити особисте листування співробітників від службової, що дозволяє мінімізувати відволікаючі від роботи моменти. Крім того, корпоративна пошта дозволяє керівництву компанії контролювати переписку співробітників і управляти потоками інформації, знизаючи залежність від людського чинника.

Використання електронної пошти на підприємствах

Електронна пошта вельми зручна у використанні і дешевша, ніж інші засоби передачі інформації (звичайна пошта, факс або телефон). Цей вид зв'язку дозволяє ефективно передавати інформацію в режимі реального часу, до того ж в найрізноманітнішому вигляді і формі, що дозволяє відправникові й одержувачеві не витрачати додаткових зусиль і часу на передрук і комп'ютерний набір.

Основні переваги електронної пошти e-mail:

- відносно низька вартість.
- простота і зручність користування.
- передача в режимі реального часу.
- можливість передачі різноманітної інформації.
- чіткість обліку і реєстрації.

За умови оплати підключення до Інтернету користування електронною поштою не вимагає додаткових витрат, що робить цю форму передачі інформації

зараз найдешевшою. Сплачується лише підключення до мережі Інтернет, і не потрібно платити за кожне відправлене і отримане повідомлення.

Також інформація за допомогою e-mail передаэється у вельми зручній формі, яка забезпечується спеціальною програмою і не вимагає додаткового набору повідомлень, якщо це документ або інша інформація, що міститься в комп'ютері або комп'ютерній мережі. Електронна пошта зручна і для одержувача, оскільки йому не потрібно переоформляти і передруковувати її. Він може використовувати її або в отриманому вигляді, або видозмінювати в необхідних цілях, не передруковуючи. Звичайно, це не лише спрощує процедуру передачі, отримання і використання інформації, але й економить час.

Електронна пошта дозволяє відправляти й отримувати повідомлення різного виду: не тільки набрані текстові повідомлення, але і файли з баз даних, текстові файли, фотографії, таблиці, мовні і музичні повідомлення. В цьому випадку інформація передається в електронному форматі, що дозволяє відправникові і одержувачеві не витрачати часу на її додаткову обробку, оскільки відсутня необхідність введення друкарської інформації або її перетворення в електронну форму. При цьому практично миттєво можна зробити скільки завгодно копій інформації і в разі потреби доповнити і розіслати її по потрібних адресах , що значно спрощує роботу з матеріалами і документами в компанії. Особливо слід відзначити легкість переадресації і розповсюдження інформації за допомогою електронної пошти.

Передача інформації, за допомогою електронної пошти чітко фіксується як у відправника, так і в одержувача. У відповідних директоріях указуються число, година і хвилина відправлення й отримання інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Інциденти кібербезпеки пов’язані з використанням електронної пошти.

Широке використання сучасних інформаційних технологій у державних та недержавних структурах, а також у суспільстві в цілому, висуває вирішення проблем інформаційної безпеки в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини.

Більше третини всіх випадків порушень безпеки відбувається через фішингових листів або шкідливих вкладень, відправлених на адреси співробітників компаній.

Фінська компанія F-Secure, проаналізувала інциденти з якими їхні фахівці зіткнулися під час роботи. Зломи систем є більш цілеспрямованими - 55%, ніж спонтанними - 45%. Хоча на загальній картині ця різниця не помітна, ситуація змінюється в залежності від сфери діяльності компанії. Розробники ігор і державні організації викликають більший адресний інтерес, а телекомунікації і страхування стають вразливими, тільки коли шахраям надається можливість проникнути в їх структури. У фінансовій сфері обидва ці види атак представлені в рівних частках.

Найбільше атак відбувається через програмні уразливості – 21% . На другому місці - 20%, знаходяться внутрішні загрози - співробітники або люди, які, користуючись довірою організації, змогли проникнути в її структури і вкрасти інформацію (дані про клієнтів, інтелектуальну власність) . На частку фішингу - 18% і шкідливих вкладень - 16% припадає в сумі 34% зломів, що робить атаки по електронній пошті найбільш болючими для компаній. Експерти F-Secure відзначили, що деякі порушення кібербезпеки так і залишаються непоміченими, а в 13% випадків, навпаки, за кібератаку приймають звичайні проблеми IT.

У 2012 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у

створенні глобального звіту про стан світової кібербезпеки. Звіт, який був складений брюссельською компанією Security & Defence Agenda, вперше повідомив у відкритих джерелах про поточну готовність до кібератак інформаційних систем різних країн. З тих даних звіту Security & Defence Agenda, неясно, чи були виставлені якісь бали для України.

Практично всі фахівці кожної з 27 країн, які були опитані в ході складання звіту, одностайно зійшлися у тому, що для підвищення ефективності боротьби з кіберзлочинністю необхідний глобальний обмін інформацією. Крім того, всі вони відзначили необхідність не просто забезпечення обміну інформацією, а саме його оперативність та швидкість у прийняті управляючих рішень.

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на ключові позиції.

Для України така тенденція є, в цілому, позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися залежно від політики та технічних суб’єктивних факторів, багато чого залишається цілком придатним.

1.2 Аналіз нормативно - правової бази у сфері електронної пошти

На сьогодні лише окремі закони України, підзаконні акти регулюють деякі аспекти функціонування системи електронного діловодства. Порядок організації електронного документообігу визначається інструкцією з діловодства установи з урахуванням вимог нормативно-правових актів у сфері діловодства, а також технічних і програмних засобів, що функціонують у конкретній установі.

Нормативно-правові акти у сфері електронного діловодства, в тому числі щодо умов використання поштових сервісів, покладають відповідальність за

виконання положень законодавства у сфері електронного документообігу на керівника органу державної влади.

07.11.2018 набув чинності Закон України «Про електронні довірчі послуги». Одним з найважливіших положень Закону № 2155 є взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів.[1]

Закон про електронні довірчі постуги, підтверджуэ право враховувати цифрові підписи в комерційних документах (контрактах, угодах та ін.), що пересилаються електронною поштою, юридично правомочними, і вони дорівнюються до підпису у письмовій формі в реальних умовах. Також використання електронної пошти не вимагає обов'язкової присутності адресата для отримання негайної відповіді. .[1]

Закон України «Про захист персональних даних» - закон України, прийнятий 1 червня 2010 року. Предметом правового регулювання Закону є правовідносини, пов’язані із захистом персональних даних під час їх обробки. Обробка персональних даних, відповідно до частини 5 статті 6 Закону здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством. [2]

Типовий порядок здійснення електронного документообігу в органах виконавчої влади, затверджений постановою Кабінету Міністрів України від 28.10.2004 р. № 1453 «Типового порядку здійснення електронного документообігу в органах виконавчої влади» (далі - типовий порядок), визначає загальні правила використання в органах державної влади поштових клієнтів. [3]

Так, п. 4 Типового порядку визначено, що орган виконавчої влади здійснює електронний документообіг через спеціальні телекомунікаційні мережі або телекомунікаційні мережі загального користування. При цьому відправлення органом виконавчої влади електронного документа через телекомунікаційні мережі загального користування здійснюється за рішенням керівника цього органу. [3]

У вересні 2015 року Державна служба спеціального зв’язку та захисту інформації України (далі - Держспецзв’язку) видала рекомендації для державних службовців щодо безпечного користування електронними поштовими скриньками під час здійснення службової діяльності.

Держспецзв’язок пропонує неухильно дотримуватися цих рекомендацій, хоча рекомендації є пропозиціями, рішення про впровадження яких приймається на розсуд адресанта таких рекомендацій,

Рекомендації включають такі положення:

- не використовувати неслужбові (неофіційні) електронні поштові скриньки та закордонні публічні поштові сервіси, насамперед російські, для організації службового листування.
- створювати службові поштові скриньки виключно на власних (відомчих) ресурсах, зареєстрованих в доменній зоні українського сегменту Інтернету gov.ua, а за відсутності таких ресурсів користуватися відповідними послугами лише від українських провайдерів.
- не використовувати службові електронні поштові скриньки для здійснення листування з особистих питань, насамперед, при підписці на різноманітні розсилки.
- використовувати складні паролі для службових електронних поштових скриньок (мінімальна довжина паролю 8 символів, наявність літер різного регістру та спецсимволів, «складність» паролю до підбору за словами тощо), а також регулярно їх змінювати (не рідше ніж один раз на місяць).
- не використовувати один пароль для декількох акаунтів, а також він не повинен, бути пов’язаний з особистими даними.
- не зберігати пароль від поштової скриньки у браузері.
- обов’язково перевіряти отримане засобами електронної пошти повідомлення встановленим антивірусним програмним забезпеченням.
- видаляти (не відкриваючи) отримані засобами електронної пошти повідомлення, якщо Вам вони здаються підозрілими, навіть за умови повідомлення антивірусу, що повідомлення чисте. Особливо якщо ви на них не очікуєте.
- якщо відправник відомий, а електронне повідомлення містить не очікувані додатки або посилання, доцільно уточнити інформацію щодо них у відправника.

- у разі виникнення питань (зокрема проблемних), пов’язаних із використанням електронних поштових скриньок, невідкладно звертатись за консультацією до відповідних адміністраторів безпеки відомства.
- вимагати від адміністраторів безпеки відомства регулярно оновлювати прикладне програмне забезпечення, що забезпечує функціонування електронної поштової скриньки, та антивірусного програмного забезпечення.

У рамках Держспецзв’язку була створена та функціонує як структурний підрозділ Команда реагування на комп’ютерні надзвичайні події України cert.gov.ua. Експертами cert.gov.ua було розроблено рекомендації щодо безпеки поштового сервісу. Рекомендації можуть бути застосовані для перевірки безпеки інформаційних каналів зв’язку, що застосовуються державними службовцями.

Певні загрози можуть існувати при використанні безкоштовного поштового клієнта. Так, безкоштовні клієнти пропонують недостатньо високий рівень конфіденційності персональних даних користувача. Для максимального усунення цього недоліку можна застосовувати послугу шифрування. Для того, щоб увімкнути режим підтримки цього протоколу, достатньо пошукати «захищений режим» у налаштуваннях браузеру. При цьому в рядку адреси повинно бути вказано «https:» замість «http:».

Окремим документом, що регулює порядок використання поштових клієнтів в міністерствах, інших центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, обласних, Київській та Севастопольській міських держадміністрацій та Секретаріаті Кабінету Міністрів України, є постанова Кабінету Міністрів України «Про електронний обмін службовими документами в органах виконавчої влади» від 17.07.2009 р. № 733 (далі - постанова № 733).

Цей документ у п.3 визначає, що для здійснення електронного обміну службовими документами між зазначеними органами державної влади та Секретаріатом Кабінету Міністрів України створюються електронні поштові скриньки з логіном kabmin_doc@ та відповідним найменуванням поштового серверу. Прикладом такої поштової скриньки може слугувати електронна адреса Державної фіскальної служби України: kabmin_doc@sfs.gov.ua.

Постанова № 733 визначає, що відповідальні особи, які працюють у структурних підрозділах з питань інформаційних технологій апаратів органів виконавчої влади, забезпечують встановлення на відповідних комп’ютерах програми електронної пошти, антивірусних програмних засобів та пристроїв для сканування документів, підготовлених у паперовому вигляді, а також функціонування електронної пошти, поновлення її адреси. .[4]

Для обслуговування цієї поштової адреси в органах виконавчої влади визначаються особи, що відповідають за здійснення електронного обміну службовими документами (далі - відповідальні особи), - по два працівники у службах, що забезпечують діяльність керівників органів виконавчої влади, і у структурних підрозділах з питань інформаційних технологій апаратів органів виконавчої влади. Секретаріат Кабінету Міністрів України формує загальний перелік відповідальних осіб органів виконавчої влади із зазначенням адрес електронної пошти вищевказаних органів, постійно уточнює такий перелік і забезпечує його надсилання органам виконавчої влади та структурним підрозділам секретаріату.

1.3 Загрози пов’язані з використанням електронної пошти

Більшість проблем, з якими зіштовхуються користувачі електронної пошти (спам, віруси, різноманітні атаки на конфіденційність листів і т.д.), пов'язані з недостатнім захистом сучасних поштових систем.

З цими проблемами доводиться мати справу і користувачам загальнодоступних публічних систем, і організаціям. Практика показує, що одномоментне вирішення проблеми захисту електронної пошти неможливо. Спамери, творці і вірусів, хакери винахідливі, і рівень захисту електронної пошти, цілком задовільний вчора, сьогодні може виявитися недостатнім. Для того щоб захист електронної пошти був на максимально можливому рівні, а досягнення цього рівня не вимагало надмірних зусиль і витрат, необхідний систематичний і комплексний, з урахуванням усіх загроз, підхід до вирішення даної проблеми.

Спам та віруси

Спам - масове розсилання кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів. [5]

Види спаму:

- реклама - цей різновид спаму трапляється найчастіше. Деякі компанії рекламують свої товари чи послуги за допомогою спаму. Вони можуть розсилати його самостійно, але частіше замовляють це тим компаніям (чи особам), які на цьому спеціалізуються. Привабливість такої реклами в її порівняно низькій вартості і досить великому охопленню потенційних клієнтів.

Донедавна зовсім не було законів, які б забороняли чи обмежували таку діяльність. Тепер робляться спроби розробити такі закони, але це досить важко зробити. Складно визначити в законі, яка розсилка законна, а яка ні. Найгірше, що компанія (чи особа), що розсилає спам, може знаходитися в іншій країні. Для того, щоб такі закони були ефективними, необхідно погодити законодавство багатьох країн, що в найближчому майбутньому майже нереально. Проте в США, де такий закон уже прийнятий, є спроби притягнення спамерів до суда.

- вимагання грошей у одержувача листа

Іноді спам використовується для того, щоб виманити гроші в одержувача листа. Такий лист містить повідомлення про те, що одержувач листа може одержати якимось чином велику суму грошей, а відправник може йому в цьому допомогти. Потім відправник листа просить перерахувати йому трохи грошей: наприклад, для оформлення документів чи відкриття рахунку. Виманювання цієї суми і є метою шахраїв.

- фішинг

Інший спосіб шахрайства за допомогою спаму одержав назву «фішинг» (англ. phishing від fishing - рибальство). В цьому разі спамер намагається виманити в одержувача листа номер його кредитних карток чи паролі доступу до електронних платіжних систем тощо. Такий лист, зазвичай, маскується під офіційне повідомлення від адміністрації банку. У ньому говориться, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде

заблоковано, і наводиться адреса сайту, який належить спамерам, із формою, яку треба заповнити. Серед даних, що потрібно повідомити, є й ті, котрі потрібні шахраям.

Інші види спаму:

- розсилання листів релігійного змісту.
- масове розсилання для виведення поштової системи з ладу (відмова сервісу).
- масове розсилання від імені іншої особи, з метою викликати до неї негативне ставлення.
- масове розсилання листів, що містять комп'ютерні віруси (для їхнього початкового поширення).

Комп'ютерний вірус - програма, що здатна створювати свої копії, модифіковані копії, які можуть цілком не відповідати оригіналу, і впроваджувати їх у різні об'єкти/ресурси ІТС без відома користувача, й направлена на деструктивну дію. Віруси діють тільки програмним шляхом. Вони, як правило, приєднуються до файлу або проникають всередину файлу. У цьому випадку кажуть, що файл заражений вірусом. Вірус потрапляє в комп'ютер тільки разом із зараженим файлом. Для активізації вірусу потрібно завантажити заражений файл, і тільки після цього вірус починає діяти самостійно. Деякі віруси під час запуску зараженого файлу стають резидентними (постійно знаходяться в оперативній пам'яті комп'ютера) і можуть заражати інші файли та програми, що завантажуються. Інші різновиди вірусів відразу після активізації можуть спричиняти серйозні пошкодження, наприклад, форматувати жорсткий диск. [5]

Види вірусів:

- віруси-невидимки (stealth-віруси) являють собою програми, що перехоплюють звертання ОС до уражених файлів або секторів дисків і „підставляють” замість себе незаражені ділянки інформації. Крім цього, такі віруси при звертанні до файлів використовують досить оригінальні алгоритми, що дозволяють „обдурювати” резидентні антивірусні монітори.

- завантажувальні віруси заражають завантажувальний сектор флоппі-диска або вінчестера (у деяких випадках Master Boot Record – MBR). Для захисту від завантажувальних вірусів досить відключити завантаження з флоппі-диска або CD-ROM в установках BIOS.
- троянські коні - програми, що маскуються під які-небудь корисні додатки (наприклад, утиліти або ж антивірусні програми), але при цьому виконують різні руйнівні дії. Трояни не впроваджуються в інші файли і не мають здатності до самодублювання. У порівнянні з вірусами троянські коні малопоширені, оскільки після запуску вони або знищують себе разом з іншими даними на диску, або знищуються самим постраждалим користувачем.
- логічна бомба - тип троянського коня, що запускається при виконанні визначених дій чи умов. Цьому можуть послужити специфічні зміни у файлі або задана дата і час.
- макровіруси, що вперше з'явилися в 1995 році, сьогодні стали найбільшою проблемою в антивірусній боротьбі. Цей вид вірусів використовує мову VBA (Visual Basic for Application) для зараження документів MS Word, MS Excel, MS Outlook і навіть MS Access. Для того, щоб уберегти себе від макровірусів, необхідно відключити автозапуск макросів при відкритті документів вищезгаданих програм.
- поліморфні віруси - різновид комп'ютерних вірусів, що використовують спеціальні алгоритми для утруднення їхнього пошуку й аналізу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.
- поштова бомба - дуже велике електронне повідомлення або кілька десятків тисяч повідомлень по електронній пошті, що відсилаються на адресу користувача з метою виведення з ладу системи.
- резидентні віруси відрізняються від нерезидентних тим, що після запуску інфікованої програми вони залишаються в оперативній пам'яті комп'ютера. У резидентних вірусів більше можливостей для контролю над комп'ютером і зараженням файлів різних програм.

- хробаки - комп’ютерні програми, що здатні саморозмножуватись, але на відміну від вірусів не заражають інші файли. Хробаки можуть створювати свої копії на комп’ютері або ж копіювати себе на інші комп’ютери в мережі.

Хакери

Найбільш типові засоби, які використовують хакери, для атаки на систему електронної пошти:

- <сніффери>, які являють собою програми, що перехоплюють усі мережні пакети, що передаються через визначений вузол. Сніффери використовуються в мережах на цілком законній підставі для діагностики несправностей та аналізу потоку даних для передачі. З огляду на те, що деякі мережеві додатки, зокрема поштові, передають дані в текстовому форматі (SMTP, POP3 та ін), за допомогою сніффер можна дізнатися текст листа, імена користувачів і паролі.

- IP-спуфінг - можливий, коли зловмисник, що знаходиться усередині організації або поза неї, видає себе за санкціонованого користувача. Атаки IP-спуфінга часто є відправною точкою для інших атак, наприклад, DoS (Denial of Service – Відмова в обслуговуванні). Зазвичай IP-спуфінг обмежується вставкою помилкової інформації або шкідливих команд у звичайний потік переданих по мережі даних. Це відбувається у випадку, якщо головне завдання полягає в отриманні важливого файлу. Однак зловмисник, помінявши таблиці маршрутизації даних і направивши трафік на хибний IP-адресу, може сприйматися системою як санкціонований користувач і, отже, мати доступ до файлів, додатків, і в тому числі до електронної пошти. [6]

Атаки для отримання паролів можна проводити за допомогою цілого ряду методів, і хоча логін і пароль можна отримати за допомогою IP-спуфінга і перехоплення пакетів, їх часто намагаються підібрати шляхом простого перебору з допомогою спеціальної програми.

- man in the middle (Людина в середині) - полягає в перехопленні всіх пакетів, переданих за маршрутом від провайдера в будь-яку іншу частину мережі.

Подібні атаки з використанням сніфферов пакетів, транспортних протоколів і протоколів маршрутизації проводяться з метою перехоплення інформації, отримання доступу до приватних мережевих ресурсів, спотворення переданих даних. Вони цілком можуть використовуватися для перехоплення повідомлень електронної пошти та їх змін, а також для перехоплення паролів та імен користувачів.

1.4 Постановка задачі

Захист кінцевих точок користувачів при роботі з електронною поштою полягає в тому, що організаціям потрібні політики безпеки для електронної пошти, щоб допомогти співробітникам правильно її використовувати, зменшити ризик навмисного або ненавмисного неправильного її використання, і щоб гарантувати, що офіційні документи, які передаються за допомогою електронної пошти, правильно обробляються.

Організування корпоративної пошти на підприємстві є дійовим рішенням, оскільки: виглядає презентабельно перед клієнтами, якщо керівник компанії вирішив зробити пошту на домені своєї компані, це більш безпечніший спосіб обміну інформацією з клієнтами.

Однак до захисту електронної пошти повинні залучатись і звичайні користувачі, оскільки цю проблему неможливо вирішити тільки технічними і програмними засобами, людський фактор відіграє важливу роль у забезпеченні захисту. Задля ефективної та безпечної роботи користувачів з електронною поштою на підприємствах буде прописана інструкція для роботи з електронною поштою.

Політика безпеки для електронної пошти є дуже актуальною і важливою. Вона гарантує використання за призначенням комп'ютерів і телекомунікаційних ресурсів компанії її співробітниками, незалежними підрядниками та іншими користувачами. Всі користувачі комп'ютерів зобов'язані використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись норм етики і дотримуючись законів.

Висновок до першого розділу

Під час розробки цього розділу було виконано:

- розглянуто кібератаки пов’язані з роботою електронної пошти;
- проаналізована статистика кібератак;
- виконано аналіз нормативно - правової бази у сфері електронної пошти;
- розглянуто загрози поштового сервісу;

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Поштові протоколи

В основному протокол відноситься до стандартного методу, що використовується на кожному кінці каналу зв'язку. Щоб мати справу з електронною поштою, повинен використовуватися спеціальний клієнт для доступу до поштового сервера. У свою чергу, вони можуть обмінюватися інформацією один з одним, використовуючи при цьому абсолютно різні протоколи. Найбільш часто використовувані протоколи електронної пошти в Інтернеті це POP3, IMAP і SMTP. Кожен з них має певну функцію і спосіб роботи.

Протокол поштового відділення третьої версії (POP3) - це стандартний протокол, використовуваний для прийому електронної пошти з віддаленого сервера на локальний поштовий клієнт. Остання версія, яка широко використовується це версія 3, звідси і термін «POP3» Дозволяє завантажувати повідомлення на ваш локальний комп'ютер і читати їх, навіть якщо користувач знаходиться в автономному режимі. .[6]

Перевага полягає в тому, що після завантаження ваших повідомлень можна відключити інтернет-з'єднання і прочитати свій e-mail на дозвіллі, не вдаючись до додаткових витрат на зв'язок. З іншого боку, за допомогою цього протоколу ви отримуєте і завантажуєте багато небажаних повідомлень (включаючи спам або віруси). POP, версія 3, підтримує розширення і кілька механізмів аутентифікації. Функції перевірки автентичності необхідні, щоб зловмисники не отримували доступ до повідомлень користувачів. Клієнт POP3 отримує електронну пошту наступним чином:

- підключається до поштового сервера на порту 110 (або 995 для з'єднань SSL / TLS);
- витягує повідомлення електронної пошти;
- видаляє копії повідомлень, що зберігаються на сервері.
- відключається від сервера.

Клієнти POP налаштовані так, щоб сервер міг продовжувати зберігати копії завантажених повідомлень.

Протокол доступу до інтернет-повідомленнями (IMAP) - це протокол отримання повідомлень електронної пошти, який використовується для доступу до неї на віддаленому веб-сервері від локального клієнта. IMAP і POP3 є двома найбільш часто використовуваними протоколами для отримання листів і підтримуються всіма сучасними поштовими клієнтами і веб - серверами. Протокол POP3 передбачає, що ваша адреса електронної пошти доступна тільки з однієї програми, а IMAP дозволяє зробити одночасний вхід відразу з декількох клієнтів. Ось чому IMAP підійде краще, якщо ви збираєтеся отримувати доступ до своєї електронної пошти з різних місць або якщо ваші повідомлення управляються кількома користувачами. Він добре працює навіть при повільному з'єднанні, наприклад, при підключенні за допомогою модему. При спробі прочитати конкретне повідомлення електронної пошти клієнт завантажує дані з сервера. Є можливість створювати і управляти папками або поштовими скриньками на сервері, видаляти повідомлення. Він також оснащений прапорами повідомлень, які вказують, чи було повідомлення прочитано, видалено або отримано. Він дозволяє користувачам виконувати пошук по поштових скриньках сервера. [7]

Налаштування IMAP:

- підключається до поштового сервера через порт 143 (або 993 для з'єднань SSL / TLS);
- витягує повідомлення електронної пошти;
- служить для підключення до закриття програми поштового клієнта і завантаження повідомлень на вимогу.

Протокол Simple Mail Transfer Protocol (SMTP) - це стандартний протокол для відправки електронної пошти через Інтернет. Протокол SMTP використовується агентом передачі пошти (MTA) для доставки електронних повідомлень на певний сервер одержувача. Протокол SMTP використовується для відправки електронної пошти від поштового клієнта (наприклад, Microsoft Outlook, Thunderbird) на сервер електронної пошти. Він також використовується для ретрансляції або пересилання

поштових повідомлень з одного поштового сервера на інший. Це необхідно в разі, якщо у відправника і одержувача є різні постачальники послуг електронної пошти.

SMTP працює в трьох портах:

- порт 25 - це незашифрований порт SMTP за замовчуванням;
- порт 2525 - він відкривається на всіх серверах SiteGround, якщо порт 25 фільтрується (наприклад, вашим інтернет-провайдером), і ви хочете відправляти незашифровані електронні листи за допомогою SMTP;
- порт 465 - він використовується, якщо ви хочете безпечно відправляти повідомлення за допомогою SMTP.

Протокол SMTP використовується агентом передачі пошти (MTA) для доставки електронних повідомлень на певний сервер одержувача. SMTP можна використовувати тільки для відправки електронних листів, а не для їх отримання.

Вибір між IMAP і POP3

Проаналізувавши протоли, вибір препадає між протоколом IMAP та протоколом POP3. Кожен з них має певну функцію і спосіб роботи.

- місце для зберігання інформації на сервері - сервер з обмеженим обсягом пам'яті є одним з основних чинників, тому слід вибирати POP3. Оскільки IMAP залишає повідомлення на сервері, він може споживати простір пам'яті швидше, ніж POP3.
- доступ до пошти - якщо потрібен доступ в будь-який час, то краще зупинитися на IMAP. Є одна вагома причина, по якій IMAP був призначений для зберігання повідомлень на сервері. Він використовується для пошуку повідомлень з декількох пристроїв - іноді навіть одночасно
- синхронізація - ще одна перевага IMAP. Отримання доступу до повідомлень електронної пошти з декількох пристроїв, всі вони повинні відображати будь – які дії, які виконуються.
- ієрархія повідомлень - IMAP дозволяє користувачам організовувати повідомлення в ієрархічному порядку і розміщувати їх у папках, це допомагає користувачам краще організовувати свою кореспонденцію.

- швидкість - POP3 має можливість завантажувати всі поштові повідомлення при підключенні. А IMAP може при необхідності (наприклад, при недостатній кількості трафіку) завантажувати тільки заголовки повідомлень або певні частини і залишати вкладення на сервері. Тому IMAP можна вважати більш швидким.
- завантаження повідомлень - якщо всі повідомлення на сервері повинні завантажуватися кожен раз, то POP3 буде працювати набагато швидше.

Кожен з описуваних протоколів має свої переваги і недоліки. Користувачі, що працюють тільки з однієї машини і використовують веб-пошту для доступу до нових електронних листів, оцінять POP3. Однак користувачі, які обмінюються поштовими скриньками або отримують доступ до своїх електронних листів з різних комп'ютерів, віддадуть перевагу IMAP.

Але протокол IMAP споживає набагато більше ЦП і ОЗУ, особливо коли він виконує процес синхронізації. Фактично високе завантаження процесора і пам'яті може відбутися як на стороні клієнта, так і на стороні сервера, якщо є багато повідомлень для синхронізації. Тому протокол POP3 менш затратний, хоча і менш функціональний. [8]

2.2 Поштові клієнти

Поштовий клієнт, клієнт електронної пошти, емейл-клієнт - комп'ютерна програма, яка встановлюється на комп'ютері користувача і призначена для одержання, написання, відправлення та зберігання повідомлень електронної пошти одного або декількох користувачів (у випадку, наприклад, кількох облікових записів на одному комп'ютері) або декількох облікових записів одного користувача.

Функції поштового клієнта

Великі поштові програми, так звані «все в одному», такі як Mozilla Thunderbird, The Bat! і Microsoft Outlook, сьогодні комбінують роботу MSA, MDA і MRA в одній програмі.

На відміну від поштового сервера, клієнт електронної пошти зазвичай відправляє повідомлення не прямо на відповідний сервер одержувача, а на один і той же поштовий сервер. Зазвичай це поштовий сервер провайдера або компанії.

Відправка пошти найчастіше здійснюється за протоколом SMTP. Клієнт електронної пошти приймає пошту з одного або декількох поштових серверів, часто це той же сервер, котрий слугує для відправки. Прийом пошти зазвичай здійснюється за протоколами POP або IMAP.

Також в функції клієнта електронної пошти може входити: сортування, зберігання повідомлень, пошук по архіву повідомлень, ведення адресної книги, фільтрація прийнятих повідомлень за різними критеріями, конвертація форматів, шифрування, організація інтерфейсів з офісними програмами та інші функції.

З одним комп'ютером можуть працювати кілька користувачів. Кожен з них може мати в поштовому клієнті власні облікові записи ти її налаштування. Для захисту поштових скриньок користувача від несанкціонованого доступу для кожного користувача може бути створене в поштовому клієнті окреме посвідчення. У посвідченні об'єднанні всі облікові записи користувача, його контакти та особисті налаштування. Посвідчення користувача можна захистити паролем для обмеження доступу до нього сторонніх осіб.

Електронні листи, що надійшли на адресу поштової скриньки користувача, накопичуються на віддаленому комп'ютері - сервері електронної пошти, а повідомлення, які користувач підготував для відправлення, тимчасово зберігаються на його комп'ютері. Доставка, як правило, виконується під час запуску поштового клієнта, при зміні посвідчення, а також може виконуватися автоматично через визначений інтервал часу або за командою користувача.

Деякі поштові клієнти надають можливість користувачу перед здійсненням доставки переглядати лише заголовки листів, що містяться в поштовій скриньці, та вибирати, які листи доставити із сервера на комп'ютер клієнта, а які залишити на сервері. Це зменшує трафік - обсяг даних, що передається мережею. Завдяки такій можливості можна запобігти отриманню спама.

До поштових клієнтів можуть бути вбудовані текстові та HTML - редактори для редагування і форматування текстів листів.

У поштових клієнтах передбачено можливість отримувати листи з різних поштових скриньок - як з сайтів веб-пошти, так і з сервера провайдера. Якщо користувач має кілька поштових скриньок, йому не потрібно звертатися до кожної з них окремо для отримання листів. Достатньо створити облікові записи для кожної поштової скриньки. [9]

Можливості поштових програм розширюються шляхом встановленя додаткових модулів - плагінів (англ. plug-in - розширення, приєднання) та додаються в нових версіях програм.

Порівняємо значення деяких властивостей поштових клієнтів Microsoft Outlook, The Bat!, Mozilla Thunderbird та Opera Mail.

Поштовий клієнт Microsoft Outlook

Microsoft Outlook - персональний інформаційний менеджер з функціями поштового клієнта і Groupware компанії Microsoft. На рисунку 2.1 зображено значок Microsoft Outlook

Рисунок 2.1 - Значок Microsoft Outlook

Крім функцій поштового клієнта для роботи з електронною поштою, Microsoft Outlook є повноцінним органайзером, що надає функції календаря, планувальника завдань, записника і менеджера контактів. Крім того, Outlook дозволяє відстежувати роботу з документами пакету Microsoft Office для автоматичного складання щоденника роботи.

Не слід плутати Outlook з продуктом Outlook Express. Outlook Express - це безкоштовний клієнт електронної пошти, вбудований в більшість версій Windows,

випущених в період з 1998 по 2003 роки. У Windows 7 Outlook Express відсутня, і замість нього з сайту можна встановити пакет програм Windows Live Essentials, одним з компонентів якого є програма Windows Live Mail - аналог програми Outlook Express. У Windows Vista аналог Outlook Express називається Пошта Windows.

Outlook може використовуватися як окремий додаток, так і виступати в ролі клієнта для поштового сервера Microsoft Exchange Server, що надає додаткові функції для спільної роботи користувачів однієї організації: загальні поштові скриньки, папки завдань, календарі, конференції, планування і резервування часу загальних зустрічей, узгодження документів. Microsoft Outlook і Microsoft Exchange Server є платформою для організації документообігу, так як вони забезпечені системою розробки призначених для користувача плагінів і скриптів, за допомогою яких можливе програмування додаткових функцій документообігу (і не тільки документообігу), не передбачених в стандартному постачанні.

Доповнення та надбудови

«Диспетчер ділових контактів» - надбудова для MS Office Outlook 2003 поставляється разом з Microsoft Office System 2003. У «Диспетчері ділових контактів» можна управляти діловими контактами, рахунками і можливими продажами, також можуть міститися додаткові відомості (наприклад, вкладення, малюнки, ділові замітки і відомості про продукцію) - це допомагає об'єднувати відомості про ділові контакти з відомостями про зустрічі, завдання, нагадування, а також взаємодіяти з іншими програмами Microsoft Office, наприклад Office Excel 2003. У таблиці 2.1 показано версії Microsoft Outlook.

Таблиця 2.1 - Версії випущені для операційної системи Microsoft Windows:

Версія	Найменування	Дата реліза	Додаткові відомості
8	Outlook 97	16 січня1997	Поширювався у складі Office 97, а також Exchange Server 5.5
8.5	Outlook 98	21 червня 1998	-
9	Outlook 2000	27 липня 1999	Поширювався у складі Office 2000, а 2.1також Exchange Server 2000

Продовження таблиці 2.1

Версія	Найменування	Дата реліза	Додаткові відомості
10	Outlook 2002	31 травня 2001	Поширювався у складі Office XP
11	Outlook 2003	20листопада2003	Поширювався у складі Office 2003
12	Outlook 2007	27 січня 2007	Поширювався у складі Office 2007
14	Outlook 2010	15 липня 2010	Поширювався у складі Office 2010
15	Outlook 2013	29 січня 2013	Поширювався у складі Office 2013
16	Outlook 2016	22 вересня 2015	Поширювався у складі Office 2016

Outlook Store - спеціальна безкоштовна версія Outlook для Windows 8, Windows 8.1 і Windows 10. Робота підтримується тільки з обліковими записами Microsoft, в той час як стандартний outlook з Office підтримує роботу з будь-якими обліковими записами.

Microsoft також випустила кілька версій Outlook під macOS. Після виходу Outlook 98, на платформі Mac його заміняв Microsoft Entourage. Але тепер Microsoft в Microsoft Office: mac 2011 знову замінила Entourage на Outlook. [10]

Поштовий клієнт The Bat!

The Bat! - програма для роботи з електронною поштою для ОС Windows. Розробляється молдавською компанією Ritlabs. На рисунку 2.2 зображено значок The Bat!

Рисунок 2.2 - Значок The Bat!

Можливості

Має багато можливостей для сортування листів, а також володіє системою для підключення додаткових модулів розширення (плагінів), призначених для захисту від спаму і вірусів. Як правило, плагіни можна завантажити з сайту розробників подібних модулів. У програмі є вбудований диспетчер пошти для POP3 серверів.

Безпека

Програма має безліч засобів для забезпечення безпеки листування. Серед них:

- захист поштової скриньки паролем
- шифрування поштової бази
- шифрування і підпис листів за допомогою S / MIME і OpenPGP
- блокування підозрілих зображень
- ігнорування скриптів і виконуваних кодів
- сортувальник листів

В The Bat! можна налаштувати автоматичне сортування листів по заданих параметрах. Програма здатна пересортувати листи по відправнику, адресату, темі, з текстом листа, тегами, розміром листи, пріоритету, датою і іншим параметрам. Серед доступних дій - переміщення, копіювання, експорт, друк листів, видалення, автовідповідь, створення нагадування, запуск зовнішнього застосування. Можливо створювати спільні правила сортування, дійсні для декількох поштових скриньок.

Віртуальні папки

Віртуальні папки спрощують роботу з потоком листів. В The Bat! є можливість створити віртуальні папки і за допомогою фільтрів налаштувати відображення потрібних листів. Віртуальні папки містять не листи, а посилання на них. Таким чином, їх використання дозволяє не витрачати місце, створюючи копії листів.

Шаблони

Доступні шаблони оформлення листів трьох рівнів: для окремого контакту, для листів, створених в певній папці, і для листів, створених в певному ящику. В The

Bat! є і швидкі шаблони, які дозволяють вставити в лист фрагменти заздалегідь набраного тексту. Швидкі шаблони можуть бути загальними для всіх ящиків.

Резервне копіювання

Також в The Bat! є можливість резервного копіювання листів (в загальному резервному файлі або в окремому для кожної поштової скриньки) або папки, адресної книги і налаштувань за запитом користувача або у автоматичному режимі за розкладом. При цьому можлива захист резервної копії паролем і додавання коментарів. [11]

Права доступу

Для кожної поштової скриньки можна встановити адміністраторські і призначені для користувача права доступу. Адміністратор може обмежити права звичайного користувача в налаштуванні програми і доступу до поштових скриньок. У таблиці 2.2 показано версії The Bat!

Таблиця 2.2 - Версії випущені для операційної системи Microsoft Windows:

Версія	Дата реліза	Додаткові відомості
1.0	Березень1997	Перша загальнодоступна версія, була випущена в березні 1997 року. Вона мала підтримку папок, фільтрів повідомлень, можливість перегляду HTML листів без використання Internet Explorer. Також була спеціальна функція Mail Ticker - повідомлення про нові повідомлення.
3.0	Вересень 2004	З'явилася можливість налаштовувати інтерфейс, створювати віртуальні папки, біометрична аутентифікація і підтримка протоколу MAPI для з'єднання з Microsoft Exchange Server.
5.0	Квітень 2011	Покращена підтримка протоколу IMAP, з'явилися нові спливаючі підказки, інформація про папку, завантажувач зображень.
6.5	Липень 2014	З'явився контекстний онлайн-довідник російською мовою, який можна викликати натисканням клавіші F1

Продовження таблиці 2.2

Версія	Дата реліза	Додаткові відомості
6.8	Березень 2015	Виправлені відомі помилки, а також підвищена стабільність роботи програми. Тепер існують дві версії програми: x86 і x64 бітна. Редакція визначається активованим ключем.
7.0	Серпень 2015	З'явилася підтримка технології синхронізації адресних книг CardDAV, а також протоколу EWS для роботи з MS Exchange Server 2007 і вище.
7.3	Вересень 2016	З'явилася підтримка алгоритмів захисту інформації, побудованих на принципах еліптичних кривих (еліптична криптографія) і досконалої прямий секретності (Perfect forward secrecy) в протоколах TLS / SSL.
8.0	Листопад 2017	Програма навчилася паралельно обробляти велику кількість потоків. 64-бітна версія The Bat! для прискорення роботи тепер використовує набір інструкцій AVX-512. З'явилася підтримка моніторів 4K.

Поштовий клієнт Mozilla Thunderbird

Mozilla Thunderbird - безкоштовна кроссплатформенна, вільно поширювальна програма для роботи з електронною поштою і групами новин, а при установці розширення Lightning, і з календарем. На рисунку 2.3 показано значок Mozilla Thunderbird

Рисунок 2.3 - Значок Mozilla Thunderbird

Є складовою частиною проекту Mozilla. Підтримує протоколи: SMTP, POP3, IMAP, NNTP, RSS. Надаються офіційні збірки для Microsoft Windows, macOS, Linux (i386), причому набір можливостей на всіх платформах однаковий. Існують також сторонніх збірок для FreeBSD, Solaris , OpenSolaris, OS / 2. Особливості:

Інтерфейс

Інтерфейс Thunderbird, як і веб-браузера Mozilla Firefox, заснований на технології XUL, розробленої Mozilla Foundation. В результаті призначений для користувача інтерфейс на всіх платформах виглядає так само, як у програм, розроблених для цієї конкретної платформи. Як і Firefox, Thunderbird підтримує візуальні теми. За замовчуванням інтерфейс програми схожий на звичний користувачам Windows інтерфейс поштового клієнта Outlook Express.

HTML

За замовчуванням Thunderbird не вказує жорстко шрифти, якими буде набиратися повідомлення в форматі HTML, вказуючи лише групу шрифтів - пропорційний або моно, що забезпечує найкращу кроссплатформенную сумісність.

Можливість розширення

Thunderbird підтримує зміну тим і установку розширень.

Спам - фільтри

Thunderbird автоматично розпізнає небажану кореспонденцію. Також можна вручну вказувати, які повідомлення є спамом, «навчаючи» подібним чином

програму. Крім того, Thunderbird може зберігати пошту як в окремих папках для кожного ящика, так і в загальній для всіх.

Віртуальні папки

Лист може відображатися в декількох папках заданих користувачем на підставі фільтрів. При цьому реально лист залишається єдиним і не займає зайвого місця, як у випадку, якби в різних папках зберігалися копії одного листа.

Розробка

19 лютого 2008 року в Mozilla Foundation був створений підрозділ Mozilla Messaging, якому доручена розробка і маркетинг продуктів, пов'язаних з передачею повідомлень, включаючи Mozilla Thunderbird.

Після виходу Thunderbird 3.0 (кодове ім'я - Shredder) побачив світло Thunderbird 3.1 під кодовою назвою Lanikai. Він побудований на движку Gecko 1.9.2 і включає функції, які були не готові до виходу третьої версії, а також невеликі зміни в інтерфейсі. Thunderbird 3.1 вийшов 24 червня 2010 року.

Thunderbird 5.0 Beta 1 - вийшов у світ 4 червня 2011, нумерація версій синхронізована з Firefox і Gecko.

Mozilla Thunderbird 45.0:

- додано новий стовпець «Кореспонденти», який об'єднує інформацію про відправника та одержувача.
- покращена підтримка чатів та команд XMPP.
- розширено опції для завдання винятків показу зазначеного в листі зовнішнього контенту.
- додана опція для відображення HTML-форматування у всіх випадках.
- задіяно сервіс OpenStreetmap для показу карт.
- підтримка перевірки орфографії і вибору словника для тесту в темі листа.
- підтримка редагування параметрів відправника в інтерфейсі написання повідомлень.

- у меню, що випадає в режимі редагування додана можливість установки розміру шрифту.
- в режимі редагування натискання Enter тепер призводить за замовчуванням до створення нового параграфа.
- в швидкий пошук і бічну панель з адресною книгою додана можливість пошуку по ніку.
- у меню роботи з заголовком листи додана можливість копіювання імені та адреси.
- підтримка виведення на друк окремих записів адресної книги через вибір відповідного пункту в контекстному меню.
- підтримка OAuth-аутентифікації сервісу Mail.ru.
- можливість використання інтерфейсу Drag & drop для переміщення відразу декількох вкладень в зовнішнє директорію.

Mozilla Thunderbird 52.0:

- нова панель інструментів панелі папок і селектор уявлень папок.
- імпорт настройки з Беккі! Інтернет-пошта.
- можливість копіювання фільтра повідомлень.
- налаштування словника відновлюються при редагуванні чернетки.
- календар: Подія тепер можна створювати і редагувати на вкладці.
- календар: Обробка отриманих пропозицій лічильника запрошень.
- чат: підтримка прямих повідомлень Twitter.

Mozilla Thunderbird 60.3.3:

- thunderbird 60 переніс бази даних безпеки (key3.db, cert8.db на key4.db, cert9.db). Thunderbird 60.3.2 які раніше містили помилку, яка потенційно видаляла збережені паролі і приватні ключі сертифікатів для користувачів, що використовують головний пароль. Версія 60.3.3 запобіжить втрату даних; користувачі, вже оновлені до версії 60.3.2 або раніше, можуть відновити віддалений файл key3.db з резервної копії, щоб завершити міграцію.

- проста текстова розмітка з * для жирного шрифту, / для курсиву, _ для підкреслення і для коду не працює, коли вкладений текст містить символи, відмінні від ASCII.
- при складанні повідомлення посилання не віддалялася, коли місце розташування посилання віддалялося в панелі властивостей посилань.
- проблеми з декодуванням повідомлень з менш поширеними кодуваннями (cp932, cp936). Це буде виправлено у версії 60.4.0.
- доступ CalDav до деяких серверів не працює. Обхід проблеми: встановіть для параметра network.cookie.same-site.enabled значення false.
- чат: Twitter не працює через зміни API на Twitter.com.

Поштовий клієнт Opera Mail

Opera Mail (стара назва M2) - клієнт електронної пошти і новинний клієнт, раніше вбудований в браузер Opera, а тепер є окремою поштовою програмою. На рисунку 2.4 зображений значок Opera Mail.

Рисунок 2.4 - Значок Opera Mail

Його інтерфейс трохи відрізняється від інших поштових клієнтів з метою забезпечення кращої інтеграції з Opera. У ньому є фільтри спаму (автоматичний і той, якого навчають - байесовский (англ. Bayesian, на прізвище автора теореми його імені Томаса Байеса)), підтримка протоколів POP3, IMAP, SMTP і ESMTP, новинних груп, новинних стрічок RSS, Atom і NNTP.

В Opera Mail використовується одна база даних, яка зберігає зміст всіх листів і сортує їх автоматично за кількома параметрами, наприклад, за типом: просто листи і листи з вкладеними файлами. Це забезпечує швидкий доступ до листів. Зміст листа

можна побачити нижче списку входять і в окремому вікні. Також, байесовский фільтр використовується для автоматичного сортування повідомлень за різними параметрами. Всі повідомлення, розташовані в базі даних, доступні за пунктом меню Читати пошту / Received view.

В Opera Mail є функція мінімізації трафіку, яка надає користувачеві доступ тільки до перших рядках листа, а не до всього листа, тим самим скорочуючи споживання трафік. Також одним з головних нововведень з виходом браузера Opera 9.64 є попередній стрічок новин. З його допомогою генерується сторінка, що містить поточну інформацію в розсилці, і користувач може ознайомитися або підписатися на розсилку, використовуючи спеціальну кнопку . Одним з мінусів поштового клієнта з моменту появи була відсутність можливості використовувати форматування при написанні листа. Цей недолік виправлений в Opera 10. Також в 10 версію браузера була вбудована система перевірки правопису.

В Opera Mail також є менеджер контактів і простий IRC-клієнт, що дозволяє користувачеві підключитися до декількох серверів одночасно. Можливо приватне спілкування і передача файлів між користувачами. В чатах можливо змінювати зовнішній вигляд, відредагувавши CSS файл (приклади).

Opera 12 (движок Presto) - остання версія браузера, в яку був вбудований поштовий клієнт. Тепер Opera Mail винесено в окремий додаток.

Тепер після розглянутих поштових клієнтів , зроблено висновки з їх функціональностей, які показані в таблиці 2.3.

Таблиця 2.3 - Аналіз поштових клієнтів

Властивості	Outlook	The Bat!	Mozilla Thunderbird	Opera Mail
Операційна система	Windows,Mac OS	Windows	Windows,Mac OS,Linux	Windows
Безкоштовне отримання нових версій	+	-	+	+

Продовження таблиці 2.3

Властивості	Outlook	The Bat!	Mozilla Thunderbird	Opera Mail
Наявність HTML-редактора	+	+	+	+
Попереднє завантаження заголовків листів	Потрібні плагіни	+	+	-
Перевірка орфографії	+	Потрібно завантаження словника	Потрібно завантаження словника	-
Шифрування повідомлень	+	+	Потрібні плагіни	-
Можливість повідомлення про надходження листів	+	+	+	+

2.3 Конфігурація поштового клієнта

Проаналізувавши таблицю 2.2 ,одним із найкращих поштових клієнтів є Microsoft Outlook. Оскільки:

- цей поштовий клієнт працює на двох операційних системах, якими частіше за все користуються користувачі: Windows та Mac OS;
- користувачі мають можливість безкоштовно отримувати нові версії цієї программи;
- у цього поштового клієнта є наявність HTML – редактора;
- Outlook може використовуватися як окремий додаток, так і виступати в ролі клієнта для поштового сервера Microsoft Exchange Server;
- дозволяє відстежувати роботу з документами пакету Microsoft Office для автоматичного складання щоденника роботи;

- Outlook Store - спеціальна безкоштовна версія Outlook для Windows 8, Windows 8.1 і Windows 10.
- є наявність шифрування повідомлень;

Тому зроблено налаштування поштового клієнта Microsoft Outlook

Для налаштування нового облікового запису потрібно виконати наступні дії:

- з основного робочого вікна програми через меню «Сервис» перейти до пункту «Настройка учетных записей...» для запуску майстра створення облікових записів. Показано на рисунку 2.5

Рисунок 2.5 - Налаштування облікового запису 1 пункт

- після запуску майстра у вкладці «Электронная почта» обрати пункт «Создать..». Показано на рисунку 2.6

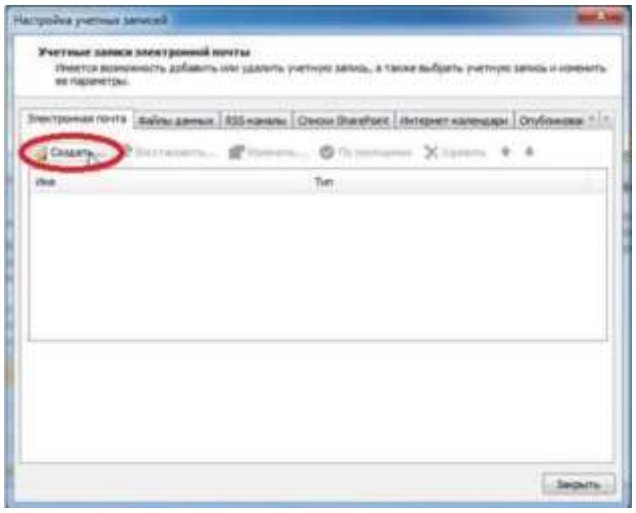

Рисунок 2.6 - Налаштування облікового запису 2 пункт

- при створенні нового облікового запису потрібно обрати одну зі служб електронної пошти, в данному випадку необхідно обрати варіант «Сервер Microsoft Exchange, Pop3, IMAP или HTTP» та натиснути кнопку «Далее >».

Показано на рисунку 2.7

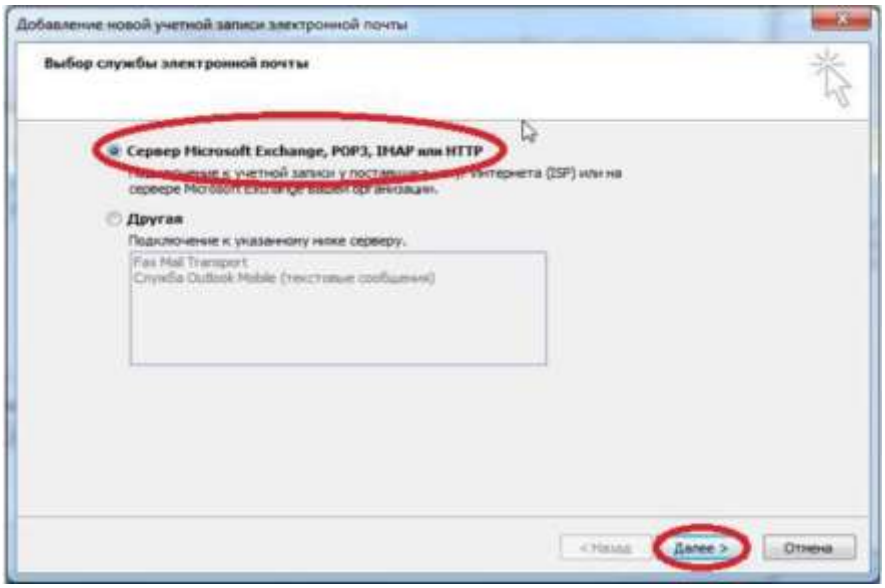

Рисунок 2.7 - Налаштування облікового запису 3 пункт

- в наступному вікні майстра налаштувань потрібно поставити відмінку на пункті «Настроить вручную параметры сервера или дополнительные типы серверов» та натиснути кнопку «Далее >». Показано на рисунку 2.8

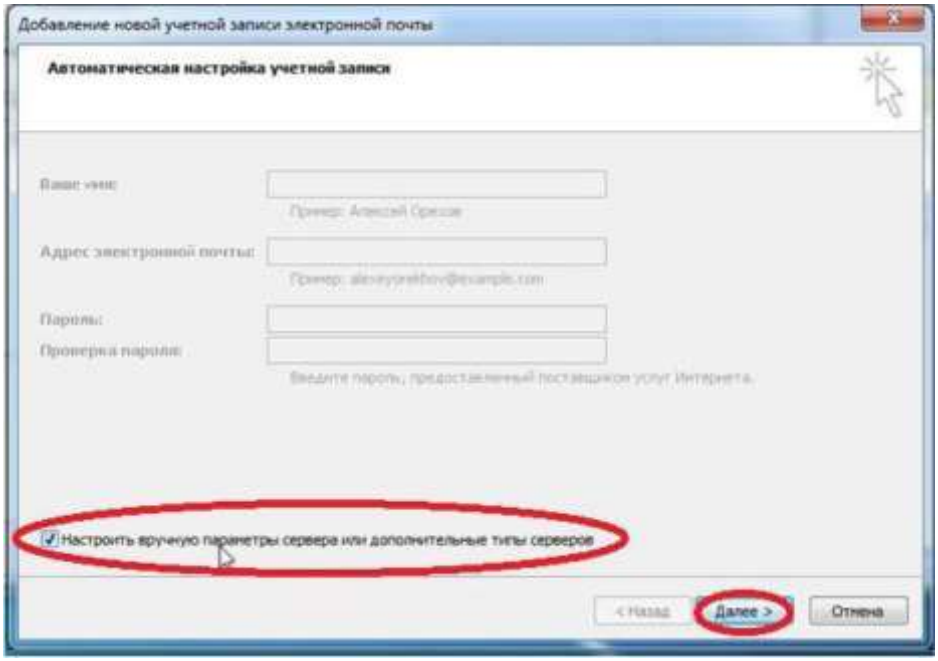

Рисунок 2.8 - Налаштування облікового запису 4 пункт

- у вікні майстра потрібно обрати зі списку службу електронної пошти, яка буде використовуватись. В даному випадку потрібно вибрати варіант «Электронная почта Интернета» та натиснути кнопку «Далее >». Показано на рисунку 2.9

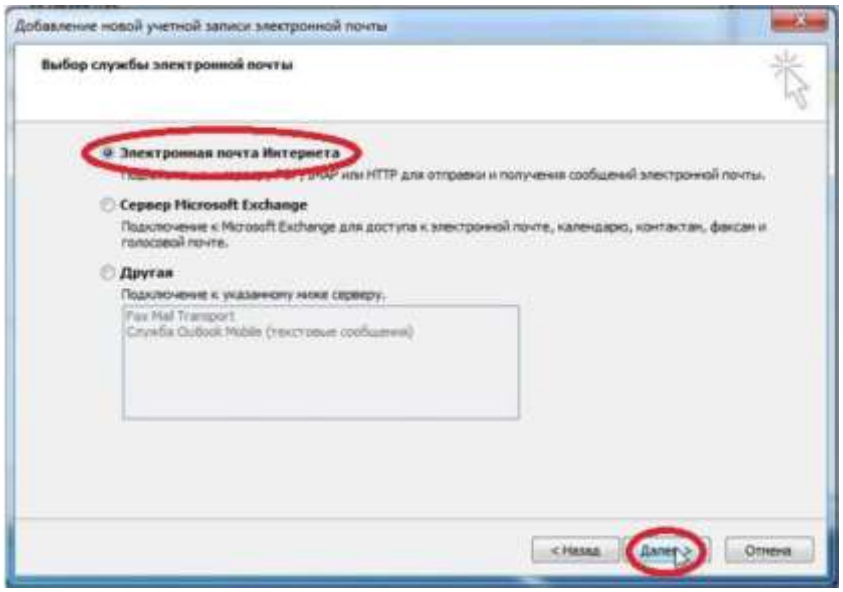

Рисунок 2.9- Налаштування облікового запису 5 пункт

При виконанні наступного кроку потрібно прописати дані, що відповідають особистим обліковим даним користувача. Заповнюються всі поля. Показано на рисунку 2.10

- підрозділ «Сведения о пользователе»:
- «Введите имя» - назва електронної скриньки в довільному вигляді;
- «Адрес электронной почты» - особиста адреса користувача в системы «Укрпост», вводиться в форматі логін@домен;
- підрозділ «Сведения о сервере»:
- «Тип учетной записи» - обрати протокол роботи в заледності від вподобань користувача
- «Pop3» або «IMAP»;
- «Сервер входящей почты» - потрібно вказати адресу серверу з якого будуть завантажуватись листи (для Укрпост потрібно вказати «mail.ukrpost.ua», для не Укрпост - свій домен);

- «Сервер исходящей почты (SMTP)» - потрібно вказати адресу серверу через який буде здійснюватись відправка листів;
- підрозділ «Вход в систему»:
- «Пользователь» - вказати і'мя (Login) користувача поштової скриньки, тобто всі символи назви поштової скриньки що йдуть до знаку «@»;
- «Пароль» - пароль поштової скриньки, при внесенні даних перевірити наявність відмітки
- «Запомнить пароль».

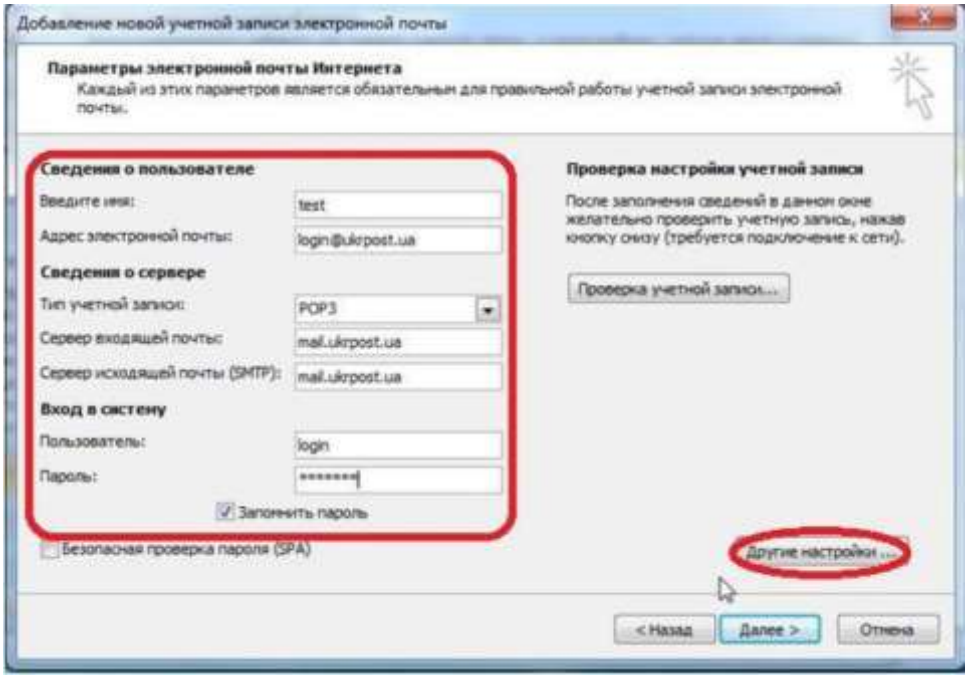

Рисунок 2.10 - Налаштування облікового запису 6 пункт

- після завершення потрібно перейти в розділ «Другие настройки...» натиснувши відповідну кнопку. В цьому розділі перейти до вкладки «Дополнительно» та перевіри правильність прописаних портів Smtp-, Pop3- або IMAP- серверів. Для коректної роботи в полі «Smtp-сервер» потрібно вказати порт 25, в полі «IMAP-сервер» має бути прописано порт 143, в полі «POP3 - сервер» має бути вказано порт 110. Наявність полів «IMAP-сервер» та «POP3-сервер» залежить від того, який тип облікового запису обрано при виконанні попереднього кроку. Показано на рисунку 2.11 та 2.12

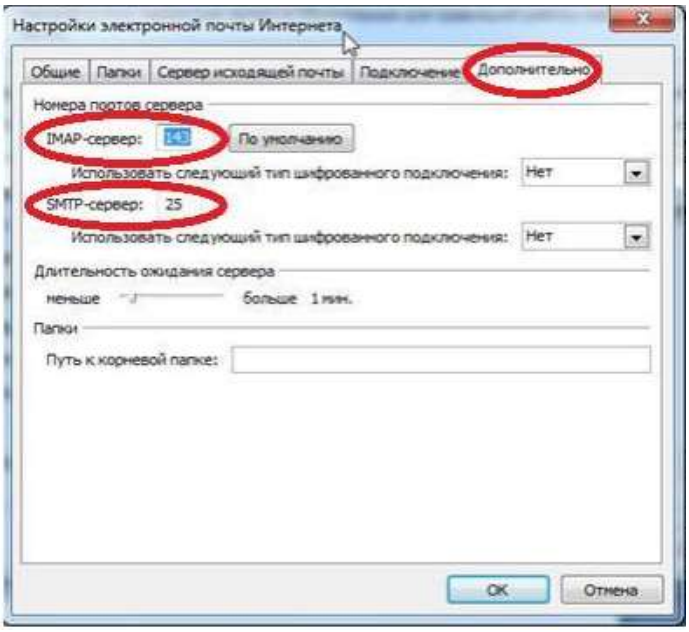

Рисунок 2.11 - Налаштування облікового запису 7 пункт

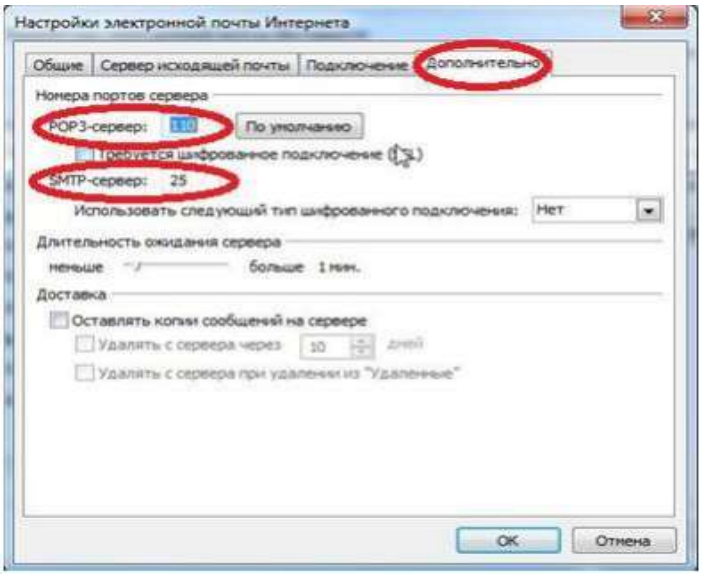

Рисунок 2.12 - Налаштування облікового запису 8 пункт

- в цьому ж розділі перейти до вкладки «Сервер исходящей почты» встановити відмітки «8MTP - серверу требуется проверка подлинности» та «Вход с помощью». Показано на рисунку 2.13

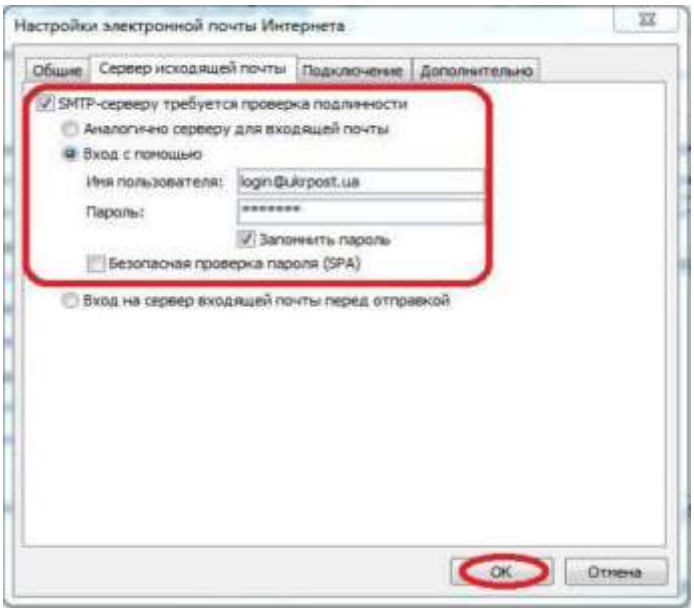

Рисунок 2.13 - Налаштування облікового запису 9 пункт

- після внесення та збереження змін в розділі «Другие настройки...» у вікні «Параметры электронной почты интернет» натиснути кнопку «Далее >» та кнопку «Готово» в наступному вікні. На цьому створення нового облікового запису завершено. Показано на рисунку 2.14 та 2.15.

Рисунок 2.14 - Налаштування облікового запису 10 пункт

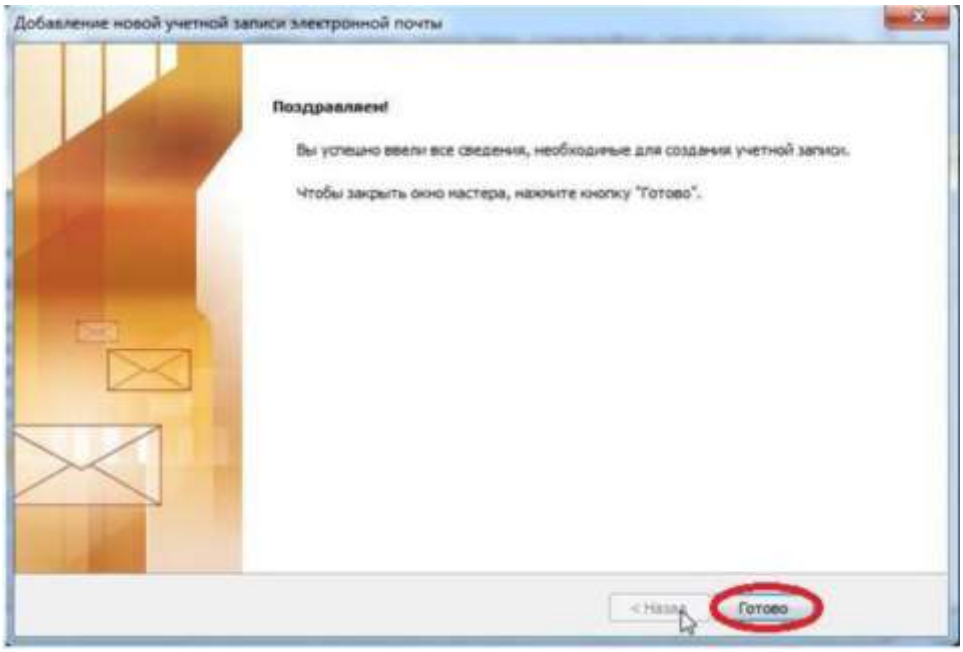

Рисунок 2.15 - Налаштування облікового запису 11 пункт

2.4 Безпека електронної пошти

Кількість користувачів електронної пошти в 2015 році склало приблизно 2,6 млрд чоловік. Очікується, що до 2019 року ця цифра збільшиться до 2,9 млрд. При цьому у багатьох користувачів є не один електронну адресу. І кожен з цих електронних скриньок може бути джерелом інформації для зловмисників. [12]

Отримавши доступ до пошти, шахрай зможе переглянути особисту переписку і провести операції з акаунтами в інших сервісах, зареєстрованих на цю адресу. Тому розглянемо кілька простих способів, які допоможуть уберегти переписку і персональні дані від крадіжки:

- використовуйте двухфакторную аутентифікацію

При цьому потрібно буде вводити пароль двічі: спершу оригінальне кодове слово або поєднання символів, придумане ще при створенні аккаунта, а потім одноразовий пароль, який отримуєте у вигляді текстового повідомлення на телефон кожен раз, коли входите в систему.

Слід пам'ятати про регулярну перевірку даних аккаунта і зміні пароля (для цього потрібно використовувати сервіси генерації паролів). Такі незначні, але вкрай істотні заходи, дозволять виявити злом і перервати доступ зловмисника до аккаунту.

- бути обережними з вкладеннями в листі

Документи форматів pdf, xls і doc відкривати з увімкненим антивірусом, так як вони можуть містити різного роду трояни і інші шкідливі програми. До запуску макросів в цих документах також слід підходити з обережністю.

Ще на поштову скриньку можуть приходити інтерактивні листи, які дозволяють завантаження контенту зі сторонніх серверів. Цим контентом можуть бути як звичайні зображення, так і js-скрипти, тому треба відключити автоматичне завантаження такого вмісту (якщо поштовий клієнт дозволяє це зробити) і включати її вручну для перевірених джерел і відправників.

Також не слід залишати електронну адресу відкритою. Це збільшує шанс потрапляння email в спамерську базу. Але якщо на пошту почали надходити небажані повідомлення, то скористайтеся спам-фільтрами, які входять до складу більшості поштових клієнтів. В якості альтернативи можна звернути увагу на сервіси, фільтруючі надходжену на пошту інформацію.

- використовуйте криптографічні протоколи TLS (SSL) для шифрування листів

Перевіряти чи включено шифрування для конкретного email, можна за допомогою інструменту CheckTLS, ввівши у відповідне поле електронну адресу. Щоб шифрувати електронні листи, можна скористатися і розширеннями для браузерів - наприклад, SecureGmail для Google Chrome і Encrypted Communication для FireFox.

Також шифрувати повідомлення можна за допомогою утиліти Pretty Good Privacy (PGP). Це безкоштовна програма, яка перетворює зміст листа в нісенітницю для всіх крім вас і одержувача. В цьому випадку обидва користувачі - відправник і одержувач - працюють з ключовою парою, що значно ускладнює процес злому повідомлення.

Не варто користуватися електронною поштою, як і будь-якими іншими сервісами з обліковими записами, при підключенні до Wi-Fi-мереж загального користування. Відкриті мережі носять в собі небезпеку, оскільки трафік не шифрується і вразливий для перехоплення - при бажанні зловмисник за допомогою спеціальних програм зможе отримати доступ до інформації.

2.5 Організація корпоративної пошти на підприємствах

Організація корпоративної пошти на підприємствах можлива декількома способами, і в міру зростання компанії всі ці способи можна пройти, або звернутися відразу до самого останнього:

- безкоштовна електронна пошта від поштових сервісів;
- іменна корпоративна пошта на майданчику хостинг-провайдера;
- власний поштовий сервер і іменні поштові корпоративні ящики.

Безкоштовна електронна пошта від поштових сервісів

Це спосіб організації корпоративної пошти, мається на увазі регістрацію і використання поштових скриньок на безкоштовних інтернет ресурсах, таких як gmail.com, ukr.net, i.ua і т.д. [13] Головний плюс - безкоштовно і легко в організації. Але мінусів, на жаль, більше:

- по-перше, страждає імідж компанії - поштові скриньки мають імена з доменними зонами поштових сервісів.Використання таких доменів для корпоративної пошти може викликати сумніви в надійності Вашого бізнесу у Ваших ділових партнерів.
- по - друге, обмеженість імен поштових скриньок - на безкоштовних поштових сервісах зареєстровані мільйони користувачів, що викликає дефіцит імен для електронних поштових скриньок;
- по-третє, обмеженість обсягу поштового сервісу: відсутність можливості тонкої настройки поштових переадресаций, анти-спам фільтрів, автовідповідачів і залежність від стабільності роботи серверів поштових сервісів.

Іменна корпоративна пошта на майданчику хостинг-провайдера

Багато компаній мають власний сайт в інтернеті, що означає наявність доменного імені виду наприклад www.ourcompany.ua і місця на сервері хостинг-провайдера. На сервері розташовується сам сайт, а також можуть розміщуватися корпоративні поштові скриньки типу: @ ourcompany.ua. При такій схемі Ви можете створювати необмежену кількість іменних поштових скриньок.

З такою корпоративною поштою можна працювати як через web-інтерфейс, так і через поштові агенти TheBat, Outlook, Mozilla ThunderBird та інші. Ще один плюс - можливість налаштування всіляких переадресацій, наприклад, пошта приходить на ящик переадресовуваний на всі ящики співробітників організації. Сервера дозволяють управляти антиспам фільтрами, управляти квотами обсягів ящиків. Мінусів не багато: немає фізичного доступу до обладнання сервера, немає можливості тонкої настройки серверів, тому що серверне ПЗ встановлено на сервері хостинг-провайдера.

Для реалізації даного рішення потрібно:

- високошвидкісний інтернет-канал;
- власний фізичний сервер;
- встановлена на сервері операційна система Windows Server або Linux;
- програмне забезпечення для організації поштового сервера, наприклад, MS Exchange Server;
- куплене доменне ім'я;

Власний корпоративний поштовий сервер дає повну свободу дій:

- розширюваність дискового простору;
- створення необмеженої кількості поштових акаунтів з будь-якими іменами і ім'ям компанії;
- можливість тонкої настройки антиспам фільтрів і переадресаций;
- легкість резервного копіювання;
- самостійний контроль надійності серверів;

Мінуси:

- відносно висока вартість рішення - доведеться купити власний сервер і запланувати витрати на його адміністрування;
- залежність як вхідної пошти, так і вихідної пошти від інтернет-каналу, якщо канал буде недоступний - Ви не зможете ні отримувати, ні надсилати листи, але цей мінус не повинен впливати на Ваш вибір, так як Інтернет-провайдери на сьогодні працюють досить стабільно.

Власний поштовий сервер і іменні поштові корпоративні ящики.

Для реалізації даного рішення будуть потрібні:

- високошвидкісний інтернет-канал;
- власний фізичний сервер;
- встановлена на сервері операційна система Windows Server або Linux;
- програмне забезпечення для організації поштового сервера, наприклад, MS Exchange Server;
- куплене доменне ім'я;

Власний корпоративний поштовий сервер дає повну свободу дій:

- розширюваність дискового простору;
- створення необмеженої кількості поштових акаунтів з будь-якими іменами і ім'ям компанії;
- можливість тонкої настройки антиспам фільтрів і переадресаций;
- легкість резервного копіювання;
- самостійний контроль надійності серверів;

Мінуси:

- відносно висока вартість рішення - доведеться купити власний сервер і запланувати витрати на його адміністрування;
- залежність як вхідної пошти, так і вихідної пошти від інтернет-каналу, якщо канал буде недоступний - Ви не зможете ні отримувати, ні надсилати листи;

2.6 Правила використання електронної пошти

Мета

Мета цих правил полягає в донесенні до всіх працівників компанії щодо того, як повинна використовуватися корпоративна електронна пошта. Кінцевою метою є гарантія того, що електронна пошта використовується ефективно для спільної справи без створення додаткового бізнес-ризику або інцидентів.

Область застосування

Всі співробітники компанії, включаючи які працюють за контрактом і тимчасовий персонал, підпадають під дію положень цих правил. Порушення правил

може призвести до дисциплінарних стягнень аж до звільнення. Крім того, дії можуть бути розцінені як протизаконні і в цьому випадку працівник несете особисту повну відповідальність перед законом за вчинені дії.

Загальні принципи

Компанія надає поштову систему співробітникам для організації робочого процесу і доступ до системи надається тільки для цього. Поштові повідомлення отримані або відправлені через корпоративну поштову систему не є приватною власністю, а складають частину внутрішнього документообігу компанії. Використання корпоративної електронної пошти в особистих цілях допустимо, однак обмежується положенням цих правил. Будь-яке приватне використання електронної пошти має виконуватися у вільний від роботи час і не може порушувати хід робочого процесу. Особисте використання електронної пошти не повинно якимось чином впливати на роботу інших співробітників, порушувати роботу електронних систем компанії або псувати репутацію компанії. [14]

Використання електронної пошти

При використанні електронної пошти звертається увага на зміст листів. Будь-які заяви, зроблені в ході електронного листування мають точно таку ж вагу, як і письмові і можуть бути використані проти компанії. Доступ до поштових веб-послуг забороняється з метою зменшення ризику потрапляння вірусів і інших шкідливих програм в корпоративну мережу компанії.

Вкладені файли

Вкладені файли являють собою реальну загрозу зараження вірусом. Багато файлів з даними по складності не поступаються невеликим програмами. Неможливо точно стверджувати, що знаходиться в файлі до тих пір, поки він не відкриється , однак якщо файл заражений - буде вже занадто пізно. Потрібно відсилати документи в форматі RTF. Це дозволяє відсилати текстову інформацію з усім необхідним оформленням, але без можливості впровадження макросів, а значить і без можливості захопити і перенести вірус. [15]

Правила використання електронної пошти

- електронна пошта надається співробітникам організації тільки для виконання своїх службових обов'язків. Використання її в особистих цілях заборонено.
- всі електронні листи, що створюються і зберігаються на комп'ютерах організації, є власністю організації і не вважаються персональними.
- організація залишає за собою право отримати доступ до електронної пошти співробітників, якщо на те будуть вагомі причини. Вміст електронного листа не може бути розкрито, крім як з метою забезпечення безпеки або на вимогу правоохоронних органів.
- конфігурувати програми електронної пошти так, щоб стандартні дії користувача, що використовують установки за замовчуванням, були б найбільш безпечними.
- вхідні листи повинні перевірятися на наявність вірусів або інших шкідливих програм.
- поштові сервера повинні бути налаштовані так, щоб відкидати листи, адресовані не на комп'ютери організації.
- журнали поштових серверів повинні перевірятися на предмет виявлення використаних незатверджених поштових клієнтів співробітниками організації, і про такі випадки повинно доповідатися.
- поштові клієнти повинні бути налаштовані так, щоб кожне повідомлення підписувалося за допомогою цифрового підпису відправника.
- необхідно організувати навчання користувачів правильній роботі з електронною поштою.
- довідники електронних адрес співробітників не можуть бути доступні всім і є конфіденційною інформацією.
- якщо за допомогою електронного листа має бути надіслана конфіденційна інформація або інформація, що є власністю організації, вона повинна бути зашифрована так, щоб її міг прочитати тільки той, кому вона призначена, з використанням затверджених в організації програм і алгоритмів.

- ніхто з відвідувачів, контрактників або тимчасових службовців не має права використовувати електронну пошту організації.
- вся інформація, класифікована як критична або комерційна таємниця, при передачі її через відкриті мережі, такі як Інтернет, повинна бути попередньо зашифрована.
- вихідні повідомлення можуть бути вибірково перевірені, щоб гарантувати дотримання політики безпеки фірми.
- користувачі не повинні дозволяти кому-небудь надсилати листи від чужого імені. Це стосується їх начальників, секретарів, асистентів або інших товаришів по службі.
- організація залишає за собою право здійснювати спостереження за поштовими відправленнями співробітників. Електронні листи можуть бути прочитані організацією, навіть якщо вони були видалені і відправником, і одержувачем. Такі повідомлення можуть використовуватися для обгрунтування покарання.
- в якості клієнтів електронної пошти можуть використовуватися тільки затверджені поштові програми.
- конфіденційна інформація не може бути надіслана за допомогою електронної пошти.
- якщо буде встановлено, що співробітник неправильно використовує електронну пошту з умислом, він буде покараний.
- не можна повідомляти стороннім особам електронні адреси фірми.
- здійснювати масову розсилку не погоджених попередньо електронних листів. Під масовим розсиланням мається на увазі як розсилка безлічі одержувачів, так і множинна розсилка одному одержувачу (спам).
- використовувати не існуючі зворотні адреси при відправці електронних листів.

2.7 Політика використання електронної пошти

Мета

Гарантувати використання за призначенням комп'ютерів і телекомунікаційних ресурсів Компанії її співробітниками, незалежними підрядниками та іншими користувачами. [16] Всі користувачі комп'ютерів зобов'язані використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись норм етики і дотримуючись законів.

Основні положення

- політика визначає вимоги інформаційної безпеки при використанні електронних поштових систем на підприємствах;
- обов'язкове для виконання всіма співробітниками, учасників процесів ІБ, партнерами та третіми сторонами, які використовують поштові системи;
- обов'язкове для виконання усіма контрагентами, що мають підписані угоди або договори про використання послуги серверів електронної пошти, в частині що їх стосується;
- політика підлягає регулярному перегляду з періодичністю 1 раз на рік для приведення системи захисту у відповідність реальним умовам. Може проводитися позаплановий перегляд при зміні переліку вирішуваних завдань, конфігурації технічних і програмних засобів. [17]

Загальні вимоги

- у підприємстві створені і експлуатуються поштові ресурси і системи, призначені для забезпечення обміну електронною поштою між учасниками процесів ІБ і зовнішніми поштовими системами, в тому числі міжнародними.
- послуга електронної пошти на серверах може бути надана іншим державним установам і комерційним організаціям. Умови надання послуги обумовлюються і закріплюються у відповідних угодах або договорах.
- служба ІТ підтримує необхідний рівень безпеки і надійності доставки електронної пошти всередині підприємства і іншим особам через зовнішні мережі в тому числі Інтернет.

- забороняється використовувати сервіс електронної пошти для організації несанкціонованих масових розсилок і спаму.
- забороняється використання електронної пошти в цілях і формах, які суперечать чинному законодавству та іншим нормативним актам.

Вимоги до серверів поштових систем :

- сервера поштових систем, як частина інформаційних ресурсів, повинні захищатися відповідно до необхідного класом захищеності.
- всі поштові повідомлення, що проходять через сервера поштових систем, повинні перевірятися антивірусним програмним забезпеченням, що блокує поширення і передачу шкідливих кодів.
- на серверах поштових систем повинно проводиться регулярне резервне копіювання повідомлень електронної пошти, системних і призначених для користувача даних. Порядок і періодичність проведення резервного копіювання, і терміни зберігання резервних копій визначаються окремо для кожної .
- на всіх серверах поштових систем повинно проводитися журнал системних, прикладних і призначених для користувача дій, подій і помилок. Журнали повідомлень повинні захищатися від несанкціонованого перегляду, модифікації або знищення.
- всі сервера поштових систем повинні мати призначених адміністраторів, що відповідають за функціональність, безпеку і працездатність серверів. На адміністраторів серверів покладається обов'язок реєстрації та зміни ідентифікаційних даних користувачів.
- внутрішні сервера поштових систем повинні бути відокремлені від зовнішніх мереж із застосуванням мережевих технічних засобів і міжмережевого екранування. Обмін повідомленнями та службовою інформацією між внутрішніми і зовнішніми серверами поштових систем здійснюється через контрольовані точки доступу.

Вимоги до сервісу електронної пошти :

- сервіс електронної пошти для співробітників призначений для ведення службової або ділової переписки, використання в технологічних процесах.
- за кожним співробітником, що використовують сервіс електронної пошти, закріплюється свій персональний адрес корпоративної електронної пошти або список адрес.
- заборонено використання чужих ідентифікаційних даних при користуванні сервісом електронної пошти.
- забороняється створення ідентифікаційних записів для сторонніх користувачів або користувачів зовнішніх мереж на внутрішніх серверах поштових систем.
- забороняється використання сервісу електронної пошти в цілях і формах, які суперечать чинному законодавству та іншим нормативним актам або не відповідають загальноприйнятим правилам етики.
- доступ до довідника адрес електронної пошти, які використовуються співробітниками в службових цілях, підлягає обмеженню.
- службові облікові записи, створювані в технологічних цілях для автоматичної розсилки або обробки повідомлень програмними засобами, не повинні надавати можливості реєстрації користувачів з ідентифікаційними даними зазначених облікових записів.
- співробітникам забороняється здійснювати автоматичне пересилання і зберігання службових поштових повідомлень на зовнішніх серверах поштових систем і ресурсах зовнішніх мереж.
- уповноважений орган залишає за собою право ведення моніторингу, протоколювання і проведення вибіркових перевірок характеру використання сервісу електронної пошти співробітниками.
- уповноважений орган залишає за собою право обмежувати співробітникам доступ до поштових ресурсів, розташованим в зовнішніх мережах.
- служба IT розробляє і підтримує в актуальному стані список клієнтських програмних засобів, призначених для використання послуги

електронної пошти всередині підприємства. Всі рекомендовані клієнтські програмні засоби повинні мати відповідні ліцензії на право використання, відповідати вимогам безпеки і інтегрованості з використовуваними інформаційними системами. [18]

Схема організації поштового сервісу повинна підтримувати :

- антивірусний контроль переданих повідомлень;
- фільтрацію небажаних повідомлень (спаму);
- безперервність надання сервісу;
- фільтрацію повідомлень по довільним критеріям;
- архів поштових повідомлень;
- можливість шифрування повідомлень електронної пошти;
- можливість підтвердженням повідомлень електронної пошти електронно - цифровим підписом;
- масштабованість сервісу як за кількістю переданих повідомлень, так і за кількістю користувачів.

Безпека зовнішнього доступу

Величезній загрозі піддається підприємство при використанні Інтернету. Варто захищати ПЗ додатковими модулями для запобігання вторгненню, атаці, просочуванню інформації.

- розробити правила під'єднування до мережі Інетернет;
- проводити регулярне обслуговування для підтримки порядку в загальнодоступних даних;
- системні адміністратори несуть відповідальність за процедури обслуговування серверів, що надають інформацію або послуги користувачам Інтернет;
- користувачі, що мають доступ до Інтернет, повинні заздалегідь пройти програму вчення, де буде роз'яснена політика компанії у сфері безпеки і відповідальність користувачів за представлення компанії в світовій мережі;
- користувачі не повинні пересилати жодної інформації, яка може завдати збитку репутації організації або їх особистої;

- користувачі можуть завантажувати програмне забезпечення Інтернет, яке допоможе їм виконувати свої функції в організації тільки після узгодження з системним адміністратором;
- організація повинна зберегти за собою право блокування доступу до всіх сайтів, які вважаються неприйнятними, а також робити реєстраційні записи про відвідини сайтів всіма користувачами, на підставі яких у будь-який час можна провести аудиторську перевірку;
- розробити архітектуру системи електронної пошти так, щоб забезпечити належну доставку повідомлень як усередині організації, так і в Інтернет. Використання посередницьких програм допускається;
- організація повинна зберігати і архівувати всі повідомлення електронної пошти, які проходять через її сервер. Архів повинен зберігатися на включеному в мережу пристрої, що запам'ятовує;
- адміністратори повинні переносити повідомлення, що архівуються, на автономний пристрій, що запам'ятовує, кожні шість місяців, видаляючи ці повідомлення з оперативних пристроїв, що запам'ятовують. Після закінчення терміну придатності даних, інформація повністю стирається з носіїв без можливості відновлення;
- організація має право сканувати вміст кожного повідомлення електронної пошти, яке проходить через її сервери, на основі заздалегідь встановлених критеріїв. Якщо повідомлення не відповідає критеріям, то воно не повинне доставлятися користувачеві;
- розмір повідомлень електронної пошти, що відправляються і отримуваних користувачами, в цілому, не повинен перевищувати встановленого ліміту. Всі останні випадки обговорюються з адміністратором;
- правило обміну конфіденційною інформацією включає розпорядження шифрувати повідомлення перед їх пересилкою і "підписувати" їх цифровими підписами;

- користувачі не повинні брати участь в розсилці шкідливих послань, що пересилаються по ланцюжку, містять погрози.

Заборонено використання сервісу електронної пошти для передачі повідомлень, що містять інформацію обмеженого доступу.

Для централізованої розсилки інформації співробітникам створюються списки розсилки. Списки розсилки не повинні надавати можливість відправки анонімних повідомлень і повідомлень від імені службових облікових записів. [19]

Для того щоб використовувати політику використання електронної пошти, необхідно розглянути правила безпеки антивірусної системи.

Оскільки антивіруси -потужна зброя з шкідливими програмами. Вони завжди мають бути активними, щоб у будь-який момент захистити програмну, мережу, дані від атаки. Будь-які порушення ходу роботи антивіруса можуть привести до зараження машини і знищення інформації.

- на всіх призначених для користувача системах ще до того, як вони будуть підключені до мережі, слід встановити програмне забезпечення для захисту від вірусів;
- користувачі повинні сприяти оновленню цього програмного забезпечення, а також не повинні відключати ці засоби;
- користувачі не повинні відключати антивірусне програмне забезпечення при запуску завантажуваного з Internet в систему користувача програмного забезпечення;
- користувачі, які завантажують будь-які дані або програми із зовнішнього носія, повинні перед завантаженням сканувати цей носій на предмет наявності на ньому вірусів;
- всі системи, підключені до мережі організації, повинні піддаватися періодичній загальній перевірці на шкідливі програми.

Відповідальність за дотримання положень Політики безпеки.

Категорично заборонена будь-яка поведінка, яка несприятливо відбивається на роботі інших осіб в системах і мережах організації, або яка може нашкодити іншим особам.

Керівництво залишає за собою право досліджувати дані, що зберігаються на всіх комп'ютерах і в мережевих системах, за допомогою засобів фізичного дослідження і електронного моніторингу. Якщо в зібраній інформації виявлені факти порушення правил інформаційної безпеки або закону, то організація може використовувати ці дані для дисциплінарних стягнень або правових санкцій. [20]

- Керівництво має право розірвати контракти і договори з підрядчиками і іншими зовнішніми користувачами, якщо вони порушують розпорядження правив або демонструють поведінку, яка заважає нормальній роботі мережі і комп'ютерних систем підприємства.

Висновок до другого розділу

Під час розробки дипломного проекту було виконано:

- аналіз поштових протоколів;
- проаналізовано найпопулярніші поштові клієнти;
- розглянута конфігурація поштового клієнта Microsoft Outlook;
- виконана рекомендація щодо захисту електронної пошти;
- виконано розробку рекомендацій щодо організації корпоративної пошти на підприємстві;
- розроблено шаблон правил використання електронної пошти;
- розроблені рекомендації щодо політики використання електронної пошти на підприємстві.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою є обґрунтувати економічну доцільність впровадження захисту інформаційної безпеки електронної пошти, порівняємо величину витрат з величиною можливої шкоди, яку може понести підприємство внаслідок втрати інформаційних ресурсів.

3.1 Розрахунок (фіксованих) капітальних витрат

3.1.1. Визначення трудомісткості розробки та опрацювання програмного продукту

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного програміста):

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин,} \quad (3.1)$$

$t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки елементу системи інформаційної безпеки;

$t_{пр}$ – тривалість тестування елементу системи інформаційної безпеки;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті ***Q*** (з урахуванням можливих уточнень у процесі роботи над алгоритмом і програмою).

Умовна кількість операторів у програмі:

$$Q = q \cdot c\ (1 + p), \text{ штук,} \quad (3.2)$$

q – очікувана кількість операторів (вибираємо кількість операторів зважаючи на те, що беремо в приклад невелике підприємство) - 25;

c – коефіцієнт складності програми -1,5 ;

p – коефіцієнт корекції програми в процесі її опрацювання - 0,5.

$$Q = 25 \cdot 1,5\ (1 + 0,5) = 39$$

Тривалість вивчення технічного завдання:

$$t_{\text{в}} = \frac{39 \cdot 1,2}{39 \cdot 1,0} = 0,6 = 1 \text{ година.} \quad (3.3)$$

Тривалість розробки елементу системи інформаційної безпеки

$$t_{\alpha} = \frac{39}{22 \cdot 1,0} = 1,77 = 2 \text{ години} \quad (3.4)$$

Тривалість тестування елементу системи інформаційної безпеки

$$t_{\alpha} = t_{\text{пр}} = 2 \text{ години} \quad (3.5)$$

Тривалість опрацювання програми на ПК

$$t_{\text{опр}} = \frac{39 \cdot 1,5}{4 \cdot 1,0} = \frac{58,5}{4} = 14,6 = 14 \text{ годин.} \quad (3.6)$$

Тривалість підготовки технічної документації на ПЗ

$$t_{\partial} = \frac{39}{17 \cdot 1,0} + \frac{39}{17} \cdot 0,75 = 4 \text{ години} \quad (3.7)$$

$t_{\text{мз}} = 2$ години

$$t = 2 + 1 + 2 + 2 + 14 + 4 = 25 \text{ годин.}$$

3.1.2. Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту *Кпз* складаються з витрат на заробітну плату виконавця програмного забезпечення *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК *Змч*:

$$K_{пз} = З_{зп} + З_{мч} = 2250 + 27 = 2277 \quad (3.9)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{ПР}, \text{ грн,} \quad (3.10)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

$$З_{ЗП} = 25 \cdot 90 = 2250 \text{ грн}$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{\partial}, \text{ грн,} \quad (3.11)$$

$t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot C_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн,} \quad (3.12)$$

де P – встановлена потужність ПК, кВт;

$C_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920.

$$\text{Смч} = 0{,}4 \cdot 1{,}68 + \frac{5000 \cdot 0{,}1}{1920} + \frac{10000 \cdot 0{,}1}{1920} = 1{,}5 \text{ грн}$$

$$з_{мч} = 1{,}5 \cdot (14 + 4) = 7 \text{ грн}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{ПЗ} = 2277 \quad (3.13)$$

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення,

3.2 Розрахунок поточних (експлуатаційних) витрат

$$С = С_з + С_{єв} + С_е + С_{ел}, \text{ грн.} \quad (3.14)$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки (Сз), складає:

$$С_з = З_{дод} = 10000 \cdot 0{,}1 \cdot 12 = 12000 \text{ грн.} \quad (3.15)$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \quad (3.16)$$

Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин.

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 1 \cdot 1728 \cdot 1{,}68 = 2903 \text{грн} \quad (3.17)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації – 22,77грн.

$$С = 12000 + 819{,}6 + 2903 + 2903 + 22{,}77 = 18648 \text{грн}$$

3.3 Оцінка можливого збитку від атаки на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);

- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Вихідні дані:

$t_п$ = 10 годин - час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин ;

$t_в$ = 3 години - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин ;

$t_{ви}$ = 1 година - час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ = 11000 - заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ = 10000 - заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О = 100000 - обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ = 5750 - вартість заміни встаткування або запасних частин, грн;

I = 1 - число атакованих вузлів або сегментів корпоративної мережі;

N = 10 - середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V = 14204 + 11858 + 673 = 26735 \quad (3.18)$$

$П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П = \frac{10000 \cdot 25}{176} \cdot 10 = 14204 \text{ грн} \quad (3.19)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, = 1420 + 4688 + 5750 = 11858 \quad (3.20)$$

$П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ВИ} = \frac{10000 \cdot 25}{176} = 1420 \quad (3.21)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_В = \frac{11000 \cdot 25}{176} \cdot 3 = 4688 \quad (3.22)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_{П} + t_{В} + t_{Ви}) = \frac{100000}{2080} \cdot (10 + 3 + 1) = 673 \quad (3.23)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_п U = 1 \cdot 10 \cdot 31249 = 312490 \quad (3.24)$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C = 312490 \cdot 0{,}1 - 18648 = 12601 \quad (3.25)$$

B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} = \frac{12601}{2277} = 5{,}53 \quad (3.26)$$

E – загальний ефект від впровадження системи інформаційної безпеки , тис. грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = 0{,}18 \text{ років.} \qquad (3.27)$$

Висновок до економічного розділу

Розробка захисту елементів інформаційної безпеки на підприємстві є економічно доцільним, так як витрати на її створення значно менші за суму збитків, завдяки не дорогій системи та мінімальній вартості комплектуючих необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

При цьому ми маємо:

- капітальні витрати склали : К = 2277(грн.);
- поточні витрати склали : С = 18648(грн.);
- величина можливого збитку: В=312490 (грн.);
- загальний ефект від впровадження системи: Е = 12601 (грн.);
- рентабельність інвестицій у безпеку складає: ROSI = 5,53 (частки одиниці);
- термін окупності капітальних інвестицій То = 0,18 (роки).

ВИСНОВКИ

У цій дипломній роботі було розглянуто та проаналізовано:

- основні переваги електронної пошти;
- інциденти кібербезпеки пов’язані з використанням електронної пошти;
- аналіз нормативно - правової бази у сфері електронної пошти;
- було розглянуто і проагалізовані загрози пов’язані з використанням електронної пошти;
- проаналізовано поштові протоколи ;
- поштові клієнти, які є найбільш популярні серед користувачів;
- виконано вибір найкращого поштового клієнта та розроблена рекомендація щодо її конфігурація;
- розроблено шаблон правил використання електронної пошти та розроблені рекомендації щодо політики використання електронної пошти на підприємстві;
- розраховано капітальні та поточні витрати, величина можливого збитку, загальний ефект від впровадження системи, рентабельність інвестицій у безпеку, термін окупності капітальних інвестицій;