МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Юридичний факультет
Кафедра економічної безпеки та фінансових розслідувань

КОВАЛЬЧУК Олександр Володимирович

Загрози, що виникають в результаті застосування шкідливого програмного забезпечення на мобільних пристроях / Threats resulting from using the malicious software on mobile devices

спеціальність: 073 - Менеджмент
магістерська програма – Управління фінансово-економічною безпекою

Магістерська робота

Виконав студент групи
МФЕБм-21
О.В. Ковальчук
_____

Науковий керівник:
к.е.н., доцент Ю.Є. Муравська
_____

Магістерську роботу допущено
до захисту:

«____» _____20__ р.

Завідувач кафедри

_____ **Н.Б. Москалюк**

ТЕРНОПІЛЬ - 2018

ЗМІСТ

ВСТУП

Актуальність теми дослідження. XXI століття, яке вже стало ерою інформаційних технологій, внесло колосальні зміни в життя окремих людей та всього суспільства в цілому. Зросла роль інформації, чисельність людей, задіяних у сфері інформаційних технологій, посилилась загальна інформатизація суспільства, зросла роль телекомунікаційних мереж і персональних комп'ютерів. Усе це привносить позитиви у розвиток комп'ютерних технологій, забезпечує особистості свободу вибору, можливість створювати та використовувати необхідні для життєдіяльності електронні комунікації, кругло добова доступність щодо можливості отримання та відправки інформації. Разом з тим, технічний прогрес надає можливість здійснювати злочини у новий спосіб, з використанням нових знарядь

Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей, вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається. З використанням високошвидкісних мобільних мереж нового покоління, загрози інформаційної безпеки для державних та приватних установ збільшуються, адже для державних та приватних установ збільшуються, адже для зловмисників відкриваються більші технічні можливості, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи, а не тільки для спілкування.

Мета даної магістерської роботи полягає у дослідженні теоретичних та практичних аспектів виявлення шкідливого програмного забезпечення на мобільних пристроях та визначенні правових засад їх нейтралізації та попередження.

Відповідно до поставленої мети було сформульовано такі **завдання**:

– охарактеризувати поняття та види загроз інформаційної безпеки для користувачів сучасних мобільних пристроїв;

- розглянути типи сучасного шкідливого програмного забезпечення на

комп’ютерах та мобільних пристроях;

- охарактеризувати загрози для мобільних пристроїв;

- розглянути відомі технології виявлення ознак шкідливого програмного забезпечення;

- провести аналіз шкідливих програм на мобільних пристроях в контексті мінімізації рівня зараження від їх дії;

- здійснити оцінку рівня захисту інформації на мобільних комп’ютерних пристроях з операційними системами «Android», «Apple iOS» та «Windows»;

- дослідити сучасні методи атак на автоматизовані системи управління військами та інформаційні мережі в зоні антитерористичної операції через мобільні пристрої;

- дослідити технічні та правові питання програмного забезпечення, у тому числі шкідливого (небезпечного) та визначити необхідність застосування кримінальної відповідальності за порушення у сфері створення та розповсюдження шкідливого програмного забезпечення для мобільних пристроїв;

- сформувати систему корпоративної інформаційної безпеки шляхом захисту мобільних пристроїв;

- запропонувати рекомендації щодо запобігання і усунення спроб несанкціонованого доступу до даних та переговорів абонентів мобільного зв’язку;

- удосконалити систему організаційно-правових заходів з метою захисту мобільних пристроїв від шкідливого програмного забезпечення;

- навести обґрунтовані висновки з досліджуваної проблематики.

Об'єктом дослідження є загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв.

Предметом дослідження виступає шкідливе програмне забезпечення на мобільних пристроях як загроза інформаційній безпеці.

Методи дослідження. Методи дослідження, що були використані при написанні магістерської роботи:

- системний підхід (в контексті дослідження технічних та правових питань програмного забезпечення, у тому числі шкідливого (небезпечного) та визначення необхідносі застосування кримінальної відповідальності за порушення у сфері створення та розповсюдження шкідливого програмного забезпечення для мобільних пристроїв);

- припущення (в процесі формування удосконаленої системи організаційно-правових заходів з метою захисту мобільних пристроїв від шкідливого програмного забезпечення);

- абстрагування (при дослідження категорії «шкідливе програмне забезпечення» в контексті інформаційної безпеки);

- аналізу і синтезу (при здійсненні аналізу шкідливих програм на мобільних пристроях в контексті мінімізації рівня зараження від їх дії).

Теоретична й методологічна основа дослідження. Питання інформаційного права та правових засад інформаційної безпеки останніми роками вивчали вітчизняні вчені Аносов А.[1], Батюк А. [2], Войтович О. [6], Війтюк В. [6], Замкова Т. [13], Комич Б. [18], Литвинюк А. [24], Мороз С. [31-34], Муравська (Якубівська) Ю. [35;67-70], Недов Р. [37], Одарченко Р. [41-43], Платоненко А. [1;14;15;47], Федорченко В. [53;65] та ін. Особливої уваги заслуговують праці іноземних вчених, таких, як: Бейкер Л. [75], Брендском А. [77], Гуд Дж. [84], Джонсон М. [84] та інші. Отримані значні результати у напрямку фундаментальних правових досліджень в інформаційній сфері. У своїх працях Аносов А. [1] та Платоненко А. [1;14;15;47] досліджують захист інформації в бездротових мережах. Муравська (Якубівська) Ю. [35;67-70] у своїх працях концептуально підходить до аналізу інформаційної безпеки суспільства. Детальніше до ознак застосування шкідливого програмного забезпечення на мобільних пристроях звертаються Войтович О., Війтюк В., Каплун В. [6] Проте динаміка інформаційних систем і технологій набула нових темпів зростання та якостей. Шаленими темпами зростає інформаційна злочинність, створено сучасне, особливо небезпечне програмне забезпечення, яке використано в економічній, терористичній, військовій, розвідувальній та в

інших сферах. Перебіг подій потребує правового та технічного аналізу їх динаміки та тенденцій нейтралізації загроз, що виникають в результаті застосування шкідливого програмного забезпечення на мобільних пристроях.

Інформаційною базою дослідження є національне та іноземне законодавство, матеріали офіційних сайтів Верховної Ради України, сайту Української міжбанківської асоціації членів платіжних систем «Єма», організацій та установ, публікації провідних науковців у сфері інформаційної безпеки.

Основні результати дослідження, що характеризують його новизну, розкривають зміст магістерської роботи, полягають в тому, що: запропоновано шляхи удосконалення системи організаційно-правових заходів з метою захисту мобільних пристроїв від шкідливого програмного забезпечення.

Практичне значення одержаних результатів. Сформульовані в роботі теоретичні положення та практичні рекомендації можуть бути використані в процесі виявлення, попередження та нейтралізації шкідливого мобільного забезпечення на мобільних пристроях.

Апробація та публікація результатів дослідження. Основні положення та висновки дослідження висвітлювалися у доповіді на тему: «Нейтралізація загроз, що виникають в результаті використання шкідливого програмного забезпечення на мобільних пристроях» та були опубліковані у збірнику «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави».

Зв’язок роботи з науковими програмами, планами, темами. Магістерська робота виконана у відповідності до тематики магістерських робіт кафедри економічної безпеки та фінансових розслідувань Юридичного факультету Тернопільського національного економічного університету.

Структура та обсяг магістерської роботи. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаних джерел зі 100 найменування на 11 сторінках, 1 додатку. Основний текст викладений на 104 сторінках.

РОЗДІЛ І
ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НА МОБІЛЬНИХ ПРИСТРОЯХ ЯК ЗАЗРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

1.1. Поняття та види загроз інформаційної безпеки для користувачів сучасних мобільних пристроїв

Захист інформації на мобільних пристроях є прийняття правових, організаційних та технічних заходів, спрямованих на забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, поширення, та від інших неправомірних дій у відношенні такої інформації, дотримання конфіденційності інформації обмеженого доступу, реалізації права на доступ до інформації.

Розвиток інформаційних технологій на сучасному етапі нерозривно пов’язаний з безпекою інформації та захистом інформації, останнє поняття (захист інформації) є складовою частиною першого (безпека інформації). У свою чергу, вона має дві складові [2, с. 343-344]:

- безпека змістовної частини (смислу) інформації та відсутність у ній спонукальних мотивів людини до негативних дій, умисно закладених механізмів негативної дії на людську психіку, або на інший блок інформації;
- захищеність інформації від зовнішньої дії (спроб неправомірного копіювання, поширення, модифікації, чи знищення).

У цілому проблема інформаційної безпеки на мобільних пристроях включає, поряд із задачами забезпечення захищеності інформації та інформаційних систем, ще два аспекти: захист від дії шкідливої інформації, забезпечення прийняття обґрунтованих рішень з максимальним використанням доступної інформації.

Забезпечення інформаційної безпеки на мобільних пристроях має вирішувати наступні основні задачі [5, с.35]:

- виявлення, оцінка та попередження загроз інформаційним системам та ресурсам;
- захист прав юридичних та фізичних осіб на інтелектуальну власність;
- збирання, накопичення та використання інформації;
- захист державної, службової, комерційної, особистої та інших типів таємниці.

Загрози інформаційним системам та ресурсам для користувачів сучасних мобільних пристроїв можна умовно поділити на основні чотири групи [7]:

1) програмні — впровадження «вірусів», апаратних та програмних закладок; знищення та модифікація даних в інформаційних системах;

2) технічні, у тому числі радіоелектронне, перехоплення інформації у лініях зв'язку, радіоелектронне придушення сигналу у лініях зв'язку та системах управління;

3) фізичні — знищення засобів обробки та носіїв інформації; крадіжка носіїв, а також апаратних чи парольних програмних ключів;

4) інформаційні – порушення регламентів інформаційного обміну; незаконне збирання та використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; дезінформація, укриття чи спотворення інформації; крадіжка інформації з баз даних.

Протистояти цим загрозам можна на основі створення та впровадження ефективних систем захисту інформації від шкідливого програмного забезпечення на мобільних пристроях.

Останнім часом розглядається й обговорюється питання інформаційного протистояння у просторі Інтернету – так звана кібервійна. Вона спрямована насамперед на дестабілізацію інформаційних систем і доступу до Інтернету державних установ, фінансових та ділових центрів, створення безладу та хаосу у державах, які покладаються на Інтернет у повсякденному житті. Міждержавні відношення та політичне протистояння може знаходити своє продовження в Інтернеті у вигляді кібервійни: вандалізму, пропаганді, шпигунстві та

безпосередніх атаках на комп'ютерні системи та сервери, шкідливого програмного забезпечення на мобільних пристроях.

З поширенням інформаційних технологій на мобільних пристроях громадяни, підприємства, державні установи у прямому розумінні стали залежними від мережі Інтернет у повсякденному житті, його використання для атак інформаційних систем іншої держави здатне нанести значні збитки економіці, створити розлад у повсякденне життя держави.

На відміну від кібератак минулого нині кібервійна є загрозою для національної безпеки і сприймається як серйозна загроза національній безпеці. Розвідувальні установи багатьох країн займаються шпигунством в Інтернеті, збирають інформацію, зламують комп'ютерні системи та мережі інших держав, займаються диверсійною діяльністю та економічним шпигунством. Згідно з висновками західних спеціалістів, лідерами у веденні кібервійни нині є Китай та Росія, представники яких категорично заперечують причетність державних установ до організації атак [9, с.60].

Подальший розвиток нових технологій на мобільних пристроях, рівень кібервійни постійно вдосконалюється і підвищує її небезпечність. Певні держави приділяють належну увагу захисту від кібервійни, і виділяють необхідні ресурси для організації систем захисту, підтримують спеціальні підрозділи, задачею яких є підвищення і вдосконалення інформаційної безпеки. Контроль над Інтернетом у наш час визначає стан національної безпеки держави.

У грудні 2012 року у Дубаї (Об'єднані Арабські Емірати) відбувся Міжнародний саміт з питань кіберпростору, на якому дійшли висновку про те, що суперечності, пов'язані з міжнародними телекомунікаціями посилюються. Зокрема, США відмовилися підписати договір, що регламентує право усіх держав здійснювати управлінням Інтернетом, у цьому їх підтримали більше 50 держав світу, зокрема Франція, Велика Британія, Канада. На іншому боці виявилися Російська Федерація, Китай, Індія та інші держави,які наполягають

на рівноправності у глобальній мережі, результатом чого стали досить невтішні висновки цього Саміту [13].

Нині основним документом, який регулює питання міжнародного співробітництва у боротьбі з кіберзлочинністю є «Конвенція про злочинність у сфері комп'ютерної інформації». У ньому сформульовано принципи із забезпечення заходів до боротьби і кіберзлочинністю на національному та міжнародному рівнях. Міжнародне співробітництво сприяє розв'язанню питань у відношенні видачі осіб, які здійснили кібернетичні злочини, загальних принципів взаємної допомоги, конфіденційності та забезпечення збереження інформації, транскордонного доступу до неї тощо [17]. У відповідності з даною Конвенцією, видача осіб іншій стороні можлива за такі типи здійснених кібернетичних злочинів: протизаконний доступ, неправомірне перехоплення, дія на дані функціонування системи, протизаконне використання пристроїв, фальшування та шахрайство з використанням комп'ютерних технологій, правопорушення, пов'язані з дитячою порнографією, порушення авторських та суміжних прав. Допускається також видача осіб іншим державам, у випадку замаху співучасті чи підбурювання до здійснення вищевказаних злочинів. Видача осіб, які здійснили злочини, можлива за наявності у двох сторін передбаченого покарання у вигляді позбавлення волі на максимальний термін не менше одного року.

Важливим документом, у рамках країн-учасниць ООН є «Резолюція з боротьби із злочинним використанням інформаційних технологій», прийнята у 2001 р., у якій вказано на необхідність співробітництва між державами та приватним сектором у боротьба із злочинним використанням інформаційних технологій [50]. Співробітництво у боротьбі із злочинами у сфері інформаційних технологій повинно досягатися шляхом уведення до законодавства відповідальності за інформаційні злочини, транснаціонального співробітництва правоохоронних органів, міжнародного обміну інформацією про проблеми злочинного використання інформаційних технологій, шкідливого програмного забезпечення на мобільних пристроях, навчання співробітників

правоохоронних органів за умови інформаційного суспільства, захисту комп'ютерних систем від несанкціонованого втручання, забезпечення зберігання інформаційних даних та своєчасний збір доказів при розслідуванні злочинів. У п. 1 Резолюції вказано, що інформаційні технології мають розроблятися таким чином, щоб сприяти попередженню та виявленню випадків злочинного використання шкідливого програмного забезпечення на мобільних пристроях, відстежуванню злочинців та збиранню доказів [50]. Цей пункт надає правоохоронним органам окремої країни здійснити виявлення та піймання злочинців у короткий термін з більшою ефективністю. Але існує можливість неправомірного доступу злочинців до вищевказаних технологій з використанням скритих можливостей систем з метою здійснення інформаційних злочинів, наприклад, крадіжка персональних даних.

У 1996 р. країнами Великої Вісімки було прийнято рішення про створення спеціальної підгрупи по боротьбі з міжнародними злочинами у сфері високих технологій — «Ліонська група» [17]. В цей же час глави країн схвалили прийняття плану, що складається з десяти пунктів, по протидії кіберзлочинам. З найбільш важливих пунктів документу, варто відмітити: створення в кожній країні контактного центру, працюючого 24 години в добу, для співпраці у боротьбі з інформаційними злочинами, надання допомоги кваліфікованими співробітниками правоохоронних органів іншим державам, розробку і використання сумісних стандартів для отримання і перевірки достовірності електронних даних у ході судового розслідування, ознайомлення із законодавчими методами боротьби з комп'ютерними правопорушеннями країн-учасниць [20].

На щорічній сесії країн НАТО, що проходила у 2009 р., була підготовлена доповідь — «НАТО і кіберзахист». У доповіді були згадані засадничі принципи, сприяючі ефективному захисту від можливих кібернетичних загроз. Так, на міжнародному рівні, було запропоновано ввести в законодавства країн, такі терміни: «кібервійна», «кібератака», «кібертероризм». Відзначалася необхідність щільнішої співпраці країн з приватними організаціями й Інтернет-

провайдерами для забезпечення захисту. Крім того, у рамках розвитку заходів по кіберзахисту країн НАТО, було рекомендовано сприяти Росії, Китаю, Бразилії і Індії, до швидкого їх приєднання до «Конвенції кіберзлочинність» [19]. Блоком країн НАТО, в Талліні, у 2008 р. був відкритий сучасний центр по проведенню досліджень і навчань в області кіберзахисту і веденню військових дій у кіберпросторі [20].

У рамках співпраці держав-учасників СНД, у 2001 р., було вироблено угоду по боротьбі із злочинами у сфері комп'ютерної інформації, за якою, сторони здійснюють співпрацю у формах обміну інформацією, проведенню розслідувань в області комп'ютерної інформації, сприяння в підготовці кадрів, проведення спільних наукових досліджень, створення інформаційних систем, обміну нормативно-правовими актами і науково-технічної літератури по боротьбі з комп'ютерними злочинами [56]. У документі також вказувалося, що співпраця між країнами СНД здійснюється на підставі запитів компетентних органів про сприяння. Час виконання запиту не повинен перевищувати 30 діб з дня його отримання. Відмова в його виконанні допустима, у разі, якщо його виконання суперечить національному законодавству запрошеної сторони. Російська Федерація прийняла Угоду з обмовкою — відмова у виконанні запиту допустима, якщо його виконання може завдати збитку суверенітету або безпеці РФ [64].

Міжнародне законодавство грає дуже важливу роль у боротьбі з кіберзлочинами. Створення 24/7 контактних центрів, законодавче визначення понять «кіберзлочини», видача осіб, що їх вчинили, міжнародна взаємодія співробітників компетентних органів, проведення навчань та обмін інформацією сприяють здійсненню ефективних методів реагування і боротьби з міжнародними злочинами, що здійснюються в кіберпросторі.

Розвиток сучасних інформаційних технологій для користувачів сучасних мобільних пристроїв має тенденції до все більшого прискорення, тому нормативно-правова база має не тільки встигати за ним, але й змінюватися,

задовольняючи у цьому всі нагальні проблеми людини, суспільства і міжнародного співтовариства у сфері інформаційної безпеки.

1.2. Типи сучасного шкідливого програмного забезпечення на комп'ютерах та мобільних пристроях

Бурхливий розвиток засобів зв'язку та інформаційних технологій визначає тенденції розвитку шкідливих програм на мобільних пристроях зв'язку. Людство вступило в еру цифрових та інформаційних технологій, інформації відводиться велика роль, вона розглядається, як стратегічно важливий ресурс. Удосконалення технології приводить не тільки до зміцнення індустріального суспільства, а і до появи нових, раніше невідомих джерел небезпеки для нього [48, с.4]. Історично одним із перших, найпростіших типів шкідливого програмного забезпечення на мобільних пристроях є класичні віруси. Нині віруси на мобільних пристроях зустрічаються вкрай рідко, їх повністю витіснили будь-які мережеві хробаки та шпигунські програми. Наразі можна нарахувати з десяток активних файлових вірусів з достатньо рідкими сплесками їх активності, які пов'язані з здатністю інфікувати виконувані файли поштових хробаків. Часто з'являються варіанти поштових хробаків типу «Mydoom», «NetSky» чи «Bagle», заражені файловими вірусами «Funlove», «Xorala», «Parite» чи «Spaces».

Основні зусилля вірусодописувачів спрямовані, окрім використання вразливості мережевих технологій, ще й на людський фактор. Кваліфіковане використання соціального інжинірингу часто сприяє поширенню вірусів на мобільних пристроях.

У троянських програмах сьогодні можна прослідкувати наступні тенденції: значне зростання чисельності програм-шпигунів, які викрадають конфіденційну інформацію; прагнення отримати тотальний контроль над інфікованими системами (їх об'єднання у зомбі-мережі, які управляються з єдиного центру). Використання інфікованих систем задля розсилання через них спаму чи

організації DDoS-атак. Більшість установ і організацій використовують мережеві технології, доступ до конфіденційної інформації отримується шляхом використання мережі Інтернет, а особи, зацікавлені у такій інформації, наймають хакерів, чи своїми зусиллями отримують доступ до інформації своїх конкурентів через незахищеність мобільних пристроїв, що підключаються через Wi-Fi до Інтернету.

Нові середовища і можливості шкідливих програм можуть свідчити про ймовірне збільшення чисельності програм, написаних на мові програмування «NET», її популярність неминуче притягне увагу вірусодописувачів. «Linux»-платформи залишатимуться у полі уваги програм класу «rootkit», та найпростіших файлових вірусів. Основна загроза для них виходитиме від виявляння уразливості у програмних продуктах для цієї платформи, які нададуть вірусодописувачам допомогу у досягненні цілей – тотального контролю за значною чисельністю комп'ютерів та мобільних пристроїв у Інтернет. Може зрости кількість шкідливих програм та кількість випадків виявлення вразливості операційної системи «Unix».

Стосовно мобільних технологій слід мати на увазі шкідливе програмне забезпечення для портативних мобільних комп'ютерних пристроїв, сотових телефонів, смартфонів та комунікаторів. Стрімке зростання популярності операційної системи «Windows Mobile 2003/05/06» та «Symbian» широкі можливості мережевої комутації цих засобів та наявність середовища розробки додатків («NET framework») неминуче призведе до появи троянських програм (для «PalmOS» такі вже існують), але й до значно небезпечніших різновидів, включно з варіантом мережевих хробаків [22, с.33]. Найбільшу загрозу безпеці мобільних пристроїв становлять хробаки – віруси, що поширюються самостійно. Хробак здатний викликати надшвидке зараження великої кількості систем, порушити працездатність мобільної мережі, або перетворити її у підконтрольну зловмиснику розподілену мережу.

Стала закономірною поява у 2012 р. мобільних ботнетів на базі мобільних пристроїв з операційною системою «Android». Першою недоброю подією стало

виявлення у січні 2012 р. IRC-бота для «Android», який працював у спаровуванні з смс-трояном. Обидві шкідливі програми названі «Foncy». У дроппері містився також root-експлойт. Усі інфіковані IRC-ботом «Foncy» смартфони залишали потенційний ботнет і були готовими до здійснення будь якої дії за командою «господаря». Того ж року нові шкідливі комп'ютерні програми використовувалися для точкових атак – атаки з використанням «ZitMo» та «SpitMo» («Zeus-« та «SpyEye-in-the-Mobile») [22, с.34].

Цілком очевидно, що найбільш витончені загрози на мобільних пристроях являють собою програми, що досліджують їх вразливі місця.

Шкідливі програми (з англ. - «malicious software» або «malware») – це програми, які призначені для того, щоб чинити шкоду і використовувати ресурси на комп'ютерах або мобільних пристроях, вибраних в якості мішені. Вони часто маскуються в легальних програмах або імітуються під них [8]. В деяких випадках вони розповсюджуються самі по собі, переходячи по електронній пошті або через заражені файли.

Першу групу складають ті програми, що вимагають програм-носіїв. До них, в основному, відносяться фрагменти програм, що не можуть існувати незалежно від програм-носіїв, в ролі яких можуть виступати деякі програмні додатки, утиліти, системні програми. В цю групу входять: люки, логічні бомби, троянські коні, віруси.

У другу групу входять програми, що є незалежними. До них відносяться окремі незалежні програми, які можуть плануватися і запускатися операційною системою. До цієї групи належать: черв'яки, зомбі, утиліти прихованого адміністрування, програми-крадії паролів, «intended»-віруси, конструктори вірусів, поліморфік-генератори.

Крім того, небезпечні програми поділяються на такі, що [22, с.31]:

- не відновлюють себе (не розмножуються). До них відносяться фрагменти програм, які повинні активізуватися під час певних дій головної програми;

- розмножуються - або фрагменти програм (віруси) , або незалежні програми (черв’яки), що здатні під час запуску створювати одну або декілька копій самих себе. Ці копії пізніше також активізуються в цій самій або іншій операційній системі.

Розглянемо їх детальніше. Однак, варто наголосити, що дані види шкідливого програмного забезпечення можуть бути застосовані рівнозначно як для копм’ютерних систем, так і для тих мобільних пристроїв, що використовують окремі операційні системи:

1. «Люк» – це прихована, недокументована точка входу в програмний модуль, яка дозволяє кожному, хто про неї знає, отримати доступ до програми в обхід звичайних процедур, призначених для забезпечення безпеки на мобільних пристроях. Люк вставляється в програму в більшості випадків на етапі налагодження для полегшення роботи – даний модуль можна буде викликати в різних місцях, що дозволяє налагоджувати окремі його частини незалежно одна від одної [98, с.197]. Крім того, люк може вставлятися на етапі розробки для подальшого зв’язку даного модуля з іншими модулями системи, але потім, внаслідок змінених умов, дана точка входу виявиться непотрібною.

Як правило, програміст розробляє програмний додаток, в який входить процедура реєстрації, або який треба довго настроювати, вводячи під час запуску багато значень. Можливо, розробник хоче надати програмі особливі привілеї або мати можливість запобігати процесу налаштування і аутентифікації, або програмісту треба мати в своєму розпорядженні надійний метод, що дозволяє активізувати програму в разі можливих збоїв.

Наявність люка дозволяє викликати програму нестандартним способом, що може серйозно відбитися на стані системи захисту (невідомо, як у такому випадку програма буде сприймати дані, середовище системи, тощо). Крім того, не завжди можна прогнозувати її поведінку.

Люки можуть з’явитися в програмах з таких причин:

- їх забули усунути (необміркований промах);

- для використання при подальшому налагодженні;
- для забезпечення підтримки готової програми;
- для реалізації таємного контролю доступу до даної програми після її встановлення (перший крок до навмисного проникнення на мобільних пристроях з використанням даної програми).

Програмні помилки не є люками. Люк – це механізм налагодження для підтримки і корегування програм. Якщо ж люки використовуються для отримання несанкціонованого доступу, то вони стають загрозою.

Запобігти люкам можна, провівши аналіз початкових текстів програм, міри безпеки повинні прийматися в основному ще на етапі розробки і оновлення програм.

Прикладом люку може слугувати випадок [95], коли при розробці системи «Multics», випробування на проникнення в яку проводилось групою «Tiger team» (команда тигрів) ВПС США, що зображала противника. Один з тактичних ходів полягав в тому, щоб відправити на вузол, працюючий під керуванням «Miltics», підроблену оновлену версію операційної системи. Версія містила в собі троянського коня, якого можна було активізувати за допомогою люка, і який дозволив команді отримати доступ до системи. Загроза була реалізована настільки добре, що розробники системи «Multics» не змогли віднайти її навіть тоді, коли вже знали про її наявність. На той час програма була спрямована на ураження комп’ютерів, однак, зважаючи на стрімкий розвиток технологій, можемо стверджувати, що мобільні пристрої, що співсумісні, наприклад, з операційною системою «Windows» також є потенційною мішенню таких загроз.

2. «Логічні бомби». Це один із самих ранішніх видів програм-загроз. Вони є попередниками вірусів і черв’яків. Логічна бомба – це код, що поміщається в деяку легальну програму. Він влаштований таким чином, що при певних умовах «вибухає». Умовою для включення логічної бомби може бути наявність або відсутність деяких файлів, певний день тижня або певна дата, а також

запуск додатку певним користувачем.

Ось приклад логічної бомби. В одному випадку логічна бомба перевіряла ідентифікаційний номер співробітника компанії, який був автором цієї бомби, і включалась, якщо цей ідентифікатор не фігурував у двох останніх нарахуваннях заробітної плати. «Вибухаючи», бомба могла змінити або видалити дані або файли, стати причиною зупинки машини або щось інше.

Другий приклад. В бібліотечній системі графства Монтгомері (Меріленд) підрядчик, якому доручили розробку комп'ютеризованої абонентської мережі, розмістив в ній логічну бомбу. При настанні певної дати ця бомба могла вивести систему із ладу, якщо замовник відмовлявся платити. Коли ж бібліотека затримала виплату грошей, підрядчик зізнався в існуванні «бомби» і пригрозив, що в разі неперерахування йому грошей він дасть «бомбі» спрацювати [22].

3. «Троянський кінь» («Trojan Horse»). До даної групи шкідливих програм відносять: програми-вандали, «дроппер»-вірусів, «злі жарти», деякі види програм-люків, деякі логічні бомби, програми вгадування паролів, програми прихованого адміністрування.

Останні чотири групи програм можуть і не існувати у вигляді «троянів», а бути цілком самостійними програмними продуктами, що також породжують шкідливі дії в операційній системі.

«Троянський кінь» – це програма, яка виконує на доповнення до основних (проектних і документованих) додаткові, але не описані в документації, дії. «Троянський кінь» – це корисна, або така, що здається корисною, програма або процедура, в якій приховано код, здатний в разі спрацьовування виконати деяку небажану або шкідливу функцію.

Аналогія зі старогрецьким троянським конем, отже, виправдана – і в тому, і в іншому випадку в оболонці, яка не викликає ніякої підозри, існує загроза. Програми такого типу є серйозною загрозою для безпеки інформаційних систем.

«Троянські коні» можуть використовуватись для виконання тих функцій, які несанкціонований користувач не може виконати безпосередньо.

За характером троянський кінь належить до активних загроз, які реалізуються програмними засобами і працюють у пакетному режимі. Троянський кінь є загрозою для будь-якого об'єкта інформаційних систем, причому ця загроза може виражатися будь-яким із способів: безпосередній вплив на об'єкт атаки, вплив на систему дозволів, опосередкований вплив. Найнебезпечнішим є опосередкований вплив, за якого троянський кінь діє в рамках повноважень одного користувача, але в інтересах іншого користувача, особу якого встановити майже неможливо.

Небезпека троянського коня полягає в додатковому блоці команд, встановленому тим чи іншим способом у початкову нешкідливу програму, яка потім пропонується (подарунок, продаж, заміна) користувачам інформаційної системи. Цей блок команд може спрацювати при виконанні деякої умови (дати, часу, або по команді ззовні). Той, хто запускає таку програму, створює небезпеку як для себе і своїх файлів, так і для всієї інформаційної системи в цілому. Отже, у деяких випадках логічні бомби також можна віднести до троянських програм.

Найбільш небезпечні дії троянський кінь може виконувати, якщо користувач, який його запустив, має розширений набір привілеїв. У цьому випадку зловмисник, який склав і впровадив троянського коня, а сам цих привілеїв не має, може виконати несанкціоновані привілейовані функції чужими руками. Або, наприклад, зловмисника дуже цікавлять набори даних користувача, який запустив таку програму. Останній може навіть не мати розширеного набору привілеїв, – це не буде перешкодою для виконання несанкціонованих дій.

Наприклад, деякий користувач-зловмисник хоче отримати доступ до файлів іншого користувача. Він пише програму, яка під час запуску змінює права доступу до файлів користувача, який її викликав, таким чином, щоб ці

файли могли прочитати інші користувачі. Далі, помістивши цю програму в загальний каталог і присвоївши їй ім’я, схоже на ім’я якоїсь корисної утиліти, автор програми якимось чином досягає того, щоб потрібний користувач запустив її. Прикладом такої програми може бути програма, яка ніби-то виводить лістинг файлів користувача в потрібному форматі.

Прикладом троянського коня, який важко виявити, може бути компілятор, змінений таким чином, щоб при компіляції вставляти в певні програми (наприклад, програми реєстрації в системі) додатковий код. За допомогою такого коду в програмі реєстрації можна створити люк, що дозволяє автору входити в систему за допомогою спеціального пароля. Такого троянського коня неможливо виявити в початковому тексті програми-реєстрації. Таким чином, і люки можна віднести до програм-троянів.

Троянський кінь - одна з найнебезпечніших загроз безпеці операційних систем. Радикальним способом захисту від цієї загрози є створення замкнутого середовища виконання програм. Бажано також, щоб привілейовані і непривілейовані користувачі працювали з різними екземплярами прикладних програм, які мають зберігатися і захищатися індивідуально. При виконанні цих заходів імовірність впровадження подібних програм буде досить низькою.

У порівнянні з вірусами троянські коні не одержують широкого поширення по досить простих причинах - вони або знищують себе разом з іншими даними на диску, або демаскують свою присутність і знищуються постраждалим користувачем.

До категорії програм-троянів відносять також «програми-вандали». Ці програми, як правило, імітують виконання якої-небудь корисної функції або маскуються під нову версію відомого програмного продукту. При цьому в якості побічного ефекту вони знищують файли, псують каталоги, форматують диски або виконують деякі інші деструктивні дії.

До троянських коней також можна віднести «дроппер»-вірусів - заражені файли, код яких підправлений таким чином, що відомі версії антивірусів не

визначають вірус у файлі. Наприклад, файл шифрується яким-небудь спеціальним чином чи упаковується рідко використовуваним архіватором, що не дозволяє антивірусу встановити факт зараження.

Слід зазначити також «злі жарти» («hoax»). До них відносяться програми, що не заподіюють комп'ютеру чи мобільному пристрою якоїсь прямої шкоди, однак виводять повідомлення про те, що така шкода вже заподіяна, або буде заподіяна за певних умов, або попереджають користувача про неіснуючу небезпеку. До «злих жартів» відносяться, наприклад, програми, що «лякають» користувача повідомленнями про форматування системи (хоча самого форматування насправді не відбувається), детектують віруси в незаражених файлах (так робить відома програма «antitime»), виводять дивні вірусоподібні повідомлення [22, с.34].

До такої ж категорії «злих жартів» можна віднести також свідомо помилкові повідомлення про нові супер-віруси. Такі повідомлення періодично з'являються в електронних конференціях і звичайно викликають паніку серед користувачів.

4. Вірус – це програма. яка може заражати інші програми, змінюючи їх (копіює програму-вірус в програму, яка, в свою чергу, може заразити інші програми).

Біологічно віруси являють собою маленькі уламки генетичного коду (ДНК або РНК), які можуть переймати структуру живих клітинок і хитрістю залучити їх до виробництва тисяч точних копій початкового вірусу. Подібно цьому інформаційний вірус містить в собі рецепт того, як точно відтворити самого себе. Попавши в середовище комп’ютера чи мобільного пристрою, типовий вірус тимчасово бере на себе керування операційної системи і потім, при контакті зараженого комп’ютера чи мобільного пристрою з незараженими програмами, вірус упроваджує в ці програми свою копію. А далі він розповсюджується таким чином через магнітні носії, через мережу.

Вірус може робити те, що робить звичайна програма. Єдина відмінність полягає в тому. що він прикріплюється до іншої програми і приховано

виконується під час роботи програми-керівника.

За час свого існування типовий вірус проходить 4 стадії [40, с.231]:

- фаза спокою. Вірус не діє, а чекає події, яка його активізує. Такою подією може бути настання певної дати, наявність іншого файлу або перевищення певного об'єму диска. Але не всі віруси притримуються цієї стратегії;

- фаза розмноження. Вірус розміщує свою копію в інші програми або в певні системні області. Потім кожна заражена програмам містить клон вірусу, який також коли-небудь почне розмножуватись;

- фаза запуску. Вірус активізується для отримання можливості виконувати функції, для яких його створено. Як і вихід з фази спокою, перехід в фазу запуску може бути спровокований різними системними подіями (у тому числі – перевищення деякої припустимої кількості нових копій вірусу);

- фаза виконання. Вірус виконує свої функції. Ці функції можуть бути безпечними (виведення на екран повідомлення) або заподіювати шкоду (видаляти файли з програмами і даними).

Більшість вірусів робить свою справу, пристосовуючись до операційної системи, в деяких випадках – до певної апаратної платформи., тобто використовують особливості і слабкості операційних систем.

5. «Хробак» - це програма, яка розповсюджується через мережу і не залишає своєї копії на магнітному носії. Він використовує механізм підтримки мережі для визначення вузла, який може бути заражений. Потім за допомогою тих самих механізмів передає своє тіло на цей вузол й або активізується, або чекає для цього певних сприятливих умов.

Мережні програми-хробаки використовують мережні з'єднання, щоб переходити з однієї системи в іншу. Одноразово активізувавшись в системі, хробак може вести себе як вірус, породжувати троянських коней, виконувати інші руйнівні або деструктивні дії.

Для свого самовідтворення хробак використовує деякий транспортний

засіб:

- електронну пошту – хробак розсилає свою копію іншим системам;
- можливості віддаленого запуску програм – хробак запускає свою копію на іншій системі;
- можливості віддаленої реєстрації – хробак входить у віддалену систему під виглядом користувача, а потім за допомогою стандартних команд копіює себе із однієї системи в іншу.

Перед тим, як копіювати себе на якусь систему, мережний хробак може спробувати визначити, чи інфікована ця система. Крім того, в багатозадачній системі він може маскуватися, присвоюючи собі імена системних процесів або якісь інші, які важко помітити системному адміністратору.

Найбільш відомим представником цього класу є вірус «Морріса» (або, вірніше, «хробак Моріса»), який вразив мережу Internet у 1988 році. Найсприятливішим середовищем для розповсюдження хробака є мережа, всі користувачі якої вважаються товаришами і довіряють один одному[22]. Відсутність захисних механізмів якнайкраще сприяє вразливості мережі.

Найкращий спосіб захисту від хробака – вжиття заходів запобігання несанкціонованому доступу до мережі.

Отже, як віруси троянські коні і хробаки на сьогоднішній день є однією із найнебезпечніших загроз інформаційної системи від шкідливого програмного забезпечення на мобільних пристроях. Для захисту від цих різновидностей шкідливих програм необхідно створювати замкнуте середовище виконання програм, розмежовувати доступ до виконуваних файлів, контролювати цілісність виконуваних файлів і системних областей, тестувати придбані програмні засоби.

6. «Зомбі» - це програма, яка приховано під’єднується до інших підключених в Інтернет комп’ютерів чи мобільного пристрою, а потім використовує цей комп’ютер чи мобільний пристрій для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі.

Зомбі використовують при атаках з відмовою в обслуговуванні, які зазвичай направляють проти Web-вузлів. Зомбі розповсюджуються на сотні комп’ютерів та на мобільних пристроїв, що належать не підозрюючим нічого третім особам, а потім використовуються для ураження вибраного в якості мішені Web-вузла за допомогою сильно збільшеного мережного трафіка.

7. «Жадібні» програми - це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його. Доступ таких програм до ресурсів системи призводить до порушення її доступності для інших програм. Безумовно, така атака буде активним втручанням у роботу системи. Безпосередній атаці в більшості випадків піддаються об'єкти системи: процесор, оперативна пам'ять, пристрої введення-виведення.

Багато комп'ютерів та мобільних пристроїв, особливо в дослідницьких центрах, мають фонові програми, які виконуються з низьким пріоритетом. Вони проводять великий обсяг обчислень, а результати їхньої роботи потрібні не так вже часто. Але при підвищенні пріоритету така програма може блокувати решту програм. Ось чому вона є «жадібною». «Тупикова» ситуація виникає тоді, коли «жадібна» програма нескінченна (наприклад, виконує явно нескінченний цикл). Але в багатьох операційних системах існує можливість обмеження часу процесора, який використовується конкретною задачею. Це не стосується операцій, які виконуються залежно від інших програм, наприклад, операцій введення-виведення, що закінчуються асинхронно до основної програми, оскільки час їх виконання не входить у час роботи програми. Перехоплюючи асинхронне повідомлення про закінчення операції введення-виведення і посилаючи знову запит на нове введення-виведення, можна досягти нескінченності програми. Такі атаки називають також асинхронними.

Другий приклад «жадібної» програми - програма, яка захоплює дуже велику ділянку оперативної пам'яті. В оперативній пам'яті послідовно розміщуються, наприклад, дані, які надходять із зовнішнього носія. Врешті-

решт пам'ять може бути сконцентрована в одній програмі, і виконання інших стане неможливим.

8. Захоплювачі паролів - це спеціально призначені програми для крадіжки паролів. Вони виводять на екран терміналу (один за одним): порожній екран, екран, який з'являється після катастрофи системи або сигналізує про закінчення сеансу роботи. При спробі входу імітується введення імені і пароля, які пересилаються власнику програми-захоплювача, після чого виводиться повідомлення про помилку введення і управління повертається операційній системі. Користувач думає, що зробив помилку при наборі пароля, повторює вхід і отримує доступ до системи. Отже, в результаті таких дій його ім'я і пароль стають відомими власнику програми-захоплювача.

Перехоплення пароля може здійснюватися й іншим способом - за допомогою впливу на програму, яка керує входом користувачів у систему, та її наборів даних.

Захоплення пароля є активним, безпосереднім впливом на інформаційну систему в цілому. Для запобігання цій загрозі перед входом в систему необхідно впевнитися, що вводиться ім'я і пароль саме системної програми входу, а не якої-небудь іншої. Крім того, необхідно суворо дотримуватися правил використання паролів і роботи з операційною системою. Слід зауважити, що більшість порушень здійснюється не через хитромудрі атаки, а через елементарну необережність. Не слід вимикати пристрій, доки не будуть закриті всі робочі програми. Необхідно постійно перевіряти повідомлення про дату і час останнього входу і кількість помилкових входів. Ці прості дії допоможуть уникнути захоплення пароля.

Крім описаних вище, існують і інші можливості компрометації паролів. Отже, слід дотримуватись правил, які рекомендуються для створення і використання паролів. Не слід записувати команди, які містять пароль, у командні процедури, слід намагатись уникати явного повідомлення пароля при запитуванні доступу по мережі, оскільки ці ситуації можна простежити і

захопити таким чином пароль. Не слід використовувати один і той самий пароль для доступу до різних вузлів. Рекомендується частіше змінювати пароль. Дотримання правил використання паролів - необхідна умова надійного захисту інформаційної системи від шкідливого програмного забезпечення на мобільних пристроях.

1.3. Характеристика загроз для мобільних пристроїв

Кожен третій житель України (33%) має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – половина (50%). Порівняно з 2015 роком у 2016 році простежується зростання частки таких людей – з 26% до 33% у випадку загального населення і з 41% до 50% у випадку осіб до 50 років. Якщо серед молоді 65% користуються смартфонами, то серед осіб літнього віку – 5%. Типовий користувач смартфонів – це молода особа не старше 40 років з вищою освітою, яка проживає у середніх і великих містах України. Більшість (66%) користуються операційною системою «Android», а 68% користувачів смартфонів мають досвід встановлення додатків. Найбільш популярними є соціальні мережі (73%), ігри (61%), навігація (51%), месенджери (49%) [4].

Нажаль неуважні, або недосвідчені користувачі мобільних пристроїв встановлюють і зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисник може отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, його можливості збільшуються в рази.

Небезпеку для інформації несуть і відкриті Wi-Fi мережі, адже кожен має змогу до них підключитись та виконувати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи

дізнавшись його у працівника. Дані проблеми захисту інформації в бездротових мережах є актуальними та поширеними. Ненадійні паролі зазвичай стають причиною хакерських атак. Після того як зловмисник підключиться до мережі, після проникнення він отримує доступ абсолютно до всіх підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі пристрої також піддаються ризику хакерської атаки. 30% користувачів використовують в якості пароля слово з топ - 10 000 паролів. Збільшення словника до 10 000 000 дасть приріст всього до 33% всіх паролів [38; 44]. Третина всіх паролів, що використовуються, зламуються шляхом банального перебору варіантів зі словника. Список найбільш часто використовуваних паролів зазнав незначних змін за минулі кілька років. Знання користувачів в області інформаційної безпеки дуже обмежені, значне їх число не збирається приділяти час захисту своїх даних: майже 17% облікових записів були захищені паролем «123456».

При цьому паролі розподілені наступним чином:

- 0.5% користувачів використовують в якості пароля password;
- 0.4% користувачів використовують в якості пароля password або 123456;
- 0.9% користувачів використовують в якості пароля password, 123456 або 12345678;
- 1.6% користувачів використовують в якості пароля слово з топ 10 паролів;
- 4.4% користувачів використовують в якості пароля слово з топ 100 паролів 100;
- 9.7% користувачів використовують в якості пароля слово з топ 500 паролів;
- 13.2% користувачів використовують в якості пароля слово з топ 1000 паролів;
- 30% користувачів використовують в якості пароля слово з топ 10 000 паролів.

Застосування таких паролів як «1q2w3e4r» і «123qwe» показує, що деякі користувачі намагаються використовувати непередбачувані поєднання символів для створення захищених паролів, проте їх зусилля як мінімум недостатні. Програми для злому паролів, засновані на словниках, в першу чергу

аналізують такі поширені варіації. У кращому випадку, це збільшить час злому буквально на кілька секунд.

Більша кількість компаній виявляють проблему шкідливого програмного забезпечення на мобільних пристроях протягом одного дня (37,3%). Протягом години це вдається зробити в 11,5% організацій, близько тижня потрібно для 31,5% фірм. Іншим компаніям потрібно більше часу. Збиток, нанесений в результаті кібератаки, виражається переважно в збої системи (58,4%), втрата даних і неавторизований доступ до них також поширені: 25,2% і 14,9% відповідно. Крім того, в результаті дій зловмисників фахівці втрачали час, не могли скористатися необхідним обладнанням, втрачали доступ до зашифрованих зловмисниками даних, несли репутаційні втрати [78]. В свою чергу, кількість сім-карт на ринку України продовжує зменшуватись, незважаючи на продаж великої кількості смартфонів на дві сім-картки (більше 90%) можна зробити висновок, що користувачі стали більше приділяти увагу економії у використанні ресурсів мережі та більш сумлінно відноситись до можливостей своїх пристроїв [62].

Перш за все, всім користувачам, які користуються мобільними телефонами, а особливо смартфонами, дуже важливо розуміти, що той пристрій який вони носять у себе у кишені це повноцінний комп’ютер з функцією постійного доступу до мережі Інтернет, мікрофоном, камерою, GPS-навігатором і приєднаним до нього одним або декількома різними гаманцями. Чому різними, тому що, перш за все, у власника такого пристрою є мобільний рахунок, з якого можна проводити певні платежі на короткі номери чи робити платні дзвінки, а до смартфонів користувачі часто прив’язують власну банківську карту для придбання певних додатків чи інших послуг. Тобто є власний мобільний рахунок у оператора і додатково прив’язана банківська карта. Всі ці рахунки можуть бути використані зловмисникам.

Варто зазначити, що для смартфонів характерні ті ж самі загрози, що і для персональних комп’ютерів, оскільки телефон, по суті, і є комп’ютером. Це обумовлює і можливість запуску шкідливого програмного забезпечення на

мобільних пристроях, і шпигунства за власниками мобільних пристроїв, і крадіжку конфіденційної інформації, крадіжку грошей з мобільних рахунків.

Розглянемо проблему троянської програми для мобільних пристроїв дещо ширше. На жаль, пересічним громадянам властиво не думати про безпеку мобільних пристроїв. І якщо на комп'ютері використання антивірусу є вже нормою, то на мобільних пристроях це все ж ще щось екзотичне. Сьогодні існує величезна кількість загроз: віруси, троянські програми, мережеві хробаки, рекламні модулі орієнтовані на абсолютно різні платформи для мобільних пристроїв.

Навіть є шпигунські програми, які відносяться до класу легальних шпигунських програм. Звертаємо увагу – «легальних» шпигунських програм. Що мається на увазі? Це програми, які можна вільно придбати, у програм є технічна підтримка, власний сайт, офіційний власник, програму можна досить просто видалили з приладу. Подібну програму можна вільно придбати, встановити на пристрій користувача і спокійно за ним стежити. Тобто перехоплювати інформацію про всі здійснені дзвінки, показувати вміст смс - листування, показувати інформацію про відвідувані сайти, знімати за допомогою камери телефону оточуючу ситуацію, визначати місце розташування власника-користувача, сканувати bluetooth чи Wi-Fi оточення, включати мікрофон і записувати інформацію про все навкруги. Встановлення подібного додатку на телефон користувача, по суті, дозволяє шпигувати за ним всюди, адже телефон практично завжди з власником. Слідкувати можна не лише в плані дій в самому телефоні, але і за безпосереднім оточенням користувача – реальним життям, де він перебуваєте, що бачить, що говорить.

З метою кращого розуміння роботи та функціональності шкідливого забезпечення на мобільних пристроях, звернемося до історії розвитку мобільних вірусів. Перші мобільні віруси не можна було навіть назвати повністю вірусами, це були більше шкідливі «смс», тобто на телефон користувача приходило певне «смс» і якщо його відкрити – воно призводило до збою роботи телефону і могло призвести до зависання телефону, була

спроможність «обнулити» телефонну книгу, здійснити певний дзвінок, тобто телефон виконував певну не потрібну користувачу функцію. Далі з'явились реальні віруси і черви. Перші віруси з'явились ще для комунікаторів на «Palm OS», «Windows CE», «Windows Mobile». Далі їм на заміну прийшов «Symbian», для якого також було створено досить багато шкідливих програм, повноцінних хробаків, які мали можливість розповсюджуватись від одного пристрою до іншого використовуючи bluetooth з'єднання і виконувати шкідливі дії. Цікаво, що тоді розповсюдження хробаків було в основному побудовано на методах соціальної інженерії. Наприклад смартфон на базі «Symbian», заражений хробаком, який розповсюджується через bluetooth. Радіус дії bluetooth передачі 10-15 метрів, при цьому автоматичної передачі не відбувається. Тобто заражений смартфон сканував оточення знаходив інші телефони із увімкненим bluetooth і намагався їм розіслати копії себе. Що ж відбувалось на стороні яка приймала? Звичайний користувач перебував у метро чи кафе і бачив на телефоні пропозицію прийняти певний файл. Ця ситуація була не висвітлена у ЗМІ і звичайної цікавості вистачало щоб прийняти файл, тим паче він міг цікаво називатись [47, с.130]. Людина приймала файл, відкривала його із цікавості і якщо приймаючий прилад був на базі «Symbian», хробак активізовувався, заражав пристрій і потім заражав інших, виконуючі нову розсилку.

Перші модифікації вірусу просто розмножувались і наносили певну шкоду, блокуючи деякі додатки у смартфоні. Більш пізніші модифікації хробака вже намагались заробляти кошти зловмисникам, тобто вірус розповсюджувався так само через bluetooth, але вже мав нову функцію – відправка «смс» на платні номери. Для цього зловмисники реєстрували короткі платні номери при відправці «смс» на які з користувача знімаються певні кошти. І троянська програма з зараженого пристрою відправляла «смс», а зловмисники таким чином отримували зиск.

У подальшому мобільні пристрої почали володіти все більшою можливістю з'єднання з Інтернет, спочатку це були WAP та GPRS з'єднання,

потім з’явились «3G» мережі, потім повноцінні Wi-Fi точки практично всюди і зараз є дуже багато місць де не підключаючись через свого GSM оператора можна мати доступ до глобальної мережі через Wi-Fi, який присутній практично всюди: в офісах, метро, кафе, вдома тощо.

Маючи доступ до Інтернету, хробаки отримали можливість перш за все більш швидко розповсюджуватись через електронну пошту, веб-сайти і наносити більш суттєву шкоду, адже вони вже могли не тільки відправляти платні «смс», але й красти дані кредитних карток про акаунти в соціальних мережах, електронній пошті і т.д. Ще раз наголошуємо, що віруси для мобільних пристроїв отримали всі ті властивості, які притаманні класичним шкідливим програмам для персональних комп’ютерів. Для того щоб провести аналогію, можна зазначити, що існує багато троянських програм, які заражаючи телефон, перетворюють його на бота і формують цілу бот-мережу, аналогічно тим про які ми говорили у першій лекції. Існують бот-нети на основі мобільних пристроїв. Так, у 2015 році у Китаї був виявлений бот-нет, який складався із 1,5 мільйона заражених пристроїв. Кожен із цих пристроїв міг або відправити «смс» на певний номер, або провести DDoS-атаку, спам-розсилку. Таким чином DDoS-атаки на сайти можуть проводитись не тільки з заражених комп’ютерів, але й з заражених смартфонів, які по суті є тими самими комп’ютерами, але які ми постійно носимо з собою [47, с.131].

Часто виникає запитання: чи існують віруси для iOS? Чи дійсно такими безпечними є «iPhone» та «iPad» у порівнянні з андроїд пристроями. Насправді, із проведеного нами дослідження можемо сказати, що взагалі класичні віруси для мобільних пристроїв, в основному, не розробляються. Переважно для мобільних пристроїв розробляють троянські програми, рекламні модулі, бекдор програми.

Варто розуміти, що шкідливі програми створюються для всіх операційних систем, на які можна встановити додаткове програмне забезпечення. Тобто якщо у телефон можна встановити додаткові програми, значить туди може потрапити шкідлива програма. Якщо вона не потрапить туди самостійно,

автоматично, то вона може зробити це з допомогою користувача, згадуємо методи соціальної інженерії. Наприклад, власнику чи користувачу мобільного пристрою запропонують встановити цікаву гру, а це виявиться і гра і шкідлива програма. Або взагалі вона не буде маскуватись під гру, а просто почне відправляти «смс» на короткі номери. Тільки пристрої з повною забороною на встановлення додаткового програмного забезпечення є захищеними. Віруси, у широкому сенсі, для «iOS», на жаль, існують і у досить великій кількості.

Тут скоріше стоїть питання яким чином ці шкідливі програми можуть проникнути на мобільний пристрій. І в цьому плані «App Store» дійсно більш захищений ніж «Google Play Market». Але тут є і зворотня сторона. Як правило, користувачі «iPhone» не готові до того що їх прилади можуть заражатись вірусами. Якщо для «Android»-пристроїв хоча б частина юзерів користуються антивірусами, то у разі виникнення епідемії вони можуть бути захищені набагато швидше. Користувачі ж «iOS» пристроїв змушені будуть чекати поки «Apple» випустить оновлення операційної системи, яке усуне вразливість [47, с.131].

Ще один аспект загроз для користувачів мобільних телефонів полягає у моделі роботи з платними послугами, які можуть бути не зовсім зрозумілі користувачу. Тобто користувача можуть ввести в оману, попросивши набрати певний номер, надіслати «смс». У всіх цих випадках з мобільного рахунку знімаються певні кошти. Також дуже популярною є послуга «смс»-підписок, коли користувачу пропонують підписатись на певний сервіс за допомогою «смс». Це може бути все що завгодно: підписка на он-лайн гру, певний сайт, будь-який сервіс, який вимагає регулярну оплату. У подальшому користувач може забути про це. Оскільки він лише один раз погоджується, а потім ініціювання зняття коштів буде відбуватись вже оператором. З користувача періодично буде зніматись певна сума коштів і він цього можете навіть не помічати. Інколи ми просто не пам’ятаємо на що підписалися, а, можливо, і взагалі цього не робили бо це зробила троянська програма. Тому варто бути дуже обережними під час використання коротких «смс» при замовленні послуг

через них. Не варто дзвонити не знайомі номери і уважно контролювати послуги на які здійснюється підписка, бути якомога більш уважними і не користуватись підозрілими сервісами.

Висновки до розділу 1

Інформаційна безпека не несе за собою можливості заробітку, оскільки потребує певних витрат, але завдяки цим витратам можливо захистити установи від значних майбутніх збитків. Враховуючи розвиток та поширення сучасних мобільних пристроїв, зростання їх апаратних можливостей, а також швидкості передачі даних в мережах мобільного зв'язку, для більш ефективного захисту треба бути уважнішим, використовувати перевірене програмне забезпечення, різні паролі для облікових записів, блокування пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати. Необізнаність користувачів та адміністраторів мереж, що призводить до великої ймовірності перехоплення інформації вирішується навчанням правилам інформаційної безпеки.

Ймовірність перехоплення інформації можна зменшити шляхом використання засобів захисту від шкідливого програмного забезпечення на мобільних пристроях в повному обсязі, але проблема відсутності коректного налаштування може залишатись, через використання нестійких паролів. Використовуючи спеціалізоване програмно-апаратне забезпечення є можливість підвищити рівень захисту мереж від зловмисних дій, а правильне налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв. Таким чином важливо поєднувати зусилля в підвищенні обізнаності користувачів фахівцями у галузі інформаційної безпеки, виробниками мобільних пристроїв, провайдерами послуг та технічного забезпечення, адже більшість користувачів, нажаль навіть не замислюється над можливістю того, що їх пристрої можуть піддаватись загрозам.

РОЗДІЛ ІІ
АНАЛІЗ ВПЛИВУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА МОБІЛЬНІ ПРИСТ РОЇ

2.1. Аналіз шкідливих програм на мобільних пристроях в контексті мінімізації рівня зараження від їх дії

Мобільний вірус для телефону або мобільний шкідлива програма – це інформаційний вірус, спеціально адаптований для мобільних пристроїв і телефонів, створений для поширення від одного зарядженого телефону на інший.

Вірус на мобільних пристроях являє собою програмний код, який відтворюється шляхом копіювання на іншу програму. Віруси можуть передаватися у вигляді вкладень в електронну пошту або в файл. Деякі віруси на мобільних пристроях набирають чинності, як тільки їх код виконується, інші віруси можуть перебувати в стані спокою. Вірус, який сам повторно розмножується, як вкладення електронної пошти або як частини мережі повідомлення називається хробак.

Віруси на мобільних пристроях можуть варіювати від легких до дуже складних. Вони можуть брати дані з зараженого телефону або відправляти підроблені повідомлення, нібито від власника телефону. Наскільки поширені мобільні телефонні віруси - ризик заразити мобільний телефон вірусом дуже великий.

Індустрія мобільних пристроїв сприймає загрозу вірусів дуже серйозно і постійно відстежує, свої мережі і робить все, щоб захистити користувачів від будь-яких ризиків мобільних вірусів телефону. Є також деякі прості заходи, щоб користувачі змогли захистити себе від шкідливого програмного забезпечення на мобільних пристроях.

Список відомого шкідливого програмного забезпечення на мобільних пристроях включає в себе не дуже багато найменувань: «Virus», «Trojan»,

«Backdoor», «Dropper», «Downloader», «Tool», «Adware», «Dialer», «Worm», «Exploit», «Rootkit» [49]. Однак, варіацій цих видів програм мільйони. Розглянемо їх детальніше.

Нерідко користувач з подивом дізнається, що в на мобільних пристроях веде активну діяльність вірус або інша шкідлива програма. Відразу виникають питання: «яким шляхом відбулося проникнення?», «чи можна це попередити?» і «як від «шкідника» позбавитися?».

Інтернет-шахраї у гонитві за інформацією, що містить особисті дані користувача, і доступом до систем керування операційною системою на мобільних пристроях, використовують безліч методів. Але основними шляхами зараження комп'ютерів і мобільних пристроїв шкідливим програмним забезпеченням на сьогодні залишаються програмні помилки, уразливості операційної системи і людський фактор.

Стрімкий розвиток сфери інформаційних технологій вимагає втілення нових розробок програмного забезпечення, щоб встигнути обійти конкурентів і завоювати прихильність користувачів. Високий рівень конкуренції обмежує розробників у часі і провокує появу помилок у коді програм, створених поспіхом і недостатньо перевірених на можливість стороннього втручання. Таким чином, з'являються шпарини для впровадження зловмисниками шкідливих програм і отримання несанкціонованого доступу до даних.

Помилки в програмному коді і логіці роботи різних програм породжують появу уразливостей у системі безпеки операційних систем і програмному забезпеченні. Свого часу уразливості поштових клієнтів «Outlook» було використано для проникнення і розповсюдження поштових хробаків «Nimda» і «Aliz» у 2001 році. Швидке розростання мережі Інтернет надає ще більше можливостей для кібершахраїв [55, с.82].

Масове використання на мобільних пристроях однотипних операційних систем дозволяє розробляти варіанти вірусів та інших шкідливих програм, користуючись притаманними їм особливостями. В результаті чого стають можливими епідемії, викликані мережевими хробаками («CodeRed», «Sasse»r,

«Slammer», «Lovesan (Blaster)» - розроблено для операційної системи «Windows», «Ramen» і «Slapper» - для «Linux»), троянськими програмами («Trojan Winlock») тощо.

Сьогодні зараження шкідливим програмним забезпеченням можливе не тільки технічним шляхом. Досить активно для досягнення цієї мети використовуються методи соціальної інженерії (розсилка спаму, фішинг, рекламні банери). Експлуатуючи такі людські якості, як неуважність, цікавість і бажання отримати безкоштовні бонуси, зловмисники провокують з боку користувача дії, що полегшують проникнення шкідливих програм до операційної системи і системних файлів.

Користувач може зіткнутися з тим, що отриманий на електронну скриньку лист пропонує перейти на сайт, де знадобиться введення пароля чи інших особистих даних для вирішення неіснуючих загроз власним фінансовим рахункам у банку або платіжній системі.

Прикладом може бути афера 2015 року [100, с.36], коли тисячі користувачів «eBay» спонукали викласти конфіденційну інформацію шляхом залякування можливим блокуванням особистих акаунтів. Електронні листи з невідомих адрес можуть містити вкладення з безкоштовним софтом, який, насправді, таким не є. Спамові розсилки іноді можна навіть не відкривати для того, щоб запустити шкідливий скрипт, достатньо лише навести курсор на лист. Яскраві рекламні банери, що зазивають на сайти, де можна отримати цікаву й корисну інформацію або доступ до безкоштовних благ, також найчастіше використовуються як пастка для надмірно цікавих користувачів, яка приводить до зараження на мобільних пристроях.

Для того, щоб зменшити загрозу зараження на мобільних пристроях шкідливим програмним забезпеченням, треба дотримуватися заходів безпеки, які включають встановлення антивірусу від перевіреного розробника. Не зайвим буде й перевірка підозрілих файлів за допомогою онлайн-сканеру вірусів. Завжди уважно варто підходити до аналізу отриманої кореспонденції –

не відкривати підозрілі листи з невідомих адрес. Не піддаватися спокусі отримати щось безкоштовно, не маючи для цього ніяких підстав.

Ще один актуальний аспект – викрадення коштів з мобільних пристроїв. Переважна більшість виявлених за останній рік шкідливих програм націлені на крадіжку грошей користувачів. У світі мобільного шкідливого програмного забезпечення, як і раніше, домінують програми, що непомітно надсилають смс-повідомлення на короткі платні номери. Використання смс-троянців залишається для зловмисників найлегшим і найдієвішим способом заробити гроші. Оскільки, будь-який мобільний пристрій, будь то смартфон або звичайний мобільний телефон, безпосередньо пов`язаний з реальними грошима користувача - з його мобільним рахунком. Саме цей «прямий доступ» зловмисники активно використовують.

2010 рік був відзначений появою нових способів крадіжки конфіденційної інформації користувачів і наживи для вірусодописувачів, які створюють шкідливе програмне забезпечення для різних мобільних платформ. Так, одна з виявлених шкідливих програм у фоновому режимі пересилала на номер зловмисника смс-повідомлення, що містять коди аутентифікації для онлайн-банківських операцій. Крім того, вперше за 6 років історії мобільного шкідливого програмного забезпечення було виявлено троянця, який здійснював дзвінки на міжнародні платні номери [60, с.18]. При цьому, як відзначили в компанії, шкідливі програми і атаки в цілому стали складнішими.

Зловмисники стали використовувати різні поєднання вже відомих технологій. Так, за рахунок широкого розповсюдження мобільного Інтернету шкідливі програми дістали можливість взаємодіяти з видаленими серверами зловмисників і одержувати від них оновлення і команди. Такі можливості можуть використовуватися злочинцями для створення мобільних ботнетів. Також змінилося співвідношення різних операційних систем для мобільних пристроїв, у зв`язку з цим змінилася і розстановка сил в середовищі сучасних мобільних шкідливих програм.

Інформація на сьогоднішній день на ринку є товаром, ціна якого може перевищувати мільйони і навіть мільярди доларів. Захист її від зміни, знищення та крадіжки з кожним роком стає все більш складним завданням. Поява на ринку мобільних комп'ютерних технологій не лише спричинила витиснення звичайних персональних комп'ютерів з різних сфер діяльності соціуму, але й призвела до збільшення кількості та появи нових видів кіберзлочиніву вигляді шкідливого програмного забезпечення на мобільних пристроях. Такі злочини часто пов'язані з викраденням персональних даних користувача.

Тому перед компаніями-виробниками та користувачами їх продукції на теперішній час стоїть завдання запровадження ефективного механізму захисту персональних даних, які містяться на мобільних комп'ютерних пристроях.

Мобільний комп'ютерний пристрій – персональний комп'ютер, який може бути зручно транспортований одною людиною і здатний бути швидко увімкнений у робочий стан, найчастіше з автономним живленням, з опціональною можливістю бути підключеним до мережі електроживлення [57, с.89].

Мобільні комп'ютери включають кілька класів комп'ютерів, перелік яких розширюється з розвитком інформаційної техніки. До них відносять: ноутбук або лептоп, нетбук, планшети, трансформери та смартфони із вбудованими сучасними мобільними операційними системами: «Symbian OS», яка створена компанією «Symbian» – спільним підприємством фірм «Motorola», «Ericsson», «Nokia» і «Psion»; «BlackBerry OS», що випускаються компанією «Research In Motion Limited» (RIM), «Windows Mobile» та «Windows Phone», що розроблені компанією «Microsoft»; «Linux», «Android», що розроблені компанією «Open Handset Alliance» (OHA), «Mac OS X» та «Apple iOS», власниками яких є компанія «Apple» [43, с.53]. Наведені мобільні комп'ютерні пристрої є багатофункціональними та виконують функції персональних комп'ютерів. Кількість інформації, персональних даних користувача, що міститься в них,

постійно збільшується з розширенням їх можливостей та становить великий інтерес для правопорушників.

На сьогоднішній день виділяють наступні загрози безпеці мобільних комп'ютерних пристроїв [40, с.230]:

1. Викрадення або втрата мобільних пристроїв. Небезпека цієї загрози полягає у тому, що зловмисник може отримати вільний доступ до мобільного пристрою, а відповідно і до персональних даних, одержавши наступну інформацію, яка збережена на цьому пристрої:

- паролі та інформація про обліковий запис електронної пошти;
- електронне листування;
- облікові дані в соціальних мережах, таких як «Facebook», «Google», «Twitter»;
- паролі, що збережені в браузері;
- інформація про кредитні операції та картки;
- паролі, збережені в таких додатках як «Amazon» і «Google Wallet» або в хмарному сервісі «iCloud»;
- номери телефонів контактів;
- відомості про захищені мережі Wi-Fi;
- фотографії і відео тощо.

2. Ненавмисне розкриття даних. На сьогоднішній день розробники надають користувачам різноманітну кількість додатків для розширення можливостей мобільних комп'ютерних пристроїв. Загроза полягає в тому, що користувач при встановлені додатків на пристрій дозволяє їм доступ до певних персональних даних. Маються на увазі, передусім, контакти та списки вхідних та вихідних дзвінків, фото- та відеофайли, інформація про Wi-Fi-мережу, історія використання пристроїв та додатків, мікрофон, ідентифікаційні дані, місцезнаходження. При цьому власник пристрою у більшості випадків не замислюється, що використовувані ним додатки можуть передавати особисту інформацію третій стороні, наприклад, дані про

місцезнаходження користувача, його присутність або відсутність у певних місцях тощо.

Група авторів «The Wall Street Journal» свого часу провела журналістське розслідування, під час якого було виявлено, що деякі програми-додатки, розроблені для мобільних операційних систем «iOS» і «Android» передають особисті дані користувача третім особам і рекламодавцям. У список програм-додатків, що перевірялися авторами, увійшла відома на «iPhone» гра «Angry Birds». Під час дослідження виявилось, що саме ця гра передавала виробнику програмного забезпечення і його партнерам не тільки ім’я користувача та пароль до «iTunes», але й місце розташування та контакти [36].

Авторами були зроблені наступні висновки:

- 56 % додатків передають унікальний номер апарата іншим компаніям (рекламним мережам) без будь-якого повідомлення або дозволу користувача;

- 47 % мобільних додатків передають дані про географічне положення;

- 5 % посилають дані про вік, стать та інші персональні дані.

Дослідження також показало, що додатки для «Apple iOS» передають більше даних, ніж додатки для «Android», проте цю тенденцію неможливо перевірити для всієї бази кількох сотень тисяч додатків для обох операційних систем [63].

Інші дослідження показали вразливість наступних додатків: «Gmail» (92% успішних атак), «H&R Block» (92%), «Newegg» (86%), «WebMD» (85%), «CHASE Bank» (83%), «Hotels.com» (83%). Лише захист додатків «Amazon» було відносно важко подолати. Для нього показник успішних атак склав менше половини – 48% [49].

3. Використовувані раніше або непрацюючі пристрої. У цьому випадку більшість користувачів не видаляють або не можуть видали інформацію зі свого старого мобільного пристрою належним чином та звертаються до сервісного центру, продають або викидають пристрій, не замислюючись, що наступний власник або робітник сервісного центру може легко отримати

доступ до величезної кількості персональних даних. Наприклад, якщо вийшла з ладу MicroSD-пам’ять (флеш-пам'ять) для мобільних пристроїв, яка містила інформацію, більшість користувачів викидають її як непотріб, не замислюючись, що зловмисник за допомогою необхідних програмних і технічних засобів може відновити інформацію на ній. «European Union Agency for Network and Information Security» (ENISA) було проведено дослідження, яке показало, що неналежним чином списані мобільні пристрої можуть привести до витоку інформації, наприклад, історія викликів, контакти, електронні листи [62].

4. Фішингові атаки. На сьогоднішній день це найбільш розповсюджений вид шахрайства. Фішинг – це вид Інтернет-шахрайства, метою якого є отримання доступу до персональних та конфіденційних даних користувача, наприклад, інформації про кредитну карту, логіни та паролі.

Одним з видів фішингової атаки є розсилка електронних повідомлень, смс-повідомлень та дзвінків від імені банків, відомих фірм та брендів, які містять у собі гіперпосилання на сайт правопорушника, що не надто відрізняється від справжнього сайту фірми, банка, бренда, пропонують взяти участь у акції або підтвердити свій логін та пароль, який користувач використовує для доступу до певного сайту, акаунтів та банківських рахунків.

5. Атаки шпигунських програм. Користувач, не підозрюючи, може встановити шкідливе програмне забезпечення, програми, додатки («Android.SmsSend», «Android.Gongfu», «Android.Plankton», «Android.GoldDream», «Android.Crusewind», «Android.SpyEye», «Android.DreamExploid», «Android.Wukong», «PhoneOS.HLLW.Ikee», «Program.ZealSpy.1.origin», «Program.LetMeSpy.1.origin» та «Program.CellSpy.1.origin») або заразити програмне забезпечення вірусами з web-сайтів (троянець «Android.CaPson.1», банківські троянці «Android.MulDrop», «Android.BankBot.29. origin», «Android.Banker.50.origin») [63]. Саме ці шпигунські програми надають правопорушникам повний або частковий контроль над мобільним пристроєм користувача.

У 2016 році фахівцями «Лабораторії Касперського» було виявлено близько 143 тис. нових модифікацій шкідливих програм для мобільних пристроїв, а число зразків мобільних вірусів («трояни») для крадіжки даних кредитних карт і розкрадання грошей з банківських рахунків користувачів збільшилася майже в 20 разів [87].

У свою чергу компанією «Avast «було проведено дослідження, яке показало, що кількість мобільних вірусів у 2016 р. в порівнянні з 2013 р. (100000 мобільних вірусів) зросла до 1 млн. [65, с.70].

У 2015 році компанією «AVG» було взагалі виявлено шкідливе програмне забезпечення під «Android», яке здатне працювати навіть при вимкненому мобільному пристрої [65, с.69].

На рисунку 2.1. подано кількість виявленого шкідливого програмного забезпечення в світі [87]:

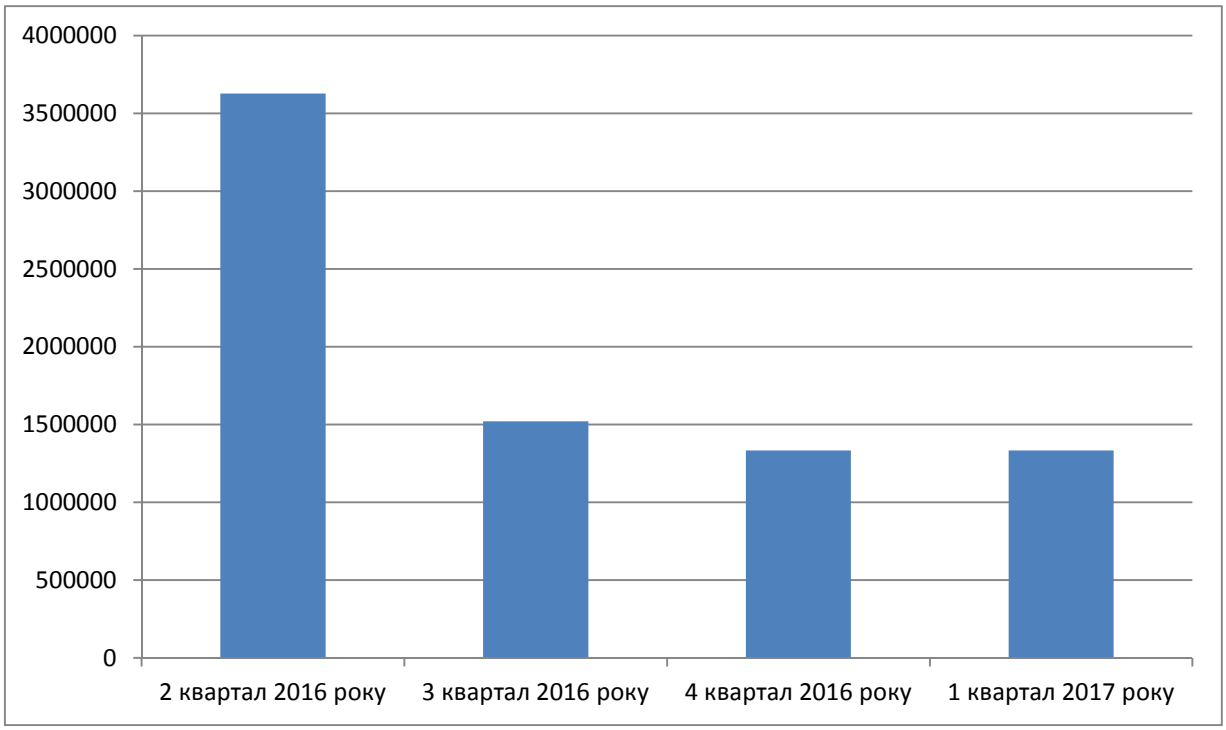

Рис. 2.1. Кількість виявленого шкідливого програмного забезпечення в світі (2016-2017 р.р.)
Джерело: IT threat evolution Q1 2017. Statistics [Electronic resource]. - Access: https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

У першому кварталі 2017 року було виявлено 1 333 605 шкідливих інсталяційних пакетів, що практично відповідає показнику в 4 кварталі 2016 року.

Таблиця 2.1. наочно ілюструє географічний розподіл за країнами здійснення атак на мобільні пристрої в 1 кварталі 2017 року:

Таблиця 2.1

Географічний розподіл за країнами здійснення атак на мобільні пристрої в 1 кварталі 2017 року (у відсотковому значенні від загальної кількості хакерських атак) (Джерело: [87])

№ п/п	Країна походження атак	Відсоткове значення здійснених атак (%)
1.	Іран	47,35
2.	Бангладеш	36,25
3.	Індонезія	32,97
4.	Китай	32,47
5.	Непал	29,90
6.	Індія	29,09
7.	Алжир	28,64
8.	Філіппіни	27,98
9.	Нігерія	27,81
10.	Гана	25,85

У першому кварталі 2017 року Іран був країною, у якій спостерігався найвищий відсоток атак на мобільні пристрої через зловмисні програми - 47,35%. Бангладеш зайняв друге місце: 36,25% користувачів отримали мобільні загрози принаймні один раз протягом кварталу.

Наступними країнами є Індонезія та Китай; частка обох країн склала трохи більше 32%. Росія (11,6%) зайняла 40-е місце в цьому рейтингу, у Франції - 8,1%, у США - 69,9%, в Італії - 7,1%, у Німеччині - 6,2% та 72% у Британії - 5,8%. Найбезпечнішими країнами були Фінляндія (2,7%), Грузія (2,5%) та Японія (1,5%) [87].

На рис. 2.2. подано кількість інстальованого шкідливого програмного забезпечення типу «Банківський Троян» виявленого антивірусними програмами [87]:

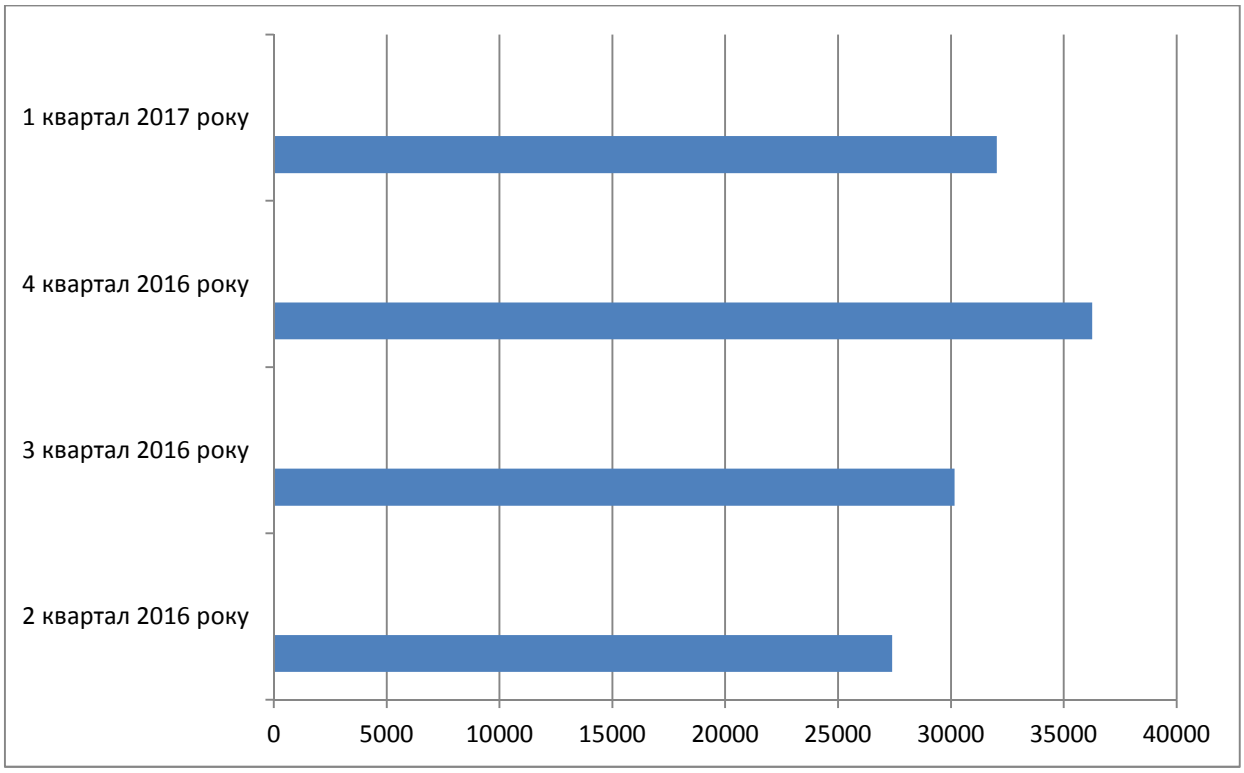

Рис. 2.2. Кількість інстальованого шкідливого програмного забезпечення типу «Банківський Троян» виявленого антивірусними програмами (2016 -2017 р.р.)
Джерело: IT threat evolution Q1 2017. Statistics [Electronic resource]. - Access: https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

За звітний період було виявлено 32 038 інсталяційних пакетів для мобільних банківських троянських програм, що в 1,1 разів більше, ніж у 4 кварталі 2016 року.

Незважаючи на те, що сім'я «Svpeng» у першому кварталі 2017 року перевищила рейтинг найпопулярніших троянських програм для мобільних банківських послуг, її діяльність зменшилася порівняно з третьою чвертю 2016 року: частка користувачів, на яких напали ці шкідливі програми в Росії, знизилася майже вдвічі - з 3,12% до 1,64% [87].

На другому місці опинилась Австралія (1,14%), де найпопулярніші загрози були сімейства троянів-банкір («AndroidOS.Acecard» та «Trojan-Banker.AndroidOS.Marcher»). Туреччина отримала показник 0.81% (див. табл..2.2.):

Таблиця 2.2

Географічний розподіл за країнами здійснення банківських троянських атак на мобільні пристрої в 1 кварталі 2017 року (у відсотковому значенні від загальної кількості хакерських атак) (Джерело: [87])

№ п/п	Країна походження атак	Відсоткове значення здійснених атак (%)
1.	Росія	1,64
2.	Австралія	1,14
3.	Туреччина	0,81
4.	Узбекистан	0,61
5.	Таджикистан	0,48
6.	Молдова	0,43
7.	Україна	0,41
8.	Казахстан	0,37
9.	Киргизстан	0,32
10.	Сінгапур	0,26

«Svpeng» залишався найпопулярнішим троянським мобільним банківським троянським вірусом протягом 2016-2017 р.р. Це сімейство мобільних банківських троянських програм використовує фішингові вікна, щоб красти дані кредитної картки, логіни та паролі з онлайн-банківських рахунків. Крім того, шахраї викрадають гроші за допомогою послуг смс, включаючи мобільний банкінг.

6. Використання Wi-Fi мережі. Хакери іноді полюють на тих, хто використовує загальнодоступні мережі Wi-Fi. Правопорушник може отримати паролі до незашифрованих веб-сайтів, пошти, передані через незашифроване з'єднання на веб-сайт тощо.

Для захисту мобільних комп'ютерних пристроїв від загроз, розглянутих вище, можна порекомендувати дотримуватись наступних правил:

1. Встановити Pin-код, пароль на телефон (або використовувати екранну блокіровку з графічним ключем), SIM-карту та карти-пам'яті.

2. Встановити антивірусні програми та постійно оновлювати їх, регулярно перевіряти мобільний пристрій на наявність вірусів.

3. Не встановлювати додатки (ігри, програми), які запитують доступ до персональної та конфіденційної інформації, та видаляти ті з них, які не використовуються.

4. Перед встановленням додатків переглядати їх рейтинги та відгуки.

5. Правильно налаштувати мобільний пристрій, оскільки він має свою систему захисту: можливість перевірки додатків на віруси та шпигунські програми, забороняти встановлення додатків з невідомих джерел, функція, яка дозволяє знайти вкрадений або втрачений мобільний пристрій.

6. Використовувати функцію, яка дозволяє або блокує доступ до Інтернету.

7. Якщо телефон містить конфіденційну інформацію, можна використовувати вбудовану функцію повного шифрування телефону або пам’яті телефону.

8. Не використовувати незахищені Wi-Fi мережі, особливо при онлайн-покупці товарів та послуг.

9. Регулярно оновлювати програмне забезпечення мобільних пристроїв з перевірених джерел.

10. Не переходити за гіперпосиланнями, які містять повідомленнях з невідомих адрес, а також не натискати на спливаючі банери та реклами.

11. Не виходити за рамки визначеної політики безпеки.

2.2. Оцінка рівня захисту інформації на мобільних комп’ютерних пристроях з операційними системами «Android», «Apple iOS» та «Windows»

Операційна система «Android» упевнено завойовує популярність, і на даний момент залишила позаду «Windows Mobile». Розширюється і список платформ, для яких зафіксовані шкідливі програми. Тепер до них додалися «iOS» (операційна система для «iPhone»/»iPod Touch»/»iPad») і «Android». Так, у серпні 2010 року була виявлена перша шкідлива програма для операційної системи «Android». Кількість шкідливих програм для iPhone, як і раніше, невелика, при цьому вони здатні заразити лише «розлочені» (з англ.. -

«jailbroken») смартфони. «J2ME», як і раніше, лідирує в рейтингу модифікацій об`єктів, що детектуються, оскільки дана платформа охоплює не тільки користувачів деяких смартфонів, а й практично кожного власника звичайного сучасного мобільного телефону.

Мобільні гаджети від «Apple», що вже стали легендою, працюють на платформі «iOS». Перший сенсорний iPhone було презентовано у 2007 році засновником компанії Стівом Джобсом. В той же час до відома користувачів було доведено, що новий мобільний пристрій працює на основі «OS X», яка використовується для комп'ютерів «Mac». Перший смартфон мав набагато менше звичних функцій, але компанія відповідально підійшла до розвитку і вдосконалення операційної системи, і вже наступна версія мала серйозні нововведення. Знаковою стала поява сервісу «AppStore», через який поширювалося фірмове прикладне програмне забезпечення.

У 2010 році з появою на ринку планшетного комп'ютера «iPad» операційна система отримала свою сучасну назву «iOS». Мобільна платформа еволюціонує щороку, поступово розширюючи функціонал і відкриваючи нові можливості для користувачів. Восени 2017 вийшла вже 11 версія операційної системи [49].

Однією з головних переваг «iOS» називають її надійність і безпеку. Ці якості забезпечуються закритістю системи і ретельним відбором мобільних додатків для поширення через «AppStore», безпечності яких надається велике значення. Прихильники «iPhone» і «iPad» впевнені, що така сувора політика компанії-виробника стовідсотково захищає від проникнення шкідливого шкідливих програм в операційну систему їх пристроїв. І це дійсно так: дотримання користувацької угоди зводить до мінімуму можливість підхопити вірус чи іншу шкідливу програму.

Але загрози все одно існують. Не кожного власника брендових гаджетів задовольняє обмежена можливість оновлення програмного забезпечення і встановлення лише схвалених і перевірених розробником додатків. Такі користувачі роблять «джелбрейк» («jailbreak») - процедуру отримання повного доступу до файлової системи «iOS», яка можлива завдяки наявності

уразливостей в системі безпеки операційної системи. Після проведених маніпуляцій разом з можливістю встановлення сторонніх додатків зростає ймовірність проникнення шкідливих програм.

Першу вірусну програму-троянця в 2008 році створила 11-річна дитина в результаті експериментів з XML-файлами. Вірус маскувався під оновлення пакету «Erica's utilities» і під час спроби видалення стирав інші файли в «iOS». Весною 2014 зафіксовано атаку на користувачів iPhone, які робили джелбрейк своїм гаджетам. Сайт, з якого почалося розповсюдження троянця «Unflod Baby Panda», імовірно знаходився в Китаї [63]. Це яскраві, але не поодинокі випадки активної діяльності шкідливого програмного забезпечення.

Метою впровадження вірусних програм до файлової системи «iOS» є отримання доступу до особистої інформації, паролів доступу до банківських сервісів і платіжних систем, стеження за користувачем, розсилка спаму і реклами тощо. Вберегтися від втручання зловмисників у роботу мобільних пристроїв «Apple» можна ретельно дотримуючись правил безпеки:

- не використовувати модифіковані версії «iOS»;
- відмовитися від джелбрейку;
- своєчасно оновлювати операційну систему після появи офіційних версій;
- для встановлення нових додатків користуватися лише «AppStore», звертати увагу на відгуки інших користувачів.

Це досить дієві правила, але зима 2015 року показала, що для розробників вірусів меж не існує. Троянський вірус-шпигун «Xagent» має офіційний сертифікат «iOS Developer Enterprise Program» і може проникати навіть на не зламані гаджети. Однією з особливостей цієї шкідливої програми є негайний рестарт після спроби його зупинки на пристроях з «iOS 7». На iPhone і iPad з восьмою версією «iOS» вірус присутній у вигляді іконки на робочому столі і не може бути запущений самостійно. Тож, варто бути уважними і своєчасно вживати заходи на підвищення безпечності і захисту власної інформації.

Віруси, трояни та інші види шкідливого програмного забезпечення — серйозна і поширена проблема платформи «Windows». Навіть в новітньої

операційної системи «Windows 8» (та 8.1), незважаючи на поліпшення безпеки, ви не застраховані від цього.

Не всі шкідливі програми направлені на роботу в операційної системи «Windows», але таких більшість. Одна з основних причин цього — широке поширення і популярність цієї операційної системи, але це не єдиний фактор. З самого початку розробки «Windows», безпека не ставилася в главу кута, як, наприклад, в UNIX-подібних системах. А всі популярні операційні системи, за винятком «Windows», в якості свого попередника мають саме «UNIX».

В даний час в тому, що стосується установки програм «Windows» склалася досить-таки своєрідна модель поведінки: програми знаходяться в різних джерелах (часто неблагонадійних) в Інтернеті і встановлюються, в той час як інші операційні системи мають власні централізовані і щодо захищені магазини додатків, з яких і відбувається встановлення перевірених програм. Так багато встановлюють програми в «Windows», звідси багато вірусів, так в «Windows» 8 і 8.1 також з'явився магазин додатків, однак, найбільш необхідні і звичні програми для робочого столу користувач продовжує скачувати з різних джерел. Є віруси для «Apple Mac OS X» [53, с.43].

Як вже було сказано, основна частка шкідливого програмного забезпечення розробляється для «Windows» і воно не може працювати на «Mac». Незважаючи на те, що віруси на «Mac» зустрічаються значно рідше, тим не менш, вони існують. Зараження може відбуватися, наприклад, через плагін «Java» в браузері (саме тому він не включається в постачання операційної системи останнім часом), при встановленні зламаних програм і деякими іншими способами. В останніх версіях операційної системи «Mac OS X» для установки додатків використовується «Mac App Store».

Якщо користувачу потрібна програма, то він може знайти її в магазині додатків і бути впевнений, що вона не містить шкідливого коду або вірусів. Шукати якісь інші джерела в Інтернеті не обов'язково. Крім цього, операційна система включає в себе такі технології як «Gatekeeper» і «XProtect», перша з яких не дозволяє запускати на «Mac» програми, не підписані належним чином,

а друга — являє собою аналог антивірусу, перевіряючи запускаються на наявність вірусів.

Таким чином, віруси для «Mac» є, однак вони з'являються значно рідше, ніж для «Windows» і ймовірність зараження нижче, у зв'язку з використанням інших принципів при установці програм.

Віруси і шкідливі програми для «Android» існують, так само як і антивіруси для цієї мобільної операційної системи. Однак, слід враховувати той факт, що «Android» є значною мірою захищеною платформою. За замовчуванням, ви можете встановлювати програми тільки з «Google Play», крім того, сам магазин додатків сканує програми на наявність вірусного коду (віднедавна). «Google Play» — магазин додатків для «Android». Користувач має можливість відключити установку програм лише з «Google Play» і завантажувати їх із сторонніх джерел, але при установці «Android 4.2» і вище запропонує вам просканувати завантажену гру або програму.

В загальних рисах, якщо ви не з тих користувачів, які скачують зламані програми для «Android», а використовуєте для цього тільки «Google Play», то ви в значній мірі захищені. Аналогічним чином, порівняно безпечними є магазини додатків «Samsung», «Opera» і «Amazon».

Операційна система «Apple iOS» є ще більшою мірою закритою, ніж «Mac OS» або «Android». Таким чином, використовуючи «iPhone», «iPod Touch» або «iPad» і завантажуючи додатки з «Apple App Store» ймовірність того, що ви скачаєте вірус практично дорівнює нулю, у зв'язку з тим, що даний магазин додатків набагато більш вимогливий до розробників і кожна програма перевіряється вручну.

Влітку 2013 року, у рамках проведеного дослідження («Georgia Institute of Technology») було показано, що існує можливість обійти процес перевірки при публікації додатка в «App Store» і включити в нього шкідливий код. Однак, навіть якщо подібне трапиться, відразу після виявлення уразливості «Apple» має можливість видалити всі шкідливі програми на всіх пристроях користувачів під управлінням «Apple iOS» [53, с.44].

До речі, аналогічно цьому, «Microsoft» і «Google» можуть віддалено деінсталювати встановлені зі своїх магазинів додатки.

Шкідливі програми для Linux. Творці вірусів не особливо працюють в напрямку «ОС Linux», у зв'язку з тим, що ця операційна система використовується малою кількістю користувачів. Крім цього, користувачі «Linux» в більшості своїй є більш досвідченими, ніж середній власник комп'ютера чи мобільного пристрою і більшість тривіальних методів розповсюдження шкідливих програм з ними просто не спрацюють.

Так само, як і в перерахованих вище операційних системах, для установки програм в «Linux», в більшості випадків, використовується своєрідний магазин додатків — диспетчер пакетів, Центр додатків» Ubuntu» («Ubuntu Software Center») і перевірені сховища цих додатків. Запустити віруси, призначені для «Windows» в «Linux» не вийде, а навіть якщо і зробити це в теорії, можна — вони не будуть працювати і представляти собою шкоду.

Але віруси для «Linux» все ж є. Найскладніше — знайти їх і інфікуватися, для цього, як мінімум, потрібно завантажити програму з незрозумілого сайту (причому ймовірність того, що в ній буде вірус — мінімальна) або отримати по електронній пошті і запустити її, підтвердивши свої наміри

«Symantec» представляє нову захист для «Android» і «iOS». Компанія «Symantec» оголосила про значне розширення портфеля технологій для мобільних пристроїв, які дозволять забезпечувати безпечну роботу електронної пошти, захист мобільних додатків і реалізації в компаніях підходу «Bring Your Own Device» («BYOD»).

Оновлені рішення включають наступні продукти і нові можливості [40]:

– «Symantec Mobile Security for Android». Програма, що надає можливість використовувати передові технології виявлення загроз, використовувані в корпоративному середовищі, для мобільних пристроїв з операційної системи «Android»;

– «Symantec Mobile Management for Configuration Manager». Програма, заснована на технологіях придбаної компанії «Odyssey Software». Забезпечує інтеграцію з «Microsoft System Center Configuration Manager» (SCCM);

– «Symantec Mobile Management» тепер забезпечує інтеграцію з продуктом «Nitro Desk Touch Down», забезпечуючи безпеку електронної пошти на пристроях під керуванням операційної системи «Android», дозволяючи задавати політики безпеки пошти;

– «Symantec Mobile Management» володіє повноцінним агентом для операційної системи «Windows7 Phone», таким чином доповнюючи вже наявні агенти для операційної системи «Android» і «iOS»;

– «Nukona AppCenter» від «Symantec» тепер може захищати дані на пристроях, керованих «iOS», за допомогою сертифікованих для «FIPS 140-2» алгоритмів шифрування;

– «Symantec PGP Viewer» for «Android» робить доступним для пристроїв з операційної системи «Android» можливість шифрування електронної пошти за допомогою «PGP Universal Server».

Розглянемо їх детальніше:

1. «Symantec Mobile Security» for «Android». Згідно з результатами опитування «Symantec» 2016 року про використання мобільних технологій у корпоративному середовищі «Stateof Mobility», 67% сучасних компаній стурбовані тим, що шкідливе програмне забезпечення проникає з мобільних пристроїв в корпоративну мережу. Останній звіт «Symantec» про погрози інтернет-безпеки показав, що кількість мобільних вразливостей збільшилася на 93%за 2011 рік, а список загроз для системи «Android» продовжує рости.

Щоб захистити підключені до корпоративних мереж пристрої на базі «Android», убезпечивши їх від шкідливих програм та інших загроз Інтернету, компанія «Symantec» представила систему «Symantec Mobile Security for Android». Продукт «Mobile Security for Android» працює на базі запатентованих технологій «Symantec», які забезпечують моніторинг і аналіз мільйонів додатків «Android», пропонованих в різних магазинах для «Android».

Використання ресурсів глобальної аналітичної мережі «Symantec Global Intelligence Network» дозволяє рішенням «Mobile Security for Android» виявляти шкідливе програмне забезпечення, так само як на мільйонах пристроїв з операційної системи «Android» з встановленою системою «Norton Mobile Security».

2. «Symantec Mobile Management for Configuration Manager». В результаті об'єднання з «Odyssey Software», колишній продукт «Odyssey Athena» став рішенням «Symantec Mobile Management for Configuration Manager».

Для своїх замовників «Symantec» пропонує три варіанти використання системи керування мобільними пристроями (MDM – «Mobile Device Management»): окрема система MDM, інтегрована MDM разом з рішенням «Symantec AltirisIT Management Suite» і комплексне рішення MDM для «Microsoft System Center Configuration Manager». Ці системи дозволяють використовувати масштабовану MDM-систему корпоративного рівня та уніфікувати управління кінцевими точками на базі однієї з двох найбільш часто впроваджуваних для менеджменту платформ.

3. «Symantec Mobile Management». Всі продукти «Symantec Mobile Management» тепер інтегруються з корпоративним клієнтом електронної пошти для операційної системи «Android - Nitro Desk Touch Down», що дозволяє забезпечити безпечний сервіс мобільного пошти для корпоративних замовників.

Пропонуючи управління спеціальним рішенням для електронної пошти на пристрої з операційної системи «Android», «Symantec» допомагає одночасно вирішити питання безпеки і управління, зокрема, розділяючи корпоративні та персональні дані.

«Symantec Mobile Management» тепер дозволяє встановити програмний агент для корпоративного управління пристроями на базі операційної системи «Windows Phone», доповнюючи існуючі інструменти контролю для «Android» і «iOS». Завдяки цій можливості корпоративні замовники зможуть забезпечувати безпеку і керувати всіма популярними платформами, встановлювати мобільні

додатки і працювати з контентом, забезпечуючи захист корпоративних даних на цих пристроях.

4. «Nukona App Centerот Symantec» захищає програми і дані на пристроях, керованих «iOS», використовуючи при цьому алгоритми шифрування, сертифіковані на відповідність «FIPS 140-2». Завдяки цьому використання пристроїв на базі «iOS» стає можливим в урядових структурах режимних та інших установах, таких як фінансові та медичні організації. Рішення допомагає забезпечити відповідність вимогам закону, дозволяючи працювати як на корпоративних пристроях, так і в рамках концепції «BYOD».

«Nukona AppCenter» забезпечує захист додатків і управління контентом для пристроїв на базі «iOS» і «Android», підтримуючи програми, створені сторонніми розробниками, такими як «Appcelerato»r і «Phone Gap». Ці нові можливості допомагають замовникам забезпечити безпеку і управління мобільними додатками, отриманими з більш широкого спектру джерел.

5. «Symantec PGP Viewer for Android». Слідом за успішною реалізацією «Symantec PGP Viewer» для «iOS», компанія «Symantec» розробила «Symantec PGP Viewer» для «Android», надаючи можливість читати зашифровані листа на пристроях з операційної системи «Android».

Доступне для завантаження через «Google Play Marketplace», додаток «PGP Viewer for Android» працює разом з «PGP Universal Server» від «Symantec», дозволяючи реєструвати користувачів і управляти криптографічними ключами. Це допомагає замовникам добиватися відповідності вимогам і запобігання витоку даних.

Відповідальність щодо захисту від шкідливого програмного забезпечення, насамперед, лежить на самому користувача. Для того щоб мінімізувати зараження мобільного пристрою «вірусами» необхідно:

– своєчасно оновлювати програми, що виправить уразливості у встановленому програмному забезпеченні;

– не використовувати обліковий запис адміністратора в щоденній роботі з операційною системою «Windows»;

– уникати зміни системних файлів і встановлення програм з невідомих джерел;
– встановити антивірус;
– створювати резервні копії всіх важливих документів і файлів.

2.3. Дослідження сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі в зоні антитерористичної операції через мобільні пристрої

У сучасній високотехнологічній війні перемагає той, хто володіє інформацією, спроможний швидко виявити противника, провести ефективну оцінку обстановки та першим завдати удару. Це означає, що перевага в здобутті інформації та ефективності управління військами здатна забезпечити перемогу навіть над противником, який має значну перевагу.

Для цього провідні армії світу ефективно використовують сучасні автоматизовані системи управління військами в зоні антитерористичної операції та зброєю за допомогою сучасних мобільних пристроїв.

Військові теоретики детально досліджують питання «інформаційного домінування», які підкріплені практичними дослідженнями [52, с.102].

На даний час в Україні також активно ведеться робота по створенню сучасних автоматизованих систем управління військами за допомогою сучасних мобільних пристроїв. Одними з основних в таких системах є питання захисту інформації та протидії атакам противника. Розвиток технології, телекомунікаційних систем та електроніки, зазначає Муравська Ю., призвів до надзвичайно швидкого зростання комунікаційних можливостей. Більшість зі складових успіху будь то бізнес, військові або державні справи в цілому ґрунтуються на передачі, придбанні і контролі інформацією [35].

Тому необхідно приділяти значну увагу безпеці у кіберпросторі під час експлуатації таких інформаційних та автоматизованих систем управління військами в зоні антитерористичної операції за допомогою сучасних мобільних пристроїв. При цьому однією із задач є аналіз можливих сучасних методів атак

за допомогою яких зловмисник може отримати доступ до системи та скоїти свій задум.

Інформаційні мережі та автоматизовані системи управління військами є предметом для атак з боку противника (хакерів) та шкідливого програмного забезпечення на мобільних пристроях.

Методи за допомогою яких проводяться сучасні атаки на системи управління військами в зоні антитерористичної операції за допомогою сучасних мобільних пристроїв можна поділити на три групи, а саме:

– «Віруси та хробаки», коли шкідливе програмне забезпечення здатне додати свій код в інші програми або файли;

– «Трояни», що маскуються під нешкідливі, навіть корисні додатки, але наносять збитки інформаційній системі управління військами в зоні антитерористичної операції після інсталяції;

– «Мережеві атаки», спрямовані на вторгнення до інформаційної мережі з метою аналізу уразливостей та в подальшому нанесення удару по інформаційній системі.

Проведемо аналіз кожного з даних методів атак.

Віруси досить швидко поширюються по інформаційній мережі та змінним носіям. У багатьох випадках мета вірусу – це ввести користувача в оману, щоб виконати шкідливі посилання, або завантажити шкідливі файли. У деяких випадках використовуються електронні поштові скриньки для ураження інформаційної системи.

1. «Resident Virus». Вірус, який живе в пам’яті цільового комп’ютера чи мобільного пристрою. Таким способом він активується кожного разу при включенні або виконанні певної дії.

2. «Non-resident Virus». За допомогою цього методу вірус активно шукає цілі для інфекції на локальній, змінній або мережевій локації. Цей тип вірусу не живе в пам’яті та існує при подальшому виявленні потенціальних цілей.

3. «Boot sector Virus». Вірус, що заражає завантажувальний сектор. Цей тип вірусів завантажується задовго до завантаження операційної системи на

інфікованому комп'ютері та мобільному пристрої та націлений на ураження файлової структури жорсткого диску.

4. «Macro Virus». Вірус, який написано на мові макросів, вбудований в «Word», «Excel», «Outlook» і інші документи. Він активується при відкритті інфікованого документу, через те, що за замовчуванням скрипти написані на мові макросів виконуються автоматично при відкритті документу.

5. «File-infecting Virus». Класична форма вірусу, коли інфікований файл, при виконанні інфікує інші файли в інформаційній системі.

6. «Polymorphic Virus». Цей тип вірусу є особливо важким для виявлення на мобільних пристроях, через те, що після виконання використовує алгоритми шифрування та копіює себе у новий файл, тим самим підчищаючи сліди за собою.

7. «Metamorphic Virus». Вірус здатний змінювати свій код при кожному зараженні. Процес переписування призводить до різних заражень, але функціональність коду залишається незмінною.

8. «Stealth Viru»s. Вірус, який використовує різноманітні методи для запобігання виявленню, наприклад шляхом видаленням себе від заражених файлів та розміщення нової інфікованої копії в іншому місці.

9. «Armored Virus». Дуже складний тип вірусу, що використовує різні методи для захисту від антивірусного програмного забезпечення, дезорієнтує його, дає зрозуміти, що він розташований десь в іншому місці ніж є насправді.

10. «Multipartite Virus». Одночасно атакує завантажувальний запис жорсткого диску та файли, що виконуються. Тим самим при виявленні та видаленні може інфікувати інформаційну систему з завантажувального запису повторно.

11. «Camouflage Virus». Тип вірусу, який хибно повідомляє антивірусне програмне забезпечення та направляє його дію на ліцензійні програми управління військами [52].

Хробак – вважається суб-класом вірусу та використовує уразливості операційної системи для поширення. Вони можуть поширюватися,

дублюватися і розмножуватися, але на відміну від вірусів, хробаки не вимагають прикріплення до файлу, або будь-якої виконуваної програми. Цей тип шкідливого програмного забезпечення можна класифікувати за типом поширення на мобільних пристроях:

1. «E-mail Worm»s. Поширюються через електронну пошту, а саме через прикріплені файли у електронному листі.

2. «Internet Worms». Поширюються безпосередньо через мережу Інтернет, користуючись відкритими портами або уразливостями системи.

3. «Network Worm»s. Поширюються по відкритих, незахищених інформаційних мережах.

4. «Multivector Worms». Мають два, або більше методів поширення. До найбільш небезпечних атак можна віднести «Boot sector Virus», «Polymorphic Virus», «Stealth Virus», «Multipartite Virus» [52, с.103].

Такі атаки можуть нанести значних збитків та витоку конфіденційної інформації з управління військами в зоні антитерористичної операції, ці атаки маскуються та перешкоджають антивірусному програмному забезпеченню на мобільних пристроях, що ускладнює процес виявлення та обеззараження інформаційної системи.

Суттєвою різницею між вірусом та трояном є те, що троян не інсталюється самостійно, він вводить в оману користувача маскуючись під корисне програмне забезпечення. Троян може розповсюджуватися за допомогою електронної розсилки у вигляді посилання або прикріпленого файлу. У Додатку А. подано ранжування кількості найбільш поширених типів вірусних атак на мобільні пристрої у світі у першому кварталі 2017 року.

Розглянемо поширені типи троянів:

1. «Remote Access Trojans (RAT) aka Backdoor Trojan». Цей тип трояна відкриває бекдор на інфікованій інформаційній системі, щоб дозволити зловмиснику отримати віддалений доступ або навіть повний контроль над системою.

2. «Trojan-DDoS». Цей вид троянів встановлюється одночасно на велику кількість комп’ютерів чи мобільних пристроїв з метою створення мережі зомбі (ботнет) машин, які будуть використані для реалізації DDoS атаки на конкретну цільову інформаційну мережу.

3. «Trojan-Proxy». Призначений для використання цільового коп’ютера як проксі-сервера, що дозволить виконати безліч операцій на мобільних пристроях анонімно, навіть реалізувати подальшу атаку на мережу за допомогою ураженого комп’ютера чи мобільного пристрою.

4. «Trojan-FTP». Призначений для відкриття FTP портів, що дозволить отримати віддалений доступ до інфікованої системи та мережі в цілому, а також вікна для подальшого поширення різноманітних загроз.

5. «Destructive Trojans». Призначені для знищення або видалення даних на інфікованій інформаційній системі.

6. «Security Software Disabler Trojans». Цей вид троянів призначений для боротьби з антивірусним програмним забезпеченням шляхом зупинки програм безпеки, брандмауеру, IPS або відключенням процесів та служб.

7. «Keylogger Trojans». Троян, який призначений для зчитування та запам’ятовування інформації під час натискання клавіш на клавіатурі інфікованої системи та з подальшою передачею цієї інформації зловмиснику, що буде використана з метою викрадення таємних даних.

8. «Trojan-PSW» (Password Stealer). Спеціально розроблений тип троянів, що використовується для крадіжки паролів на інфікованій інформаційній системі.

9. «Trojan-Spy». Призначений для шпигування за інформаційною системою, викрадення паролів, інформації про кредитні картки, секретної інформації, збирання скріншотів з коп’ютера та ведення інших шпигунських дій на ураженій системі.

10. «Cryptolock Trojan» (Trojan.Cryptolocker). Новий тип троянів, що з’явився у 2013 році та призначений для шифрування та замикання окремих файлів на інфікованій системі [53].

Наслідки ураження інформаційної системи даним типом шкідливого програмного забезпечення можуть значно відрізнятися, від заміни робочого простору до відкриття бекдорів на мобільних пристроях, що дозволить іншим вірусам уразити інформаційну систему або дозволить зловмиснику отримати віддалений доступ до системи, видалити важливі системні файли.

Значно загрозливішими для програмного забезпечення на мобільних пристроях управління військами є мережеві атаки. У цьому випадку ми маємо справу з пасивним методом атаки, який застосовується для аналізу мережевого середовища, збору інформації щодо відкритих портів або інших вразливих місць інформаційної системи. Залежно від процедур під час нападу або типу уразливості, мережеві атаки на управління військами в зоні антитерористичної операції можуть бути класифіковані наступним чином:

1. «Social Engineering». Відноситься до психологічної маніпуляції людьми в інформаційній мережі. Мета полягає у несанкціонованому отриманні доступу до конфіденційної інформації, крадіжки даних, промислового шпигунства і переривання обслуговування.

2. «Phishing attack». Тип атак, що використовує соціальну інженерію для викрадення конфіденціальної інформації – найбільш поширена мета таких атак полягає у викраденні інформації щодо до кредитних карток жертви. Фішинг атака, як правило спочатку розповсюджують електронні листи, що ведуть користувачів на заражені сайти, які маскуються під банківські системи.

3. «Social Phishing». Мета такого типу атак полягає в отриманні конфіденційної інформації і отриманні доступу до особистих файлів. Засіб враження полягає у розповсюджені шкідливих посилань через мережу Інтернет та за допомогою обману переконання користувачів натиснути на такі посилання.

4. «Spear Phishing Attack». Тип атак, що орієнтований на конкретних осіб та на конкретні компанії. Мета такого типу атак полягає реалізації промислового шпигунства та крадіжки конфіденційної інформації.

5. «Watering Hole Attack». Найбільш складний тип атак, що базується на комплексному підході до ураження інформаційної системи конкретного користувача. Спочатку зловмисник вивчає звички потенційної жертви, збирає історію про відвідувані веб-сайти та обирає найбільш популярні портали, що мають вразливість у безпеці. Наступним кроком є інсталяція свого шкідливого коду або програми у такий веб-сайт.

6. «Vishing» («Voice Phishing or VoIP Phishing»). Тип атаки, що комбінує соціальну інженерію та телефонну систему. Зловмисник маскує номер телефону під реально існуючого абонента з адресної книги або під банківську установу та шляхом обману здобуває конфіденційну інформацію або банківські рахунки.

7. «Port scanning». Тип атаки де зловмисник сканує порти на цільовій інформаційній системі, щоб з'ясувати де знаходяться активні та відкриті порти з метою ураження системи шкідливими послугами, що пов'язані з конкретними портами.

8. «Spoofing». Тип атаки, що маскує зловмисника, програму або адрес під інший шляхом фальсифікації даних з метою несанкціонованого доступу до інформаційної системи.

9. «Denial of Service Attack (DoS Attack) and Distributed Denial of Service Attack (DDoS Attack)». Атака пов'язана з призупиненням надання послуг або повною зупинкою інформаційної системи шляхом створення потужної активності фальсифікованих користувачів в системі та великої кількості запитів до бази даних, що призводить до завантаження відповідної інформаційної системи.

10. «Ping of Death (PoD)». Атака, що базується на відправці спотвореного або шкідливого пінгу на цільову інформаційну систему з метою переповнення буферу.

11. «Smurf Attack». Атака яка повторює дії «Ping of Death» з маскуванням IP адреса зловмисника.

12. «Bluesnarfing». Атака, що дозволяє отримати доступ до інформації на пристрої за допомогою зв’язку Bluetooth.

Будь-який пристрій з включеним режимом Bluetooth на «виявити» може бути схильним до такого типу атак. Мережеві атаки не руйнують ресурси або дані. Активна фаза відбувається коли зловмисник застосовує комбінований метод і поєднує мережеву атаку з будь яким типом вище розглянутих атак.

Отже, трояни та мережеві атаки реалізуються через інформаційні мережі, опираючись на сучасні методи розповсюдження інформації на мобільних пристроях при цьому користуючись знаннями соціальної інженерії з управління військами. Ці методи реалізації атак на інформаційні системи не руйнують ресурси або дані, найбільш небезпечними їх можна вважати при використанні комбінованого методу, коли до ураженої цільової системи додають шкідливий вірус.

Віруси та хробаки являються найбільш небезпечними методами реалізації атак зловмисника на інформаційні системи та мережі. Противники, які зможуть реалізувати цей тип атаки спроможні отримати інформацію з управління військами в зоні антитерористичної операції, знищити дані та файли на цільовому робочому місці оператора, нанести пошкодження комплектуючим інформаційної мережі або системи та отримати повний доступ до керування окремим робочим місцем оператора.

На основі проведеного аналізу сучасних методів атаки на інформаційні системи та мережі можна виділити віруси та черв`яки, як найбільш небезпечні методи атак на мобільних пристроях. Серед яких «Boot sector Virus», «Polymorphic Virus», «Stealth Virus», «Multipartite Virus» є особливо небезпечними методами атаки.

Такі атаки можуть нанести значних збитків та витоку конфіденційної інформації, ці атаки маскуються та перешкоджають антивірусному програмному забезпеченню з управління військами, що ускладнює процес виявлення та обеззараження інформаційної системи.

Висновки до розділу 2

Мобільний вірус для телефону або мобільний шкідлива програма – це інформаційний вірус, спеціально адаптований для мобільних пристроїв і телефонів, створений для поширення від одного зарядженого телефону на інший. На сьогоднішній день виділяють наступні загрози безпеці мобільних комп'ютерних пристроїв:

1. Викрадення або втрата мобільних пристроїв з інформацією на них: паролі та інформація про обліковий запис електронної пошти; електронне листування; облікові дані в соціальних мережах; інформація про кредитні операції та картки; номери телефонів контактів; фотографії і відео тощо.
2. Ненавмисне розкриття даних.

Список відомого шкідливого програмного забезпечення на мобільних пристроях включає в себе не дуже багато найменувань: «Virus», «Trojan», «Backdoor», «Dropper», «Downloader», «Tool», «Adware», «Dialer», «Worm», «Exploit», «Rootkit». Однак, варіацій цих видів програм мільйони.

Основна частка шкідливого програмного забезпечення розробляється для «Windows» і воно не може працювати на «Mac». Віруси і шкідливі програми для «Android» існують, так само як і антивіруси для цієї мобільної операційної системи. Однак, слід враховувати той факт, що «Android» є значною мірою захищеною платформою. Операційна система «Apple iOS» є ще більшою мірою закритою, ніж «Mac OS» або «Android». Творці вірусів не особливо працюють в напрямку «ОС Linux», у зв'язку з тим, що ця операційна система використовується малою кількістю користувачів.

Методи за допомогою яких проводяться сучасні атаки на системи управління військами в зоні антитерористичної операції за допомогою сучасних мобільних пристроїв можна поділити на три групи, а саме: «Віруси та хробаки», «Трояни», «Мережеві атаки». Сьогодні зараження шкідливим програмним забезпеченням можливе не тільки технічним шляхом. Досить активно для досягнення цієї мети використовуються методи соціальної інженерії (розсилка спаму, фішинг, рекламні банери).

РОЗДІЛ ІІІ
УДОСКОНАЛЕННЯ СИСТЕМИ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ЗАХОДІВ З МЕТОЮ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1. Застосування кримінальної відповідальності за порушення у сфері створення та розповсюдження шкідливого програмного забезпечення для мобільних пристроїв

Науково-технічний прогрес неможливий без широкомасштабного впровадження в управлінську діяльність, у різні сфери науки, техніки і виробництва електронно-обчислювальної техніки і мереж електрозв'язку. Це вимагає розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. У цьому відношенні базовими нормативними актами в Україні є: Кримінальний кодекс України, закони України «Про захист інформації в автоматизованих системах» від 5 липня 1994 р. (ВВР. — 1994. — № 31), «Про зв'язок» від 16 травня 1995 р. (в редакції від 5 червня 2003 р.) (ВВР. — 1995. — № 20); «Положення про технічний захист інформації в Україні», затверджене Указом Президента України від 29 вересня 1999 р. № 1229, та ін.

У розділі XVI КК у статтях 361, 362, 363 [21] передбачена відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), їх систем чи комп'ютерних мереж та мереж електрозв'язку.

Під шкідливими програмними засобами, призначеними для несанкціонованого втручання в роботу комп'ютерних мереж та мереж електрозв'язку (в тому числі мобільних пристроїв, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, слід розуміти програми (програмні блоки, програмне забезпечення), розроблені спеціально для несанкціонованого втручання в роботу техніки або мереж електрозв'язку,

використання яких спричиняє або створює загрозу заподіяння шкоди інформаційним відносинам

Безпосередній об'єкт злочину, передбаченого ст. 361-1 КК [21], становлять суспільні відносини власності на інформацію та відносини надання й отримання послуг електрозв'язку. Незаконне втручання в роботу мереж електрозв'язку з об'єктивної сторони характеризується проникненням, вторгненням у мережі електрозв'язку, що завжди пов'язане з порушенням режиму роботи цих систем чи їх складових частин. Це втручання повинне бути незаконним - системи електрозв'язку належать певному власнику - юридичній або фізичній особі і на втручання в їх роботу винна особа не має ні дійсного, ні передбачуваного права.

Способи незаконного вторгнення в роботу мереж електрозв'язку можуть бути різними:

- підключення до ліній зв'язку,
- використання різних технічних пристроїв («жучків») для прослуховування і фіксування інформації, яка є в обігу систем електрозв'язку та ін.

Наслідками такого діяння має бути: знищення, перекручення, блокування інформації або порушення встановленого порядку її маршрутизації. Зміст понять «знищення» і «перекручення» інформації мереж електрозв'язку тотожні поняттям «знищення» і «перекручення» комп'ютерної інформації (див. коментар п. 1 цієї статті).

Блокування інформації — це таке порушення інформаційних потоків мереж електрозв'язку, внаслідок якого суб'єкт-передавач інформації не може донести інформацію до абонента, а той не може цієї інформації отримати. Маршрутизація інформації — це порушення обрання послідовності вузлів мережі передачі інформації, якою інформація передається від джерела до приймача інформації.

Злочин вважається закінченим з моменту настання одного із зазначених наслідків — перекручення чи знищення комп'ютерної інформації, знищення хоча б одного носія такої інформації, при першій формі, при другій -

поширення (введення) у базу даних ЕОМ (комп'ютерів), їх систем чи мереж комп'ютерного вірусу, а при третій — з моменту знищення, перекручення, блокування інформації або з моменту порушення встановленого порядку її маршрутизації.

До предметів злочину, передбаченого ст. 361-1 КК [21], закон відносить специфічні програмні та технічні засоби. Об'єктивна сторона. Злочин, передбачений ч. 1 ст. 361 І КК, відноситься до злочинів із формальним складом, тобто вважається закінченим з моменту вчинення одного з альтернативних діянь, зазначених у диспозиції.

Розглядувана норма передбачає такі форми об'єктивної сторони:

1) створення шкідливих програмних або технічних засобів з метою використання, розповсюдження або збуту;

2) розповсюдження шкідливих програмних або технічних засобів;

3) збут шкідливих програмних або технічних засобів.

Створення шкідливих програмних або технічних засобів являє собою результат діяльності щодо розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу. Зазначимо, що створення буде кримінально караним тільки за наявності відповідної ознаки суб'єктивної сторони - мети використання, розповсюдження або збуту.

Розповсюдження шкідливих програмних засобів. Специфіка предмета цього злочину визначає особливості його розповсюдження які полягають у такому: до розповсюдження, у цьому складі, слід відносити не тільки надання оплатного або безоплатного доступу до певних предметів невизначеному колу осіб (традиційне розуміння розповсюдження), але також їх поширення низкою принципових способів, зумовлених особливостями предмета. До числа таких способів належать: самовідтворення; «закладання» в програмне забезпечення; розповсюдження з використанням інформаційної мережі.

Розповсюдження шкідливих програм способом самовідтворення означає, що розробник передбачає можливість шкідливої програми створювати свої копії. Цей спосіб найчастіше застосовується для розповсюдження «вірусів».

Найяскравішим прикладом комп'ютерного вірусу є так званий вірус Моріса. У листопаді 1988 року ним було уражено комп'ютерні системи Корнельського (Нью-Йорк), Стенфордського, Прінстонського (Нью-Джерсі), Гарвардського університетів, Центр Массачусетського технологічного інституту, заражено близько 1000 вузлів мережі Arpanet, серед постраждалих виявилася велика кількість урядових організацій, клінік і приватних компаній. Вірус переповнював пам'ять «зараженого» комп'ютера, чим виключав можливість роботи а інформацією, яка в ньому зберігалася. Збитки, завдані цим вірусом, оцінювалися фахівцями у 98 мільйонів доларів.

Спосіб «закладання» шкідливих програмних засобів у програмне забезпечення на мобільних пристроях полягає в тому, що особа, яка розповсюджує ці засоби, включає шкідливу програму до складу використовуваного програмного забезпечення. Один із таких способів розповсюдження шкідливих програм одержав назву «троянський кінь». Суть його полягає в тому, що винний розповсюджує якесь корисне програмне забезпечення, наприклад, текстовий редактор, перекладач або навчальну програму, однак крім корисних функцій програма містить і приховані, призначені для порушення права власності на інформацію.

Розповсюдження шляхом використання інформаційних мереж полягає, як правило, у наданні доступу до шкідливих програм шляхом їх розміщення на мережевих носіях інформації або в розсиланні електронною поштою копій шкідливих програм. Для прикладу розповсюдження шкідливих програм шляхом надання доступу розглянемо вирок Кіровського районного суду м. Кіровограда в справі -57/08 від 16 січня 2009року з обвинувачення А. у вчиненні злочину, передбаченого ч. І ст. 361-1 КК. У вироку зазначається, що А., користуючись локальною інформаційною мережею гуртожитків, діючи умисно, завантажив у власний комп'ютер програмні засоби. Ці засоби пізніше під час експертизи було визнано програмами для віддаленого зчитування паролів або нейтралізації засобів захисту програм чи інформації, які після встановлення паролів та їх нейтралізації дають можливість доступу до певної

інформації, програми, мережі, операційної системи та здійснення непомітно для власника чи законного користувача несанкціонованої передачі інформації сторонній особі. Після цього А. надав вільний доступ до свого комп'ютера всім абонентам локальної мережі. Суд правильно кваліфікував дії А. за ч. 1 ст. 361-1 КК як розповсюдження шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу комп'ютерної техніки [21].

Слід зауважити, що можливими є комбінації названих специфічних способів розповсюдження шкідливих програмних засобів, наприклад, розповсюдження «троянського» програмного забезпечення за допомогою електронної пошти або самовідтворення переданих електронною поштою копій шкідливих програм.

Виходячи з викладеного, можна дати таке визначення розповсюдження шкідливого програмного забезпечення: оплатне або безоплатне надання копій шкідливих програм або доступу до них невизначеному колу осіб, а також їх «закладання» в програмне забезпечення або розповсюдження за допомогою комп'ютерних мереж чи поширення шляхом самовідтворення.

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Однак і це діяння має певну специфіку. Крім простого передавання таких засобів, можливим є їх установлення в ЕОМ чи мобільного пристрою, системи або комп'ютерні мережі, які продаються або передаються на іншій основі, наприклад, здаються в оренду.

Збут шкідливих програмних або технічних засобів відрізняється від розповсюдження тим, що він пов'язаний з відчуженням предмета. Тобто якщо при розповсюдженні предмет залишається в особи (шкідливе програмне забезпечення продовжує знаходитися на мережевому ресурсі, з якого розповсюджується, повертається шкідливий технічний засіб, що передавався для використання), то в результаті збуту він відчужується, тобто не залишається в особи, яка його збуває.

Отже, під збутом шкідливих програмних або технічних засобів слід розуміти їх оплатне або безоплатне відчуження. Типовим прикладом збуту шкідливих програм є продаж дисків з записаними на них шкідливими програмами.

Суб'єкт цього злочину загальний, ним є фізична, осудна особа, що досягла 16-річного віку. Суб'єктивна сторона. Оскільки злочин, передбачений ст. 361-1 КК, відноситься до злочинів із формальним складом, зміст його суб'єктивної сторони визначається лише психічним ставленням до діяння і полягає в усвідомленні суспільної небезпечності та протиправності створення, розповсюдження або збуту шкідливих програмних і технічних засобів та бажанні вчинення таких дій.

У цій формі умисел може бути тільки прямим, а його специфіка виражається в тому, що свідомістю особи обов'язково охоплюється розуміння того, що створювані або розповсюджувані засоби спеціально призначені для несанкціонованого втручання в роботу на мобільних пристроях.

Отже, у Кримінальному кодексі України передбачена окрема стаття (ст. 361-1 КК), що встановлює відповідальність за створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів, мобільних пристроїв), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку.

На рівні підзаконних нормативних актів термін «програмний засіб» визначається як:

а) 2000 рік - взаємопов'язана сукупність програм, процедур, правил, документів і даних, що стосуються функціонування обчислювальної системи (що є, по суті, визначенням програмного забезпечення); [Постанова КМУ Про затвердження Порядку локалізації програмних продуктів (програмних засобів) для виконання Національної програми інформатизації від 16.11.1998 № 1815]

б) 2009 рік - як комп'ютерна програма, взаємопов'язана сукупністю комп'ютерних програм, процедур, правил, документації та даних (комбінація розуміння ПС як відокремленої програми, і як ПЗ) [Постанова КМУ Про затвердження загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів від 12.08.2009 № 869].

Відповідно, під програмним засобом розуміється як одна комп'ютерна програма, так і програмне забезпечення в цілому.

Відповідно до Закону «Про авторське право і суміжні права» комп'ютерна програма - це набір інструкцій у вигляді слів, цифр, коду, схем, символів чи в будь-якому іншому вигляді, виражені у формі, придатній для зчитування комп'ютером, які приводять його в дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах).

При такому підході з обсягу предмета злочину, передбаченого ст. 361-1 КК за формальними ознаками «випадає» один з найбільш доступних і поширених способів злому сайтів - SQL ін'єкція. Суть таких ін'єкцій - впровадження в дані (передані через GET, POST запити або значення «Cookie») довільного SQL коду. Якщо сайт вразливий і виконує такі ін'єкції, то це може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів і виконання довільних команд на сервері, що атакується.

SQL ін'єкція не є комп'ютерною програмою, а є тільки модифікованим запитом до бази даних, яка може бути можлива через некоректну обробку вхідних даних, що використовуються в SQL-запитах, зокрема, через відсутність фільтрації вхідних параметрів.

Однак, оскільки об'єктом посягання є комп'ютерна інформація та право власності на неї, то очевидно, що така дія не «випадає» з кримінально-правового регулювання в цілому, і при належній мірі суспільної небезпеки та

розміру заподіяного збитку повинна бути кваліфікованою за ч. 1 або ч. 2 ст. 361 КК.

Тут важливо зазначити, що диспозиція ст. 361-1 КК в принципі не передбачає варіант «використання шкідливого програмного засобу», а тільки «створення з метою використання», «поширення» або «збут» такого ПЗ. Таким чином, безпосереднє використання суб'єктом ним же створеної шкідливої програми на мобільних пристроях і отримання з її допомогою несанкціонованого доступу до інформації або порушення роботи комп'ютера утворює сукупність злочинів (ст. 371-1 і ст. 371 КК).

3.2. Формування системи корпоративної інформаційної безпеки шляхом захисту мобільних пристроїв

Компанії серйозно стурбовані безпекою мобільних пристроїв, що мають доступ до корпоративних даних, однак недооцінюють заходи, необхідні для контролю за їх використанням. Більше половини фахівців, що приймають рішення в області IT-безпеки, висловили серйозну стурбованість проблемами безпечного використання мобільних пристроїв в корпоративних мережах. Захист IT-інфраструктури будь-якої компанії являє собою цілий комплекс заходів, що включає такі захисні бар'єри як резервне копіювання, боротьба з витоком даних, відображення кібератак і багато інших процедур. Але недооцінювати важливість використання технологій «управління мобільними пристроями» (MDM) не можна.

Можливості MDM-технологій:

- застосування обмежень на установку і запуск програмного забезпечення на корпоративних мобільних пристроях (установка без обмежень неконтрольованого нового програмного забезпечення може завдати значної шкоди для корпоративних мереж);
- віддалене управління смартфонами і планшетами, що дозволяє блокувати доступ і видаляти інформацію у випадку крадіжки або втрати пристрою;

– захист пристроїв за допомогою PIN-кодів, а додатків, які мають доступ до корпоративних даних, за допомогою стійких паролів;

– керування настройками і політиками безпеки на мобільних пристроях нових співробітників;

– запобігання витоку конфіденційної корпоративної інформації засобами контролю додатків і шифрування.

Безпека даних забезпечує наступне:

1. Інтеграція з «Active Directory» (AD) на сервері підприємства. Вона забезпечується введенням профілю користувача або єдиної точки доступу в корпоративну мережу та реалізується на сервері зі встановленою операційною системою «Windows NT». Це служба каталогів, що дозволяє адміністраторам застосовувати групову політику для забезпечення однаковості налаштування користувацької робочого середовища, розгортати програмне забезпечення на безлічі комп'ютерів та мобільних пристроях через групові політики, встановлювати оновлення операційної системи, прикладного та серверного програмного забезпечення на всіх комп'ютерах та мобільних пристроях в мережі, використовуючи «Службу оновлення» «Windows Server». Засіб управління «Active Directory» зберігає дані і налаштування середовища в централізованій базі даних. Мережі «Active Directory» можуть бути різного розміру - від кількох сотень до кількох мільйонів об'єктів.

2. Апаратне шифрування даних. Для мобільних комп'ютерів «iPAD» з операційною системою «iOS» програмно-апаратне шифрування здійснюється для всіх даних автоматично; при цьому проводиться 256-розрядне шифрування за допомогою алгоритму «AES». Для пристроїв «Samsung» виконується 256-розрядне шифрування за стандартом «AES» з апаратним прискоренням, для пристроїв «Galaxy SII» підтримується апаратне шифрування.

3. Захист пошти і додатків сторонніх розробників шляхом шифрування файлів введенням персонального ключа.

Крім помилок осіб, які обслуговують інформаційні системи, в тому числі на мобільних пристроях, існує ряд загроз, що пов’язані з розробленням,

впровадженням та супроводом програмного забезпечення. Часто помилка в програмі викликає колапс системи і призводить до порушення критеріїв конфіденційності, цілісності чи доступності при захисті інформації від несанкціонованого доступу. Аналізуючи можливі загрози з точки зору найбільшої небезпеки для інформаційної системи, слід виділити шкідливе програмне забезпечення на мобільних пристроях.

Шкідливе програмне забезпечення - це будь-яка програма, що може бути написана з метою нанесення шкоди або для використання ресурсів атакованого комп'ютера чи мобільних пристроїв, або програмні продукти.

Джерелами помилок у програмному забезпеченні на мобільних пристроях можуть бути логічні помилки розробників програмного забезпечення, непередбачені ситуації, які проявляються в модернізації, заміні чи додаванні нових апаратних засобів, встановленні нових додатків, виході на нові режими роботи програмного забезпечення на мобільних пристроях, появі раніше не зафіксованих нештатних ситуацій, віруси, якими інфіковані програми, спеціальні програмні компоненти, які передбачені розробниками програмного забезпечення для різного роду цілей.

Однак, практика доводить [12, с.39-40], що винуватцями помилок у програмах найчастіше бувають самі програмісти. Один із загальних законів практичного програмування полягає в тому, що жодна програма не дає бажаних результатів при першій спробі трансляції та виконання. Найкращим шляхом для розроблення якісного програмного забезпечення є тестування програм та систем. Тестування - оцінка якості програмного забезпечення на мобільних пристроях методом експериментальної перевірки - шляхом виконання тестів. Мета тестування - виявити наявність помилок чи неузгодженостей. Іншими словами, це знаходження помилок (локалізація - задача діагностики), досягнення відсутності помилок. Це спосіб семантичної перевірки програми, який полягає в опрацюванні програмою послідовності різноманітних контрольних наборів тестів з відомими результатами. Тести підбираються так, щоб вони охопили найрізноманітніші типи можливих ситуацій.

Тестову перевірку на мобільних пристроях можна провести також шляхом додання до програми, що перевіряється, додаткових операторів, які будуть сигналізувати про перебіг її виконання й отримання результатів. Після проведення необхідних змін програмне забезпечення на мобільних пристроях повинне бути перетестовано. Для усунення можливості модифікації розробленого і протестованого програмного забезпечення слід застосувати інструменти криптографічного захисту, які реалізуються шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування чи відновлення змісту інформації, підтвердження її справжності, цілісності, авторства. Найкращим вибором для розробленого програмного комплексу є встановлення зашифрованого паролю на системну та адміністративну частину, використання ключів, що будуть відомі лише спеціалістам з необхідним рівнем доступу в інформаційній системі. Процес входу в програму на мобільних пристроях таким способом подібним до процесу авторизації або аутентифікації, однак має ключову відмінність - дані для входу кодуються з використанням одного зі стандартів шифрування даних, що значно підвищує криптостійкість програми та унеможливлює її шкідливу модифікацію.

Зашифровані дані однозначно залежать від ключа складним і запутаним способом. Кожний біт початкових даних впливає на кожний біт зашифрованих даних, що відкидає можливості розшифрування зловмисником. Поширення одного незашифрованого біта на велику кількість зашифрованих бітів приховує статистичну структуру початкових даних. Визначити, як статистичні характеристики зашифрованих даних залежать від статистичних характеристик початкових даних, досить непросто. Для бездоганного захисту ідентифікаторів має місце вровадження або додавання контекстного ідентифікатора до кожного блоку шифротексту. Міжнародний стандарт шифрування даних IDEA з цього погляду є дуже ефективним алгоритмом.

Створення об'єктів інтелектуальної власності, списків партнерів і клієнтів, а також комерційних секретів потребує від компаній значних зусиль, тому

одним з основних пріоритетів у їх роботі є захист цих мобільних даних за допомогою простих у використанні і легких в управлінні засобів захисту на основі політик [29]. Якщо пристрій, що належить співробітнику, використовується в робочих цілях, то виникає ряд додаткових питань, що стосуються конфіденційності користувача, контролю за пристроєм, порядку використання пристрою, політики безпеки та захисту даних, на які необхідно знайти відповідь для забезпечення захищеності комерційних даних. У зв'язку з цим ми пропонуємо наступні загальні правила захисту мобільних пристроїв:

1. Блокування пристрою. При втраті мобільного пристрою необхідно блокувати пристрій паролем (стійким або з обмеженою кількістю спроб введення), після яких дані на пристрої стираються або пристрій блокується.

2. Використання криптографічних засобів. Необхідно використовувати шифрування знімних носіїв, карт пам'яті – всього, до чого може отримати доступ зловмисник.

3. Заборона на збереження паролів в браузері мобільного пристрою. Не можна зберігати паролі в менеджерах паролів браузерів, навіть мобільних. Бажано встановити обмеження на доступ до листування поштового та смс, використовувати шифрування.

4. Заборона використання менеджерів паролів для корпоративних облікових записів. Існує безліч додатків, створених для зберігання всіх паролів на мобільному пристрої. Доступ до програми здійснюється введенням майстер-ключа. Якщо він недостатньо стійкий, вся парольна політика організації компрометується.

5. Заборона на установку програмного забезпечення з неперевірених джерел. Бажано використовувати програмного забезпечення відомих розробників.

6. Використання корпоративних політик та засобів антивірусного захисту. Якщо це можливо, дозволить уникнути безлічі загроз (в тому числі нових), а в разі втрати або крадіжки пристрою, здійснити його блокування і знищення даних на ньому.

7. Обмежити список даних, які можна передавати через хмарні сервіси.

Сучасні мобільні пристрої і додатки орієнтовані на використання безлічі хмарних сервісів. Необхідно стежити, щоб конфіденційні дані і дані, які стосуються комерційної таємниці, не були випадково синхронізовані або відправлені в один з таких сервісів.

Для полегшення управління мобільними пристроями працівників компаній було сформовано та запропоновано принципи побудови політики захисту мобільних пристроїв «Bring Your Own Device» та «Mobile Device Management». Вони включають в себе вище вказані правила захисту мобільних пристроїв, а також враховують особливості введення корпоративної діяльності. «Mobile Device Management» (MDM) – «управління мобільними пристроями». Використання рішень класу MDM дозволяє здійснити управління і контроль над різними типами мобільних пристроїв.

MDM – це технологія управління всіма мобільними пристроями, а технологія BYOD – орієнтована на специфіку управління пристроями співробітників в корпоративному середовищі. BYOD ближче до тактичного і в деяких аспектах стратегічного рівня управління інформаційними технологіями та інформаційною безпекою, тоді як MDM передбачає прикладну технічну реалізацію, і знаходиться скоріше на операційному рівні [88].

В загальному випадку системи типу MDM – це допоміжне програмне забезпечення, що дозволяє управляти мобільними пристроями на кожному етапі життєвого циклу, від ініціалізації до виводу з експлуатації. Одна із головних задач MDM – досягнення оптимального стану між безпекою і зручністю використання мобільних пристроїв, при мінімізації затрат на обслуговування. Це досягається за рахунок таких можливостей систем типу MDM [88]:

– централізоване управління мобільними налаштуваннями (парольні політики, параметри шифрування);

– заборона запуску небажаних додатків;

– інвентаризація програмних та апаратних засобів на мобільних пристроях;

– встановлення політики безпеки, сертифікатів безпеки і паролів на пристроях користувачів;

– налаштування WiFi і VPN відповідно до корпоративних стандартів;

– інсталювання мобільних додатків, ведення чорного та білого списків програм;

– надання віддаленої підтримки користувачів;

– віддалене блокування пристрою і знищення корпоративних даних в разі його втрати або крадіжки;

– налаштування обмеження для пристроїв, наприклад, заборона передачі даних в роумінгу, відключення камери, використання USB, Bluetooth, магазинів додатків («AppStore», «Google Play» та ін.);

– контроль відповідності пристрою встановленим корпоративним політикам;

– виконання резервного копіювання і шифрування даних на пристроях;

– здійснення групової підготовки, конфігурування та обслуговування пристроїв.

Виходячи з функціональних можливостей систем типу MDM пропонуємо загальний сценарій впровадження MDM [88]:

1. Ініціалізація, до якої входять такі етапи – інвентаризація, аналіз потреб користувачів в частині використання пристроїв та інформаційних ресурсів, класифікація інформаційних ресурсів, визначення інформаційних ризиків і моделювання загроз.

2. Розробка політики та стандарту застосування мобільних пристроїв та розробка регламентів захисту і управління мобільними пристроями.

3. Налаштування базових компонентів управління, дослідна експлуатація механізмів управління, масштабування системи.

4. Реалізація сервісу супроводу мобільних пристроїв, контроль використання мобільних додатків, контроль застосування і дотримання корпоративних політик для мобільних пристроїв, моніторинг діяльності користувачів.

5. Вивід пристроїв з обігу та розробка і виконання правил утилізації мобільного пристрою, реалізація регламенту дій у разі крадіжки або втрати мобільного пристрою.

З іншого боку, рішенням питання забезпечення політики безпеки інформації в корпоративній мережі є впровадження технології BYOD. Системи типу BYOD – це програмне забезпечення, яке управляє доступом до мережі користувачів, що підключаються до різних мережних пристроїв (точки Wi-Fi, комутатори, VPN концентратори). І залежно від того, чи знаходиться користувач в Інтернеті або всередині мережі, це програмне забезпечення встановлює відповідний профіль із заданими правами. А інтелектуальна мережна інфраструктура виконує завдання з реалізації прав доступу для кожного конкретного користувача. Основою ж для застосування такого сучасного підходу є розробка корпоративних політик використання особистих пристроїв. Для коректного забезпечення такого підходу, системи типу BYOD мають такі можливості [12]:

– плавне розміщення з використанням автоматичної реєстрації і створення профілю пристрою забезпечує збереження рівня продуктивності користувача.

– конвергентне управління для провідних і безпровідних мереж, клієнтських пристроїв.

– оптимізоване планування ресурсів з повним відстеженням трафіку і дій користувачів при використанні концепції BYOD.

– повна масштабована продуктивність провідних і безпровідних мереж.

– модульна система прямого управління дозволяє додавати ресурси і функції в міру необхідності.

Маючи такі функціональні можливості, технологія BYOD має такий сценарій впровадження в корпоративну мережу:

1. Визначення стратегії BYOD, розробка корпоративної політики, інвентаризація, аналіз потреб користувачів в частині використання пристроїв та інформаційних ресурсів, моделювання загроз інформаційної безпеки, розробка регламенту управління ризиками, розробка регламенту реагування на інциденти

безпеки, розробка нормативних документів, що розмежовують сфери відповідальності співробітників і організації при використанні персональних пристроїв, розробка стандарту щодо застосування особистих пристроїв в корпоративному середовищі.

2. Впровадження централізованих механізмів управління персональними пристроями співробітників, інтеграція централізованої системи управління з діючими інфраструктурними та прикладними системами і засобами захисту, навчання персоналу.

3. Контроль (періодичний аудит).

4. Супровід, модернізація – робота служби технічного супроводу. Відповідно до цього можна виділити ключові переваги систем типу BYOD:

– ідентифікація, управління мережею і доступом до додатків для будь-яких користувацьких пристроїв;

– безпека доступу до мережі і додатків незалежно від місцезнаходження;

– організація провідних і безпровідних мереж з використанням єдиного інтерфейсу прямого управління;

– спрощення проектування мереж для забезпечення масштабованості провідних і безпровідних локальних мереж;

– забезпечення доступу для мобільних пристроїв до мультимедійного вмісту.

В цілому, можна зробити висновок, що при сучасному розвитку інформаційних технологій та широкому використанні мобільних пристроїв, обидва рішення надають широкий набір заходів з нейтралізації шкідливого програмного забезпечення на мобільних пристроях.

3.3. Запобігання і усунення спроб несанкціонованого доступу до даних та переговорів абонентів мобільного зв’язку

24 жовтня 2016 року Україна приєдналась до глобальної освітньої кампанії для боротьби з шахрайством і з використанням шкідливого програмного забезпечення (питання стосувалося й програм такого роду на мобільних

пристроях) [45]. Завдяки спеціально розробленим інформаційним матеріалам українці дізналися про заходи безпеки для захисту від шахраїв, що діють через мобільні пристрої та розробки. Ми відмічаємо вкрай низький рівень обізнаності українців як щодо шкідливого програмного забезпечення в цілому, так і власне щодо захисту мобільних пристроїв від кібератак. Навіть про те, що підключення до Інтернету через загальнодоступну мережу чи точку доступу Wi-Fi може становити загрозу для конфіденційних даних, наші громадяни задумуються рідко. Багато хто навіть ризикує проводити розрахункові операції через безкоштовний Wi-Fi. Користуються популярністю серед українців і так звані джейлбрейки програмного забезпечення, які відкривають повний доступ до файлової системи пристроїв і дають можливість встановлювати додатки з неофіційних джерел

Тим не менш, кожен користувач мобільних пристроїв може звести до мінімуму вірогідність злочинних дій, дотримуючись основних правил безпеки:

- завантажувати мобільні додатки тільки з офіційних магазинів та від надійних розробників;
- встановлювати антивірусні програми на пристрої;
- ніколи не вносити конфіденційну інформацію платіжних карт у форми інтернет-ресурсів, що мають підозрілий вигляд або на який привело посилання з листа електронною поштою чи смс, отриманого від невідомого відправника.

Змістовні інформаційні матеріали про найпоширеніші методи шахрайства із використанням мобільних пристроїв та засоби захисту від них вже адаптовані для українців та доступні для ознайомлення в окремому розділі на сайті Асоціації ЄМА [45]. Матеріали представлені у зручних та зрозумілих форматах інфографіки, листівок та відео з порадами, які допоможуть користувачам мобільних пристроїв захиститись від шкідливого програмного забезпечення. А поради будуть корисні як для приватних власників смартфонів і планшетів, так і для підприємств.

Правоохоронні органи наголошують на тому, що використання кібершахраями шкідливого програмного забезпечення для мобільних пристроїв

набуває загрозливих масштабів. І сьогодні ми маємо приділяти більше уваги розповсюдженню інформації з цього приводу як серед населення, так і серед бізнесу, а також об'єднати зусилля держави і приватного сектору для протидії кіберзлочинам. Глобальна освітня кампанія «Europole Mobile Malware Awareness Campaign» – перший крок на цьому шляху.

До освітньої кампанії долучилися 22 держави-члени Європейського союзу, а також Колумбія, Норвегія та Україна. Проведення кампанії підтримують більше 45 партнерів по всьому світу: компанії та організації, які працюють у сфері інтернет-безпеки, фінансові інститути, уряди країн, які долучилися до ініціативи, профільні організації [1, с.90].

Сьогодні через мобільні пристрої користувачам доступно все більше вельми цінних сервісів, що вимагають уважного ставлення до безпеки (в числі яких, наприклад, мобільний банкінг, платежі і мобільні ідентифікатори). Відповідно, хакери чудово розуміють, що, організувавши витік даних аутентифікації через мобільний пристрій, вони зможуть отримати неавторизований доступ до онлайн-ресурсів, що представляє собою високу цінність. Зокрема, хакери будуть намагатися отримати доступ до фінансової інформації, облікових даних для доступу до соціальних мереж, до даних контрактів в мережах мобільного зв'язку. Так чи інакше, часом, цього може виявитися достатньо для повноцінного здійснення крадіжки особистості. Ця загроза стає особливо актуальною в даний час, коли ми спостерігаємо зростання числа нових мобільних додатків – згідно з дослідженням «Application Resource Center (Applause)», 90% компаній має намір до кінця цього року збільшити обсяг своїх інвестицій в розробку мобільних додатків [1]. Існує незаперечна потреба вже зараз захищати корпоративні ресурси, у тому числі інтелектуальну власність компаній та персональні дані користувачів, особливо з урахуванням такого великого числа використовуваних сьогодні пристроїв, на яких може бути запущено шкідливий код.

Якщо ми не звернемо на це належної уваги, то фактично ми залишаємо кінцевих користувачів і, в особливості, компанії в центрі уваги зловмисників, у

розпорядженні яких сьогодні накопичується все більше ресурсів і які все активніше вдаються у своїй діяльності новітніх технологій. Вони є експертами з розповсюдження шкідливого програмного забезпечення, вони з умислом використовують неофіційні репозиторії додатків, вбудовують шкідливий код в повідомлення електронної пошти, розсилають шкідливі смс і заражають браузери, і вони без найменших вагань готові скористатися будь-слабкістю або уразливістю. Саме тому постачальникам програм слід уважно поставитися до подібних погроз і зробити все необхідне, щоб допомогти споживачам відчути себе в безпеці, пропонуючи рішення, які забезпечують надійний захист від цих вразливостей.

Неуважні, або недосвідчені користувачі мобільних пристроїв випадково встановлюють зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисники можуть отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, можливості зловмисників збільшуються в рази.

Безпека мобільних пристроїв, на нашу думку, забезпечується:

1. Політикою парольного захисту, до якої відносяться встановлення пароля і періоду його дії. Так, для планшетних комп'ютерів «iPad» потрібно ввести складний пароль, що складається з букв і цифр, загальна кількість символів не повинно бути менше п'яти.

Правила використання PIN включають довжину, складність, історію, автоблокування при неправильному введенні. Доступ до віртуального корпоративного «Робочого столу», що встановлюється на мобільний апарат співробітника, здійснюється тільки після введення аутентифікаційних даних імені та пароля.

2. Обмеженнями на використання пристроїв і доступу до сервісів. Для пристроїв на основі операційної системи «Android» обмеження відносяться до

управління мікрофоном і камерою, доступом до магазину додатків «Play Market» («Android Market»), використання GPS-приймача, централізованої налаштуванні мережі Wi-Fi, додатком «MS Exchange ActiveSync». Вони також належать до використання спеціального сервісу «C2DM», що надає API для відправки повідомлень додаткам, встановленим на пристроях «Android». Застосування даного сервісу є способом передачі повідомлення користувальницьких додатків, зареєстрованому в системі, але в даний момент неактивного.

Для пристроїв на основі операційної системи «iOS» («iPhone» / «iPad») обмеження ставляться до використання фотокамери і GPS-приймача, доступу до «iTunes», «YouTub»c, «AppStore», централізованої настройки пошти, календарів, Wi-Fi, SCEP («Simple Certificate Enrollment Protocol»). В останньому випадку обмеження ставляться до застосування протоколу масштабованої видачі та анулювання цифрових сертифікатів.

3. Установленими на підприємстві правилами та угодами. Наприклад, правилами може обмежуватися можливість передачі або синхронізації користувальницьких файлів (документів, таблиць, презентацій) між сервером і клієнтом.

Небезпеку для інформації несуть відкриті Wi-Fi мережі, адже кожен має змогу до них підключитись та виконувати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи дізнавшись його у працівника.

Ненадійні паролі зазвичай стають причиною хакерських атак. Після того як зловмисник підключиться до мережі, він отримує доступ абсолютно до всіх підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі пристрої також піддаються ризику хакерської атаки.

Загальну модель перехоплення та захисту інформації в бездротових мережах можемо подати через сукупність кроків з можливими шляхами перехоплення та захисту інформації:

1. Стандартна взаємодія пристрою з глобальною мережею через роутер (нормальний стан). Модель описує нормальний стан роботи мережі, інформація з мобільного пристрою передається через бездротову мережу, без втручання зловмисника.

2. Вплив зловмисника на бездротову мережу з метою перехоплення інформації з пристрою. В даному випадку бездротова мережа піддається впливу зловмисника.

Розглядається вплив на об’єкт з використанням локальної бездротової мережі. Зловмисник з використанням спеціального програмного та апаратного забезпечення намагається проникнути в мережу. Метою таких дій є бажання отримати доступ до мережі, що може дати йому змогу перехоплювати інформацію з пристроїв підключених до мережі. Також зловмисник може змінювати параметри об’єкта таким чином, що клієнт мережі може нічого не помітити, але буде передавати зловмиснику свої дані, чи відвідувати саме ті ресурси, в яких зацікавлений зловмисник.

3. Засоби захисту адміністратора для бездротової мережі. При взаємодії клієнта мережі через об’єкт можливі декілька сценаріїв роботи, а саме:

- відкрита мережа без використання шифрування, до якої може підключитись кожен;

- з використання шифрування (WEP, WPA/WPA2 – Personal, WPA/WPA2 Enterprise).

Окрім даних інструментів адміністратор може використовувати ще додаткові програмні (антивірусне програмне забезпечення, сканер мережі, брандмауер) та програмно-апаратні засоби (NGFW, «Radius-server», хмарні сервіси).

Дані інструменти захисту можуть працювати окремо, або взаємодіяти між собою, окрім цього більшість з них має можливість захистити від впливу з глобальної мережі.

4. Вплив зловмисника на інформацію через глобальну мережу та вразливості зв’язку між нею та роутером.

Якщо адміністратор мережі лишив налаштування об’єкту «за замовчуванням», або не встановив захищені налаштування, то вплив на локальну бездротову мережу можливий віддалено, з використанням глобальної мережі та вразливості в налаштуваннях. Таким чином зловмисник може впливати на конфігурацію та налаштування бездротової мережі перебуваючи навіть в іншій країні.

5. Засоби захисту адміністратора для каналу зв’язку між глобальною мережею та роутером.

Завдяки використанню стійкого пароля та зміни логіна для доступу до налаштувань, обмеження кількості спроб авторизації та забороні доступу до налаштувань локальної мережі з використанням глобальної, адміністратор може мінімізувати можливості зловмисника. Для додаткового захисту необхідно використовувати програмно–апаратні засоби.

6. Прямий вплив зловмисника на адміністратора через бездротову мережу.

Завдяки використанню спеціальних програмних та програмно-апаратних засобів, зловмисник може видавати себе за адміністратора мережі та виконувати зловмисні дії від його особи, окрім цього можливе блокування або створення перешкод для захисту.

7. Засоби протидії адміністратора від прямого впливу зловмисника на бездротову мережу.

Завдяки програмним та програмно-апаратним засобам адміністратор може не тільки захистити мережу від проникнення, а і обмежити доступ та захистити себе від нападу зловмисника.

8. Прямий вплив зловмисника на адміністратора через глобальну мережу.

Використовуючи зловмисне програмне забезпечення та вразливості в налаштуваннях зловмисник може задіяти глобальну мережу та виконувати дії аналогічні п.6.

9. Засоби протидії адміністратора від прямого впливу зловмисника на глобальну мережу.

Аналогічно до п.7, адміністратор повинен захищати мережу від впливу через глобальну мережу.

10. Вплив зловмисника на бездротову мережу через глобальну з використанням хмарних технологій.

З використанням сучасних хмарних технологій зловмисник може виконувати необхідні йому обчислення для злому на віддалених, але високопродуктивних програмно - апаратних засобах.

11. Захист бездротової мережі адміністратором через глобальну з використанням хмарних технологій.

Завдяки використанню сучасних хмарних технологій адміністратор також має програмно-апаратні засоби, які дозволяють йому аналізувати та відслідковувати спроби несанкціонованого доступу завдяки спеціальним хмарним сервісам.

12. Захист бездротової мережі адміністратором з використанням «radiusserver». Для конфігурації локальної мережі підприємства використовують дану модель захисту, яка робить практично неможливим перехоплення інформації в захищеній мережі.

13. Захист бездротової мережі адміністратором з використанням NGFW.

З використанням даного програмно-апаратного засобу можна захистити мережу як локально, так і від впливу з глобальної мережі, а також з використанням хмарних сервісів, що дає змогу поєднати в собі інструменти описані в п. 3, 5, 7, 9, 11, що робить його універсальним засобом моніторингу та захисту мережі, як локальної, так і глобальної.

Використовуючи спеціалізоване програмно-апаратне забезпечення є можливість підвищити рівень захисту мереж від зловмисних дій, а правильне

налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв.

Необізнаність користувачів та адміністраторів мереж, що призводить до великої ймовірності перехоплення інформації вирішується навчанням правилам інформаційної безпеки. Ймовірність перехоплення інформації можна зменшити шляхом використання засобів захисту в повному обсязі, але проблема відсутності коректного налаштування може залишатись, через використання нестійких паролів.

Абоненти мобільного зв'язку України з пристроями типу «Android» у 2016-2017 р.р. піддавалися вірусній смс-атаці «Samsapo A», яка здійснювалася шляхом масової розсилки смс-повідомлень, що містять шкідливе програмне забезпечення [47, с.131].

Основною ознакою шкідливого програмного забезпечення є наявність в тексті смс-повідомлення посилання на шкідливий сайт «motosan.ru». Повідомлення надходять з номера з адресної книги абонента або з невідомого номера.

Дія вірусу при відкритті повідомлення і переході абонента за наявним в тексті посиланням:

- власникові телефону пропонується встановити додаток «Google Play»;

- вірус зберігається на карті пам'яті телефону і без участі власника відправляє смс;

- смс пересилається за номерами контактів адресної книги абонента, за вартістю згідно тарифного плану оператора мобільного зв'язку;

- при відкритті одержаного смс-повідомлення з рахунку власника смартфону також знімається 4 гривні за кожне повідомлення про доставку;

- вірус передає список контактів адресної книги та іншу персональну інформацію на сервер зловмисника;

- вірус відкриває доступ зловмиснику для установки інших вірусів без участі власника зараженого смартфону.

Якщо було здійснено перехід по посиланню та було завантажено вірус, рекомендуємо виконати наступні дії:

1. Перевірити наявність інсталяційного файлу шкідливого програмного забезпечення і видалити його.

2. Перевірити, чи вірус було встановлено: перейти в розділ Менеджера програм «налаштування-опції» і знайти в розділі завантажений і встановлений додаток «Google Play» з розміром близько 200 Кб. (Важливо не переплутати з офіційним додатком «Google Play Маркет»).

3. Якщо наявний встановлений додаток «Google Play» (розмір приблизно 204 Кб) необхідно натиснути на нього і далі натиснути «видалити».

Заходи з попередження спроб ураження мобільного телефону шкідливим програмним забезпеченням «Samsapo A»:

1. При одержанні смс-повідомлення, що містить посилання на шкідливий сайт «motosan.ru», не слід переходити за вказаним посиланням, а одразу видалити SMS-повідомлення.

2. Користувач ні в якому разі не повинен погоджуватися на інсталяцію програм, що не відносяться до «Google Маркета».

3. Користувачу слід відключити можливість інсталяції програм з невідомих джерел шляхом зняття відповідної галочки в меню «Безпека» налаштувань телефону.

4. Користувачу необхідно встановити антивірусне програмне забезпечення для «Android». Його можливо встановити з безкоштовних джерел антивірусного програмного забезпечення «Google».

5. Користувачу слід завантажити останні антивірусні оновлення та провести перевірку абонентського мобільного пристрою на наявність шкідливого програмного забезпечення.

Наступні поради допоможуть уникнути проблем з вірусами на телефоні:

1. Перейти на прихований режим Bluetooth. Якщо в телефоні є Bluetooth можливості, переконатися, що функцію Bluetooth можливості переключені на прихований або невидимий режим, якщо спеціально не потрібно, щоб бути

видимим. Це допоможе застерегти інші Bluetooth-пристрої від пошуку телефону (якщо їм не буде надано необхідного дозволу) і, отже, допоможе захистити телефон від хробаків, які поширюються з використанням технології Bluetooth.

2. Варто бути уважними при відкритті вкладень. При прийомі вкладень, відправлених через Bluetooth або MMS, проявляти обережність, так як вони можуть включати в себе шкідливу програму забезпечення. Переконатися, що програма або прихильність відбувається з відомого джерела, і насторожено ставитися до відкриття файлів, які мають незнайомий прикріплений до них текст, навіть якщо вони надходять від знайомих.

3. Завантажувати контент тільки з надійного джерела. Надійні джерела включають в себе портали операторів та інших відомих брендів, які гарантують адекватний захист від вірусів та іншого шкідливого програмного забезпечення. Однак, шкідливі програми або шахрайські користувачі можуть фальсифікувати появу надійного джерела.

4. Завантажити в телефон антивірусне програмне забезпечення. Антивірусне програмне забезпечення запобігає зараженню телефону вірусом.

Окремо варто виділити категорію «діалер» як програмне забезпечення на мобільних пристроях . Діалер («Dialer») - шкідливе програмне забезпечення, що краде гроші з телефонних рахунків.

Діалери, з'явилися ще за часів повільного Інтернет, до якого користувач підключався за допомогою модему і телефонної лінії. Користь кіберзлочинців від зараження комп'ютера або мобільного пристрою таким «вірусом» полягає в крадіжці грошей, шляхом використання дорогого інтернет-з'єднання, з подальшим виставленням рахунків за телефонні дзвінки. Хоча, в нинішній час, мало хто використовує модем для виходу в Інтернет з комп'ютера за допомогою телефону, такий вид шахрайства, як «Dialer», не втратив своєї актуальності.

Природно, не маючи модему, комп'ютер не схильний до таких загроз, однак, поява гаджетів, які використовують сім-карту і мобільних телефонів дало новий сплеск поширенню даного виду шкідливого програмного

забезпечення на мобільних пристроях. При зараженні мобільного телефону, шкідливе програмне забезпечення додзвонюється на платний телефонний номер, при цьому відключаючи на пристрої динамік, щоб приховати свою активність. Через короткий час всі кошти на телефонному рахунку списуються на користь платного номера, про що жертва дізнається, в більшості випадків, після активності вірусу. Ні про що не підозрюючи, користувач кладе чергову суму грошей собі на рахунок. Тільки після декількох прецедентів зникнення грошей зі свого рахунку, жертва намагається з'ясувати причину, що в більшості випадків не приводить до успіху, оскільки «Dialer» добре маскується в операційній системі телефону.

Шахрая, на чий номер був здійснений дзвінок, складно притягнути до відповідальності, тим більше повернути вкрадені гроші. Це обумовлено тим, що платний номер, на який відбувався дзвінок, може бути зареєстрований в іншій країні, де знайти кіберзлочинця практично неможливо. Боротьба з цим видом шахрайства зводиться до блокування платних номерів, запідозрених у зловмисних діях. Однак, це не панацея, оскільки сучасні діалери здатні віддалено змінювати номер, на який здійснюється дзвінок.

Існує маса програмного забезпечення, яке можна віднести до категорії «Dialer», але вони приносять користь, а не шкоду користувачеві. Більшість таких програм використовують принцип автодозвону або повторного з'єднання з Інтернет. До них можна віднести багато менеджерів завантажень, програми автодозвону для телефонів та інше. Функції таких програм зручні, оскільки можуть включити переадресацію дзвінків, коли цільовий номер зайнятий, або розірвати з'єднання з Інтернет для перевірки залишку коштів на рахунку та повторного приєднання. При цьому великий відсоток таких програм несе в собі приховану загрозу, оскільки вони можуть бути написані з метою крадіжки грошей з особового рахунку.

Для того щоб на 100% забезпечити себе від таких неприємностей, краще не тримати гроші на своєму телефонному рахунку. У такому випадку, діалер не

зможе реалізовувати свої шкідливі функції, однак, при цьому з телефону буде неможливо подзвонити.

Інший варіант - це встановлювати тільки ліцензоване програмне забезпечення від перевірених розробників. Тоді шанс зараження вірусом або шкідливим програмним забезпеченням скоротиться в десятки разів.

Третій, оптимальний варіант, який підійде як простим, так і досвідченим власникам гаджетів - це установка антивірусного програмного забезпечення. У цьому випадку дії користувача контролює антивірусна програма, яка відстежує підозрілу активність телефону і блокує або попереджає про можливий несанкціонований дзвінок.

Використання загальнодоступних мереж Wi-Fi в громадських місцях залишається важливим методом доступу до Інтернет. Однак, варто пам'ятати, що переважна більшість Wi-Fi мереж громадських місцях: в парках, кафе, бібліотеках, мають дуже низький рівень захисту від злому. Отже, отримавши доступ до керування ними, шахраї можуть дістати доступ до конфіденційної інформації користувачів - списків пошукових запитів, інформації про пересування, приватних файлів та багато іншого.

Для того, що б не потрапити в тенета шахраїв, необхідно дотримуватися простих правил безпеки при роботі з громадськими Wi-Fi мережами. Ці правила стосуються всіх видів пристроїв – портативних мобільних комп’ютерів, планшетів, смартфонів:

1. Встановити антивірус.

2. Вимкнути функцію автоматичного виявлення та підключення до доступних мереж.

3. Не здійснювати жодних грошових операцій: перекази, покупки, регулярні платежі.

4. Не вимикати брандмауер.

5. Використовувати безпечний протокол з'єднання HTTPS.

6. Вимкнути загальний доступ до файлів і папок.

Висновок до розділу 3

Використання в корпоративних мережах захисту інформації рішень класу MDM дозволяє здійснити управління і контроль над різними типами мобільних пристроїв. MDM – це технологія управління всіма мобільними пристроями, а технологія BYOD – орієнтована на специфіку управління пристроями співробітників в корпоративному середовищі. Їхні переваги очевидні: централізоване управління мобільними налаштуваннями (парольні політики, параметри шифрування);

– заборона запуску небажаних додатків;

– інвентаризація програмних та апаратних засобів на мобільних пристроях;

– встановлення політики безпеки, сертифікатів безпеки і паролів на пристроях користувачів;

– налаштування WiFi і VPN відповідно до корпоративних стандартів;

– інсталювання мобільних додатків, ведення чорного та білого списків програм;

– надання віддаленої підтримки користувачів;

– віддалене блокування пристрою і знищення корпоративних даних в разі його втрати або крадіжки;

– налаштування обмеження для пристроїв, наприклад;

– контроль відповідності пристрою встановленим корпоративним політикам;

– виконання резервного копіювання і шифрування даних на пристроях;

– здійснення групової підготовки, конфігурування та обслуговування пристроїв.

Безпека мобільних пристроїв від шкідливого програмного забезпечення, на нашу думку, забезпечується:

1. Політикою парольного захисту, до якої відносяться встановлення пароля і періоду його дії.

2. Обмеженнями на використання пристроїв і доступу до сервісів.

3. Установленими на підприємстві правилами та угодами.

ВИСНОВКИ

Магістерська робота присвячена вивченню теоретичних та практичних аспектів нейтралізації загроз, що виникають в результаті використання шкідливого програмного забезпечення на мобільних пристроях. Основні положення магістерської роботи:

1. Охарактеризовано поняття та види загроз інформаційної безпеки для користувачів сучасних мобільних пристроїв.

Загроза інформаційній безпеці – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Загрози інформаційним системам та ресурсам для користувачів сучасних мобільних пристроїв можна умовно поділити на основні чотири групи:

- фізичні, тобто крадіжка носіїв, знищення засобів обробки інформації, а також апаратних чи парольних програмних ключів;
- технічні, у тому числі радіоелектронне перехоплення інформації у лініях зв’язку, радіоелектронне придушення сигналу у лініях зв’язку та системах управління;
- програмні, тобто знищення та модифікація даних в інформаційних системах, впровадження «вірусів», апаратних та програмних закладок;
- інформаційні, які становлять порушення регламентів інформаційного обміну: дезінформація,несанкціонований доступ до інформаційних ресурсів,незаконне збирання та використання інформації, незаконне копіювання даних в інформаційних системах, укриття чи спотворення інформації, крадіжка інформації з баз даних.

2. Розглянуто типи сучасного шкідливого програмного забезпечення на комп’ютерах та мобільних пристроях:

- першу групу складають ті програми, що вимагають програм-носіїв. До них, в основному, відносяться фрагменти програм, що не можуть існувати незалежно від програм-носіїв, в ролі яких можуть виступати деякі програмні додатки,

утиліти, системні програми. В цю групу входять: люки, логічні бомби, троянські коні, віруси.

- в другу групу входять програми, що є незалежними. До них відносяться окремі незалежні програми, які можуть плануватися і запускатися операційною системою. До цієї групи належать: черв'яки, зомбі, утиліти прихованого адміністрування, програми-крадії паролів, «intended»-віруси, конструктори вірусів, поліморфік-генератори.

3. Охарактеризовано загрози для мобільних пристроїв. Зазначено, що для смартфонів характерні ті ж самі загрози, що і для персональних комп'ютерів, оскільки телефон, по суті, і є комп'ютером. Це обумовлює і можливість запуску шкідливого програмного забезпечення на мобільних пристроях, і шпигунства за власниками мобільних пристроїв, і крадіжку конфіденційної інформації, крадіжку грошей з мобільних рахунків.

Кожен третій житель України (33%) має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – половина (50%). Якщо серед молоді 65% користуються смартфонами, то серед осіб літнього віку – 5%. Типовий користувач смартфонів – це молода особа не старше 40 років з вищою освітою, яка проживає у середніх і великих містах України. Більшість (66%) користуються операційною системою «Android», а 68% користувачів смартфонів мають досвід встановлення додатків. Найбільш популярними є соціальні мережі (73%), ігри (61%), навігація (51%), месенджери (49%).

Ненадійні паролі зазвичай стають причиною хакерських атак: 30% користувачів використовують в якості пароля слово з топ - 10 000 паролів.

4. Розглянуто відомі технології нейтралізації та попередження ознак шкідливого програмного забезпечення.

Для захисту мобільних комп'ютерних пристроїв від загроз рекомендовано дотримуватись наступних правил:

а) встановити Pin-код, пароль на телефон, SIM-карту та карти-пам'яті.

б) встановити антивірусні програми та постійно оновлювати їх, регулярно перевіряти мобільний пристрій на наявність вірусів.

в) не встановлювати додатки (ігри, програми), які запитують доступ до персональної та конфіденційної інформації, та видаляти ті з них, які не використовуються.

г) перед встановленням додатків переглядати їх рейтинги та відгуки.

д) правильно налаштувати мобільний пристрій, оскільки він має свою систему захисту.

е) використовувати функцію, яка дозволяє або блокує доступ до Інтернету.

є) якщо телефон містить конфіденційну інформацію, можна використовувати вбудовану функцію повного шифрування телефону або пам’яті телефону.

ж) не використовувати незахищені Wi-Fi мережі, особливо при онлайн-покупці товарів та послуг.

з) регулярно оновлювати програмне забезпечення мобільних пристроїв з перевірених джерел.

и) не переходити за гіперпосиланнями, які містять повідомленнях з невідомих адрес, а також не натискати на спливаючі банери та реклами.

і) не виходити за рамки визначеної політики безпеки.

5. Проведено аналіз шкідливих програм на мобільних пристроях в контексті мінімізації рівня зараження від їх дії.

Зазначено, що масове використання на мобільних пристроях однотипних операційних систем дозволяє розробляти варіанти вірусів та інших шкідливих програм, користуючись притаманними їм особливостями. В результаті чого стають можливими епідемії, викликані мережевими хробаками («CodeRed», «Sasse»r, «Slammer», «Lovesan (Blaster)» - розроблено для операційної системи «Windows», «Ramen» і «Slapper» - для «Linux»), троянськими програмами («Trojan Winlock») тощо.

В результаті проведеного дослідження вказано, що:

- 56 % додатків передають унікальний номер апарата іншим компаніям (рекламним мережам) без будь-якого повідомлення або дозволу користувача;
- 47 % мобільних додатків передають дані про географічне положення;
- 5 % посилають дані про вік, стать та інші персональні дані;

- додатки для «Apple iOS» передають більше даних, ніж додатки для «Android», проте цю тенденцію неможливо перевірити для всієї бази кількох сотень тисяч додатків для обох операційних систем.

Інші дослідження показали вразливість наступних додатків: «Gmail» (92% успішних атак), «H&R Block» (92%), «Newegg» (86%), «WebMD» (85%), «CHASE Bank» (83%), «Hotels.com» (83%). Лише захист додатків «Amazon» було відносно важко подолати.

У першому кварталі 2017 року Іран був країною, у якій спостерігався найвищий відсоток атак на мобільні пристрої через зловмисні програми - 47,35%. Бангладеш зайняв друге місце: 36,25% користувачів отримали мобільні загрози принаймні один раз протягом кварталу. Наступними країнами є Індонезія та Китай; частка обох країн склала трохи більше 32%. Росія (11,6%) зайняла 40-е місце в цьому рейтингу, у Франції - 8,1%, у США - 69,9%, в Італії - 7,1%, у Німеччині - 6,2% та 72% у Британії - 5,8%. Найбезпечнішими країнами були Фінляндія (2,7%), Грузія (2,5%) та Японія (1,5%).

6. Здійснено оцінку рівня захисту інформації на мобільних комп’ютерних пристроях з операційними системами «Android», «Apple iOS» та «Windows».

Зазначено, що операційна система «Android» упевнено завойовує популярність, і на даний момент залишила позаду «Windows Mobile». Віруси, трояни та інші види шкідливого програмного забезпечення — серйозна і поширена проблема платформи «Windows». Віруси і шкідливі програми для «Android» існують, так само як і антивіруси для цієї мобільної операційної системи. Розширюється і список платформ, для яких зафіксовані шкідливі програми. Тепер до них додалися «iOS» (операційна система для «iPhone»/»iPod Touch»/»iPad») і «Android». Метою впровадження вірусних програм до файлової системи «iOS» є отримання доступу до особистої інформації, паролів доступу до банківських сервісів і платіжних систем, стеження за користувачем, розсилка спаму і реклами тощо. Вберегтися від втручання зловмисників у роботу мобільних пристроїв «Apple» можна ретельно дотримуючись правил безпеки:

– не використовувати модифіковані версії «iOS»;

– відмовитися від джелбрейку;

– своєчасно оновлювати операційну систему після появи офіційних версій;

– для встановлення нових додатків користуватися лише «AppStore», звертати увагу на відгуки інших користувачів.

Для того щоб мінімізувати зараження «вірусами» операційної системи «Windows» чи «Android» мобільного пристрою необхідно:

– своєчасно оновлювати програми, що виправить уразливості у встановленому програмному забезпеченні;

– не використовувати обліковий запис адміністратора в щоденній роботі з операційною системою «Windows» чи «Android»;

– уникати зміни системних файлів і встановлення програм з невідомих джерел;

– встановити антивірус;

– створювати резервні копії всіх важливих документів і файлів.

7. Досліджено сучасні методи атак на автоматизовані системи управління військами та інформаційні мережі в зоні антитерористичної операції через мобільні пристрої.

Зазначено, що на даний час в Україні також активно ведеться робота по створенню сучасних автоматизованих систем управління військами за допомогою сучасних мобільних пристроїв. Одними з основних в таких системах є питання захисту інформації та протидії атакам противника. Методи за допомогою яких проводяться сучасні атаки на системи управління військами в зоні антитерористичної операції за допомогою сучасних мобільних пристроїв можна поділити на три групи, а саме:

– «Віруси та хробаки», коли шкідливе програмне забезпечення здатне додати свій код в інші програми або файли;

– «Трояни», що маскуються під нешкідливі, навіть корисні додатки, але наносять збитки інформаційній системі управління військами в зоні антитерористичної операції після інсталяції;

– «Мережеві атаки», спрямовані на вторгнення до інформаційної мережі з метою аналізу уразливостей та в подальшому нанесення удару по інформаційній системі.

Такі атаки можуть нанести значних збитків та витоку конфіденційної інформації з управління військами в зоні антитерористичної операції, ці атаки маскуються та перешкоджають антивірусному програмному забезпеченню на мобільних пристроях, що ускладнює процес виявлення та обеззараження інформаційної системи.

На основі проведеного аналізу сучасних методів атаки на інформаційні системи та мережі можна виокремлено віруси та хробаки, як найбільш небезпечні методи атак на мобільних пристроях. Серед яких «Boot sector Virus», «Polymorphic Virus», «Stealth Virus», «Multipartite Virus» є особливо небезпечними методами атаки.

8. Досліджено технічні та правові питання програмного забезпечення, у тому числі шкідливого (небезпечного) та визначити необхідність застосування кримінальної відповідальності за порушення у сфері створення та розповсюдження шкідливого програмного забезпечення для мобільних пристроїв.

Науково-технічний прогрес неможливий без широкомасштабного впровадження в управлінську діяльність, у різні сфери науки, техніки і виробництва електронно-обчислювальної техніки і мереж електрозв'язку. Це вимагає розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. У цьому відношенні базовими нормативними актами в Україні є: Кримінальний кодекс України, закони України «Про захист інформації в автоматизованих системах», «Про зв'язок», «Положення про технічний захист інформації в Україні» та ін.

У Кримінальному кодексі України передбачена окрема стаття (ст. 361-1 КК), що встановлює відповідальність за створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого

втручання в роботу електронно-обчислювальних машин (комп'ютерів, мобільних пристроїв), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку. До предметів злочину, передбаченого ст. 361-1 КК, закон відносить специфічні програмні та технічні засоби. Злочин, передбачений ч. 1 ст. 361 І КК, відноситься до злочинів із формальним складом, тобто вважається закінченим з моменту вчинення одного з альтернативних діянь, зазначених у диспозиції. Розглядувана норма передбачає такі форми об'єктивної сторони:

- створення шкідливих програмних або технічних засобів з метою використання, розповсюдження або збуту;
- розповсюдження шкідливих програмних або технічних засобів;
- збут шкідливих програмних або технічних засобів.

Тут важливо зазначити, що диспозиція ст. 361-1 КК в принципі не передбачає варіант «використання шкідливого програмного засобу», а тільки «створення з метою використання», «поширення» або «збут» такого програмного забезпеення. Таким чином, безпосереднє використання суб'єктом ним же створеної шкідливої програми на мобільних пристроях і отримання з її допомогою несанкціонованого доступу до інформації або порушення роботи комп'ютера чи мобільного пристрою утворює сукупність злочинів (ст. 371-1 і ст. 371 КК).

9. Сформовано систему корпоративної інформаційної безпеки шляхом захисту мобільних пристроїв.

Зазначено, що компанії серйозно стурбовані безпекою мобільних пристроїв, що мають доступ до корпоративних даних, однак недооцінюють заходи, необхідні для контролю за їх використанням. Більше половини фахівців, що приймають рішення в області IT-безпеки, висловили серйозну стурбованість проблемами безпечного використання мобільних пристроїв в корпоративних мережах. Якщо пристрій, що належить співробітнику, використовується в робочих цілях, то виникає ряд додаткових питань, що стосуються конфіденційності користувача, контролю за пристроєм, порядку використання пристрою, політики безпеки та захисту даних, на які необхідно

знайти відповідь для забезпечення захищеності комерційних даних. У зв’язку з цим у магістерській роботі запропоновано наступні загальні правила захисту мобільних пристроїв:

- блокування пристрою. При втраті мобільного пристрою необхідно блокувати пристрій паролем (стійким або з обмеженою кількістю спроб введення), після яких дані на пристрої стираються або пристрій блокується;
- використання криптографічних засобів. Необхідно використовувати шифрування знімних носіїв, карт пам'яті – всього, до чого може отримати доступ зловмисник;
- заборона на збереження паролів в браузері мобільного пристрою. Не можна зберігати паролі в менеджерах паролів браузерів, навіть мобільних. Бажано встановити обмеження на доступ до листування поштового та смс, використовувати шифрування;
- заборона використання менеджерів паролів для корпоративних облікових записів. Існує безліч додатків, створених для зберігання всіх паролів на мобільному пристрої. Доступ до програми здійснюється введенням майстер-ключа. Якщо він недостатньо стійкий, вся парольна політика організації компрометується;
- заборона на установку програмного забезпечення з неперевірених джерел. Бажано використовувати програмного забезпечення відомих розробників;
- використання корпоративних політик та засобів антивірусного захисту. Якщо це можливо, дозволить уникнути безлічі загроз (в тому числі нових), а в разі втрати або крадіжки пристрою, здійснити його блокування і знищення даних на ньому;
- обмежити список даних, які можна передавати через хмарні сервіси. Сучасні мобільні пристрої і додатки орієнтовані на використання безлічі хмарних сервісів. Необхідно стежити, щоб конфіденційні дані і дані, які стосуються комерційної таємниці, не були випадково синхронізовані або відправлені в один з таких сервісів.

Рекомендовано застовування «Mobile Device Management» (MDM) – «управління мобільними пристроями». Використання рішень класу MDM дозволяє здійснити управління і контроль над різними типами мобільних пристроїв. Одна із головних задач MDM – досягнення оптимального стану між безпекою і зручністю використання мобільних пристроїв, при мінімізації затрат на обслуговування. Це досягається за рахунок таких можливостей систем типу MDM:

– централізоване управління мобільними налаштуваннями (парольні політики, параметри шифрування);

– заборона запуску небажаних додатків;

– інвентаризація програмних та апаратних засобів на мобільних пристроях;

– встановлення політики безпеки, сертифікатів безпеки і паролів на пристроях користувачів;

– налаштування Wi-Fi і VPN відповідно до корпоративних стандартів;

– інсталювання мобільних додатків, ведення чорного та білого списків програм;

– надання віддаленої підтримки користувачів;

– віддалене блокування пристрою і знищення корпоративних даних в разі його втрати або крадіжки;

– налаштування обмеження для пристроїв, наприклад, заборона передачі даних в роумінгу, відключення камери, використання USB, Bluetooth, магазинів додатків («AppStore», «Google Play» та ін.);

– контроль відповідності пристрою встановленим корпоративним політикам;

– виконання резервного копіювання і шифрування даних на пристроях;

– здійснення групової підготовки, конфігурування та обслуговування пристроїв.

Безпека мобільних пристроїв забезпечується:

1. Політикою парольного захисту, до якої відносяться встановлення пароля і періоду його дії. Так, для планшетних комп'ютерів «iPad» потрібно ввести

складний пароль, що складається з букв і цифр, загальна кількість символів не повинно бути менше п'яти. Правила використання PIN включають довжину, складність, історію, автоблокування при неправильному введенні. Доступ до віртуального корпоративного «Робочого столу», що встановлюється на мобільний апарат співробітника, здійснюється тільки після введення аутентифікаційних даних імені та пароля.

2. Обмеженнями на використання пристроїв і доступу до сервісів. Для пристроїв на основі операційної системи «Android» обмеження відносяться до управління мікрофоном і камерою, доступом до магазину додатків «Play Market» («Android Market»), використання GPS-приймача, централізованої налаштуванні мережі Wi-Fi, додатком «MS Exchange ActiveSync». Для пристроїв на основі операційної системи «iOS» («iPhone» / «iPad») обмеження ставляться до використання фотокамери і GPS-приймача, доступу до «iTunes», «YouTub»c, «AppStore», централізованої настройки пошти, календарів, Wi-Fi, SCEP («Simple Certificate Enrollment Protocol»).

3. Установленими на підприємстві правилами та угодами. Наприклад, правилами може обмежуватися можливість передачі або синхронізації користувальницьких файлів (документів, таблиць, презентацій) між сервером і клієнтом. Небезпеку для інформації несуть відкриті Wi-Fi мережі, адже кожен має змогу до них підключитись та виконувати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи дізнавшись його у працівника. Ненадійні паролі зазвичай стають причиною хакерських атак.

10. Удосконалено систему організаційно-правових заходів з метою захисту мобільних пристроїв від шкідливого програмного забезпечення. Загальну модель перехоплення та захисту інформації в бездротових мережах подано через сукупність кроків з можливими шляхами перехоплення та захисту інформації:

1. Стандартна взаємодія пристрою з глобальною мережею через роутер (нормальний стан). Модель описує нормальний стан роботи мережі, інформація з мобільного пристрою передається через бездротову мережу, без втручання зловмисника.

2. Вплив зловмисника на бездротову мережу з метою перехоплення інформації з пристрою. В даному випадку бездротова мережа піддається впливу зловмисника. Метою таких дій є бажання отримати доступ до мережі, що може дати йому змогу перехоплювати інформацію з пристроїв підключених до мережі.

3. Засоби захисту адміністратора для бездротової мережі. При взаємодії клієнта мережі через об’єкт можливі декілька сценаріїв роботи, а саме: відкрита мережа без використання шифрування; з використання шифрування.

4. Вплив зловмисника на інформацію через глобальну мережу та вразливості зв’язку між нею та роутером. Таким чином зловмисник може впливати на конфігурацію та налаштування бездротової мережі перебуваючи навіть в іншій країні.

5. Засоби захисту адміністратора для каналу зв’язку між глобальною мережею та роутером. Завдяки використанню стійкого пароля та зміни логіна для доступу до налаштувань, обмеження кількості спроб авторизації та забороні доступу до налаштувань локальної мережі з використанням глобальної, адміністратор може мінімізувати можливості зловмисника.

6. Прямий вплив зловмисника на адміністратора через бездротову мережу. Завдяки використанню спеціальних програмних та програмно-апаратних засобів, зловмисник може видавати себе за адміністратора мережі.

7. Засоби протидії адміністратора від прямого впливу зловмисника на бездротову мережу. Завдяки програмним та програмно-апаратним засобам адміністратор може не тільки захистити мережу від проникнення, а і обмежити доступ та захистити себе від нападу зловмисника.

8. Прямий вплив зловмисника на адміністратора через глобальну мережу. Використовуючи зловмисне програмне забезпечення та вразливості в

налаштуваннях зловмисник може задіяти глобальну мережу та виконувати дії аналогічні п.6.

9. Засоби протидії адміністратора від прямого впливу зловмисника на глобальну мережу. Аналогічно до п.7, адміністратор повинен захищати мережу від впливу через глобальну мережу.

10. Вплив зловмисника на бездротову мережу через глобальну з використанням хмарних технологій. З використанням сучасних хмарних технологій зловмисник може виконувати необхідні йому обчислення для злому на віддалених, але високопродуктивних програмно - апаратних засобах.

11. Захист бездротової мережі адміністратором через глобальну з використанням хмарних технологій. Завдяки використанню сучасних хмарних технологій адміністратор також має програмно-апаратні засоби, які дозволяють йому аналізувати та відслідковувати спроби несанкціонованого доступу завдяки спеціальним хмарним сервісам.

12. Захист бездротової мережі адміністратором з використанням «radiusserver». Для конфігурації локальної мережі підприємства використовують дану модель захисту, яка робить практично неможливим перехоплення інформації в захищеній мережі.

13. Захист бездротової мережі адміністратором з використанням NGFW. З використанням даного програмно-апаратного засобу можна захистити мережу як локально, так і від впливу з глобальної мережі, а також з використанням хмарних сервісів, що дає змогу поєднати в собі інструменти описані в п. 3, 5, 7, 9, 11, що робить його універсальним засобом моніторингу та захисту мережі, як локальної, так і глобальної.

Отже, на сьогодні у сфері інформаційної безпеки вже склалася правова та організаційна системи боротьби зі злочинами у кіберпростопі. Дослідження шляхів та методів попередження та нейтралізації загроз від шкідливого програмного забезпечення на мобільних пристроях є актуальною тематикою дослідження на майбутнє.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Аносов А. О. Модель перехоплення та захисту інформації в бездротових мережах / А.О.Аносов, А.В. Платоненко // Сучасний захист інформації. – 2017. - № 2(30). – С. 90-94.

2. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2014. – С. 343–384.

3. Бойко М. П. Системи стільникового зв’язку : конспект лекцій. – Одеса : ОНАЗ, 2014. – 76 с.

4. Використання смартфонів в Україні: [Електронний ресурс]. – Режим доступу: http://lead9.com/slide/slide.pdf.

5. Власова Л.А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.

6. Войтович О. П. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів / О.П.Войтович, В.О.Війтюк, В.А.Каплун // Інформаційні технологій та комп’ютерна інженерія. – 2013. - № 3. – С.4-5.

7. Вонг К. Электронный учебник для начинающих изучение информационной экономики, общества и политики. / К.Вонг, Ф. Сайо. UNDP-APDIP, 2015. - 59 с.: [Електронний ресурс]. – Режим доступу: http://www.unesco.kz/publications/ci/moscow/undp-foss-ru.pdf

8. Все про кіберзахист та інформаційну безпеку: [Електронний ресурс]. - Zillya антивірус – Режим доступу: http://zillya.ua.

9. Гавриленко А. А. Діяльність ТОВ «Ліга Закон» щодо протидії піратству комп’ютерних програм / А. А. Гавриленко // Організація протидії злочинам у сфері інтелектуальної власності та комп’ютерних технологій: доповіді провідних вчених, представників громадськості, державних службовців та працівників ДСБЕЗ на міжвідомчому семінарі-нараді; від. ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь. – К.: ДДСБЕЗ, 2009. – С. 59–72.

10. Герман Б. Стрибки через G: 3G–4G–5G: [Електронний ресурс]. – Режим доступу: http://gazeta.dt.ua/business/stribki-cherez-g3g-4g-5g-nishoviy-mobilniy-zv-yazok-5gne-zaminit-soboyu-4g-optimizovane-dlyapokrittya-znachnih-teritoriy.html

11. Демчик С. Л. Безпека інформаційних систем шляхом створення якісного програмного забезпечення / С.Л.Демчик // Інформатика та системні науки. – 2016. – С. 15-18.

12. Жованик М.О. Загальні принципи захисту мобільних пристроїв в корпоративній мережі / М.О. Жованик // «Young Scientist». – 2015. - № 5(20). – С. 39-42.

13. Замкова Т.В. Проблемы защиты информации в современных информационных системах / Т.В. Замкова.: [Електронний ресурс]. – Режим доступу: http://www.rae.ru/snt/?section=content&op=show_article&article_id=3893

14. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах/ А. В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р. – С. 40-44.

15. Зайцева-Калаур І.В. Інформаційне право : [Навчальний посібник] / І.В.Зайцева-Калаур. – Тернопіль: ФО-П Шпак В.Б., 2014. - 185 с.

16. IT-витрати найбільших компаній світу склали $895 млрд. : [Електронний ресурс]. - сайт ВКурсе. – Режим доступу: http://vkurse.ua/ua/business/it-raskhody-krupneyshikh-kompaniy-mira-sostavili-895-mlrd.html.

17. IT українською: [Електронний ресурс]. – Режим доступу: http://it-ua.info/

18. Комич Б.М.Основні принципи діяльності із захисту інформації. Захист інформації в інформаційних системах. – 2012. – № 2 (22). – С. 216-230.

19. Конвенція про кіберзлочинність // Офіційний вісник України від 10.09.2007 р. – № 65. – Ст. 2535.

20. Кривогин М.С. Международно-правовые аспекты борьбы с кибернетическими преступлениями / М.С. Кривогин // Государство и право: теория и практика: материалы междунар. заоч. науч. конф. (г. Чита, март 2017 г.). – Чита : Изд-во «Молодой ученый», 2017. — С. 77-79.

21. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III: [Електронний ресурс] / Верховна Рада України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2341-14.

22. Кузьменко Б.В. Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти / Б.В.Кузьменко, Ю.О.Заїка // Теорія управління. – 2013. - № 7. – С. 29-35.

23. Лебідь С. А. Протидія підрозділів ДСБЕЗ правопорушень у сфері інтелектуальної власності / С. А. Лебідь // Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: доповідь провідних вчених, представників громадськості, державних службовців та працівників ДСБЕЗ на міжвідомчому семінарі-нараді / відп. ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь. – К., 2009. – С. 13–15.

24. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування // А.А. Литвинюк.: [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

25. Манжай І.А. Проблеми захисту інформації на мобільних комп'ютерних пристроях з операційними системами Android та Apple iOS / І.А.Манжай // Наукові записки ХЕПУ. – 2015. - № 1(17). – С. 82-88.

26. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Джабраил Матиев: [Електронний ресурс]. – Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/

27. Мережі стільникового зв'язку. Навчальний портал НУБіП: [Електронний ресурс].–Режим доступу:nhttp://elearn.nubip.edu.ua/mod/page/view.php?id=23714

28. Михайлов С.К. Расчёт вариации задержки (IPDV) для телефонного соединения / С.К. Михайлов, Т.П. Сергеева // T-Comm - Телекоммуникации и Транспорт. – 2016. - № 7. – С. 87-89.

29. Мобильная безопасность: все ,что нужно знать: [Електронний ресурс]. – Режим доступу: http://freeprotection.ru/mobilnaya-bezopasnost-vsyo-chto-nuzhno-znat/.

30. Мобільний зв'язок в Україні: [Електронний ресурс]. – Режим доступу: http://uateka.com/uk/article/society/1227/.

31. Мороз С.І. Обґрунтування використання хмарних сервісів в агробізнесі // Ефективна економіка: [Електронний ресурс]. − 2014. − № 5. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3012.

32. Мороз С. І. Free та open source software в управлінні аграрними підприємствами. / С. І. Мороз, І. І. Шрамко // «Efektivní nástroje moderních věd – 2015»: materiály XI mezinárodní vědecko - praktická konference, Praha, 29.03-05.04.2015. Díl 6: Ekonomické vědy. – Praha: Publishing House «Education and Science» s.r.o. – S. 3-5.

33. Мороз С. І. Free-засоби маніпулювання даними в управлінні / С. І. Мороз // Ключови въпроси в съвременната наука - 2013: материали за IX международна научна практична конференция, София (Республика България), 17-25 април 2013. – Том 5. Икономики. – София: «Бял ГРАД-БГ» ООД. – С. 47-50.

34. Мороз С. І. Використання вільно розповсюджуваного програмного забезпечення в управлінні підприємствами. / С. І. Мороз // Матеріали науково-практичної конференції «Аграрна наука XXI століття: реалії та перспективи», м. Дніпропетровськ, 19.- 21.02.2013. – Дніпропетровськ: Друкарня «Стандарт» (ПП Бойко В.В.), 2013. – С. 88−90.

35. Муравська (Якубівська) Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз / Ю. Є. Муравська (Якубівська) // Економіка та суспільство [Електронне наукове фахове видання]. - № 9. – Мукачево : Мукачівський державний університет, 2017. Режим доступу: http://www.economyandsociety.in.ua/

36. На Украине не хотят внедрять 5G без перехода на 4G: [Електронний ресурс]. – Режим доступу: http://www.macdigger.ru/iphoneipod/na-ukraine-xotyat-vnedrit-5g-bezperexoda-na-4g.html

37. Недов Р. С. Виявлення та документування злочинів у сфері інтелектуальної власності, що вчиняються в мережі Інтернет / Р. С. Недов // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – Дніпропетровськ: ДДУВС, 2009. – С. 307–320.

38. Некоторые интересные факты о подборе паролей: [Електронний ресурс]. – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153530.

39. Нерсесян А. С. Кримінально-правова охорона прав інтелектуальної власності : [монографія] / А. С. Нерсесян. - Хмельницький : Видавництво Хмельницького університету управління та права, 2010. - 192 с.

40. Одарченко Р.С. Обгрунтування основних вимог до систем безпеки стільникових мереж 5-го покоління / Р.С. Одарченко // Проблеми інформатизації та управління, 2(54)’2016 59. - Безпека інформації. - Вип №3 (Том 21). – 2015.- С. 229-235.

41. Одарченко Р.С. Стратегії розвитку операторів стільникового зв’язку в Україні / Р.С. Одарченко // Наукоємні технології. — Том 26, № 2 (2015). — С. 141-148.

42. Одарченко Р.С. Аналіз вразливостей систем захисту інформації в мережах Wi- Max та методів їх усунення / Р.С. Одарченко, Ю.В.Беженар, А.О. Ксендзенко // Защита информации. Сб. научных трудов.- К.: НАУ, 2011. – Вып. 18. – С. 39-44.

43. Одарченко Р.С. Економічна ефективність впровадження систем захисту стільникових мереж 4G / Р.С.Одарченко, С.Ю. Лукін // Системи обробки інформації. Збірник наук. праць Інформаційна та економічна безпека. – Х.: Вид-во Харківського університету Повітряних Сил ім. Івана Кожедуба. – 2012. – Вип. №4 (102) Том 2 - С. 51-56.

44. Опубликованы наиболее часто используемые пароли 2016 года: [Електронний ресурс]. – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153680 (20.02.2017).

45. Офіційний сайт Української міжбанківської асоціації членів платіжних систем Єма: [Електронний ресурс]. – Режим доступу: https://ema.com.ua/protect-your-smartphone/

46. Питання створення національної мережі мобільного зв'язку державних органів. Журнал «Wireless.ua»: [Електронний ресурс]. – Режим доступу:mhttp://www.wireless.ua/1649-pitannyastvorennya-nacionalnoyi-merezhi.html

47. Платоненко А. В. Загрози інформаційної безпеки для користувачів сучасних мобільних пристроїв та засоби їх захисту / А. В. Платоненко. // Сучасний захист інформації. – 2017. – №1. – С. 128–132.

48. Попередження та розкриття кіберзлочинів: Курс лекцій / За ред. Д.Й. Никифорчука. – К. : НАВС, 2013 – 300 с.

49. Проблемы безопасности мобильных устройств,систем и приложений: [Електронний ресурс]. – Режим доступу до ресурсу: http://itzashita.ru/mobilnyie-ustroystva/bezopasnost-mobilnyih-ustroystv-sistem-i-prilozheniy-chast-1.html.

50. Резолюція, прийнята Генеральною Асамблеєю 55/63 Боротьба із злочинним використанням інформаційних технологій.

51. Сети и Стандарты Мобильной Связи в Украине: [Електронний ресурс]. – Режим доступу: http://blog.jammer.su/2017/07/seti-standartymobilnoj- svjazi-ukraina/

52. Сєвєрінов О.В. Аналіз сучасних методів атак наавтоматизовані системи управління військами та інформаційні мережі / О.В. Сєвєрінов, А.Г. Хрєнов, А.О. Поляков // Системи обробки інформації. – 2015. – № 9. – С. 101-104.

53. Сєвєрінов О.В. Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків / О.В. Сєвєрінов, В.М.Федорченко, В.І.Перепадя // Системи озброєння і військова техніка. – 2016. – № 4. – С. 42-45.

54. Скалозуб Л. П. Збірник методичних рекомендацій з викриття та документування злочинів у сфері інтелектуальної власності та високих

технологій / [Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь, Т. В. Дутченко та ін.]. – 2016. - К.: ДДСБЕЗ МВС України. – 188 с.

55. Сливченко В. В. Діяльність міліції громадської безпеки щодо виявлення та запобігання злочинам та правопорушенням у сфері інтелектуальної власності / В. В. Сливченко // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення: матеріали Всеукраїнської наук.-практич. конф. (м. Донецьк, 12 листопада 2010 р.); Донецький юрид. ін-т ЛДУВС ім. Е. О. Дідоренка. – Донецьк: ДЮІ ЛДУВС, 2010. – С. 81–83.

56. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации.

57. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко, Київ, ДУТ, Сучасний захист інформації. Науковий журнал. – 2015. – № 4, с. 86 – 90.

58. Створення глобальної культури кібербезпеки та оцінка національних зусиль по захисту найважливіших інформаційних інфраструктур A/RES/64/211 [Електронний ресурс]. – Режим доступу: http://daccess-dds-ny.un.org/doc/ UNDOC/GEN /N09/474/51/PDF/N0947451.pdf?OpenElement.

59. Технологии мобильной святи пятого поколения (5G)/ ERICSSON. Аналитический доклад – 284 23-3204 Uen | Июнь 2013 г. – 10 стр.: [Електронний ресурс]. – Режим доступу: https://www.ericsson.com/res/region_RECA/docs/whitepapers/wp-5g-ru.pdf

60. Тихвинский В.О. Возможности технологии 5G для создания сетей широкополосного беспроводного доступа в малых и средних населенных пунктах / Региональный семинар МСЭ для стран СНГ «Оптимальные решения по обеспечению широкополосного доступа в малых и средних населенных пунктах». – 2015г., 30с.

61. Уголовно-правовая ответственность бизнеса – 2017: [Електронний ресурс] : Юридические новости. - Режим доступу: http://pravo.ru/interpravo/legislative/viev/27/7page=20

62. Украинцы постепенно отказываются от лишних SIM-карт: [Електронний ресурс]. – Режим доступу: http://itc.ua/news/ukraintsyi-postepenno-otkazyivayutsya-ot-lishnih-sim-kart (20.02.2017).

63. Уязвимости платформы Android. Настоящее ибудущее: [Електронний ресурс]. – Режим доступу до ресурсу: https://habrahabr.ru/company/drweb/blog/142993/.

64. Федеральный закон РФ от 01.10.2008 № 164-ФЗ «О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерных технологий.

65. Федорченко В.Н. Анализ угроз для мобильныхустройств и способов их защиты / В.Н. Федорченко, И.В. Гензерский, Н.Ю. Шевякова // Системи обробки інформації. – 2017. – № 7. – С. 68-71.

66. Федотов Н.Н. Форензика – компьютерная криминалистика. – М. : Юридический Мир, 2017. – 432 с.

67. Якубівська Ю. Є. Вплив промислового шпигунства на сферу інтелектуальної власності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. -К. : УДУФМТ, 2013. - № 4 (69). - С. 158-162.

68. Якубівська Ю. Є. Світові тенденції розвитку кіберзлочинності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Економічні науки. - К. : УДУФМТ, 2014. - № 5-6 (76-77). - С. 125-130.

69. Якубівська Ю. Є. Трансфер технологій як чинник інноваційного розвитку / Ю. Є. Якубівська // Наука молода: Збірник наукових праць молодих вчених Тернопільського національного економічного університету. – Тернопіль : «Економічна думка», 2013. – № 20. - С. 197-202.

70. Якубівська Ю. Є. Цільові атаки в контексті промислового шпигунства / Ю. Є. Якубівська // Проблемы развития внешнеэкономических связей и привлечения иностранных инвестиций: региональный аспект: сб. науч. тр. – Донецк : ДонНУ, 2014. – Т. 2. - С. 368-372.

71. Японія запустить 5G зв'язок у 2020: [Електронний ресурс]. – Режим доступу: https://www.rbc.ua/ukr/lnews/poniyazapustit-svyaz-5g-2020-1465221969.html

72. Юридичні послуги on-line: [Електронний ресурс] / Bitlex legal provider. - Режим доступу: https://www.bitlex.ua/uk

73. Alvarez-Jimenez. Connecting the dots: twenty-first century technologies to tackle twenty-first century challenges in early intervention / M. Alvarez-Jimenez, J.F. Gleeson // Aust. – 2016. - P.1194–1196.

74. Amidon P. Widening privacy concerns / P. Amidon // Online. - 2015. - 16 (4). – P.64-67.

75. Baker L. Needed: An ethical code for library administrators / L. Baker // Journal of Library Administration. - 2016. - 16 (4). – P. 1-17.

76. Benjamin L.M. Privacy, computers and personal information: Towards equality and equity in an information age / L.M. Benjamin // Communications and the Law. - 2017. - 13 (2). – P. 3-16.

77. Branscomb A.W. Who Owns Information?: From Privacy to Private Access / A.W. Branscomb // New York: Basic Books. A division of Harper Collins Publishers. – 2015. – 256 p.

78. Cisco исследовала основные тенденции в сфере информационной безопасности на украинском рынке: [Електронний ресурс]. – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153526.

79. Collier G. Information privacy. Just how private are the details of individuals in a company's database? / G. Collier // Information Management and Computer Security. – 2016. - 3 (1). – P. 41-45.

80. Cyber defence?: [Електронний ресурс]. - NATO OTAN. - Режим доступу: http://www.nato.int/cps/en/natolive/topics_78170.htm

81. Focht K.T. Information compilation and disbursement: moral, legal and ethical considerations / K.T. Focht, D.S. Thomas // Information Management and Computer Security. – 2015. - 2 (2). – P. 23-28.

82. Fouty K.G. Online patron records and privacy: Service vs Security / K.G. Fouty // The Journal of Academic Librarianship. – 2016. - 19 (5). – P. 289-293.

83. Froehlich T.J. Re-thinking ethical issues in an online environment. / T.J. Froehlich // Online Information '17, edited by D.I. Raitt & B. Jeapes. Oxford: Learned Information. – 2017. - P. 415-422.

84. Goode J. Putting out the flames: The etiquette and law of e-mail / J.Goode, M. Johnson // Online. – 2014.- 15 (6). – P. 61-66.

85. GSA Evolution to LTE report: [Електронний ресурс]. – Режим доступу: http://www.gsacom.com/downloads/pdf/GSA_Evolution_to_LTE_report_060514.php4

86. Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers: [Електронний ресурс]. – Режим доступу: https://motherboard.vice.com/en_us/article/hacker-claims-to-push-malicious firmware-update-to-32-million-home-routers (20.02.2017).

87. IT threat evolution Q1 2017. Statistics: [Electronic resource]. - Access: https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

88. MDM и BYOD – смешать, но не взбалтывать: [Електроннbй ресурс]. – Режим доступу: www. Library.croc.ru

89. Shattucks J. Computer matching is a serious threat to individual rights. In Computers, Ethics and Social Values / J. Shattucks // edited by D.G. Johnson & H. Nissenbaum. New Jersey: Prentice-Hall. – 2016. - P. 305-311.

90. Smith M.M. Online information ethics: Online searching and the searching self / M.M. Smith // Proceedings of the 15th National Online Meeting, May 2017, edited by M.E. Williams. – 2017. - Medford, NY: Learned Information. - P. 399-405.

91. Software-defined networking: [Електронний ресурс]. - Режим доступу: http://en.wikipedia.org/wiki/Softwaredefined_networking

92. Spinello R.A. Ethical Aspects of Information Technology / R.A. Spinello // New Jersey: Prentice-Hall Inc. – 2016. – P. 125-134.

93. Stair R.M. Principles of Information Systems. A Managerial Approach / R.M. Stair // Boston: Boyd & Fraser. – 2015. – P. 78-85.

94. Szczypiorski K. HICCUPS: Hidden Communication System for Corrupted Networks / K. Szczypiorski. – Warsaw University of Technology, Institute of Telecommunications. – 2017. – P. 34-40.

95. Tactile Internet: [Електронний ресурс]. – Режим доступу: http://www.itu.int/en/ITUT/techwatch/Pages/tactile-internet.aspx

96. Thomas D. Software Defined Networks An Authoritative Review of Network Programmability Technologies / D. Thomas // O'Reilly Media. - 2016. -384 p.

97. Understanding 5G:Perspectives on future technological advancements in mobile. ANALYSIS. - GSMA Intelligence. – 2014. - 26 p.

98. Ware W.H. The new faces of privacy / W.H. Ware // The Information Society. – 2016. - 9 (3). – P. 195-211.

99. What are the G7 and G8: [Електронний ресурс] / G7 Information Centre. - Режим доступу: http://www.g8.utoronto.ca/what_is_g8.html

100. Zorkoczy P. Information Technology: An Introduction. 2nd edition / P. Zorkoczy. – 2015. - London: Pitman Publishing. - 214 p.