МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ
ДОНЕЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
МАРІУПОЛЬСЬКА МІСЬКА РАДА
ГОЛОВНЕ УПРАВЛІННЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
В ДОНЕЦЬКІЙ ТА ЛУГАНСЬКІЙ ОБЛАСТЯХ
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
В ДОНЕЦЬКІЙ ОБЛАСТІ
ДОНЕЦЬКЕ УПРАВЛІННЯ КІБЕРПОЛІЦІЇ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗБІРНИК МАТЕРІАЛІВ НАУКОВОГО КРУГЛОГО СТОЛУ

«Кібербезпека в системі національної безпеки України: проблеми та перспективи розвитку»

12 КВІТНЯ 2019 РОКУ

Маріуполь – 2019

УДК 004.738.5(06)
ББК 32.971.353я

Кібербезпека в системі національної безпеки України: проблеми та перспективи розвитку: збірник матеріалів круглого столу, м. Маріуполь, 12 квітня 2019 р. / Маріупольський державний університет; уклад. Шабельнік Т. В., Морозова А. О. – Маріуполь: МДУ, 2019. – 76 с.

Рекомендовано до друку засіданням Вченої ради економіко-правового факультету Маріупольського державного університету (протокол № 8 від 26 березня 2019 р.)

Золотухін Д.Ю.,
заступник Міністра інформаційної політики України

БОРОТЬБА З ФЕЙКОВИМИ НОВИНАМИ:ДОСВІД УКРАЇНИ ТА РЕКОМЕНДАЦІЇ

1. Сутність проблеми та можливі шляхи реагування.

“Фейкові новини” (“фейки”) є узагальненим терміном, який є продуктом медіапростору та ЗМІ, де існує необхідність надати певному явищу або феномену коротку назву для зручності у використанні. Використання цього словосполучення значно ускладнює роботу над науково-практичним та юридичним формулюванням конкретного визначення для цього феномену.

У науковому та сучасному медійному середовищі такі словосполучення мають назву “мемів”. За визначенням американського еволюційного біолога Річарда Доукінза, “мем” – лінгвістично-культурна одиниця, що описує певне явище та стає загальноприйнятою для широкого вжитку.

У широкому сенсі це словосполучення визначається як *сукупність інструментів, що застосовується з метою маніпулювання суспільною свідомістю, і, частіше всього, виражається у інформаційному повідомленні (текст/фото/відео, чи їх комбінація), що містить неправдиву чи частково правдиву інформацію та поширюється традиційними засобами масової інформації, соціальними мережами чи іншими доступними шляхами розповсюдження інформації, і має на меті сформувати у свідомості споживачів (реципієнтів) певне ставлення до явища чи об’єкту реального світу*. Наприклад, сформувати ксенофобські настрої щодо якоїсь конкретної соціальної групи через поширення негативної та емоційно зарядженої інформації про цю соціальну групу.

Через невизначеність підходів до розуміння цього явища під категорію “фейкових новин” зазвичай потрапляють два явища:

- навмисно створені інформаційні повідомлення, які мають на меті здійснення маніпулювання,
- інформаційні повідомлення, що є результатом непрофесійного та неетичного виконання своїх обов’язків співробітниками медіа.

Однак, оскільки в обох випадках на аудиторію споживачів інформації здійснюється шкідливий вплив, що обумовлює важливість протидії обом типам “фейкових новин”.

На особливу увагу заслуговує той факт, що навмисно створені для маніпулювання аудиторією інформаційні повідомлення є різновидом т.зв. “активних заходів”, які є однією з форм роботи спецслужб та розвідувальних органів. Активні заходи (спеціальні заходи впливу, спеціальні інформаційні операції, інформаційно-психологічні спеціальні операції) використовуються спецслужбами з метою цілеспрямованої та спланованої зміни політичного дискурсу певної спільноти або суспільної думки.

Так, наприклад, “фейковою новиною” є інформація про нібито заклик Дмитра Яроша до лідера чеченських бойовиків Доку Умарова, яку 1-2 березня 2014 року розповсюдили провідні російські ЗМІ. В подальшому ця новина була використана для легітимізації застосування Російською Федерацією своєї армії на території України. Це свідчить про спланований та підготовлений завчасно характер цієї інформаційної операції.

Крім того, таким прикладом є створення російськими ЗМІ (зокрема, Russia Today) віртуального образу “диспетчера Карлоса”, який повідомив, що Боїнг малайзійських авіаліній рейсу МН17 збито українським винищувачем.

Практика планування та здійснення “активних заходів” з розповсюдження дезінформації включає в себе використання подій чи фактів, що дійсно відбулися в реальності, однак в інформаційному повідомленні їх подають в неповному або спотвореному вигляді, чи в контексті емоційного забарвлення.

Нерідко поширення фейкових новин прискорюється завдяки реплікуванню журналістами та редакторами онлайн-платформ гучних та скандальних новинних матеріалів (що є типовим для фейків). Тобто, фейк поширюється без належної перевірки фактів, з метою підвищення рейтингів чи відвідуваності інформаційних ресурсів. В цілому, гонитва окремих ЗМІ за увагою споживачів інформації істотно сприяє успішній реалізації “активних заходів” та здійсненню впливу на широку аудиторію.

Таким чином, ідентифікація та детекція “фейкової новини” за формальними ознаками є дуже ускладненою. Будь-які дії законодавчого, адміністративного чи експертного характеру щодо визначення, атрибуції та описання інформаційного повідомлення в якості “фейкової новини” неминуче призведуть до необхідності чітко регламентувати межі повноважень та компетенції суб’єкта, який здійснює таку діяльність.

Наприклад, чіткий та сталий перелік ознак “фейку” і жорстко регламентований підхід до визначення “фейкових новин” не дасть змогу ефективно протидіяти гнучким та поліморфним гібридним загрозам інформаційного простору, що будуть влаштовуватися спецслужбами для обходу встановлених процедур. Характерною ознакою “фейкових новин” є постійне вдосконалення механізмів маніпуляції та її поширення, що нівелює спроби уніфікації їх визначення в рамках формальних ознак.

І навпаки, надто широке коло повноважень інституції, яка буде визначати “фейкові новини” на підставі суб’єктивних суджень (без жорсткої регламентації меж та чітких критеріїв і ознак) може призвести до виникнення ризиків для свободи слова.

Таким чином, реагування на “фейкові новини” шляхом їх ідентифікації і описання розцінюється як малоефективна з точки зору розвитку стратегічних комунікацій.

Крім вищеописаних труднощів адміністративно-правового підходу до протидії “фейковим новинам”, питання щодо ефективності викликає практика “розвінчування фейків”.

Процес “розвінчування фейків” полягає у такій послідовності дій:

1) викладення недостовірної чи маніпулятивної інформації та її джерела (що, доречі, мимоволі сприяє її додатковому поширенню);

2) опис інструментів та підходів перевірки такої інформації;

3) обґрунтування недостовірності чи маніпулятивності інформації за допомогою аргументів та фактів;

4) висновок про те, що поширена інформація є недостовірною чи маніпулятивною.

З точки зору практики комунікації, така конструкція є досить складною для сприйняття широкими аудиторіями і позитивно оцінюється тільки експертами або зацікавленими саме в такому контенті споживачами.

Враховуючи це, а також очевидний факт невідповідності ресурсів, які витрачаються Російською Федерацією на створення та поширення “фейкових новин” у величезних масштабах, та ресурсів компетентних державних інституцій і недержавних організацій, що покликані протидіяти “фейковим новинам”, реактивна протидія розповсюдженню “фейків” розцінюється багатьма експертами галузі як неефективна.

У той же час, представники державних інституцій різних країн Європейського Союзу (наприклад, країн Балтії) наголошують на тому, що вони “не боряться з фейками, а просувають свій наратив”. Тобто провідні державні і недержавні експерти відмовляються від реактивної протидії розповсюдженню “фейкових новин” на користь формуванню свого порядку денного в конкурентному інформаційному середовищі. Такий підхід дозволяє уникнути порядку денного, нав’язаного ззовні завдяки зовнішнім маніпуляціям. Натомість дозволяє працювати над просуванням своїх меседжів в інформаційний простір.

Одним з перших суб’єктів, хто почав просувати таку методику боротьби з “фейковими новинами”, є Міністерство інформаційної політики України. Цей підхід не виключає необхідності реагування на “фейкові новини” шляхом перевірки, спростування брехливої інформації і надання об’єктивної інформації щодо конкретних питань. Однак проактивна діяльність державних інституцій стосовно конкурентного представлення своєї комунікаційної позиції в інформаційному середовищі була визначена пріоритетною.

2. Законодавче врегулювання

Визнання проблематики “фейкових новин” та дезінформації на законодавчому рівні є необхідним кроком для організації подальшої системної протидії інформаційному впливу на суспільство.

Для цього необхідно:

- визнати факт існування “фейкових новин” та реальної загрози, що становить дезінформація для безпеки держави;
- усвідомити необхідність відповідальності етичного та правового характеру за розповсюдження такої інформації;

- закріпити у якості пріоритету державної політики проактивний характер державних стратегічних комунікацій як форми боротьби з дезінформацією;
- визначити просування власного наративу та побудову ефективної і стійкої системи державних стратегічних комунікацій як пріоритетного напряму протидії фейкам.

За відсутності законодавчого визнання проблеми інформаційної агресії боротьба з дезінформацією залишатиметься неузгодженою системою локальних ініціатив неурядових інституцій та окремих дій органів державної влади без створення системи превентивної протидії.

Україна, опинившись з 2014 року в умовах широкомасштабної дезінформаційної кампанії з боку РФ, більше двох років вибудовувала власне нормативно-правове забезпечення протидії фейкам. При цьому, в контексті європейської та євроатлантичної інтеграції України, така діяльність ретельно узгоджувалася з точкою зору закордонних партнерів, які постійно наголошували на необхідності пріоритету питань свободи слова над питаннями національної безпеки.

Водночас, саме завдяки ухваленню на початку 2017 року Доктрини інформаційної безпеки в Україні був чітко визначений механізм протидії інформаційній агресії, передбачено компетенції відповідальних органів влади у цій сфері та запроваджено підхід, який враховував пріоритети громадського суспільства та закордонних партнерів України.

Таким чином, інституціоналізація системи захисту інформаційного простору держави є пріоритетним кроком у напрямку протидії дезінформації та фейковим новинам.

3. Питання відповідальності

Окрім вже зазначених вище нормативно-правових та адміністративних аспектів протидії “фейковим новинам”, потребує визначення механізм притягнення до відповідальності суб’єктів поширення дезінформації.

Принципи демократичного розвитку сучасних цивілізованих держав полягають в тому, що права і свободи людини і громадянина мають найвищу цінність. При цьому, пріоритет прав та свобод неодмінно супроводжується обов’язками, які забезпечують прийнятний порядок співіснування усіх членів суспільства. Існування прав і свобод, які не кореспондуються з відповідними обов’язками, може призвести до конфлікту в суспільстві і деформації демократичних інститутів.

Держава в особі органів державної влади є монополістом на застосування механізмів відповідальності та санкцій за невиконання обов’язків. Ці механізми реалізуються через уповноважені державні органи (суд, органи сектору безпеки та оборони, регуляторні органи тощо). Водночас, наділення органів державної влади повноваженнями щодо притягнення до відповідальності за поширення “фейкових новин” несе в собі ризик зловживання таким правом та навіть цензурування ЗМІ, що не відповідає принципам демократичного суспільства.

Крім того, суб'єктивний характер оцінювання "фейкових новин" обумовлює необхідність проведення експертиз (в т.ч. і неурядовими структурами) з метою уникнення безпідставного притягнення до відповідальності.

З огляду на вищезазначене, пріоритетна роль у системі притягнення до відповідальності за поширення "фейкових новин" має належати не державі, а профільним інституціям громадянського суспільства (ІГС).

Зважаючи на монополію держави на застосування примусу та необхідність дотримання принципів невтручання в діяльність ЗМІ, оптимальними видаються два механізми притягнення до відповідальності за поширення фейкових новин:

- змішаний, коли притягнення до відповідальності здійснюється уповноваженим Законом органом влади за висновком ІГС. При цьому санкції матимуть адміністративний характер (попередження, позбавлення ліцензій, відкриття кримінального провадження тощо);
- недержавний, коли висновок ІГС є достатнім для відповідної реакції суспільства, публічного осуду, що тягне за собою публічну недовіру суб'єкту поширення дезінформації та нівелює його значущість у соціумі (відмова від акредитації на заходах, втрата аудиторії тощо).

Найбільш ефективним є недержавний механізм з наступних підстав. По-перше, втрата довіри до ЗМІ та його фактичне "забуття" має довготривалий ефект. По-друге, публічного осуду не можна унинути за допомогою адміністративних механізмів (наприклад, шляхом оскарження застосування санкції). По-третє, таке рішення засноване на колегіальній узгодженій позиції експертів, що виключає можливість впливу зацікавленої сторони на кінцеве рішення.

Втім, що найважливіше, такий спосіб заснований на принципах саморегуляції та невтручання держави в діяльність ЗМІ. А отже, виключається можливість владного впливу на сферу масової інформації.

Водночас, недержавний спосіб потребує існування ефективного та загальновизнаного в суспільстві органу саморегуляції ЗМІ, механізму прийняття рішення таким органом та застосування відповідного рішення. Адже без належної підтримки суспільством такого рішення, його ефективність буде мінімальною та матиме радше декларативний ефект.

Саме тому на період становлення відповідних громадянських інституцій можливе тимчасове застосування змішаного механізму, який передбачатиме, по-перше, систему стримувань і противаг (держава не може застосувати санкцію без рішення ІГС), а, по-друге, наявні чітко передбачений Законом суб'єкт застосування санкції, механізм прийняття рішення, види санкцій тощо.

Основною проблемою застосування такого механізму є необхідність існування ініціативи від суб'єктів ІГС та підтримки такої ініціативи журналістською спільнотою.

4. Інші способи протидії "фейковим новинам"

Притягнення до відповідальності як спосіб реагування на дезінформацію є найбільш очевидним, втім, не найефективнішим способом. Недоліком такого підходу є те, що притягнення до відповідальності – це реагування на вже здійснений факт. А фейки та інші т.зв. "активні заходи" зазвичай створюються так, щоб швидко поширюватись, фіксуватись у свідомості споживачів та гнучко підлаштовуватись під будь-які зміни, у тому числі нормативно-правового характеру. Будь-яке спростування, у тому числі публічне визнання компетентним органом фейкового характеру новини не зможе повністю нівелювати ефект від поширеної інформації.

Тому важливо враховувати і інші способи протидії фейковим новинам, у т.ч. ті, на яких було наголошено вище:

1) поширення власного наративу;
2) спростування і розвінчування фейків;
3) застосування механізмів суспільної відповідальності за поширення "фейкових новин" і розбудову саморегуляції та співрегуляції медіасередовища;
4) підвищення медіаграмотності суспільства.

Підвищення медіаграмотності суспільства – комплекс превентивних заходів із вдосконалення здатності громадян самостійно виявляти фейки, опиратися маніпулятивному впливу, підлаштовуватися під зміни інформаційного середовища, розвивати власне критичне сприйняття інформації.

Таким чином, діяльність МІП у сфері протидії "фейковим новинам" сконцентрована на вищевикладених напрямках роботи та реалізовується в рамках проектних і програмних ініціатив зі створення системних спроможностей українського уряду і громадського суспільства нівелювати шкідливий маніпулятивний вплив, що створює загрози поступальному демократичному розвитку України на шляху інтеграції до Європейського Союзу та Північно-Атлантичного Альянсу.

Селич В.А.,
начальник Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України, підполковник поліції

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Будь-яка діяльність людини у суспільстві неможлива без чіткої регламентації, передбаченої нормативно-правовими актами та законами.

Стурбованість міжнародного співтовариства щодо розвитку кіберзлочинності знайшла відображення, зокрема, у таких міждержавних угодах, як: Всесвітній саміт з інформаційного суспільства та Конвенції Ради Європи «Про кіберзлочинність» (2001 р.), Бангкокська декларація з попередження злочинності та кримінального правосуддя (2005 р.), Бухарестська декларація про міжнародне співробітництво в боротьбі з

тероризмом, корупцією і транснаціональною організованою злочинністю (2006 р.). У цих документах йдеться про спільне протистояння кіберзлодіям шляхом прийняття відповідних законодавчих актів, які не будуть суперечити ні законам окремої держави, ні пунктам договорів, які ратифікувала ця держава.

Основні положення щодо попередження кіберзлочинів викладено у Конвенції про кіберзлочинність від 23.11.2001, яка була ратифікована Верховною Радою України у 2005 році. Потреба прийняття Конвенції обумовлена необхідністю зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними шляхом встановлення кримінальної відповідальності за таку поведінку [1].

Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще декілька років тому. Незважаючи на зусилля правоохоронних органів, спрямовані на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а навпаки, постійно збільшується. Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності.

Прикладом цьому може служити Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні» , який мав на меті розвитку національної складової глобальної інформаційної мережі Інтернет, забезпечення широкого доступу громадян до цієї мережі, ефективного використання її можливостей для розвитку вітчизняної науки, освіти, культури, підприємницької діяльності, зміцнення міжнародних зв'язків, належного інформаційного забезпечення, здійснення органами державної влади та органами місцевого самоврядування своїх повноважень, повнішого задоволення потреб міжнародного співтовариства в об'єктивній, комплексній інформації щодо різних сфер суспільного життя в Україні, а також вирішення інших завдань [2].

В березні 2016 року Указом Президента України від 15 березня 2016 року № 96/2016 було затверджено рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [3]. Таким чином, в нормативно-правовій базі України з’явився уніфікований нормативно-правовий акт, в якому передбачено створення «активного кіберзахисту» та забезпечення належних умов для безпечного використання кіберпростору, інтересах держави і суспільства. Проте, в Стратегії використовуються поняття та терміни, офіційне тлумачення яких досі не визначено національним законодавством України. Деякі з них вжиті у відповідності до ратифікованої Україною Конвенції Ради Європи про кіберзлочинність 2001 р. Наразі, законодавець пропонує надати офіційне

тлумачення деяким термінам в Законі України «Про основні засади забезпечення кібербезпеки України» [4].

Перш за все необхідно зазначити, що до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» блок національного законодавства не містив профільного Закону, а питання щодо регулювання суспільних відносин у визначеній сфері відсилались до множинних норм загального характеру. Деякі спеціальні норми були закріплені на рівні Указу Президента України.

Так, необхідно зазначити, що в деякій мірі Закон не відповідає умовам сьогодення, і прийнятий, так би мовити, на «перспективу», оскільки існують питання, що потребують роз'яснення, наприклад: на Кабінет Міністрів України покладаються завдання щодо затвердження нормативно-правових актів щодо вимог та забезпечення функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Також законодавець не визначає вичерпний перелік та не надає певних критеріїв, за якими слід робити розподіл об'єктів критичної інфраструктури, крім об'єктів критичної інфраструктури у банківській системі України.

Отже, система національного законодавства України потребує удосконалення, у розрізі закріплення спеціальних норм, які б мали можливість регулювання суспільних відносин у сфері протидії кіберзлочинності та забезпечення кібербезпеки.

Список використаних джерел

1. Конвенція про кіберзлочинність: Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/994_575

2. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31.07.2000 № 928/2000 База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/928/2000

3. Стратегія кібербезпеки України: указом Президента України від 15 березня 2016 року № 96/2016 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/96/2016

4. Про основні засади забезпечення кібербезпеки України: проект Закону України від 05.10.2017 // База даних «Законодавство України»/Верховна Рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657

Толюпа С.В.,
доктор технічних наук, професор,
професор кафедри кібербезпеки та захисту інформації
Київського національного університету імені Тараса Шевченка

ТАКСОНОМІЯ СИСТЕМ ВИЯВЛЕННЯ АТАК ТА НАПРЯМКИ ЇХ ПОБУДОВИ

На сьогодні, при стрімкому розвитку мережевих технологій і глобальної інформатизації суспільства на перший план висуваються проблеми забезпечення високого рівня захищеності інформаційних систем. Зі збільшенням числа комп'ютерних інцидентів, пов'язаних з безпекою, почали стрімко розроблятися системи виявлення атак (СВА).

Традиційно СВА класифікуються відповідно до двох характеристик: методу виявлення і рівня системи, на якому здійснюється захист. На сьогодні системи виявлення вторгнень і атак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що більшість існуючих класифікацій СВА дуже абстрактні, не є повними, і у них значні важливі характеристики (елементи) потребують доповнень та узагальнень.

У цьому матеріалі показано сучасний погляд на таксономію систем виявлення атак, а також уявлення про побудову системи виявлення вторгнень. Щоб зробити цю класифікацію всеосяжною і повною, окрім звичних ознак, таких, як: середовище моніторингу, метод виявлення, архітектура, характер відповіді, принцип роботи та час реакції, були включені такі характеристики: джерело аудиту, технологія побудови, парадигма виявлення та режим збору даних (рис. 1.).

Окремо необхідно відзначити СВА, що засновані на ***методах Data Mining***. Виявлення атаки за допомогою ***прихованої марковської моделі***.

Рис. 1. Класифікаційні ознаки систем виявлення і запобігання атак

Прихована марковська модель являє собою статистичну модель, де система моделюється як процес Маркова з невідомими параметрами. Задача методу полягає в оцінці прихованих параметрів, що базуються на параметрах, які спостерігаються. Виявлення атак за ***допомогою байєсовських мереж***. Байєсовська мережа являє собою модель, яка кодує імовірнісні взаємозв'язки між змінними. Основний метод застосування баєсовських мереж передбачає незалежність серед атрибутів. Виявлення атак за допомогою ***методів кластеризації***. Методи кластеризації групують дані в кластери на підставі схожості об'єктів. Виявлення невідомих мережевих атак найчастіше будується саме на методах кластеризації. Однорідні групи зі схожими характеристиками або кластери формуються шляхом розбиття набору елементів без будь-яких позначок. Виявлення атак за допомогою ***методу опорних векторів***. Даний метод є одним з найбільш популярних методів класифікації. Метод будує оптимальну гіперплощину в просторі характеристик: $w \times x - b = 0$, що розділяє нормальні і аномальні елементи. У підсумку завдання можна звести до квадратичного програмування: $min \parallel \omega \parallel \frac{2}{H}/2 + c \sum_{i=1}^{N} \xi_i$, при $c_i\ (wx_i\text{-}b) \geq 1\text{-}\xi_i$, $1 \leq i \leq N$, де ξ_i - величина помилки на об'єктах x_i.

Виявлення атак за ***допомогою правил нечіткої логіки***. Нечіткі системи виявлення мережевих вторгнень використовують множину нечітких правил для визначення ймовірності конкретних або загальних мережевих атак. Нечітка множина може бути сформована для опису трафіку в конкретній мережі. Нечіткі асоціативні правила формуються на основі звичайних навчальних вибірок. Тестований зразок класифікується як нормальний, якщо згенерований сукупністю правил показник буде вище певного порогового значення. Зразки з більш низьким показником вважаються аномальними.

Звичайно протидіяти вторгненням і атакам, базуючись тільки на одному з методів малоефективно, тому необхідно підійти до цього питання комплексно і побудувати інтелектуальну систему протидії вторгненням. При побудові такої інтелектуальної (експертної) системи пропонується вибрати нечітку модель. Це

пов’язано з тим, що значна частина інформації про причини і джерела атак може бути отримана тільки експертним шляхом або у вигляді евристичних описів процесів. Для визначення джерел атак система безпеки має бути представлена моделлю тієї інформаційної мережі, на яку вона орієнтується. Така модель ділить завдання переміщення інформації між комп’ютерами через середовище мережі на кількість рівнів менш великих і під задач, що легше вирішуються. Кожна з цих підзадач вирішується за допомогою одного рівня мережі. Тому первинне завдання після фахівця безпеки може бути представлене декомпозицією завдань безпеки з окремих рівнів мережі.

Список використаних джерел

1. Толюпа С.В., Штаненко С.С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 3. 2018р. с. 56-66.

2. Debar, H., Dacier, M., and Wespi, A. (2000), “A Revised Taxonomy for Intrusion-Detection Systems,” presente dat Annalesdes communications, vol. 55, 2000, pp. 361-378.

Александров О. В.,
Начальник управління нагляду за додержанням законів, виконанням судових рішень у кримінальному провадженні та при проведенні оперативно-розшукової діяльності військової прокуратури об’єднаних сил України, полковник юстиції

ОСОБЛИВОСТІ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Розвиток сучасних інформаційних технологій, удосконалення виробництва і розширення сфери застосування новітньої кібернетичної техніки дали можливість зародження специфічного, складного виду злочинних діянь, де комп’ютерне оснащення та електронна інформація є об’єктом протиправного посягання. Поряд з позитивними здобутками, інформатизація супроводжується побічним, негативним явищем криміногенного характеру, до якого відносять злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

На сьогодні злочини в сфері використання комп’ютерів є однією з груп суспільно небезпечних діянь, яка динамічно розвивається та набирає обертів. Взагалі, комп’ютерна злочинність – це особливий вид злочинів, пов’язаних із незаконним використанням сучасних інформаційних технологій і засобів комп’ютерної техніки [1]. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Згідно із чинним законодавством України, кримінальну відповідальність за злочини у сфері використання електронних

обчислювальних машин, комп'ютерних мереж і мереж електрозв'язку передбачено у Розділі XVI Кримінального кодексу України.

Переважна більшість складів злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (далі – комп'ютерні злочини) є матеріальними, а тому виявляються за наслідками. Отже, під час кваліфікації цих злочинів та їх відмежування від суміжних складів злочинів, необхідно оцінювати розмір та характер заподіяної шкоди з точки зору характеристики її предмету. Так, предметом більшості комп'ютерних злочинів є комп'ютерна інформація [2] або комп'ютерна система, автоматизована система, комп'ютерна мережа чи мережа електрозв'язку). Саме злочинний вплив на ці предмети або їх злочинне використання дає підстави визначити наявність об'єкту цих злочинів, тому що вони є невід'ємною частиною охоронюваних розглядуваними нормами суспільних відносин.

При кваліфікації комп'ютерного злочину у будь-якому випадку слід оцінювати розмір завданої шкоди, тому що це має критичне значення для наявності конкретного складу злочину. Зокрема, злочин, передбачений ст. 363 КК України, вважається закінченим лише якщо заподіяно значну шкоду, а при наявності такого розміру шкоди при вчиненні злочину, передбаченого ст. 361 КК України, кваліфікацію слід проводити за ч. 2 цієї статті. При цьому слід пам'ятати, що шкода у статтях 361–363-1 КК України може полягати в заподіянні матеріальних збитків, які зазвичай є позитивними (позитивна майнова шкода), які оцінюються, виходячи з витрат власника на придбання комп'ютерної інформації, пропорційно зниженню цієї вартості, спричиненої злочином, або виходячи з вартості компонентів комп'ютерної системи (програмних чи технічних), які зазнали негативного злочинного впливу, або виходячи із витрат на відновлення комп'ютерної інформації чи компонентів комп'ютерної системи тощо. Тобто це прямі збитки для потерпілого, підтверджені певними документами. Крім того, збитки від такого злочину можуть мати непряме вираження (опосередковане тощо) та виражатися в упущеній вигоді, що є результатом, наприклад, укладання завідомо невигідної угоди, зниження авторитету, невиконання умов договорів тощо [3].

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в нематеріальних видах шкоди, що зумовлено використанням комп'ютерів, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та управління ними. Така шкода може виражатися у порушенні нормальної роботи підприємств (установ чи організацій), зупиненні або порушенні складних технологічних процесів, зниженні обороноздатності держави, підриві авторитету державних органів, підприємств, установ або організацій, створенні загрози або заподіянні шкоди життю чи здоров'ю громадян, порушенні безпеки руху транспорту тощо. Так у практиці правоохоронних органів можуть виникати випадки, коли в результаті незаконного втручання в роботу автоматизованих систем управління порушувався виробничий процес,

створювалася загроза життю багатьох осіб. Характер шкоди в кожному конкретному злочині, як правило, залежить від тих суспільних відносини, які виступають не основним безпосереднім, а додатковим об'єктом. Це можуть бути відносини в різних сферах життєдіяльності людини, пов'язані з використанням комп'ютерів, систем, комп'ютерних мереж і мереж електрозв'язку. Перешкоджаючи інформаційним відносинам, злочинець завдає або загрожує завдати шкоди тим суспільним відносинам, для інтенсифікації яких застосовуються комп'ютерні технології. Отже, велике значення для кваліфікації має визначення додаткового обов'язкового або факультативного об'єкта злочину та шкоди, яку він зазнав.

Таким чином, злочини із використанням комп'ютерних технологій стають дедалі більш розповсюдженими, але вони і досі залишаються феноменами, бо наука ще не здатна чітко встановити правове регулювання відповідальності за дані злочини, оскільки вони мають ряд своїх особливостей та технології досить стрімко розвиваються, що і зумовлює появу нових видів злочинів із використанням комп'ютерних технологій.

Список використаних джерел

1. Судова практика розгляду справ про злочини у сфері використання електроннообчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютернихмереж і мереж електрозв'язку / Верховний Суд України: інформаційний сервер //[Електронний ресурс]. – Режим доступу:http://www.scourt.gov.ua/clients/vs.nsf/0/C8EABE11C12BFF3AC22576EE004F1E65?OpenDocument&CollapseView&RestrictToCategory=C8EABE11C12BFF3AC22576EE004F1E65&Count=500&.

2. Пашнєв Д. В. Властивості комп'ютерної інформації як предмету злочину / Д. В. Пашнєв // Вісник Кримінологічної асоціації України :збірник наукових праць [Редкол. Л. М. Давиденко, Т. А. Денисова,О. М. Джужа та ін.]. – № 1. – Х. : ХНУВС, 2012. – 308 с. – С. 115-125.

3. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. –К. : Видавничий дім «Скіф», 2012. – 728 с.

Оксаніченко Р. В.,
старший оперуповноважений
в особливо важливих справах ГУ СБУ, полковник

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби[1].

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

1) несанкціонований доступ — 2 %
2) укорінення вірусів — 3 %;
3) технічні відмови апаратури мережі — 20 %;
4) цілеспрямовані дії персоналу — 20 %;
5) помилки персоналу (недостатній рівень кваліфікації) — 55%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Відповідно до вимог законів України "Про інформацію", "Про державну таємницю" та "Про захист інформації в автоматизованих системах" основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Порушники технічного захисту інформації можуть створювати такі потенційні загрози для безпеки інформації в інформаційних системах:

- загрози конфіденційності (несанкціонованого одержання) інформації всіма потенційними і можливими каналами її витоку, особливо каналами побічних електромагнітних випромінювань і наведень, таємними каналами зв'язку в імпортному обладнанні та розвідувальними закладними пристроями;
- загрози цілісності (несанкціонованої зміни) інформації;
- загрози доступності інформації (несанкціонованого або випадкового обмеження) та ресурсів самої інформаційної системи;
- загрози проникнення комп'ютерних вірусів;
- загрози радіочастотних засобів електромагнітного ураження високопрофесійних порушників.

Загрози порушників технічного захисту інформації можуть здійснюватись:

- ✓ технічними каналами: акустичними, оптичними, хімічними тощо;

- ✓ каналами спеціального впливу шляхом формування полів і сигналів для руйнування системи захисту або порушення цілісності інформації;
- ✓ несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання засобів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Основні прийоми захисту від загроз такого роду однакові і полягають у забезпеченні заборони несанкціонованого доступу до ресурсів комп'ютера, а також до підключеним до нього пристроям; неможливість несанкціонованого використання ресурсів комп'ютера після отримання до них доступу; своєчасне виявлення факту несанкціонованих дій і усунення їх причин та наслідків[2].

Основним засобом заборони несанкціонованого доступу до ресурсів обчислювальних систем є підтвердження автентичності користувачів і розмежування їх норов на доступ до певних інформаційних ресурсів. Підтвердження автентичності користувача забезпечується виконанням процедури його ідентифікації, перевіркою автентичності ідентифікованої особи та здійсненням контролю за всіма діями, обумовленими приписаними даному користувачеві повноваженнями доступу.

Ідентифікація користувача включає в себе реєстрацію в системі безпеки обчислювального пристрою унікального реєстраційного імені користувача (логіна) і відповідного цьому користувацькому імені – пароля. Встановлення автентичності користувача (аутентифікація) полягає в перевірці істинності його повноважень. Для особливо надійного впізнання при ідентифікації і аутентифікації користувача іноді використовуються спеціальні технічні засоби, що фіксують і розпізнають індивідуалізують людини фізичні та лінгвістичні характеристики (голос, відбитки пальців, структура зіниці, мовні особливості і т.д.). Однак такі методи вимагають значних витрат, і тому використовуються рідко, так що основним і найбільш масовим засобом ідентифікації залишається парольний доступ.

На сьогодні все більшої популярності набуває такий криптографічний засіб захисту інформації, як електронний цифровий підпис (ЕЦП). Він вже став досить часто використовуваним способом ідентифікації і аутентифікації користувача в банківській та інших сферах діяльності. Електронний цифровий підпис являє собою приєднане до якого-небудь тексту його криптографічне (зашифроване певним способом) перетворення, що дозволяє перевірити одержувачу тексту справжність його авторства і автентичність самого тексту.

Список використаних джерел

1. Хоффман Л. Дж. Современные методы защиты информации // — М.: Сов. радио, 1980 – 560 с.

2. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння:

ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

Ціон П.О.,
заступник начальника Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України, майор поліції

КІБЕРБЕЗПЕКА: ВИКЛИКИ ДЛЯ УКРАЇНИ

Особливе місце в системі національної критичної інфраструктури України посідає інформаційна інфраструктура, ефективний захист якої виступає необхідним елементом забезпечення її національної безпеки. Інформаційна інфраструктура охоплює безліч елементів критичної інфраструктури держави і, отже, може бути визначена як критична інформаційна інфраструктура.

До основних секторів критичної інфраструктури держави, що має тісний зв'язок з інформаційною інфраструктурою, відносять системи управління в уряді, обороні, кредитно-фінансові і банківські системи, інформаційні системи науково-дослідного сектору, промисловості, енергетики, в тому числі атомній, транспорті, водопостачанні, комунальному господарстві, телекомунікації, цивільній обороні.

Перелік інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави затверджується Кабінетом Міністрів України та відноситься до інформації з обмеженим доступом.

Визначається, значне зростання інтенсивності проведення кібератак, які здійснюються на інформаційно-телекомунікаційну критичну інфраструктуру в Україні.

Відповідно до частини 2 пункту 2 Постанови Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» кібератакою є несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи [1].

Кібератаки, спрямовані через глобальну мережу Інтернет на сервери державних установ, великих компаній, фінансових установ, політичних партій та ЗМІ, а останнім часом й на інформаційно-телекомунікаційну інфраструктуру воєнних об'єктів.

На окрему увагу заслуговує проблема забезпечення безпеки функціонування державних органів влади, збройних сил, правоохоронних органів та спецслужб (будівель, належної інфраструктури тощо) у кризових

ситуаціях. Відповідні інфраструктурні об'єкти у розвинених країнах світу, як правило, також відносять до критичної інфраструктури.

Аналізуючи наведені випадки здійснення кібератак, треба зазначити, що характер і форми комп'ютерних нападів, від яких має бути розроблений захист, можуть істотно різнитися. Але, незважаючи на різноманітність типів атак, наслідки від них на найвищому рівні, як правило, включають: несанкціонований доступ або перехоплення інформації (втрата конфіденційності); несанкціонована зміна інформації, програмного забезпечення, обладнання і т.д. (втрата цілісності); блокування транзакцій та/або відключення системи (втрата готовності).

Загрози критичній інфраструктурі можна також розглядати не тільки з точки зору характеру їх походження, але і визначення елементів критичної інфраструктури, на які ці загрози спрямовані: фізичні елементи, зокрема, обладнання та ресурси об'єктів критичної інфраструктури; системи управління та комунікації, зокрема системи автоматичного управління та регулювання роботи об'єктів, системи зв'язку тощо; персонал об'єктів, зокрема диспетчерський, оперативний персонал, який безпосередньо забезпечує функціонування критичної інфраструктури у реальному часі.

Найбільшу загрозу безпеці об'єктів критичної інфраструктури становлять саме скоординовані атаки з використанням програмних вірусів. Такий вид атаки поєднує підготовчий етап (дії, що створюють на об'єкті нові вразливі місця) та атакуючі дії (використання уразливих місць). При цьому, підготовчі дії можуть здійснюватися значно раніше за часом, ніж сама атака, можуть бути задіяні працівники (інсайдери) підприємства, що є об'єктом нападу, та здійснені різноманітні відволікаючі маневри.

Визначення спрямованості дії загроз методологічно дозволяє більш системно підійти до формування державної політики і організації системи захисту критичної інфраструктури.[2]

Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»» затверджено Стратегію кібербезпеки України. Відповідно до положень пункту 4.3 розділу 4 вищезазначеної Стратегії кіберзахист критичної інфраструктури перш за все полягає в комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури.[3]

Однією з вагомих причин загрози вчинення кібератаки на критичну інформаційну інфраструктуру України є відсутність єдиних регламентованих стандартів до кіберзахисту таких об'єктів. Саме тому вважаю за необхідне створити спеціальні підрозділи з кіберзахисту на об'єктах критичної інформаційної інфраструктури.

Виходячи з цього, потрібно встановити єдині кваліфікаційні вимоги для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз із упровадженням для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам.

Отже, аналіз стану забезпечення інформаційної безпеки показує необхідність удосконалення системи адміністративно-правового регулювання інформаційної безпеки. Одночасно з цим постає потреба у виробленні нових засобів, методів і способів забезпечення інформаційної безпеки державного управління, моніторинг інформаційного середовища, наявності загроз та небезпек.

Список використаних джерел

1. «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави»: Постанова Кабінету Міністрів України від 23.08.2016 № 563// База даних «Законодавство України»/ Верховна Рада України. URL: http://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF

2. «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015// База даних «Законодавство України»/ Верховна Рада України. URL:http://zakon5.rada.gov.ua/laws/show/287/2015

3. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М./ ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ/ URL: http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf

Черновол В. С.,
інспектор Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України,
старший лейтенант поліції

ПРОБЛЕМИ КВАЛІФІКАЦІЇ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН ЯК ЗНАРЯДДЯ ВЧИНЕННЯ ЗЛОЧИНУ:ЗАКОРДОННИЙ ДОСВІД

Сучасний стан інформатизації суспільства створює нові, раніше не знайомі вітчизняному законодавству, форми злочинної поведінки, відкриває нові «горизонти» для професійної злочинності.

З криміналістичної точки зору такі вчені, як П.Д. Біленчук, М.А. Зубань та В.О. Голубєв умовно поділяють кіберзлочини на дві окремі категорії: злочини, в яких електронно-обчислювальні машини є об’єктом кримінального

правопорушення та злочини, які об'єднують протизаконні акції, для здійснення яких як знаряддя в досягненні злочинної мети використовуються ЕОМ.

До злочинів, в яких ЕОМ виступає знаряддям вчинення злочину, можна віднести: шахрайства, комп'ютерний саботаж (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, з метою блокування та створення перепон для нормального функціонування ЕОМ, або комп'ютерної мережі), вимагання та шантаж; розтрата, розкрадання коштів, кібербулінг, кібершпигунство, тощо.

Вітчизняна практика свідчить, що дедалі частіше ЕОМ використовуються не як спосіб вчинення злочину, або як спосіб його приховання, а саме як знаряддя вчинення злочину. Разом з цим, через розповсюдженість проявів такої злочинної активності постає нагальна проблема в кваліфікації дтаких діянь та питання необхідності внесення змін до чинного кримінального законодавства.

В чинному Кримінальному кодексі України передбачено лише один розділ, який пов'язано з кіберзлочинами – Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». У деяких статтях передбачено вчинення злочину з використанням електронно-обчислювальної техніки як особливо кваліфікований склад злочину, яскравим прикладом в такому випадку є ч.3 ст. 190 КК України «Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки».

Кримінальним кодексом Естонії передбачено розмежування за статтями, відповідно до якого: ст. 143 «Шахрайство» та ст. 268 «Комп'ютерне шахрайство».

Розглянемо типову для двох обраних країн ситуацію вчинення злочину, коли особа, маючи умисел на заволодіння чужим майном, вносить зміни у базу даних комерційного банку щодо розміру депозитного вкладу чи кредиту тощо, тим самим одержуючи майно, або утримуючись від необхідності сплати коштів, заподіюючи тим самим шкоду банку.

Відповідно до кримінального законодавства України обов'язковою ознакою такого правопорушення є незаконні операції з використанням електронно-обчислювальної техніки, які виступають способом вчинення обману при шахрайстві. У всіх інших випадках, коли особа шляхом дії чи бездіяльності порушила і інформаційні відносини, забезпечені комп'ютерними технологіями, і будь-які інші, кваліфікація повинна відбуватися за правилами сукупності злочинів.

Відповідно ж до КК Естонії, якщо у складі діяння наявна хоча б одна з ознак об'єктивної сторони, передбачених у ст. 268, а саме: отримання чужого майна, майнової або іншої вигоди шляхом введення комп'ютерних програм або інформації, їх модифікації, знищення, блокування або іншого виду втручання в процес обробки інформації, що впливає на результат обробки інформації і

обумовлює заподіяння прямого майнового або іншого шкоди власності іншої особи, злочин може бути кваліфіковано саме як комп'ютерне шахрайство.

Відповідальність за вчинення цього виду шахрайств вже задекларована в кримінальному законодавстві різних країн через активне використання. Але дедалі частіше постає питання щодо оцінки та кваліфікації злочинів, які є менш розповсюдженими, наприклад, людству вже відомі випадки вчинення умисних вбивств за допомогою інформаційних технологій та електронно-обчислювальних машин, які виступають в подібних злочинах у якості знаряддя вчинення злочину.

Одним досить цікавим з точки зору кримінально-правової оцінки є випадки, коли за допомогою дистанційного підключення до програми управління автоматичної інсулінової помпи виникає можливість вчинення вбивства людини шляхом втручання в роботу подачі пристрою і змінити дозування інсуліну.

На щастя такі випадки поодинокі, але згодом можлива популяризація таких видів вбивств, тоді постане нагальна потреба у кваліфікації таких злочинів для притягнення осіб до кримінальної відповідальності.

Наприклад, за Кримінальним кодексом Грузії таке діяння можна буде кваліфікувати за ч.2 ст. 324-1 «Кібертероризм, тобто протиправне заволодіння охоронюваної законом комп'ютерною інформацією, її використання або загроза використання, що спричинило смерть людини або інші тяжкі наслідки».

Відповідно до чинного кримінального законодавства України таке діяння повинно буде кваліфікуватися за правилами сукупності злочинів, тобто ч.1 ст. 115, ч.1 ст. 361, що не є доцільним відповідно до принципу економії кримінальної репресії.

Таким чином, у зв'язку з швидким розвитком інформаційних технологій, а також інформатизацією всіх процесів у суспільстві виникає нагальна потреба у внесенні змін до основних нормативно-правових актів, які регламентують загальний порядок використання електронно-обчислювальних машин в приватній та комерційній діяльності окремих суб'єктів та встановлюють необхідну та доцільну юридичну відповідальність за порушення цих правил, зокрема з точки зору кримінально-правової охорони суспільних інтересів, прав та свобод громадян.

Список використаних джерел

1. Черновол В.С.: Кримінологічна характеристика та заходи протидії кібертероризму/Університетські кримінально-правові та кримінологічні читання : зб. тез доп. І Всеукр. курсант.-студент. наук.-практ. конф. (16.06.2017 р., м. Харків) / МОН України ; МВС України, ХНУВС ; Кримінол. асоц. України. – Харків,2017.-с. 163-166.

2. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду/ Збірник наукових праць Харківського національного університету Повітряних Сил. 2016. № 4(49). С. 168-172. URL: http://www.hups.mil.gov.ua/periodic-app/article/17271.

Пефтієв О.В.,
начальник відділу супроводження
та розвитку інформаційних систем і баз даних
Головного управління Національної поліції у Донецькій області

ОСНОВНІ НАПРЯМИ ЗАХИСТУ ВІД КІБЕРВТРУЧАННЬ УПРАВЛІННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДТРИМКИ ГУ НП В ДОНЕЦЬКІЙ ОБЛАСТІ

Підтримка достатнього рівня інформаційної безпеки правоохоронних органів має велике значення для забезпечення життєво важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Отже, діяльність Національної поліції України значною мірою пов’язана з отриманням та використанням відомостей обмеженого доступу, розголошення яких може спричинити порушення конституційних прав громадян, а також зниження ефективності роботи поліції щодо превенції, розкриття та розслідування правопорушень.

У процесі здійснення своєї діяльності співробітники поліції отримують інформацію про режим і характер роботи підприємств, розташованих на території, що обслуговується, відомості, що стосуються особистого життя громадян, а також іншу інформацію (наприклад, службового характеру). Така інформація, а також відомості про окремі методи, прийоми і результати роботи поліції складають службову таємницю. Розголошення таких відомостей, а також витік інформації про плановані органами внутрішніх справ заходи щодо охорони громадського порядку і боротьби зі злочинністю порушує нормальну їх діяльність і значно знижує ефективність.

У своїй діяльності для службових цілей Національна поліція використовує наступні види мереж, а саме:

1. Мережу Інтернет, затверджену Наказом Національної поліції України від 21.02.2017 №141 «Про систему Інтернет у телекомунікаційній мережі Національної поліції України». Використання системи Інтернет є складовою частиною телекомунікаційного забезпечення Національної поліції України і надає можливість організувати обмін інформацією між сервісами, користувачами системи Інтернет Національної поліції України та глобальною мережею Інтернет.

2. Відомчу мережу, затвердженоу Наказом Міністерства внутрішніх справ України від 04.07.2016 №596 «Про єдину цифрову відомчу телекомунікаційну мережу МВС» (далі - ЄЦВТМ). ЄЦВТМ є сучасною логічно цілісною мультисервісною багаторівневою інформаційно-телекомунікаційною мережею МВС, що здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв’язку та включає сукупність технічних засобів й обладнання мережі доступу і транспортної телекомунікаційної мережі для

забезпечення передачі інформації (даних), яка (які) належить (належать) до державних інформаційних ресурсів регіонального, районного та міського рівнів, для потреб користувачів, а також надає підключеним до неї віддаленим один від одного користувачам системи МВС весь різновид телекомунікаційних послуг і сервісів фіксованого телефонного, документального, радіозв'язку, аудіо- та відеоселекторного зв'язку тощо, як у звичайних умовах, так і під час особливого періоду чи запровадження в державі надзвичайного стану.

Так, Управлінням інформаційно-аналітичної підтримки Головного управління Національної поліції в Донецькій області створено ряд умов запобіганню від загроз зовнішнього та внутрішнього периметру.

Для зниження ризиків компрометації критично важливих систем з боку зовнішніх порушників особлива увага приділяється ресурсам, доступним із зовнішніх мереж. Як показує практика, переважна більшість успішних атак засновані на експлуатації вразливостей не на неофіційних сайтах організацій та їх серверів, а будь-яких інших ресурсах компанії, які не повинні бути доступні на мережевому рівні.

Для захисту мережі Інтернет від атак на веб-додатки застосовуються міжмережеві екрани, а саме міжмережевий екран FortiGate, який забезпечує максимальний захист як проти мережевих загроз, так і проти загроз прикладного рівня, з ефективними настройками правил кореляції. Для контролю за ресурсами на мережевому периметрі забезпечуються регулярні сканування ресурсів, доступних з зовнішніх мереж.

Що стосується захисту відомчої мережі від атак з боку внутрішнього порушника, ведеться парольна політика, яка забороняє використання простих паролів, а також існують вимоги до регулярної зміни паролів (раз в 30 днів). Також необхідно звернути особливу увагу на застарілі версії ПЗ, на відкриті протоколи передачі даних і на зберігання важливої інформації у відкритому вигляді на серверах і робочих станціях співробітників. Крім базових заходів захисту інформації, на регулярній основі проводиться аудит безпеки інформаційних систем і тестування на проникнення з боку зовнішнього і внутрішнього порушника, а заради захисту персональних станцій співробітників поліції встановлюється якісний продукт ESET Endpoint Security та набори додатків до веб браузерів, наприклад, AdGuard та захисту з'ємних носіїв, наприклад USB Protection & Recovery.

УІАП ГУНП в Донецькій області постійно ведеться оновлення застарілих версій ПЗ на актуальні.

Доцільним є питання поширення ноутбуків, нетбуків та планшетних комп'ютерів, що надало можливість користувачам працювати з інформацією не тільки безпосередньо на робочому місці, а і під час поїздок, відряджень тощо. Але треба зазначити, що це дає не тільки можливості, а і породжую небезпеки. Однією з таких небезпек є втрата ноутбуку (нетбуку, планшетного комп'ютера), або його крадіжка. Якщо здійснити пошук в Інтернет, то ми легко знайдемо багато прикладів, коли таким чином втрачалася вважлива та

конфіденційна інформація. Основним завданням безпеки роботи з інформацією є, все ж таки, не збереження пристрою, а саме захист цієї інформації. На жаль жоден з методів на забезпечує захисту інформації у одному дуже простому випадку – коли зловмисник просто виймає жорсткий диск, або інший носій, що використовується для збереження інформації, і приєднує його до власного комп'ютера для отримання доступу до інформації. Якщо не вжити заходів для шифрування інформації, то вся інформація буде доступна зловмиснику у відкритому вигляді, тому УІАП ГУНП в Донецькій області рекомендує проводити шифрування інформації. Якщо застосувати цей надійний метод захисту інформації у разі використання з'ємних носіїв немає можливості, то слід скористатися створенням зашифрованого розділу, або зашифрованого віртуального диску. Єдине, що можна зауважити, що для з'ємного носія краще скористатися варіантом створення зашифрованого розділу.

Існують ряд недоліків у використанні точок доступу і клієнтських пристроїв Wi-Fi, а також недоліків в архітектурі та організації бездротового доступу. Серед недоліків варто відзначити використання механізму WPS для спрощення процесу налаштування бездротової мережі. Для підключення до точки доступу використовується спеціальний PIN-код, що складається тільки з цифр. Порушник може підібрати PIN-код і підключитися до точки доступу, саме тому ГУНП в Донецькій області не використовує пристрої Wi-Fi.

УІАП ГУНП в Донецькій області постійно проводить аудит своїх систем та мереж на скомпроментованість та її можливість, що надавало та надає певні переваги перед новими видами загроз.

Трифонов В.В.,
провідний інженер-програміст
відділу супроводження
та розвитку інформаційних систем і баз даних
Головного управління Національної поліції у Донецькій області

СПОСОБИ ЗАХИСТУ БАЗ ДАНИХ

Дані в базах даних повинні зберігатися з гарантуванням безпеки та конфіденційності. Інформація не повинна бути загубленою, або викраденою. Загрози втрати конфіденційної інформації стали звичайним явищем у сучасному комп'ютерному світі. Якщо в системі захисту є недоліки, то даним може бути завдано шкоди, такої як: порушення цілісності даних, втрата важливої інформації, потрапляння важливих даних до сторонніх осіб.

Основні методи захисту баз даних включають в себе: захист паролем, шифрування даних та програм, розмежування прав доступу до об'єктів бази даних.

Захист паролем являє собою простий і ефективний спосіб захисту БД від несанкціонованого доступу. Паролі встановлюються користувачами або адміністраторами БД. Облік і зберігання паролів виконується самою СУБД.

Зазвичай, паролі зберігаються в певних системних файлах СУБД в зашифрованому вигляді. Після введення пароля користувачу СУБД надаються всі можливості по роботі з БД.

Парольний захист стає слабким засобом, особливо якщо пароль не шифрується. Недолік полягає в тому, що всі користувачі, які використовують однаковий пароль, з точки зору обчислювальної системи не відрізняються. Незручність парольного захисту для користувача полягає в тому, що пароль треба запам'ятовувати, або записати. При недбалому відношенні до записів пароль може стати надбанням інших.

Контроль доступу до бази даних. Запобігти атакам кіберзлочинців допоможуть обмеження дозволів та привілеїв. Крім базових системних дозволів, слід застосувати:

- Обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією.
- Обмеження використання основних процедур тільки певними користувачами.
- Уникнення використання і доступу до баз даних в неробочий час.

Також для запобігання атакам зловмисників потрібно вимкнути всі служби і процедури, які не використовуються. Крім того, базу даних слід розміщувати на сервері, недоступному безпосередньо через мережу Інтернет, щоб запобігти віддаленому доступу зловмисників до корпоративної інформації.

Не буває невразливих систем захисту. Настирливий зловмисник завжди може знайти спосіб подолати всі системи контролю і захисту. Тому під час роботи з дуже важливими даними необхідно реєструвати у відповідному журналі всі події, що стосуються функціонування системи захисту. У зв'язку з цим система захисту має надавати можливість виконувати дії:

1) Реєструвати всі спроби отримання доступу до системи баз даних, у тому числі й безуспішні. Ця реєстрація мас бути максимально повною (повинні реєструватися відомості про те, хто отримував доступ, або намагався його отримати, з якого термінала або вузла мережі, о котрій годині тощо)

2) Реєструвати дії користувачів та використання всіх ресурсів системи, зокрема й даних, а також інші дії та події, які можуть вплинути на захист даних.

3) Надавати користувачам, які мають адміністративні повноваження, можливість переглядати й аналізувати результати реєстрації, виявляти небезпечні ситуації, встановлювати причини їхнього виникнення та знаходити користувачів, відповідальних за порушення політики безпеки.

Шифрування критично важливої інформації. Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації. У випадку використання уразливості, або отримання доступу до сервера або системи, зловмисники в першу чергу спробують викрасти бази даних, які, зазвичай, містять багато цінної інформації. Кращий спосіб захистити базу даних — зашифрувати її для осіб, які намагаються отримати доступ без авторизації.

Список використаних джерел

1. Нужний Є.М. Інструментальні засоби електронного офісу. Навчальний посібник — ЦУЛ, 2017 – 296 с.
2. МЕТОДИ ЗАХИСТУ БАЗ ДАНИХ [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/17_PMN_2014/Informatica/4_171996.doc.htm

Кравець В.М.,
Національна академія СБ України
кандидат технічних наук, старший науковий співробітник

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Серед вітчизняних науковців не один рік точаться дискусії щодо співвідношення понять інформаційна та кібернетична безпека. Один підхід визначає кібернетичну безпеку складовою інформаційної безпеки, що стосується лише протидії шкідливій активності в електронних мережах [1], відповідно до іншого – кібернетична безпека є більш широким поняттям, яке ототожнюється з поняттям інформаційної безпеки [2; 3]. У США формування концепції інформаційної безпеки передбачає запобігання завданню фізичної шкоди інформаційному потенціалу шляхом застосування технічних засобів і має назву кібернетичної безпеки. У Російській Федерації інформаційну безпеку розглядають як соціальне, а не чисто технічне явище [4].

Сучасна державна політика України у сферах національної безпеки і оборони, яка формувалася в умовах зовнішньої агресії з боку Російської Федерації, визначає інформаційну та кібернетичну безпеку як окремі рівнозначні напрямки забезпечення (п. 4 ст. 3 Закону України «Про національну безпеку України»).

На нашу думку, ця дискусія може бути вирішена у межах концепції безпеки інформаційної сфери. Так, відповідно до попередніх досліджень автора [5; 6] ключовим елементом системи понять, пов’язаних з безпекою інформаційної сфери, є інформація. Національна безпека в інформаційній сфері – це такий стан інформаційного розвитку та захищеності особи, суспільства, держави (духовного, правового, технічного), за якого сторонні інформаційні впливи не мають вирішального значення при прийнятті рішень, спрямованих на забезпечення власних (особистих, суспільних, державних) інтересів. Основними об’єктами безпеки інформаційної сфери, які потребують захисту та розвитку, є інформаційні ресурси, інформаційний простір та інформаційно-телекомунікаційна інфраструктура.

Поняття "кібернетика" у значенні наукової дисципліни введено у 1948 році Н. Вінером, який уперше визначив принципове значення інформації у процесах управління. Концепція кібернетики породжена синтезом багатьох наукових напрямів. По-перше, як загальний підхід до опису і аналізу діяльності живих організмів та обчислювальних машин (автоматів). По-друге, із спостереження

аналогій між поведінкою спільнот (груп) живих організмів і людського суспільства та можливістю описати їх за допомогою загальної теорії управління й інформації. І, нарешті, із синтезу теорії передавання інформації і статистичної фізики, який підштовхнув Н. Вінера до найважливішого відкриття, що пов'язує кількість інформації з негативною ентропією у різних системах. Таким чином, основною тезою дослідження Н. Вінера є подібність інформаційних процесів управління та комунікації в машинах, живих організмах і суспільстві. Відтак, Н. Вінер визначає кібернетику як науку про управління, комунікацію, обробку інформації у технічних системах, людському суспільстві і живих організмах [7].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кібернетична безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі, а кіберпростір – це простір, утворений сукупністю інформаційно-телекомунікаційних систем.

З огляду на викладене, кібернетична безпека є складовою національної безпеки в інформаційній сфері, яку загалом утворюють:

- безпека інформації (захист інформації з обмеженим доступом, розвиток національних інформаційних ресурсів);
- комунікативна безпека (захист інформаційного простору від зовнішніх інформаційних впливів, протидія маніпулюванню громадською думкою, розвиток національного інформаційного простору);
- кібернетична безпека (безпека інформаційно-телекомунікаційних систем та мереж, розвиток інформаційно-комунікаційних систем).

З урахуванням розвитку сучасних інформаційно-комунікаційних технологій та постійного перетворення інформації, її багаторазового поширення, зміни форм зберігання і передачі, досить складно сьогодні провести межу між інформаційним та кібернетичним простором. Разом з тим, пропонуємо розрізняти комунікативну та кібернетичну безпеку таким чином. Якщо питання стосується безпеки даних, технологій чи засобів їх автоматизованої обробки і зміст цих даних немає суттєвого значення при прийнятті рішень суб’єктом інформаційної діяльності, то це питання кібернетичної безпеки. Якщо при цьому принципове значення має зміст інформації, що обробляється, то це питання комунікативної безпеки. Зокрема, будь-яка соціальна мережа є інформаційною системою у кіберпросторі. Якщо атака спрямована на дані у соцмережі, і при цьому неважливий їх зміст, їх контент, то це питання кібернетичної безпеки. Якщо під впливом інформації із соціальної мережі, її користувачі приймають упереджене рішення щодо вибору кандидата у Президенти США, то це питання комунікативної безпеки.

Список використаних джерел

1. Дубов. Д. Сучасні тренди кібербезпекової політики: висновки для України (жовтень 2010 року) : аналітична записка [Електронний ресурс] // Національний інститут стратегічних досліджень при Президентові України : [сайт]. URL : http://www.niss.gov.ua/articles/294 (дата звернення: 29.03.2019).

2. Супрунов Ю.М. Деякі проблемні питання нормативного забезпечення розгортання систем кібернетичної оборони провідних країн світу в контексті інформаційної безпеки України // Актуальні проблеми управління інформаційною безпекою держави : збірник матеріалів науково-практичної конференції, 22 березня 2011 р. : у 2 ч. К.: Вид-во НА СБ України, 2011. Ч. 2. С. 68-72.

3. Яковів І.Б. Парадигма кібербезпеки на основі атрибутивно-трансфертного підходу до сутності інформації // Інформаційна безпека: виклики і загрози сучасності : збірник матеріалів науково-практичної конференції, 5 квітня 2013 р. К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2013. С. 153-161.

4. Соболь С. Ю. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности // Научно-техническая информация. 2003. №11. С.10-15. Сер. "Организация и методика информационной работы".

5. Панченко В.М. Поняття інформаційної безпеки в сучасному юридичному дискурсі // Інформаційна безпека людини, суспільства, держави. 2009. № 2 (2). С. 22–27.

6. Панченко В.М. Співвідношення понять: інформаційна та кібернетична безпека // Інформаційна безпека людини, суспільства, держави. 2013. № 2 (12). С. 20–23.

7. Цит. за: Кольман Э.Я. О философских и социальных идеях Норберта Винера. М. : Издательство иностранной литературы, 1958. С. 5–22.

Істомін Д.Г.,
директор Департаменту інформаційних технологій
Маріупольської міської ради

ПІДХОДИ ПІДВИЩЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

У наш час, коли інформаційні технології вже міцно пов’язані з бізнес-процесами більшості компаній, а способи і методи мережевих атак постійно удосконалюються і розвиваються, все ще існує думка, що установка звичайного мережевого екрану на кордоні мережі достатньо для захисту внутрішніх корпоративних ресурсів. Це, на жаль, не зовсім так, а, вірніше, зовсім не так.

Як приклад малої ефективності звичайного брандмауера користувач системи може самостійно натиснути на посилання, отримане від добре знайомого друга в соціальній мережі або поштою, завантажити і запустити

вірус, який, використовуючи відомий експлоїт неоновленої операційної системи або програми, отримає права адміністратора і буде виконувати зловмисну задачу зсередини корпоративної мережі. При цьому копії вірусу будуть активно розсилатися по контакт листу ураженої системи. В Інтернеті доступні онлайн системи для тестування підозрілих файлів різними антивірусними програмами, але ними в першу чергу користуються ті ж зловмисники для написання нових «непомітних» вірусів. У зв'язку з цим у наш час існує така величезна кількість бот-нет мереж, досить просто купити номера крадених кредитних карток, і все більше злам комп'ютерів стає звичайним методом заробляння грошей. Тому завдання забезпечення безпеки вимагає комплексного підходу на всіх рівнях мережевої інфраструктури і комп'ютерних ресурсів.

Процес побудови безпечної мережевої інфраструктури починається з планування. На цьому етапі перераховуються сервіси, які будуть використовуватися в мережі, пов'язані з ними ризики, визначаються необхідні кроки і механізми для зниження цих ризиків. На підставі даних, отриманих на етапі планування, розробляється відповідний дизайн мережевої інфраструктури і створюється набір політик безпеки. Після цього йде етап безпосереднього впровадження. Оскільки безпека це не кінцевий результат, а процес, впровадженням і первинним налаштуванням якої-небудь системи захисту нічого не закінчується. Рішення безпеки вимагають постійної «уваги»: відстеження подій безпеки, їх аналізу та оптимізації відповідних політик.

Від написання ефективних політик безпеки та їх суворого дотримання залежить робота всього комплексу захисту. Правильні політики повинні бути зафіксовані документально, не мати великої кількості винятків. На все обладнання повинні регулярно встановлюватися оновлення. Також велику загрозу для безпеки складають прості паролі, помилки в конфігурації пристроїв, використання налаштувань за замовчуванням, незахищених протоколів і технологій.

Для забезпечення повної безпеки всієї IT інфраструктури необхідно впроваджувати механізми захисту на всіх рівнях мережі від кордону до комутаторів доступу. На рівні доступу рекомендується використовувати керовані комутатори з підтримкою функціоналу захисту протоколів ARP, DHCP, STP. Авторизувати користувачів при підключенні за допомогою технології 802.1x. Підключати співробітників в різні VLAN залежно від їх функціональних обов'язків і задавати правила взаємодії і доступу до різних ресурсів на рівні розподілу.

При підключенні до мережі WAN та Інтернет важливо крім брандмауера мати можливість сканувати трафік на рівні додатків, перевіряти наявність загроз за допомогою IPS систем. Прикордонне обладнання повинно бути стійким до DoS і DDoS атак. Вкрай рекомендується для виходу користувачів в Інтернет використовувати проксі сервери з додатковою перевіркою на віруси, небажане, шкідливе і шпигунське ПЗ. На проксі додатково можна організувати

веб- та контент- фільтрацію. Також важлива наявність рішення для перевірки пошти на предмет спаму і вірусів. Усі корпоративні ресурси, до яких потрібно забезпечити доступ ззовні в цілях безпеки повинні бути винесені в окрему демілітаризовану зону DMZ. Для віддаленого доступу використовувати технологію VPN з шифруванням переданих даних.

Для управління всім мережевим обладнанням повинні використовуватися захищені протоколи SSH, HTTPS, SNMPv3. Для можливості аналізу логів час на пристроях має бути синхронізований. Для розуміння, який трафік ходить в мережі, наскільки завантажено обладнання, які події на ньому відбуваються, використовувати протоколи Syslog, RMON, Sflow, NetFlow. Дуже важливо вести облік, хто, коли і які зміни вносить у конфігурацію устаткування.

Список використаних джерел

1. Simmonds, A; Sandilands, P; van Ekert, L (2004). An Ontology for Network Security Attacks. Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323. ISBN 978-3-540-23659-7. doi:10.1007/978-3-540-30176-9_41.

2. Хоффман Л. Дж. Современные методы защиты информации // — М.: Сов. радио, 1980 – 560 с.

Неласа Г.В.,
кандидат технічних наук, доцент,
доцент кафедри захисту інформації,
Запорізького національного технічного університету
Кузьменко А.В.,
студент Запорізького національного технічного університету
Матвейчук О.В.,
студент Запорізького національного технічного університету

АНАЛІЗ МОВИ ПРОГРАМУВАННЯ Q# ЯК ІНСТРУМЕНТУ КВАНТОВОЇ КРИПТОГРАФІЇ

Квантовий алгоритм являє собою класичний алгоритм, який задає послідовність унітарних операцій із зазначенням, над якими саме кубітами їх треба здійснювати. Квантовий алгоритм задається або у вигляді словесного опису таких команд, або за допомогою їх графічного запису у вигляді системи вентилів[1].

Природною моделлю для квантових обчислень є квантовий комп'ютер як співпроцесор, подібний до того, який використовується для GPU, FPGA та інших допоміжних процесорів. Первинна логіка керування виконує класичний код на класичному "хост" комп'ютері. Якщо це доречно і необхідно, хост-програма може викликати підпрограму, яка виконується на додатковому процесорі. Після завершення підпрограми хост-програма отримує доступ до результатів підпрограми.

Квантова криптографія – розділ криптології, що базується на застосуванні підходів та методів квантової механіки (зокрема, квантової передачі інформації та квантових обчислень) до проблем криптографії та криптоаналізу. Добре відомими прикладами квантової криптографії є застосування квантової комунікації для безпечної передачі секретного ключа (квантовий розподіл ключа) та використання квантових комп'ютерів, що дозволить зламати низку відомих схем шифрування із відкритим ключем та підпису (зокрема, алгоритм RSA і схему Ель-Гамаля).

Перевага квантової криптографії полягає в тому, що вона дозволяє розв'язати низку важливих криптографічних задач, для яких доведена неможливість розв'язання за допомогою лише класичної (тобто, неквантової) комунікації. Зокрема, квантова механіка гарантує, що вимірювання певної квантової величини збурює її, що може бути використано для виявлення втручання сторонньої особи до процесу квантового розподілу ключа [2,3].

Під час конференції Ignite, яка відбулася 26 вересня 2017 року, Microsoft оголосила, що вона планує випустити нову мову програмування, спеціалізовану для використання у квантових комп’ютерах. 11 грудня 2017 року Microsoft випустила Q# (Q-sharp) у складі Quantum Development Kit[4]. Q# – це предметно-орієнтована мова програмування, яка використовується для вираження квантових алгоритмів. Вона повинна використовуватися для написання підпрограми, що виконується на додатковому квантовому процесорі під контролем класичної хост-програми та комп'ютера. Доки квантові процесори не будуть широко доступні, підпрограми Q# виконуються на симуляторі. Q# забезпечує невеликий набір примітивних типів разом із двома способами (масивами і кортежами) для створення нових, структурованих типів. Він підтримує базову процедурну модель для написання програм з циклами і операторами if / then. Конструкції верхнього рівня у Q# - це типи, операції та функції, визначені користувачем.

Методи квантової криптографії можуть бути реалізовані за допомогою мови програмування Q#, що дозволить реалізовувати більш складні алгоритми для шифрування та передачі інформації у майбутньому. Тому вважаємо перспективним вивчення мови програмування Q# у професійній підготовці фахівців з кібербезпеки.

Список використаних джерел

1. Michael A. Nielsen. Quantum Computation and Quantum Information : A catalog record. / Michael A. Nielsen, I. Chuang. - Cambridge University Press, 2010. – 704 c.

2. Daniel J. Bernstein. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? / Daniel J. Bernstein // Department of Computer Science (MC 152) The University of Illinois at Chicago. – 2009. – 12 c.

3. Gerhardt I. Perfect eavesdropping on a quantum cryptography system / Ilja Gerhardt, Qin Liu, Ant´ıa Lamas-Linares, Johannes Skaar, Christian Kurtsiefer,

Vadim Makarov // National Research Foundation and the Ministry of Education, Singapore, and the Research Council of Norway. – 2010. – 7c.

4. The Q# Programming Language / Microsoft. – Режим доступа: URL: https://docs.microsoft.com/en-us/quantum/language/?view=qsharp-preview/ - 12.11.2017 г.

Івохін Є.В.,
доктор фізико-математичних наук,
професор, професор кафедри системного аналізу
та теорії прийняття рішення
Київського національного університету імені Тараса Шевченка

СУЧАСНІ НАПРЯМКИ ДОСЛІДЖЕНЬ ПРОЦЕСІВ ІНФОРМАЦІЙНОГО РОЗПОВСЮДЖЕННЯ ТА ВПЛИВУ

Серед особливо яскравих прикладів впровадження нових технологічних рішень у соціумі виділяються соціальні мережі. Основна ідея створення соціальних мереж – здійснення нового віддаленого способу спілкування. Соціальні інтернет-сервіси надають можливість повідомляти інформацію в різних форматах: текстовому, графічному, відео, аудіо. На основі використання соціальних сервісів з'являються значні можливості для об'єднання, координації та маніпулювання людей з боку зацікавлених осіб, які переслідують певні цілі. Саме соціальні мережі активно використовувалися як засіб для миттєвого обміну повідомленнями на тій території, де може виникнути проблема зі зв'язком. Беручи до уваги технологічний розвиток і комунікаційний потенціал засобів зв'язку та соціальних мереж, можна очікувати, що соціальні мережі зможуть виступати потужним інструментом, що може впливати на громадський порядок і безпеку. Зі збільшенням доступності широкосмугового доступу в мережу Інтернет та розвитком мобільного Інтернету обсяги інформації та показники використання соціальних мереж будуть тільки зростати.

Соціальні мережі все частіше стають об’єктами та засобами інформаційного управління і місцем інформаційного протиборства. Тому, серед завдань, що є дуже актуальними у суспільстві, слід відзначити дослідження та моделювання процесів розповсюдження та впливу інформації. Це призводить до необхідності вивчення та розробки моделей, що враховують рівні інформованості учасників процесу (тобто ті обсяги інформації, якими вони володіють на момент прийняття рішень), і, як наслідок, до потреб вирішення задач інформаційного впливу, інформаційного управління та інформаційного протиборства.

Створення моделей інформаційного впливу дозволяє досліджувати залежність поведінки суб’єктів від їх інформованості та джерел впливу. На основі таких моделей можна ставити та розв’язувати задачу інформаційного управління (визначення впливів з точки зору керуючого суб’єкта) з метою досягнення необхідної поведінки. І, врешті, вміючи розв’язувати задачу інформаційного управління, з’являється можливість змоделювати інформаційне

протиборство – взаємодію декількох суб'єктів, що мають антагоністичні інтереси і здійснюють вплив на один і той же суб'єкт, що підлягає управлінню. Якщо моделі інформаційного впливу (соціального впливу в термінах соціології) є предметом багатьох досліджень вже достатньо довгого періоду, то проблеми моделювання інформаційного управління і протиборства (особливо з появою можливості аналізу інформації з соціальних мереж) практично не досліджуються.

Ще однією важливою особливістю даних про соціальні події та явища, яка характерно проявляється у соціальних мережах, є постійна модифікація їх складу. Динамічний підхід – напрямок у вивченні соціальних мереж, в якому об'єктами досліджень є зміни в мережевій структурі з часом: з'являються нові учасники, деякі учасники припиняють взаємодію, виникають нові зв'язки, деякі зв'язки застарівають за умов, що учасники перестають взаємодіяти. Це призводить до структурних змін в соціальних мережах в цілому і в окремих спільнотах.

Розроблення методів та підходів підтримки прийняття рішень для аналізу та розв'язування задач розповсюдження та впливу інформаційних потоків в соціальних мережах, створення технологій моделювання й прогнозування рівнів інформаційного впливу дозволять вдосконалювати технологічні рішення для проектування засобів інформаційної безпеки та способів ведення інформаційного протиборства. Проведення аналізу процесів проникнення та впливу інформації в соціумі з метою перевірки концепцій і технологічних рішень, з метою створення критичних технологій інформаційного захисту та безпеки з урахуванням динаміки змін соціального середовища є однією з найважливіших задач у сучасному інформаційному просторі України.

Список використаних джерел

1. Брайчевський С.М. Сучасні інформаційні потоки: актуальна проблематика /С.М. Брайчевський, Д.В. Ланде //Науково-технічна інформація. – Сер.1. – Вип.11. – 2005. – С. 21-33.

2. Араманович И.Г. Уравнения математической физики / И.Г.Араманович, В.И. Левин. – М.: Наука, 1969. - 288 с.

3. Kermack W. O. A Contribution to the Mathematical Theory of Epidemics / W. O. Kermack, A. G. McKendrick // Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character, 1927. – Vol. 115. – Iss.772. – P.700-721.

4. Хайрер Э. Решение обыкновенных дифференциальных уравнений / Э.Хайрер, С. Нерсетт, Г.Ваннер. –М: Мир, 1990.-512 с.

5. Федотов А.М. Модель самоорганизации в агентных системах с передачей сообщений/ А.М.Федотов, С.Г.Ломакин // Математическое моделирование и вычислительно-информационные технологии в междисциплинарных научных исследованиях: Материалы IV Всероссийской конференции. - 2014. - Иркутск: Институт динамики и теории управления СО РАН. - С.42.

Нікітін А.В.,
кандидат фізико-математичних наук, доцент,
старший науковий співробітник
факультету комп'ютерних наук та кібернетики
Київського національного університету імені Тараса Шевченка

АНАЛІЗ АСИМПТОТИЧНИХ ВЛАСТИВОСТЕЙ ЕВОЛЮЦІЙНОЇ МОДЕЛІ ПОШИРЕННЯ ІНФОРМАЦІЇ В УМОВАХ АПРОКСИМАЦІЇ ПУАССОНА

Актуальність теми. Стрімкий розвиток процесу інформатизації есіх сфер життя суспільства, що суттєво впливає на стан економіки, національну безпеку, інтелектуальний потенціал суспільства тощо, дає можливість оцінити важливість інформаційного впливу на соціальні спільноти. У науковій літературі з'явилисz публікації, які описують процес поширення інформації, можливості використання її у власних інтересах, як для поширення «потрібної» інформації, так і для протидії небажаним тенденціям у суспільстві. Істотними питаннями, що виникли у цій сфері, є побудова та аналіз моделей, які б адекватно описували цей процес. Ми пропонуємо моделі, записані у вигляді стохастичних еволюційних рівнянь з марковськими переключеннями та імпульсним впливом в умовах некласичних схем апроксимації.

Основні положення. Стохастична еволюційна система в ергодичному марковському середовищі задається стохастичним диференційним рівнянням [1]

$$du^{\varepsilon}(t) = C(u^{\varepsilon}(t), x(t/\varepsilon^2))dt + d\eta^{\varepsilon}(t), \quad u^{\varepsilon}(t) \in \mathrm{R} \tag{1}$$

де $u^{\varepsilon}(t)-$ випадкова еволюція, $t \geq 0$; $\varepsilon > 0$ – малий параметр серій; $C(u,\cdot) \in C^2(\mathrm{R}^d)$ – функція регресії; $x(t)$ – рівномірно ергодичний марковський процес у стандартному фазовому просторі $(X, \mathbf{X})$. Імпульсний процес збурень $\eta^{\varepsilon}(t),\ t \geq 0,$ у схемі апроксимації Леві визначається співвідношенням

$$\eta^{\varepsilon}(\mathrm{t}) = \int_0^t \eta^{\varepsilon}(ds, x(s/\varepsilon^2)); \tag{2}$$

де сукупність процесів з незалежними приростами $\eta^{\varepsilon}(t,x), t \geq 0, x \in X$, задовольняють умовам пуассонової апроксимації:

Р1: *Апроксимація середніх:*

$$\int_R v\Gamma^{\varepsilon}(d\,\mathrm{v}, x) = \varepsilon(a(x) + \theta_a(x)),\ \ \theta_a(x) \to 0, \varepsilon \to 0,$$

$$\int_R \mathrm{v}^2\,\Gamma^{\varepsilon}(d\,\mathrm{v}, x) = \varepsilon(b(x) + \theta_b(x)),\ \ \theta_b(x) \to 0, \varepsilon \to 0.$$

Р2: *Умова на функцію розподілу:*

$$\int_R g(\mathrm{v})\Gamma^{\varepsilon}(d\,\mathrm{v},x)=\varepsilon^2(\Gamma_g(x)+\theta_g(x)),\ \theta_g(x)\to 0,\varepsilon\to 0$$

для всіх $g(v)\in C_3(R)$.

Р3: *Рівномірна квадратична інтегровність:*

$$\lim_{c\to\infty}\int_{|v|>c} v^2\Gamma_0(dv,x)=0.$$

Р4: *Відсутність дифузійної складової:*

$$b(x)=\int_R v^2\Gamma_0(dv,x).$$

Модель (1) перепишемо у наступному вигляді

$$dL^{\varepsilon}(t)=C(L^{\varepsilon}(t),x(t/\varepsilon^2))dt+d\eta^{\varepsilon}(t) \qquad (4)$$

Тут $C(L,x)=\alpha_1(x)L_0(x)+\alpha_2(x)L_0(x)L(t)-\alpha_2(x)L^2(t)$,

$\alpha_1(x)=\alpha_{11}(x)\alpha_{12}(x)$ – зовнішній канал;

$\alpha_2(x)=\alpha_{21}(x)\alpha_{22}(x)$ – внутрішній канал

де $\alpha_{11}>0$ $\alpha_{21}>0$ – інтенсивність (число рівноцінних інформаційних контактів на одиницю часу ;

$\alpha_{12}>0,\ \alpha_{22}>0$ – ймовірність бути завербованим (схильність до сприйняття інформації).

$L(t)$ – число «завербованих» адептів;

$L_0(x)-L(t)$ – число ще не «завербованих» адептів;

$\eta^{\varepsilon}(t)$ моделює імпульсні впливи.

Твердження1. *При виконанні умов пуассонової апроксимації, справедливою є слабка збіжність*

$$L^{\varepsilon}(t)\to\hat{L}(t)\ ,\ \varepsilon\to 0$$

Граничний процес визначається генератором

$$\mathbf{L}\varphi(w)=\hat{C}(L)\varphi'(w)+\Gamma\varphi(w)$$

де

$$\hat{C}(L)=\int_X \pi(dx)(\alpha_1(x)L_0(x)+\alpha_2(x)L_0(x)L(t)-\alpha_2(x)L^2(t))$$

$$\Gamma\varphi(\omega)=\tilde{a}\varphi'(\omega)+\int_R[\varphi(\omega+v)-v\varphi'(v)]\tilde{\Gamma}_0(dv)$$

$$\tilde{a}=\int_X \pi(dx)a(x),\qquad \tilde{\Gamma}_0(v)=\int_X \pi(dx)\Gamma_0(dv,x)$$

Твердження2. *Нехай існує функція Ляпунова* $V(L) \in C^3(\mathbf{R}^d)$ *системи*

$$\frac{dL}{dt} = \beta(L)$$

де

$$\beta(L) = \hat{C}(L) + \hat{a} = \int_X \pi(dx)(\alpha_1(x)L_0(x) + \alpha_2(x)L_0(x)L(t) - \alpha_2(x)L^2(t)) + \hat{a}$$

яка задовольняє умовам

C1: $|\Gamma_L^1(x)R_0\hat{\mathrm{L}}V(L)| < \mathrm{M}_1 V(L),\ M_1 > 0;$

C2: $|\Gamma_L^1(x)R_0\Gamma_L^1(x)V(L)| < \mathrm{M}_2 V(L),\ M_2 > 0;$

C3: $|\Gamma_L^1(x)R_0\mathbf{C}(x)V(L)| < \mathrm{M}_3 V(L),\ M_3 > 0;$

C4: $|\mathbf{C}(x)R_0\hat{\mathrm{L}}V(L)| < \mathrm{M}_4 V(L),\ M_4 > 0;$

C5: $|\mathbf{C}(x)R_0\Gamma_L^1(x)V(L)| < \mathrm{M}_5 V(L),\ M_5 > 0;$

C6: $|\mathbf{C}(x)R_0\mathbf{C}(x)V(L)| < \mathrm{M}_6 V(L),\ M_6 > 0.$

Крім того, нехай виконуються нерівності

$$\alpha(L)V'(L) < -c_1 V(L);\ \ |\int_R \mathrm{v}^2\,\Gamma_0(d\,\mathrm{v}, x)| < c_2(x);$$

де $c_1 > 0$ *та* $\hat{c}_2 = \int_X \pi(dx)c_3(x) > 0$

Тоді система (4) асимптотично дисипативна.

Висновки за темою. Твердження 1 демонструє поведінку схожих соціальних систем, які піддаються інформаційним впливам. Зрозуміло, що будуть флуктуації. Твердження 2 показує, чи буде система близька до усередненої.

Список використаних джерел

1. Korolyuk V.S. Stochastic Models of Systems / V.S. Korolyuk, V.V.Korolyuk // Kluwer, Dordrecht. – 1999. – 185 c.

2. Koroliuk V.S. Stochastic Systems in Merging Phase Space / V.S. Koroliuk, N. Limnios // World Scientific, Singapore, 2005. – 330 c.

3. Михайлов, А.П. Модели информационной борьбы / А. П. Михайлов, Н. А. Маревцева // Матем. моделирование, 2011, том 23, номер 10, 19–32

Шабельник Т.В.,
доктор економічних наук, професор,
в.о. зав. кафедри математичних методів та системного аналізу
Маріупольського державного університету

НЕОБХІДНІСТЬ НАВЧАННЯ НАСЕЛЕННЯ НАВИЧКАМ ПРАВИЛЬНИХ ДІЙ ПІД ЧАС ІНЦИДЕНТІВ КІБЕРЗАГРОЗ

В умовах прогресивного розвитку інформаційно-телекомунікаційних технологій залежність від їх постійного використання стає вже критичною і продовжує збільшуватися. Кібератаки прогресують з такою швидкістю, що захист лише технічними засобами стає малоефективним.

Збільшується кількість кібератак на людей, коли завдяки введенню людини в оману зловмисники захоплюють контроль над комп'ютером, телефоном, кредитними картками тощо Так, найпоширенішими наслідками таких атак виступають: крадіжка грошей з банківського рахунку, поширення приватної інформації у соцмережах та шантаж, шифрування зловмисниками комп'ютера та отримання доступу до цінної корпоративної інформації тощо.

Розглянемо технологію та види зазначених кібератак більш детально.

Перший вид кібератаки. Будь-яка особа отримує листа електронною поштою від знайомих, співробітників або організацій, яким людина довіряє, наприклад, банку. Такий лист спонукає людину відкрити вкладення, перейти за посиланням чи ввести свій пароль. Після відкриття вкладення або переходу за посиланням комп'ютер чи мобільний пристрій буде «зараженим», і далі він контролюєтеся зловмисниками.

Другий вид кібератаки. Будь-яка особа отримує SMS або дзвінок з повідомленням, щодо отримання певного виграшу і потребується перейти за посиланням, або надати номер кредитної картки.

Такі види кібератак, що спрямовані на отримання доступу до систем та інформації завдяки введенню людей в оману, називаються соціальна інженерія. Кібератаки через електронну пошту називаються «фішинг» [2], а по SMS – «вішинг» [1].

Для запобігання та протидії наведених вище видів кібератак необхідним є виконання базових правил безпеки.

Отже, актуальним є навчання населення навичкам розпізнавання зазначених кібератак, а саме, базових навичок з таких тем, як безпечне налаштування мобільного телефону та WI-FI у публічних місцях, розпізнавання небезпечних сайтів, безпечне налаштування домашнього інтернету та пристроїв, які до нього підключені, захист дітей в інтернеті, використання безпечних паролів тощо.

Навчальні матеріали мають виглядати сучасно та приваблювати пересічних громадян. Навчання має бути доступним у будь-який час, з різних джерел, як з використанням паперових носіїв, так і з комп'ютерів та мобільних пристроїв.

Одним з ефективних форматів навчання виступає створення спеціального порталу з навчання базових навичок кібербезпеки для населення, який буде містити навчальні матеріли і на якому можна отримати підтримку фахівця або інших користувачів у разі необхідності. Подібні портали існують у розвинених країнах.

Навчання має проводитися не тільки через інтернет, але й через використання традиційних каналів таких, як телебачення, радіо, газети. Ці канали найбільш поширені серед людей, які нещодавно почали використовувати інтернет та мобільні телефони і найбільш часто стають жертвами шахраїв.

Важливим є питання максимального охоплення кількості громадян. Тому це має бути не просто сайт з навчальними матеріалами, а саме спеціалізована соціальна програма, побудована за усіма останніми трендами, включаючи цікавий та сучасний контент, інтерактивні електронні курси, сучасні методики просування програми та використання різноманітних каналів і методів навчання для різних категорій населення.

Список використаних джерел

1. ВІШИНГ: ЯК ТЕЛЕФОННІ ШАХРАЇ КРАДУТЬ НАШІ ГРОШІ І ЩО ІЗ ЦИМ РОБИТИ [Електронний ресурс]. – Режим доступу: http://nabat.in.ua/novosti/vishing-yak-telefonni-shaxra%D1%97-kradut-nashi-groshi-i-shho-iz-cim-robiti/

2. Що таке фішинг [Електронний ресурс]. – Режим доступу: http://antivirus.pp.ua/fishing_ua.php

Свірський Б.М.,
кандидат юридичних наук, професор,
професор кафедри права та публічного адміністрування,
Маріупольського державного університету

ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

В останні роки збільшується використання у найрізноманітніших сферах життєдіяльності суспільства комп’ютерних і телекомунікаційних технологій, у тому числі інтернет-технологій, що разом з великою кількістю переваг принесло також і чимало загроз.

Конституція України (ч.1 ст. 17) визначає: захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. [1]

Реалізація цих загроз може завдати значної шкоди як на мікро -, так і на макрорівні в межах суверенних держав, а також і в світовому масштабі. Це призвело до розуміння необхідності вирішення комплексу проблем нейтралізації або мінімізації цієї нової сукупності загроз, у тому числі за допомогою такого інструментарію, як вдосконалення кримінально-правових

норм, що регулюють спектр відносин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку.

Розвиток методів обробки інформації за допомогою комп'ютерів призвів до застосування цих машин в усіх галузях національної економіки та інших сферах суспільного життя. Значна кількість таких машин об'єднана комп'ютерними мережами, деякі з них набули інтернаціонального характеру. За цих умов виникли і набули суспільної небезпеки різні діяння, що заподіюють шкоду нормальній роботі комп'ютерів та комп'ютерних мереж.

Важливим і своєчасним було прийняття 5 жовтня 2017 року парламентом - закону України «Про основні засади забезпечення кібербезпеки України» (далі Закон).[2]

Предметом закону є правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Вперше на законодавчому рівні визначаються основні терміни, що стосуються предмету регулювання у цьому Законі, такі як: кібератака; кібербезпека; кіберзагроза; кіберзахист, кібероборона, кібертероризм тощо.

Разом з тим, шляхи до вдосконалення вищезазначенного інституту були зроблені ще у 2014-2015 роках, коли законодавець вніс зміни до розділу XVI КК, але вони були більш косметичними та апріорі не могли відреагувати на Закон, який був прийнятий у 2017році.[3]

Системний аналіз понятійного апарату Закону дає підстави стверджувати про необхідність розширення переліку статей розділу з метою реалізації вимог Закону та приведення їх до відповідності чинного законодавства.

Так, на думку автора, розділ XVI КК необхідно розширити низкою нових кримінально-правових норм різного спрямування, а саме: доповнити розділ статтями які дають: а) визначення поняття *кіберзлочин* (за аналогом ст. 364 КК); б) визначити такий склад злочину як *кібертероризм* та встановити кримінальну відповідальність; в) визначити такий склад злочину як *кібершпигунство* та встановити кримінальну відповідальність; г) визначити такий склад злочину як *кібершатака* та встановити кримінальну відповідальність.

Наприклад, відповідно до ст. 2 Закону до Кримінального Кодексу України необхідно внести поняття (а також сконструювати нові склади злочинів) у наступній редакції:

Кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням, а також передача або збирання за допомого засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології,

програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю.

Кібертероризм – терористична діяльність, тобто діяльність, що здійснюється у кіберпросторі або з його використанням із закликами застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини, або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою.

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

Таким чином, в Україні в останні часи створюються необхідні правові умови щодо протистояння можливим загрозам безпекового використання електронно-обчислювальних машин (комп'ютерів).

Список використаних джерел

1. Конституція України від 28.06.1996р // Відомості Верховної Ради України (ВВР), 1996 № 30 ст. 141

2. «Про основні засади забезпечення кібербезпеки України» Закон України від 05.10.2017р //Відомості Верховної Ради України (ВВР), 2017 № 45 ст. 403

3. Кримінальний кодекс України. Закон України від 05.04..2001р //Відомості Верховної Ради України (ВВР), 2001 № 25-26 ст. 131

Хараберюш І.Ф.,
доктор юридичних наук, професор,
професор кафедри права
та публічного адміністрування
Маріупольського державного університету

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОКРЕМОЇ ОРГАНІЗАЦІЇ

Однією з визначних ознак сучасного світового соціального прогресу є зростання значимості інформації в суспільних відносинах. Суспільні інформаційні відносини постійно розвиваються, особливо з удосконаленням техніки та технологій збирання, обробки, зберігання та передавання інформації. Поряд із позитивними здобутками в інформаційному суспільстві виникли соціальні проблеми щодо забезпечення інформаційної безпеки.

На основі проведених досліджень Фурашевим В.М. сутності понять «кіберпростір» та «інформаційний простір» встановлено, що:

- кіберпростір є невід'ємною складовою інформаційного простору;

- поняття «кібербезпека» та «інформаційна безпека» є тотожними за своєю сутністю. Застосування будь-якого з цих понять не змінює сутності процесу або явища, лише може внести термінологічну плутанину. Тому краще застосовувати поняття «кібербезпека» як термін, що більш чітко відображає сутність процесу, явища [1, с. 168]. Але, ми вважаємо, коректнішим буде вживання терміну «інформаційна безпека» як поняття більш загального і ширшого за кібербезпеку.

Для забезпечення інформаційної безпеки перспективним вважається системний підхід, заснований на інтеграції різних підсистем зв'язку, підсистем забезпечення безпеки в єдину систему із загальними технічними засобами, каналами зв'язку, програмним забезпеченням і базами даних. Застосування системного підходу пов'язане з рішенням ряду складних різнопланових окремих завдань у їх тісному взаємозв'язку: обмеження доступу до інформації; технічного й криптографічного захисту інформації; обмеження рівнів паразитних випромінювань технічних засобів; технічної захищеності об'єктів; охорони й оснащення їх охоронною сигналізацією.

Необхідною умовою реалізації системного підходу є блокування всіх технічних каналів витоку й несанкціонованого доступу до інформації, тому для створення ефективних систем захисту інформації в першу чергу необхідно визначити можливі канали витоку інформації і їх характеристики.

Основними об'єктами інформаційної безпеки (на рівні захисту інформації) організації є:

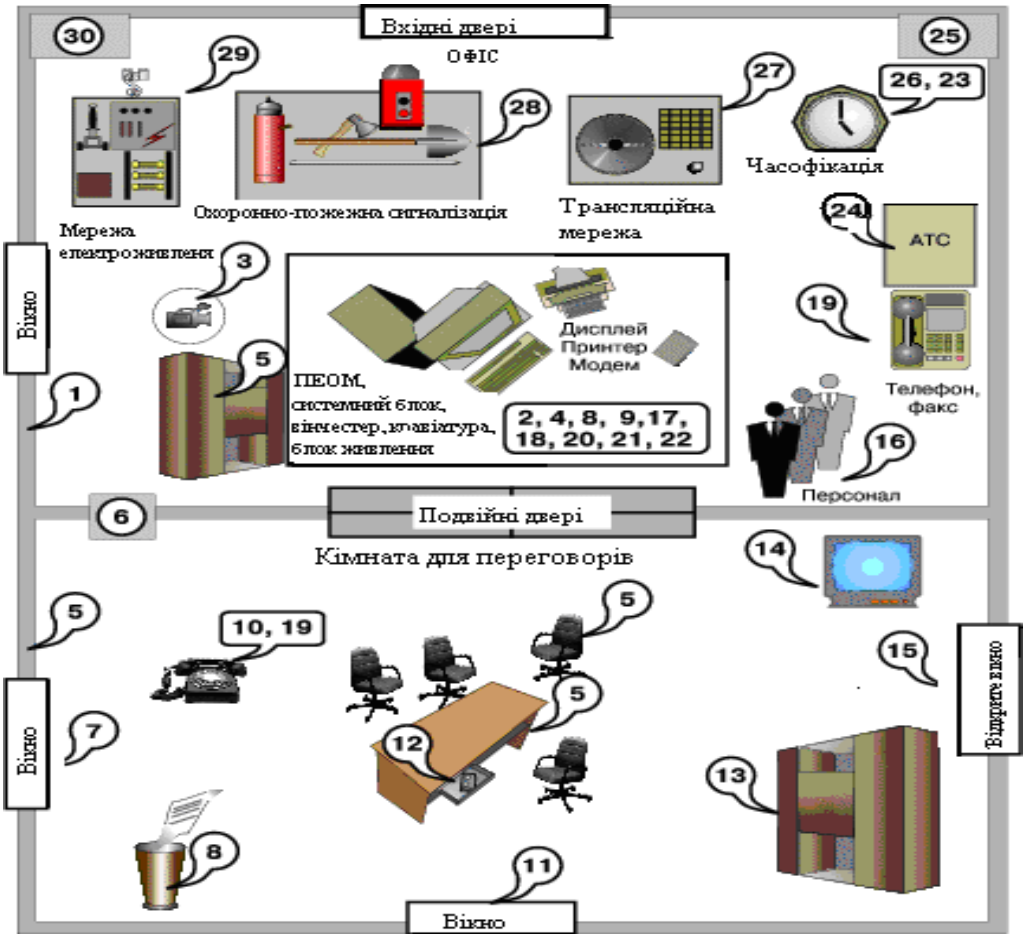
1) інформація з обмеженим доступом;

2) технічні засоби приймання, обробки, зберігання та передання інформації (ТЗПІ), а саме: системи та засоби інформатизації (обчислювальна техніка, інформаційно-обчислювальні комплекси, мережі та системи); програмні засоби;

автоматизовані системи управління; системи зв'язку; технічні засоби отримання, передання та обробки інформація з обмеженим доступом; засоби тиражування і виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації, їх інформативні фізичні поля;

3) допоміжні технічні засоби і системи (ДТЗС), тобто технічні засоби і системи, які не належать до ТЗПІ, але розташовані в приміщеннях, де оброблюється інформація з обмеженим доступом. До них відносять технічні засоби відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, система часофікації, енергопобутові прилади тощо, а також самі приміщення, де циркулює інформація з обмеженим доступом.

На мал.1 наведено узагальнюючу схему можливих каналів витоку і несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі [2].



Мал. 1. Схема каналу витоку і несанкціонованого доступу до інформації в офісі

На малюнку визначені такі канали витоку інформації:

1 - витік за рахунок структурного звуку в стінах і перекриттях; 2 - знімання інформації зі стрічки принтера, погано стертих дискет і т. п.; 3 - знімання

інформації з використанням відеозакладок; 4 - програмно-апаратні закладки в ПЕОМ; 5 - радіо-закладки в стінах і меблях; 6 - знімання інформації з системи вентиляції; 7 - лазерне знімання акустичної інформації з вікон; 8 - виробничі й технологічні відходи; 9 - комп'ютерні віруси, логічні бомби й т. п.; 10 - знімання інформації за рахунок наведень і "нав'язування"; 11 - дистанційне знімання відео інформації (оптика); 12 - знімання акустичної інформації з використанням диктофонів; 13 - розкрадання носіїв інформації; 14 - високочастотний канал витоку в побутовій техніці; 15 - знімання інформації спрямованим мікрофоном; 16 - внутрішні канали витоку інформації (через обслуговуючий персонал); 17 - несанкціоноване копіювання; 18 - витік за рахунок побічного випромінювання термінала; 19 - знімання інформації за рахунок використання «телефонного вуха»; 20 - знімання з клавіатури й принтера акустичним каналом; 21 - знімання з дисплея по електромагнітному каналу; 22 - візуальне знімання з дисплея й принтера; 23 - наведення на лінії комунікацій і сторонні провідники; 24 - витік через лінії зв'язку; 25 - витік мережею заземлення; 26 - витік мережею часофікації; 27 - витік трансляційною мережею й гучномовним зв'язком; 28 - витік охоронно-пожежною сигналізацією; 29 - витік мережею електроживлення; 30 - витік мережею опалення, газо- і водопостачання.

Принцип утворення небезпечних сигналів у технічних засобах полягає в тому, що кожен технічний засіб містить ті чи інші фізичні перетворювачі, функції яких засновані на різних фізичних принципах дії. Лише маючи уявлення про принцип дії кожного з таких перетворювачів, можна виявити неконтрольовані прояви фізичних полів, що утворюють канали витоку.

Захист інформації від витоку технічними каналами забезпечують проектно-архітектурними рішеннями, проведенням *організаційних* і *технічних* заходів, а також виявленням портативних закладних пристроїв.

Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

До основних організаційних заходів відносять:

- залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ);
- категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;
- використання на об'єкті сертифікованих ТЗПІ та ДТЗС;
- встановлення контрольованої зони навколо об'єкта;
- залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;
- організацію контролю та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах використання технічних засобів, що підлягають захисту;

- відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Технічні заходи – це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень. Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал/завада у місцях можливого розміщення технічних засобів розвідки або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.

Таким чином, *захист інформації* організації – це сукупність фізичних, адміністративних, апаратних, програмних, криптографічних засобів, робота яких спрямована на запобігання нанесенню збитків інтересам власника інформації, що досягається атестацією системи комп'ютерної безпеки та застосуванням певних організаційних та правових заходів.

Інформаційна безпека організації досягається комплексним застосуванням фізичних, адміністративних, апаратних, програмних засобів і криптографічних методів захисту, а також організаційних та правових заходів.

Список використаних джерел

1. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. 2012. № 2(5). С. 162-175.

2. Василюк В. Об'єкти захисту інформації. методи та засоби захисту інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2006. № 2(13). С. 88-102.

Крівенко С. В.,
кандидат технічних наук, доцент,
доцент кафедри математичних
методів та системного аналізу
Маріупольського державного університету

УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ WIRELESS SENSOR NETWORK

Концепція розумного міста включає в себе об'єднання різних сучасних технологій і рішень, здатних забезпечити комфорт і зручність отримання послуг, безпеку громадян, раціональне споживання ресурсів, тощо. Це призвело до створення концепції «Інтернет речей», яка все більше набирає популярності [1]. Основою концепції служить мережа фізичних об'єктів, наділених

технологіями, що дозволяють їм взаємодіяти між собою, а також із зовнішнім середовищем. Концепція Інтернет речей передбачає, що будь-який об'єкт, якому може бути присвоєно IP-адресу, і який може передавати дані в мережі, є частиною глобальної мережі. Зокрема, такою «річчю» може бути людина з серцевим імплантатом, датчик тиску в колесі сучасного автомобіля, і багато інших об'єктів.

Інфраструктура розумних міст розвивається швидше, ніж засоби її захисту, що залишає великий простір для діяльності як допитливих дослідників, так і зловмисників. Для побудови подібних систем застосовуються технології автоматичної ідентифікації, вимірювальні прилади, а також засоби комунікації (провідні та безпровідні мережі). Часто в якості засобу комунікації використовуються бездротові мережі, передача інформації в яких здійснюється радіоканалом. Подібна система датчиків, пов'язаних радіоканалом утворює Wireless Sensor Network. Вимога автономності цих систем накладає наступні обмеження: система повинна бути максимально перешкодо- та відмовостійка, надійна, споживати мало енергії, і мати достатню обчислювальну потужність для вирішення поставлених завдань.

Зростає необхідність в належному забезпеченні інформаційної безпеки таких систем. Можливі загрози полягають у несанкціонованому доступі до потокам даних, їх блокуванню або зміні. При здійсненні будь-якої з цих загроз можуть виникнути небезпечні або критичні ситуації.

З цього випливає необхідність застосування криптографічного захисту даних. В силу обмежень в якості бази найбільш часто застосовуються мікроконтролери, побудовані на архітектурі RISC і платформою AVR (мале енергоспоживання, невелика потужність, малий розмір пам'яті) [2].

Для написання програм для мікроконтролерів AVR поширене використання двох мов: Assembler й C/C++. Багато вільно поширюваних криптографічних бібліотек реалізованих на мові C/C++. Що дає можливість використовувати такі алгоритми:

• Симетричні алгоритми шифрування даних, що передаються (AES, 3DES)

• Асиметричні алгоритми шифрування (ECC)

• Обчислення контрольної суми (CRC)

• Використання криптографічних хеш-функцій, а також їх комбінації.

Для спрощення та оптимізації криптографічних засобів захисту інформації, реалізованих на платформі AVR XMEGA, компанія Atmel апаратно реалізувала деякі захисні алгоритми:

• Симетричні алгоритми шифрування AES і 3DES

• Контрольні суми CRC-16 і CRC-32

• Найбільш популярним алгоритмом асиметричного шифрування зараз є криптографічний алгоритм RSA, заснований на складності розкладання великих чисел на множники.

• Також набирають популярності алгоритми, засновані на еліптичних кривих, що дають аналогічну RSA криптостійкість при меншій довжині ключа.

Основні передумови для використання еліптичної криптографії на пристроях малої потужності:

• Менша кількість обчислень, довжина ключів і кількість споживаного обсягу пам'яті при тій же криптостійкісті, що і у звичайних асиметричних криптографічних алгоритмів (RSA)

• Менше енергоспоживання в порівнянні з симетричними алгоритмами

• Більш швидка робота алгоритмів у порівнянні з RSA

У цій роботі були розглянуті три криптографічні бібліотеки: TinyECC, Micro-ECC, Relic-Toolkit. Остання бібліотека є найповнішою з підтримуваних на мікроконтролерах архітектури AVR, і була обрана для побудови захищеного каналу зв'язку.

Висновки. Використання тільки симетричною криптографії веде до необхідності організації захищеного каналу зв'язку для передачі ключів шифрування, однак не завжди існує можливість організувати цей канал.

Алгоритми, засновані на протоколі Діффі-Хеллмана, знімають необхідність організації захищеного каналу, однак, в силу своєї вразливості до неодноразово згадуваної атаки «зловмисник посередині», вимагають додаткових заходів безпеки, аутентифікації за допомогою цифрового підпису при обміні відкритими частинами ключів.

Використання алгоритму генерації ключів ECDH в поєднанні з цифровим підписом може бути виправдане в силу його більш високої надійності щодо звичайного протоколу Діффі-Хеллмана, а також у зв'язку з тим фактом, що генерація ключа необхідна не при кожному обміні даними, а тільки через певні проміжки часу. У швидкості ж шифрування/розшифрування алгоритм AES зі згенерованим ключем не поступається звичайному алгоритму AES.

Список використаних джерел

1. Wireless Sensor Networks. Technology and Protocols // Edited by Mohammad Abdul Matin. - North South University, Bangladesh.- 2012. - 308 p. DOI: 10.5772/49376

2. Евстифеев А.В. Микроконтроллеры AVR семейств Tiny и Mega фирмы ATMEL // А.В. Евстифеев А.В.-М.: Издательский дом «Додэка_XXI».- 2008. - 560с.

Дяченко О. Ф.
старший викладач кафедри математичних методів та системного аналізу Маріупольського державного університету

АКТУАЛЬНІСТЬ ВДОСКОНАЛЕННЯ ПРОЦЕСУ ПІДГОТОВКИ БАКАЛАВРІВ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА

Стан підготовки бакалаврів з кібербезпеки повинен відповідати тому рівню загроз інформаційної безпеки, який існує зараз у світі. Вітчизняні експерти сходяться на думці, що для поліпшення ситуації в цій сфері необхідно

своєчасно оновлювати та корегувати програми підготовки у ЗВО.

Професійна компетентність бакалаврів з кібербезпеки забезпечує новий вид професійних компетентностей – здатність аналізувати мережеві трафіки, роботу засобів виявлення вторгнення; вміння виявляти і знищувати комп'ютерні віруси; працювати з нормативними правовими актами; володіти та використовувати методи і засоби вияву загроз безпеки автоматизованими системами, забезпечення конфіденційності; формувати вимоги до захисту інформації; здійснювати розрахунки та інструментальний контроль за показниками технічного захисту інформації; володіти методами аналізу і формалізації інформаційних процесів об'єктів і зв'язків між ними та ін.

Аналізуючи навчальні плани спеціальності 125 Кібербезпека можна виділити дві групи дисциплін: дисципліни, що формують технічні знання і аналітичні вміння, і дисципліни, що формують комп'ютерні знання і вміння. Навчальний процес з дисциплін, що формує технічні знання і аналітичні вміння, спрямований на формування знань видів систем, їх структури, організації функціонування, методів і засобів проектування цих систем і дослідження їх якості. Навчальний процес з комп'ютерних дисциплін спрямований на формування знань про засоби і методи розробки інформаційних і програмних продуктів, інформаційних технологій і комп'ютерних систем. На наш погляд, підготовка бакалаврів з кібербезпеки повинна передбачати реалізацію таких завдань: аналіз змісту комп'ютерних та технічних дисциплін з позицій їх можливостей у формуванні знань і умінь із забезпечення фахової компетентності. Що дозволяє зробити висновки, що математична підготовка є фундаментом для більшості професійно-орієнтованих дисципліни. Оскільки математичні знання виконують роль методологічної основи наукового знання та базової складової більшості профілюючих дисциплін. Математичні дисципліни вивчаються студентами цієї спеціальності на першому та другому курсах.

Визначимо, які конкретно знання та вміння з математичних дисциплін необхідні під час вивчення дисциплін циклу професійної підготовки. Так, вивчаючи дисципліни «Теорія інформації та кодування», «Основи криптографічного захисту інформації», «Комплексні системи захисту інформації» для вдалого шифрування даних студент повинен знати алгебру висловлень та алгебру множин, вміти виконувати дії над множинами, знати поняття однозначного відображення, оберненого відображення, сюр'єктивного та ін'єктивного відображення, знати малу теорему Ферма та теорему Ейлера, вміти розв'язувати конгруенції, створювати та аналізувати розподіли випадкових величин, тощо.

У дисципліні «Теорії ризиків» для виконання моделювання ризику використовуються знання з «Теорії ймовірностей» та «Математичних методів і моделей», зокрема використовують лінійне та стохастичне програмування, теорію ігор; теорію нечітких множин та ін.

Дисципліна «Теорія кіл, сигналів і процесів у системах технічного захисту

інформації» базується на знаннях лінійної та векторної алгебри, диференціального числення та його застосування, інтегрального числення та його застосування, рядів, диференціальних рівнянь. Для більш глибоко вивчення цієї фахової дисципліни необхідні також знання з теорії функцій комплексної змінної, рядів Фур'є й розклад функцій за ортогональними базисами [2].

Інтеграція математичних та профільних дисциплін виступає чинником забезпечення освітніх вимог до професійної підготовки бакалаврів з кібербезпеки та сприяє подоланню головного недоліку та парадоксу сучасної освітньої системи – засвоєнню зростаючого об'єму знань за обмежений час навчання.

Список використаних джерел

1. Прошкін В.В. Зміст інтеграції університетської науки та освіти / В.В. Прошкін // Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія «Педагогіка і психологія». Педагогічні науки, 2014. – № 2 (8). – С. 108-114.

2. Шевченко С.М. Математичні компетенції майбутніх фахівців інформаційної безпеки / С.М. Шевченко, Ю.Д. Жданова // Сучасний захист інформації. – 2016. – №4. – С. 90-96.

Морозова А. О.,
асистент кафедри математичних методів та системного аналізу Маріупольського державного університету

ОСНОВНІ МЕТОДИ ШИФРУВАННЯ ІНФОРМАЦІЇ У СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ

Шифрування – це кодування даних з метою захисту від несанкціонованого доступу. Процес кодування називається шифруванням, а процес декодування – розшифруванням. Саме кодоване повідомлення називається шифрованим, а застосований метод називається шифром.

Основна вимога до шифру полягає в тому, щоб розшифрування (і, можливо, шифрування) були можливі тільки за наявності санкцій, тобто деякої додаткової інформації (або пристрою), яка називається ключем шифру. Процес декодування шифровки без ключа називається дешифруванням.

Галузь знань про шифри, методи їх побудови та розкриття називається криптографією. Властивість шифру протистояти розкриттю називається криптостійкістю або надійністю і, зазвичай, визначається складністю алгоритму дешифровки.

У практичній криптографії криптостійкість шифру оцінюється з економічних міркувань. Якщо розкриття шифру коштує (в грошовому еквіваленті, включаючи необхідні комп'ютерні ресурси, спеціальні пристрої тощо) більше за саму зашифровану інформацію, то шифр вважається достатньо надійним [1].

Симетричні криптосистеми (симетричне шифрування) – спосіб шифрування, в якому для шифрування та дешифрування використовується один й той же криптографічний ключ.

Ключ шифрування має зберігатись у секреті обома сторонами та має бути обраним до початку обміну повідомленнями. Процес розшифрування заключається в тому, щоб ще раз скласти шифровану послідовність з тією самою гамою шифру:

Описаний метод має суттєвий недолік. Якщо відома хоча б частина висхідного повідомлення, то все повідомлення може бути легко дешифроване.

Більшість симетричних шифрів використовують складну комбінацію великої кількості підстановок та перестановок. Багато таких шифрів виконуються у декілька (до 100) проходів, використовуючи на кожному проході ключ проходу. Множина «ключів проходів» для всіх проходів називається розкладом ключів. Зазвичай, він утворюється з ключа шляхом виконання над ним певних операцій, у тому числі перестановок та підстановок.

Найважливішими параметрами усіх алгоритмів симетричного шифрування є:

• стійкість;
• довжина ключа;
• кількість раундів;
• довжина блоку, якій оброблюється;
• складність апаратно/програмної реалізації;
• складність перетворень.

До переваг симетричної системи можна віднести:

• порівняно високу швидкість (приблизно на 3 порядки вищу ніж у асиметричних систем);
• простота реалізації (за рахунок більш простих операцій);
• менша необхідна довжина ключа для відповідної стійкості;

Але є також суттєві недоліки, які практично призводять до того, що ця система майже не використовується на сьогодні .

• складність керування ключами у великій мережі. Це означає квадратичне збільшення кількості ключів, які необхідно генерувати, зберігати, передавати та знищувати у мережі. Для мережі з 10 абонентів потрібно 45 ключів, для 100 – вже 4950, для 1000 – 499500;

• складність обміну ключами. Для застосування симетричної системи необхідно вирішити проблему надійної передачі ключів кожному абоненту, тому що необхідний секретний канал для передачі кожного ключа обом сторонам [2].

Криптографічна система з відкритим ключем (або асиметрична криптосистема, асиметричне шифрування) – це система шифрування, при якій відкритий ключ передається відкритим (тобто незахищеним) каналом зв'язку та використовується для шифрування повідомлень. Для розшифрування повідомлень використовується секретний (або приватний) ключ.

Наявність двох ключів – відкритого та закритого – й робить цю систему асиметричною. Відкритий ключ розсилається усім, хто бажає відправляти повідомлення адресату, а приватний ключ зберігається адресатом і не повинен нікому відправлятись. Навіть якщо знати відкритий ключ та все відправлене розшифроване повідомлення, неможливо знайти приватний ключ.

До переваг асиметричної криптосистеми можна віднести:

• не потрібно передавати закритий ключ будь-якими каналами зв'язку;

• на противагу симетричній криптосистемі, секретний ключ зберігається тільки у однієї сторони;

• у симетричній криптосистемі варто змінювати ключ після кожного сеансу передачі даних, у асиметричній ключі можна тримати незміненими достатньо довгий час;

• у більшості мереж кількість ключів при асиметричному шифруванні набагато менша, ніж при симетричному.

Недоліки:

• хоча повідомлення шифруються надійно, але самі сторони «засвічуються» самим фактом передачі (на чому може бути побудована атака);

• асиметричні алгоритми використовують набагато довші ключі, ніж симетричні;

• у чистому вигляді асиметричні системи вимагають значних обчислювальних ресурсів, тому на практиці вони частіше використовуються разом з іншими алгоритмами [3].

Список використаних джерел

1. Тема 23. Шифрування [Електронний ресурс] / http://oim.asu.kpi.ua/ – Режим доступу до ресурсу: http://oim.asu.kpi.ua/files/DM/23_Cryptography.pdf.

2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – Санкт-Петербург: БХВПетербург, 2009 – 576 с.

3. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. – М.: Аст, Астрель, 2006 – 447 с.

Toliupa S.,
Doctor of Engineering Science, Professor
Nakonechnyi V., Romanova A.
Taras Shevchenko National University of Kyiv

STEGANOGRAPHY AND CIBERNETIC SPACE

Cryptography is doubtlessly one of the most effective, developed and approbated methods to be used when it comes to the protection of information resources. Nevertheless, it might be more effective to hide the communication channel itself instead of making unreadable the information within it. The practice of concealing data within text- or media-file is called *steganography* and has its roots deep in the history of the humankind.

A considerable number of steganographic methods are well-known and implemented in various steganosystems and applications. There are some methods of information concealment, though, that receive the attention not so much. The reasons of such lack of popularity can differ depending on specific solutions: their complexity for one, low cost-effectiveness of their realization for another. In any instance, they are either poorly described or are not widely used regardless of their perspectiveness.

The purpose of this article is to conduct an analysis and suggest possible practical use of steganographic solutions that are known and can be applied to a variety of information security systems, and yet lack either theoretical basis or practical application.

Below, we present an analysis and suggest possible practical use of steganographic solutions that are known and can be applied to a variety of information security systems, and yet lack either theoretical basis or practical application.

Classification of steganographic methods

By the method of selecting a container one can distinguish non-alternative, selective and constructive methods of steganography.

Non-alternative methods imply the choice of the first possible container made in order to conceal a message. Selective methods imply that a covert message has to reproduce special statistical characteristics of the container noise. In constructive methods a container is generated by the steganosystem itself.

By the way of access to the secret information there are methods for stream and fixed containers.

By the type of organization there are methods for systematic and non-systematic containers. In the first ones bits of noise and of the container itself can be distinguished. In the latter ones they are impossible to specify.

By the concealment principle there are two main classes: methods of direct substitution and spectral methods. The first use container redundancy and replace the insignificant areas of the container with the bits of a secret message, while the second hide the data using the spectral representation of the elements in the environment where the concealed data is embedded (for example, coefficients of the arrays of Fourier transforms).

By purpose one can distinguish the methods for the data secret transmission or storage and methods for concealing data in digital objects in terms of copyright protection.

A special group is represented by methods that use characteristic file format properties:

- Reserved fields, which are usually filled with zeros and are not taken into account by the program;
- Special data formatting (the shift of words, sentences, paragraphs or selecting specific positions of characters);
- Erasing file identifier captions etc.

Internet of Things and cyber-physical systems

A cyber-physical system is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. Examples of CPS are autonomous automobile systems, medical monitoring, smart grids, automatic pilot avionics etc.

The Internet of Things (IoT) is the network of physical devices, vehicles and other items embedded with electronics, sensors, software and network connectivity, which enable them to collect and exchange data. It is more or less an instance of a class of cyber-physical systems.

The network steganography uses communication protocols' control elements and their functionality to hide information inside. The modifications can be carried out either over a single network protocol (applied to the Protocol Data Unit, the time relations between PDUs or both) or to several protocols at the same time (inter-protocol steganography). Such network steganography methods can be applied to the systems mentioned above, too. The IoT is believed to be a phenomenon that will expand its influence greatly within the next few years. What is more, as the items within the IoT possess a vast variety of sensors and software, they can be used to conceal data in [1].

A variety of steganographic solutions was analyzed. Among them such methods were selected that are not either widely used in software applications or lack attention in general. Nevertheless, their perspective usage was discussed. Taking into account all the fact mentioned above, the next directions of development of steganography are suggested:

- Steganography in cyber-physical systems and the Internet of Things in particular;
- The use of stream containers;
- Semantic and syntactic methods;
- Some enhancement in steganoanalysis technics;
- Biochemical steganography practical application.

Information is surely becoming an asset of the highest value. Seeing as the cyberspace is more of a battlefield for different forces continuously confronting each other, it is obvious that information security sphere requires the best solutions possible. Steganography has proven to be an effective means of secret data concealment ensured with centuries of practical use. And, just as any other science, it is in the state of constant development. Being aware of perspective ways to use its methods for our cause, we get access to numerous up-to-date possibilities of providing information security of the highest level.

LITERATURE

1. Serghii Toliupa, Anna Romanova Perspective steganographic solutions and their application // Proceedings of the VII Inter University Conference "Engineerof XXI Century" at the University of Bielsko-Biała (ATH), December 08,2017, Bielsko-Biała, Poland. Volume 2. – P. 269-278.

2. Konakhovich G. F., Puzyrenko A. YU.: Computer steganography. Theory and practice with Mathcad (Rus). MK-Press Kyiv, Ukraine 2006.

3. Aditit Sharma: Security and Information Hiding based on DNA Steganography. International Journal of Computer Science and Mobile Computing, Vol. 5, March 2016: *www.ijcsmc.com*.

Зал К.,
студент ОС «Бакалавр» спеціальності «Системний аналіз»,
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

КОНЦЕПЦІЯ РОЗУМНОГО МІСТА

Ідеї, що послужили основою для виникнення концепції «розумного міста», з'явилися ще в 1960-1970-х рр., однак їх практичне застосування почалося з 1990-х рр. У цей період у змісті концепції «розумне місто» акцентувалася саме роль ІКТ, і пріоритет в управлінні розвитком міського простору мала держава, а населенню відводилася пасивна роль. Сучасне «розумне місто» починає включати в себе не тільки інфраструктурний розвиток простору на основі ІКТ, але і відкриту взаємодію влади, бізнес-структур та населення. Мета таких заходів – поліпшити життя людей за допомогою підвищення рівня комфорту і безпеки, якості та ефективності обслуговування в різних сферах, оптимізації витрат на ряд високо експлуатованих ресурсів.

На сьогоднішній день Smart City включає в себе наступні ключові складові:

-Smart Energy: передбачає ряд рішень, що застосовуються в галузях енергопостачання та енергозбереження;

-Smart Water: передбачає управління водними ресурсами (модернізація водних систем, моніторинг споживання води за секторами, системи екологічної безпеки та контролю повеней);

-Smart Buildings: передбачає створення або облаштування окремих будівель, які акумулюють в собі всі інженерні та інформаційні системи і інтегруються в єдину систему управління (BMS – building management system).

-Smart Transportation: передбачає створення системи інтелектуальних транспортних і логістичних систем, які забезпечують моніторинг і управління трафіком, дозволяють контролювати оплату дорожніх зборів, реагувати надзвичайні ситуації, керувати світлофорами.

-Smart Government: передбачає застосування інформаційних технологій для надання державних послуг широкому колу осіб і дозволяє оптимізувати роботи різних департаментів.

Загальні рекомендації щодо впровадження систем Smart City:

- залучення громадян та інших зацікавлених сторін у вигляді державних, громадських і бізнес інституцій;
- виключення ізольованих і застарілих рішень на користь застосування і розробки нових передових автоматизованих систем;

- заохочення ініціативних груп і організацій, які виступають в ролі розробників інноваційних моделей функціонування сучасного міста;
- створення всеосяжної стратегії даних і платформ даних для реалізації проектів у даному напрямку;
- створення інноваційних лабораторій для стимулювання нових розробок, спрямованих на збереження екосистеми та підвищення рівня комфорту і безпеки громадян;
- забезпечення безпеки даних;
- залучення представників міської інфраструктури до розробки, фінансування та реалізації ініціатив, спрямованих на впровадження систем «розумного міста»;

У загальному розумінні це система, яка дозволяє якнайефективніше використовувати існуючі ресурси міських служб і забезпечувати максимальну безпеку міського життя. Таке місто постійно нарощує число та якість надаваних населенню послуг, забезпечуючи стійке середовище, яке сприяє підвищенню комфорту та якості життя. Із позиції публічного управління, розумне місто – це керована комплексна та багатофакторна муніципальна система, що вміщує у себе зазначені складові та вписує їх у контекст сталого розвитку. Метою розвитку цієї системи є забезпечення підвищеного комфорту міського життя та безпеки навколишнього середовища – ключової вимоги, що завжди визначатиме зміст критерію «розумності» в управлінні містом.

Список використаних джерел

1. Бойкова М. В. Будущее городов. Города как агенты глобализации и инноваций / М. В. Бойкова, И. Н. Ильина, М. Г. Салазкин. – 2011. – Режим доступа : https://cyberleninka.ru/article/n/buduschee-gorodov-goroda-kak-agenty-globalizatsiii-innovatsiy.

2. Воронкова В. Людина в освітньому просторі smart-суспільства / В. Воронкова, О. Кивлюк // Interdisciplinary studies of complex systems. – 2017. – № 10-11. – С. 88-95.

3. Жукович І. А. Smart-міста як новий об’єкт статистичних досліджень: визначення терміна / І. А. Жукович // Статистика України. – 2015. – № 1. – С. 18-22.

4. Концепція Київ Смарт Сіті 2020. – Режим доступу: https://www.kyivsmartcity.com/concept.

5. Кунанець Н. Е. Особливості формування цілей соціальних та соціо-комунікаційних складових у проектах «розумних міст» / Н. Е. Кунанець, Р. М. Небесний, О. В. Мацюк // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. – 2016. – № 854. – С. 257-274.

6. Смарт-сіті чи електронне місто: сучасні підходи до розуміння впровадження е-урядування на місцевому рівні / С. А. Чукут, В. І. Дмитренко // Інвестиції: практика та досвід. – 2016. – № 13. – С. 89- 93.

Захарова Г.,
студентка ОС «Бакалавр»
спеціальності «Системний аналіз»
Науковий керівник Дяченко О.Ф.
Маріупольський державний університет

ПРИНЦИП РОБОТИ VPN

З кожним роком електронний зв'язок вдосконалюється, і до інформаційного обміну пред'являються все більш високі вимоги швидкості, захищеності та якості обробки даних.

І в цій доповіді ми розглянемо VPN -підключення: що це таке, його переваги та недоліки, способи використання VPN -з'єднання.

Отже, віртуальна приватна мережа VPN – це технологія, що забезпечує захищений (закритий від зовнішнього доступу) зв'язок логічної мережі поверх приватної або публічної при наявності високошвидкісного Інтернету. Таке мережне з'єднання комп'ютерів (географічно віддалених один від одного на солідну відстань) використовує з'єднання типу «точка – точка». Науково такий спосіб з'єднання називається VPN-тунель (або тунельний протокол). Підключитися до такого тунелю можна за наявності комп'ютера з будь-якою операційною системою, в яку інтегровано VPN-клієнт, здатний робити «стрнибок» віртуальних портів з використанням протоколу TCP/IP в іншу мережу.

VPN -з'єднання необхідно для:

- анонімної роботи в мережі інтернет;
- завантаження додатків, в разі, коли IP адреса розташована в іншій регіональній зоні країни;
- безпечної роботи в корпоративному середовищі з використанням комунікацій;
- простоти і зручності налаштування підключення;
- забезпечення високої швидкості з'єднання без обривів;
- створення захищеного каналу без хакерських атак;

Коли відбувається підключення через VPN, в заголовку повідомлення передається інформація про IP адресу VPN-сервера і віддалений маршрут. Інкапсульовані дані, що проходять загальною або публічною мережею, неможливо перехопити, оскільки уся інформація зашифрована. Етап VPN-шифрування реалізується на стороні відправника, а розшифровуються дані у одержувача по заголовку повідомлення за наявності загального ключа шифрування. Після правильної дешифровки повідомлення між двома мережами встановлюється з'єднання, яке дозволяє також працювати в публічній мережі (наприклад, обмінюватися даними з клієнтом 93.88.190.5). Що стосується інформаційної безпеки, то Інтернет є вкрай незахищеною мережею, а мережа

VPN з протоколами OpenVPN, L2TP /IPSec ,PPTP, PPPoE – цілком захищеним і безпечним способом передачі даних.

Дуже важливо зрозуміти, що зв'язок виду «точка-точка» дає можливість кожному з'єднанню функціонувати таким чином, щоб усі контакти були в однині і їх складно було отримати третім особам. Цікаво, що ключі, які використовуються для шифрування, через певний час змінюються, а це заважає зламати дані користувача і почати їх використовувати в своїх цілях. Є ще одна перевага, яка полягає в тому, що окремий користувач або декілька таких користувачів можуть захищено користуватися інтернетом, і в тому, щоб цілими офісами і компаніями виходити у світовий інтернет з захищеними «тилами». Наприклад, якщо в окремо взятій компанії є власна DSL адреса, то краще використовувати VPN, а не користуватися Інтернетом за допомогою ISDN BRI-з'єднання.

Основними недоліками цих мереж є налаштування, їх впровадження і, звичайно ж, підтримка. У більшості випадків використання VPN мереж має на увазі використання досить потужних систем шифрування, зокрема-3DES. Крім цього, для того, щоб використовувати подібні технології, необхідно мати періоди зміни шифрувальних ключів, щоб зберігати безпеку особистих даних на високому рівні.

Список використаних джерел

1. Салливан К. Прогресс технологии VPN. PCWEEK/RE, – М.: №2, 1999;

2. Інформаційний портал: htmlka.com : [Електронний ресурс]. – Режим доступу : − http://htmlka.com/preimushchestva-i-nedostatki-vpn/

3. Інформаційний портал: tvoi-setevichok.ru : [Електронний ресурс]. – Режим доступу : https://tvoi-setevichok.ru/korporativnaya-set/vpn-podklyuchenie-chto-eto-takoe-i-dlya-chego-nuzhen-vpn-kanal.html#_vpn

Какацій Р.,
ОС «Бакалавр»
спеціальності «Кібербезпека»
науковий керівник Кривенко С.В.
Маріупольський державний університет

АНАЛІЗ РИЗИКІВ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ

У зв'язку зі стрімким розвитком технологічних процесів, що відбуваються в нашому суспільстві, актуальність і важливість систем захисту інформації будь-якої компанії вже зараз не викликає сумнівів. Їх впровадження істотно зменшує ризики кібернетичних та фінансових втрат. Використання системи захисту є найголовнішою складовою в забезпеченні безпроблемної виробничої діяльності усіх підрозділів підприємства, що позначається на його прибутковості та розвитку.

Поява локальних і глобальних мереж надала користувачам нові можливості використання інформаційних потоків даних, що посилило необхідність створення належної системи інформаційної безпеки.

Для будь-якого підприємства ведення своєї діяльності, наприклад, створення і впровадження проектів, використання територіально віддалених одна від одної філій, оперативне поширення інформаційних ресурсів серед співробітників і партнерів, неможливе без високопродуктивної та надійної корпоративної мережі.

Наприкінці 80-х років постало питання про проблему захисту мережі в плані фізичної вразливості, коли вважалося, що головні втрати і беззахисність корпоративної мережі полягають в проблемі зсередини. Рішенням було використання організаційних заходів захисту з метою недопущення сторонніх осіб до активів організації. А вже до середини 90-х з'явилася ще й зовнішня небезпека для системи вже з боку мережі Інтернет.

Метою роботи є аналіз основних можливостей використання корпоративної мережі на підприємстві, оцінка можливих ризиків інформаційної безпеки корпоративної мережі і їх наслідки, а також вивчення початкових робіт при створенні власної мережі компанії. Оцінювання ризиків в цій роботі полягає у визначенні характеристик ризиків корпоративної інформаційної системи та її ресурсів.

Корпоративна мережа – це комунікаційна система, що належить та/або керується єдиною організацією відповідно до правил цієї організації.

Використання корпоративної мережі дозволяє організувати ряд дуже важливих можливостей, таких як єдиний електронний документообіг; зберігання загальних архівів документів компанії; дистанційний режим доступу до файлів, серверів з базами даних; забезпечення централізованого доступу користувачів до мережі Інтернет. Використання цих технологій дуже полегшує розвиток внутрішніх процесів компанії, а також дає організації незаперечні переваги перед конкурентами: оперативний контроль діяльності усіх структурних підрозділів; оперативна і своєчасна реакція на зміни в роботі підприємства; доступ до всіх інформаційних резервів в реальному часі.

Вирішуючи проблему безпеки корпоративної мережі, необхідно розглядати всі характеристики системи в сукупності, щоб прийти до єдиного правильного рішення побудови найбільш безпечної та вигідної системи захисту інформації, яка визначає ризик витоку інформації з корпоративної мережі і наслідки її несанкціонованого використання, використовуючи при цьому аналіз ризиків.

Інформаційні ризики тісно пов'язані з будь-якими діями по відношенню до інформації: створення, зберігання, оброблення, передавання та використання. Тому виникла потреба в аналізі ризиків інформаційної безпеки, що дозволяє визначити можливі і вже існуючі загрози безпеки, їх рівень ймовірності нанесення збитків компанії, якими засобами і маніпуляціями мінімізувати до прийнятного рівня надмірно небезпечні події проти системи.

Аналіз ризиків корпоративної мережі відбувається в кілька етапів:

1. оцінка ймовірності реалізації загрози – можливі загрози, які становлять небезпеку для функціонування мережі.

2. оцінка важливості ризику – розраховується економічна доцільність проведення заходів щодо мінімізації заподіяної шкоди.

3. формування звіту з уразливими місцями мережі, існуючими і майбутніми загрозами і список контрзаходів щодо захисту системи – нейтралізація виявлених загроз або проведення профілактичних заходів.

На сьогодні існує безліч різних систем, для яких дуже складно підібрати правильну і стовідсотково безпечну методику оцінки ризиків. Тому для побудови ефективної системи захисту корпоративної мережі необхідно використовувати комплексний підхід на основі існуючих методик і розглянути три важливі складові: економічну вартість, продуктивність і безпеку.

Список використаних джерел

1. Гарасим Ю.Р. Структура технологій функціонування систем захисту інформаціїкорпоративних мереж зв'язку / Ю.Р. Гарасим, В.Б. Дудикевич // матер. IV Міжнар. наук.-практ.конф. "Спеціальна техніка у правоохоронній діяльності". – К., 2009. – С. 226–228.

2. Draft,E. Authentication Policy for Federal Agencies / E. Draft. – Federal Register. – 2003. – Vol. 68 (No. 133).

3. Гарасим Ю.Р. Інформаційна безпека захищених корпоративних мереж зв'язку / Ю.Р. Гарасим,В.Б. Дудикевич // Вісник Національного університету "Львівська політехніка" "Автоматика,вимірювання та керування". – 2009. – № (639). – С. 124–132. 4

Конєва О.,
ОС «Бакалавр»
спеціальності «Системний аналіз»
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ IoT

Internet of Things (IoT) – це глобальна мережа підключених до Інтернету фізичних пристроїв – «речей», оснащених сенсорами, датчиками і пристроями передачі інформації. Ці пристрої об'єднані за допомогою підключення до центрів контролю, управління і обробки інформації.

Основні складові IoT технології – це міжмашинна взаємодія (Machine-to-Machine, M2M), вона дозволяє машинам обмінюватися інформацією або ж передавати її в односторонньому порядку. Це можуть бути провідні і бездротові системи моніторингу датчиків або будь-яких параметрів пристроїв.

IoT з кожним роком набирає все більшої популярності. Розвиток концепції Інтернету речей та її впровадження в різні сфери передбачає наявність десятків

мільярдів автономних пристроїв. За даними Ericsson Mobility Report сьогодні в світі налічується більше 16 млрд підключених пристроїв. Однак зі зростанням «інтелектуальної» споживчої електроніки, зростають вимоги до їх безпеки. На сьогоднішній день основні проблеми захисту інформації IoT це:

- неоднорідність пристроїв (у кожного пристрою різноманітні можливості саме тому дуже складно підібрати універсальні заходи захисту);
- неоднорідність технологій (Wi-fi, Blutooth, NFC і т.д.);
- обмеження пропускної здатності мережі;
- перехід на IPv6;
- стандартизація архітектури і протоколів, сертифікація пристроїв;
- стандартні облікові записи від виробника, слабка автентифікація;
- відсутність підтримки з боку виробника для усунення вразливостей;
- складності в оновленні програмного забезпечення і операційної системи;

Найбільш перспективним способом захисту даних є використання криптографічного протоколу. Універсального протоколу для всіх IoT не існує, тому в кожному напрямку IoT є свої. Наприклад, в електроенергетиці застосовують протоколи: IEC 60870-5, DNP 3, FOUNDATION Fieldbus, ICCP, Modbus. У нафтогазі застосовують протоколи: IEC 60870-5, DNP 3, Modbus. У водопостачання входять протоколи: DNP 3, Modbus. В автоматизації будівлі застосовують протоколи: LonWorks (or LonTalk, or ANSI / CEA 709.1-B), DyNet, INSTEON, X10, ZigBee, X-Wave і KNX / Konnex. У промисловісті застосовують протоколи: DF1, FOUNDATION Fieldbus, Profibus, PROFINET 10 CC-Link, CIP, ControlNet, DeviceNet, Ethernet / IP, EtherCAT, EGO, FINS, Host Link, SERCOS, SRTP, Sinec H1.

Також для захисту інформації був створений цілий ряд галузевих спілок і консорціумів виробників IoT: Thread Group, Open Interconnect Consortium, AllSeen Alliance і Industrial Internet Consortium. Ці союзи займаються адаптацією сімейства стандартів безпеки ISO 27000, розробляють рамкову концепцію стандартизації безпеки в сфері IoT і захисту особистих даних.

У 2017 р компанією Amazon створений сервіс AWS IoT Device Defender. Цей сервіс повністю керований, він допомагає захистити парк пристроїв IoT. AWS IoT Device Defender виконує безперервний аудит конфігурацій IoT, щоб не допускати відхилень від рекомендацій з безпеки.

З ростом популярності і масштабів Інтернету речей його пристрої почали вживатися зловмисниками як платформа для організації найпотужніших кібератак. Існує 4 основних напрямки захисту від DDoS-атак.

Самостійний захист. Написання скриптів або користуванна брандмауером. Дуже малоефективний спосіб, може спрацювати тільки проти атак невеликої мережі до 10 машин.

Спеціалізоване обладнання. Пристрої розгортаються перед серверами і маршрутизаторами, фільтруючи вхідний трафік. У цього методу є 2 недоліки: для їх обслуговування потрібен висококваліфікований персонал, у них обмежена пропускна здатність.

Захист від провайдера. На жаль, щоб справлятися з найостаннішими DDoS-атаками, провайдеру потрібно купувати дороге обладнання. Багато провайдерів прагнуть продавати свої послуги якомога дешевше, тому надійного захисту від серйозних DDoS-атак вони забезпечити не в змозі. Частковий вихід з ситуації – кілька провайдерів, які у випадку атаки відбивають її спільним зусиллями.

Сервіс захисту сервера від DDoS-атак від ProHoster. Оскільки основна маса обладнання розташована в Нідерландах, то ProHoster застосовує найбільшу в Європі мережу очищення трафіку від ботів, відому також як хмара захисту від DDoS.

На сьогоднішній день безпечного Інтернету речей немає. Існує небезпека, яку недоцільно ігнорувати. В іншому випадку виникнуть загрози як життю, так здоров'ю людини, її фінансам та майну. Варто тільки зловмисникам проявити інтерес до будь-кого з нас, і наші вірні помічники зі світу IoT перетворюються в зрадників та відкривають доступ в світ своїх власників.

Список використаних джерел:

1. IoT – Internet of Things [Електронний ресурс]. – Режим доступу : https: // www.lessons-tva.info/articles/net/013.html

2. Substation SCADA Protocol Conversion [Електронний ресурс]. – Режим доступу : https://virtualaccess.com/substation-scada-protocol-conversion/?gclid=EAIaIQobChMIpO_vjNyN4QIVBcwYCh0mcwEDEAAYASAAEgLxXPD_BwE

3. AWS IoT Device Defender [Електронний ресурс]. – Режим доступу : https://docs.aws.amazon.com/en_us/iot/latest/developerguide/device-defender.html

4. DDoS-атака [Електронний ресурс]. – Режим доступу : https://ddos-guard.net/ru/terminology/attacks/ddos-ataka

5. Форсайт Д., Поинс Ж. Комп’ютерне зір. Сучасний підхід. : Пров. з англ. – М: Видавничий будинок «Вільямс», 2004. – 928 с. : іл. – Хрон. тит. англ.

Овсяницький В.,
студент ОС «Бакалавр» спеціальності «Системний аналіз»,
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

АНАЛІЗ ПОРУШНИКІВ ТА ЗАГРОЗ В БЕЗДРОТОВИХ МЕРЕЖАХ

Як і безліч інших інноваційних технологій, бездротові мережі мають не тільки вигоди, але і ризики. Поширення бездротових мереж породило ціле покоління хакерів, спеціалізованих на винаході нових засобів зламу корпоративних інфраструктур і атак користувачів.

У бездротових мережах використовується відкрите середовище з практично повною відсутністю контролю. Забезпечити еквівалент фізичної безпеки дротових мереж тут ніяк не вдасться. Бездротовий сегмент мережі стає

доступним з іншого поверху або ззовні: єдиним фізичним кордоном бездротової мережі є рівень самого сигналу. Тому, на відміну від провідних мереж, де точка підключення користувача відома, до бездротових під'єднатися можливо з будь-якої точки в досяжності сигналу. При цьому приймач, що працює тільки на прослуховування, взагалі неможливо визначити.

Одне з визначень мережевої атаки – мережева атака може бути визначена як будь-який метод, процес або засіб, що використовується для виконання зловмисної спроби порушення мережевої безпеки[1].

Причини атак на корпоративні мережі:

Корисливі особисті і ідеологічні мотиви: бажання наживи, промислове шпигунство, політика, тероризм, расизм. Невдоволення колишніх або існуючих співробітників, зведення рахунків з компанією. Вони можуть прагнути вплинути на інформаційну надійність або фінансову стабільність компанії. Задоволення від вирішення складних завдань. Цей мотив характерний для окремої категорії атакуючих, яким подобається сам процес проникнення в надзахищені мережеві системи і сховища. Вони зазвичай просто розважаються або намагаються привернути увагу до наявних мережевих вразливостей.

Розглянемо найбільш поширені загрози для бездротової мережі.

Атаки на локальному рівні. Такі атаки зазвичай виникають, коли відкрито доступ до комп'ютерних приміщень. Як відомо, бездротові мережі являють собою окремі сегменти кабельної мережі. Відповідно, будь-яка бездротова точка доступу може бути використана як плацдарм для атаки. Деякі мережні пристрої можуть бути більш уразливі, ніж інші, в першу чергу зловмисники атакують саме їх. Більшість успішних зламів бездротових мереж сталося саме в результаті неправильної конфігурації точок доступу або клієнтського ПЗ.

DoS – атаки. Слабка захищеність протоколів стандарту 802.11 укупі з низьким рівнем підготовки системних адміністраторів багатьох мереж, що використовують цей стандарт, роблять можливим проникнення в бездротову мережу. Реальність є такою, що протоколи сімейства 802.11 уразливі до DoS-атак, які дозволяють заглушити будь-яку точку доступу, порушити функціонування мережі і перехопити дані. DoS-атака є важливою складовою частиною атак man-in-middle. Суть такої атаки полягає в заміні діючої системи мережі точки доступу своєю власною. Більш проста реалізація атаки «людина посередині» полягає в підміні якогось клієнтського хоста, що набагато простіше здійснити, оскільи не потрібно конфігурувати впроваджуваний хост як точку доступу, а потрібно тільки імітувати IP і підміняти вузли MAC.

Система автентифікації. Імперсоналізація авторизованого користувача – серйозна загроза будь-якій мережі, не тільки бездротової. Однак, в останньому випадку визначити справжність користувача складніше. Звичайно, існують SSID, і можна намагатися фільтрувати за MAC-адресами, а й те й інше передається в ефірі у відкритому вигляді, і те й інше нескладно підробити. А підробивши, як мінімум «відкусити» частину пропускної здатності мережі, вставляти неправильні фрейми з метою порушення авторизованих комунікацій.

Існує помилкове переконання, що імперсоналізація користувача можлива тільки в разі MAC-автентифікації або застосування статичних ключів та схеми на основі 802.1x, такі як LEAP, є абсолютно безпечними. Інші схеми, скажімо, EAP-TLS або PEAP, більш надійні, але вони не гарантують стійкості до комплексної атаки, що використовує кілька факторів одночасно.

Традиційні засоби захисту безсилі проти принципово нових класів бездротових загроз. При цьому ситуація ускладнюється тим, що необхідно захищати також і своїх користувачів (які можуть перебувати і поза офісом), не порушуючи при цьому функціонування мереж сусідів, яким би підозрілим воно не виглядало. Проте існують методи захисту від подібних загроз як бездротових, так і провідних мереж і користувачів, що дозволяють впевнено і безпечно розгортати і використовувати бездротові мережі.

Для організації безпечної роботи бездротової мережі (включаючи інфраструктуру і користувачів) служить підхід, який в цілому збігається з підходом «багаторівневої безпеки», що застосовується для традиційних провідних мереж. Він включає в себе:

• забезпечення безпеки периметра бездротової мережі (точки доступу і клієнтських пристроїв);

• забезпечення безпеки сеансів зв'язку (автентифікація, шифрування, аж до VPN);

• постійний цілодобовий моніторинг ефіру, починаючи з фізичного рівня.

Список використаних джерел

1. Портал: [Електронний ресурс]. - Moluch.ru - інформаційний портал. – Режим доступу: https://moluch.ru/conf/tech/archive/5/1115/

2. Портал: [Електронний ресурс]. - Wi-life.ru - інформаційний портал. – Режим доступу: http://wi-life.ru/treningi/wi-fi-3/praktikum/ataki-na-set-wi-fi

3. Портал: [Електронний ресурс]. - Securitylab.ru- інформаційний портал. – Режим доступу: https://www.securitylab.ru/analytics/216360.php

4. Портал: [Електронний ресурс]. - Stud.wiki- інформаційний портал. – Режим доступу: http://stud.wiki/programming/3cb56b2bd78a5c53b95236c6_0.html

Панов К.В.,
студент ОС «Бакалавр»
спеціальності «Системний аналіз»,
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

ТЕХНОЛОГІЯ HONEYPOT

Технологія Honeypot – ресурс безпеки, призначення якого полягає в тому, щоб зазнати нападу. Засоби Honeypot відрізняються від класичних засобів забезпечення безпеки тим, що вони не покликані вирішувати будь-яку конкретну задачу. Навпаки, Honeypot – гнучкий засіб, який може бути застосовано в різних ситуаціях. Наприклад, засоби Honeypot можуть запобігати

або виявляти атаки. По суті, Honeypot включають в себе деяку функціональність практично всіх засобів забезпечення безпеки.

На відміну від таких механізмів, як міжмережеві екрани і системи виявлення вторгнень, технологія Honeypot не вирішує певні завдання.

Технології Honeypot надають аналітикам деякі переваги:

1) збір змістовної інформації;
2) невимогливість до системних ресурсів;
3) простота установки, конфігурації та експлуатації;
4) наочність необхідності використання.

Головними проблемами засобів Honeypot є:

1) обмежена область бачення;
2) можливість розкриття Honeypot;
3) ризик злому і атаки вузлів сторонніх організацій.

Традиційно, професіонали безпеки дізнавалися про зловмисників, вивчаючи, які вживали кошти. Коли система була скомпрометована, адміністратори знаходили кошти зловмисників, залишені ними на атакованій системі. Таким чином, робилося безліч припущень, заснованих на зафіксованих засобах. Ця методика подібна археології, де професіонали намагаються зрозуміти вікові культури, аналізуючи зібрані матеріали. Така методика ефективна, але при цьому існує можливість отримати набагато більше інформації про зловмисників. Крім дослідження засобів, має сенс ідентифікувати зловмисників, визначити, наскільки добре вони організовані, і виявити їх методи.

Дослідницькі Honeypot мають велике значення, надаючи платформу для вивчення загроз. Існує можливість переглядати всі, аж до натискання клавіш, можуть бути застосовані при зборі інформації про загрози та для моделювання нових варіантів атак, збору раніше невідомих засобів і технік атак і для розуміння мотивацій зловмисників. Отримана інформація може бути застосована для попередження або виявлення, можливостей протоколювання.

На сьогоднішній день найбільший інтерес представляють високоінтерактивні динамічні Honeypot – системи, оскільки з завданнями низкоінтерактивних систем справляються інші елементи корпоративної мережі: мережеві сканування успішно запобігають міжмережевими екранами і системами виявлення та запобігання вторгнень, а також правильною конфігурацією елементів мережі, а інформація про конкретні дії зловмисника, вжиті для здійснення доступу в корпоративну мережу, ма єнабагато більшу цінність, ніж інформація про факт проникнення в мережу, яка також може бути отримана від міжмережевих екранів і засобів виявлення вторгнень.

Динамічні ж Honeypot – системи мають великий потенціал розвитку. У таких системах можуть бути застосовані ідеї, що зарекомендували себе в інших типах систем, а також запропоновані і принципово нові підходи.

Список використаних джерел

1. Бібліографія: [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – Режим доступу: http://uk.wikipedia.org/wiki/Бібліографія

2. Портал: [Електронний ресурс].– SecurityLab.ru - інформаційний портал. – Режим доступу: https://www.securitylab.ru/analytics/275420.php

3. Портал: [Електронний ресурс].– SecurityLab.ru - інформаційний портал. – Режим доступу: http://citcity.ru/15560/

Пурдик К.О.,
студентка ОС «Бакалавр»
спеціальності «Системний аналіз»,
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

DOS АТАКИ В БЕЗДРОТОВИХ МЕРЕЖАХ НА ФІЗИЧНОМУ РІВНІ МОДЕЛІ ISO

Аномалія типу «відмова в обслуговуванні» DoS (від англ. Denial of Service) є мережева атака, проведена зловмисником щодо мережного об’єкта, чиє функціонування він бажає порушити (уповільнити або припинити). Найбільш характерним проявом DoS є «затоплення» (англ.looding) каналу зв’язку або конкретного мережного пристрою величезною кількістю мережних пакетів. В залежності від типу пакетів це може призвести до перевантаження каналу і, як наслідок, неможливості проходження по ньому легітимного трафіку, або до заповнення доступного обсягу оперативної пам’яті і завантаження ресурсів процесора.

DoS може бути проведена не лише шляхом відправки величезного числа пакетів. Можливі ситуації, коли її можна викликати малим числом пакетів. Це можливо у випадку наявності специфічної уразливості в програмній або апаратній реалізації пристрою. Виявлення DoS у разі відправки величезного числа пакетів не представляє труднощів, на відміну від DoS, проведеної за допомогою незначної кількості пакетів. Необхідно відзначити, що існує ще різновид DoS, так звана розподілена DoS (від англ. Distributed Denial of Service, DDoS). Цей тип DoS характерний участю величезного числа атакуючих мережевих пристроїв.

Оскільки середовище передачі в бездротових мережах є загальнодоступним, кожний з абонентів може зайняти його для ексклюзивного доступу. Ситуація дуже схожа на принцип роботи коаксіального Ethernet, коли в разі виходу з ладу термінатора або одного з мережевих адаптерів вставала вся мережа. В Інтернеті досить просто виявити кілька вільно розповсюджуваних пристроїв, що генерують сигнал достатньої потужності для виведення з ладу Wi-Fi сети.

Обладнання стандарту IEEE 802.11 використовує неліцензований спектр частот. Коли перешкоди виробляються навмисно для порушення зв’язку, це називається радіочастотна перешкода (англ. RFjamming). Це означає, що

джерело перешкод знаходиться в межах поширення і обумовлено двома основними факторами. По-перше, близькість джерела перешкод до приймача. По-друге, потужність передачі.

Для успішного проведення атаки, джерело перешкод (або атакуючий) повинен згенерувати сигнал, досить потужний, здатний заглушити основні частоти. Під час генерації сигналу-завади атакуючий може націлюватися на певну вузьку смугу частот, або, якщо дозволяє потужність, більш широку. Сигнал–перешкода може передаватися безперервно або розраховуватися таким чином, щоб впливати на найбільш критичні місця.

Використовувана атакуючим стратегія визначається частково, шляхом оцінки виду сигналу, генерованого обладнанням, характеристикою використовуваних антен, доступною потужністю, і страхом перед виявленням і захопленням нападника. Бездротовий зв'язок за своєю природою є радіомовленням. А такий радіосигнал легко заглушити, або перехопити. Атакуючий фізично може підслухати, або впливати на бездротову мережу.

Підслуховування: Підслуховування, перехоплення і читання повідомлень чужими приймачами. Мобільні пристрої і мережі поділяють бездротове середовище. Більшість радіоз'єднань використовує ВЧ-спектр (високо частотний спектр) і радіопередачу за своєю природою. Передані по радіохвилях сигнали можуть бути легко перехоплені приймачами, налаштованими на відповідну частоту. Таким чином, передані повідомлення можуть підслуховуватися і замінятися підробленими повідомленнями.

Для того, щоб провести радіочастотну атаку в:

• IEEE 802.11, атакуючий повинен бути близько до точки доступу, що атакується;

• IEEE 802.16, атакуючий повинен бути близько до базової станції, що атакується;

• WMN, атакуючий може провести атаку в будь-якому місці.

Через велику зону покриття і досить щільне розташування маршрутизаторів бездротової мережі, мережі WMN більш уразливі від DoS-атак фізичного рівня.

Способи виявлення втручання та захисту бездротових мереж

Спочатку перерахуємо варіанти захисту, які можуть бути використані на точці доступу для обгороджування мережі від чужих користувачів:

1. SSID Cloaking – приховання імені мережі. Доступ дозволяється тільки клієнтам, які знають це ім'я.

2. MAC Filtering – фільтрація за MAC адресами. Доступ дозволяється тільки клієнтам, адреси мережевих адаптерів яких записані в точці доступу.

3. Shared key Authentication – аутентифікація із загальним ключем. Доступ дозволяється лише тим клієнтам, які пройшли перевірку, використовуючи загальний ключ.

Важливо відзначити, що ці методи не забезпечують конфіденційності даних, що передаються мережею, вони просто обмежують доступ до мережі. Тобто, навіть якщо усі ці засоби включені на точці доступу, зловмисник зможе, включивши свій безпровідний адаптер в "monitor mode", слухати ефір і виловлювати усю інформацію, що передається

Найбільш розповсюдженими атаками фізичного рівня на такі об'єкти, як канали передачі даних, є:

• фізичне пошкодження;

• несанкціоновані зміни у функціональному середовищі;

• вимкнення фізичних каналів передачі даних;

• постановка шумів по всій полосі пропускання каналу.

Тим не менш, для побудови мереж доступу найбільш розповсюдженим рішенням є використання безпроводових технологій (Wi-Fi). Такє рішення найменш захищено від згаданих вище атак. Єдиною можливістю захисту від несанкціонованого доступу до інформації при використанні такої лінії зв'язку є шифрування даних.

Для запобігання можливим атакам, спрямованим на несанкціоновані зміни у функціональному середовищі, необхідно, перш за все, забезпечити обмеження фізичного доступу до каналів, комутаційних вузлів та дата-центрів, розробити та реалізувати політику віддаленого доступу до мережного обладнання, розгорнути допоміжні системи відеоспостереження та контролю доступу. Важливим фактором при забезпеченні надійності роботи інформаційно-комунікаційних систем можна вважати резервування найбільш критичних каналів, мережних пристроїв та серверів.

Список використаних джерел

1. Портал:[Електронний ресурс] – Securitylab.ru - інформаційний портал. – Режим доступу: https://www.securitylab.ru/analytics/216360.php

2. Портал: [Електронний ресурс]. – Safe-Surf.Cyberleninka.ru - інформаційний портал. – Режим доступу: https://safe-surf.ru/users-of/article/330/

3. Портал: [Електронний ресурс]. – Cyberleninka.ru - інформаційний портал. – Режим доступу: https://cyberleninka.ru/article/n/osobennosti-ddos-atak-v-besprovodnyh-setyah

Сахно О.С.,
студентка ОС «Бакалавр»
спеціальності «Системний аналіз»,
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

БЛОКЧЕЙН ТЕХНОЛОГІЯ ДЛЯ АВТЕНТИФІКАЦІЇ

На сьогоднішній день система автентифікації побудована на логінах і паролях, але вона незручна і ненадійна. Проблема полягає в тому, що люди не

хочуть запам'ятовувати довгі комбінації, віддаючи перевагу максимально простим, всупереч рекомендаціям безпеки. Це відкриває шахраям доступ до багатьох даних. На додаток, отримання одного пароля, через часте використання єдиної комбінації для більшості сервісів, створює нову проблему безпеки. Так, отримавши всього один пароль, з його допомогою, або ж на його основі, можуть бути підібрані варіанти комбінація для всіх входів. Рішенням цієї проблеми стала багатофакторна автентифікація особистості на основі блокчейн. Багатофакторна автентифікація побудована на спільному використанні декількох факторів автентифікації. Наприклад, в деяких сучасних ноутбуках наявний сканер відбитка пальця. Таким чином, при вході в систему суб'єкт повинен пройти цю процедуру, а потім ввести пароль. Вибираючи для системи той чи інший фактор або спосіб автентифікації, необхідно, перш за все, відштовхуватися від необхідного ступеня захищеності. Блокчейн – побудована за певними правилами безперервна послідовність блоків, що містять інформацію. Блокчейн-технологія дозволяє відстежувати і керувати особистими цифровими даними безпечним і ефективним способом, що забезпечує захист від шахраїв. Системи автентифікації на основі блокчейна дозволяють здійснювати ідентифікацію особистості з використанням цифрових підписів з відкритим ключем, захищеним криптографічно. В результаті, автентифікація на блокчейні має на увазі лише перевірку, чи підписана транзакція правильним ключем. Сам ланцюжок блоків може вільно передаватися будь-якому користувачеві Інтернету без ризику втрати вмісту. Розібратися в тому, що таке блокчейн, стане простіше, якщо заглибитися в тонкощі роботи з цією системою: будь-які зміни без підтвердження криптографічними ключами відхиляються, передача закритого ключа надає повний доступ до блоку. Передача доступу до блоків відбувається в автоматичному режимі за принципом цифрового підпису – ввів код, підтвердив передачу права, і процес завершено. Що стосується безпеки будь-яку централізовану базу даних можна зламати, внести в неї зміни. Зламати один з блоків і змінити інформацію в ньому сенсу немає, оскільки ламати доведеться усі блоки, а для цього потрібні гігантські обчислювальні потужності. Спроба зламу обов'язково буде помічена іншими учасниками мережі. До плюсів технології можна віднести те, що це універсальна технологія, застосовна в різних сферах життя, блокчейн також: зменшує транзакційні витрати, дозволяє установам позбутися зайвих статей витрат. До мінусів варто віднести масштабованість. Сьогодні блокчейн не здатний забезпечувати велику кількість транзакцій за короткий час. Як висновок, варто додати, що цілком можливо зараз саме той час, коли технологія проходить обкатку наживо у вельми значущих сферах суспільного життя, і незабаром ми побачимо ще більше проектів і платформ, які використовують блокчейн. Нові проекти-блокчейн будуть ґрунтуватися на його головних перевагах – відкритості, захищеності, безпечності.

Список використаних джерел

1. Портал:[Електронний ресурс] // Alpari.com – інформаційний портал. – Режим доступу : https:// alpari.com/ru/beginner/glossary/blockchain/

2. Портал:[Електронний ресурс] // Prostocoin.com – інформаційний портал. – Режим доступу : https://prostocoin.com/blog/blockchain – guide

3. Портал:[Електронний ресурс] // Cyberleninka.ru – інформаційний портал. – Режим доступу : https://cyberleninka.ru/article/n/sistemnyy-analiz-tehnologii –obmena–i–hraneniya–dannyh–blockchain

Титаренко К.
Студентка 1 курсу
спеціальності «Кібербезпека»
науковий керівник Дяченко О.Ф.
Маріупольський державний університет

WEB-ДОДАТКИ ТА ЇХ ЗАХИСТ

Безпека web-додатків знаходиться в першій десятці трендів і загроз інформаційної безпеки вже понад 10 років. Сучасні бізнес-процеси та повсякденне життя все більше і більше залежать від використання веб-додатків в найрізноманітніших аспектах: від складних інфраструктурних систем до IoT пристроїв. Проте, навіть з використанням цих засобів безпечніше веб не став, більш того, майже усі уразливості "класичного інтернету" практично в незмінному вигляді мігрували до мобільної розробки.

Раніше захист веб-додатків складався з грамотного налаштування сервера, чищення сайту від непотрібних файлів і ділянок коду з мінімальним контролем. Дійсно, канали були слабкі, DDoS не був поширений, вразливостей було мало, додатки були простими, дії користувачів були передбачені декількома сценаріями. Згодом ускладнювалися web-додатки, серверна інфраструктура і взаємодія, код ставав все більш об'ємним і громіздким – це набагато збільшило "поверхню атаки". Web став дуже популярним, в ньому з'явилися можливості фінансового зростання, що привернуло в цю сферу бажаючих незаконно скористатися чужою працею.

На сьогоднішній день майже усі брандмауери web-додатків покликані захистити від основних типів загроз властивих web-сайтам. А саме, це такі загрози:

- SQL ін'єкція;
- міжсайтовий скриптинг (XSS);
- міжсайтова підробки запитів (CSRF);
- розподілена відмова в обслуговуванні (DDoSатаки,);
- відсутність таймаута сесії;
- зворотний шлях в директоріях.

Є два способи організації захисту Web-додатків. Перший – це усунення вразливостей шляхом аналізу вихідного коду, а другий грунтується на використанні накладених засобів захисту інформації. В ідеалі обидва підходи необхідно комбінувати, однак практика показує, що в залежності від специфіки бізнесу підприємства і додатків, що використовуються, превалює зазвичай один з методів.

Підхід, який використовує усунення вразливостей шляхом аналізу коду, є найбільш витратним. Для його реалізації необхідна підтримка з боку широкого кола експертів, що володіють розумінням всієї прикладної абстракції мережевої взаємодії, що включає в себе логіку і алгоритми роботи програми, компоненти Web-технологій, програмне забезпечення та операційне середовище сервера. У деяких випадках використання цього підходу існує низка серйозних труднощів. Наприклад, при нестачі ресурсів або використання програмного забезпечення з закритим кодом, а також якщо Web-додаток було придбано як готовий продукт і він не є повністю самостійною розробкою. При цьому підприємства з розвиненою Web-інфраструктурою, які змогли організувати цикл безпечної розробки своїх додатків з використанням аналізу коду, стикаються з проблемою внесення коригувальних змін у продуктивні системи в силу особливостей їх роботи.

Підхід, що базується на використанні спеціальних накладених мережевих засобів захисту, найбільш доцільний і фундаментальний і підходить як організаціям з налагодженими процесами пошуку вразливостей у своїх сервісах, так і тим, хто цього не робить. У цьому контексті найбільш оптимальний засіб – WAF (Web Application Firewall). WAF – це міжмережевий екран, який накладає певний набір правил на те, як відбувається взаємодія сервера і клієнта, обробляючи HTTP-пакети. В основі лежить той же принцип, що й у звичайних фаєрволів – контроль і аналіз усіх пакетів, що надходять від клієнта. WAF спирається на набір правил, за допомогою якого виявляється факт атаки по сигнатурам – ознаками активності користувача, які можуть означати напад. Брандмауер інтернет-додатків ще називають третьою лінією оборони. У такій парадигмі першою лінією оборони є міжмережеві екрани, другий – системи IPS, і, нарешті третій – WAF.

Web Application Firewall поділяють на 2 типи: апаратний і програмний. Найбільшого поширення отримав другий, зважаючи на більш просту реалізацію. За принципом дії WAF можна розподілити на три типи:

1. Реалізовані у вигляді зворотного проксі-сервери.
2. Працюючі в режимі маршрутизації / моста.
3. Вбудовані в web-додатки.

Як і будь-який універсальний метод, WAF має ряд недоліків. Основна проблема сучасних WAF криється в їх архітектурі, заснованій на загальному принципі. Усі вони використовують сигнатурний аналіз для визначення типу загроз. Недолік такого підходу очевидний – його легка виявленість і відносно легкий спосіб обходу. Один з можливих варіантів вирішення цієї проблеми ми

бачимо в застосуванні методів поведінкового аналізу. Принцип такого підходу в корені відрізняється від сигнатурного. Такий підхід в теорії може закрити вразливості, пов'язані з сигнатурним аналізом. Цей напрямок найбільш перспективний у вирішенні проблем безпеки web-сайтів.

Список використаних джерел

1. Захист веб-додатків [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://www.ereading.club/bookreader.php/1012355/DJ-Andrey-sXe__Zaschita_veb-prilozheniy.html.

2. Василенко І.В. Захист інформації [Електронний ресурс]. – Режим доступу до ресурсу: http://www.hups.mil.gov.ua/periodic-app/article/15259/soi_2016_1_27.pdf

3. Крістіна Шатц. Дослідження методів захисту веб – додатків [Електронний ресурс]. – Режим доступу до ресурсу: http://www.zgia.zp.ua/gazeta/MNPIK_91.pdf

4. Ельдар Бейбутов. Захист Web-додатків [Електронний ресурс]. – Режим доступу до ресурсу: http://lib.itsec.ru/articles2/Oborandteh/zaschita-web-prilozheniy-po-vzroslomu

ЗМІСТ