ISSN 2409-7292

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ТЕЛЕКОМУНІКАЦІЙ

Є ЧЛЕНОМ МІЖНАРОДНОГО СОЮЗУ
ЕЛЕКТРОЗВ'ЯЗКУ

СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ

№4(32), 2017

Україна,03110,Київ,
вул.Солом'янська,7

Тел.+38(044)248-86-07
+38(044)249-29-27
www.dut.edu.ua

Реферативна інформація видання представлена у загальнодержавній реферативній базі даних «Україніка наукова», наукометричній базі Google Scholar та публікується у відповідних тематичних серіях УРЖ «Джерело»

ПЕРЕДПЛАТНИЙ ІНДЕКС 86480

Шановні читачі та автори журналу «Сучасний захист інформації»!

Вітаю Вас з виходом 4-го випуску журналу в 2017 році! Рік завершується і на передодні новорічних свят, по традиції, всі підводять підсумки року, що минає. Підведемо і ми підсумки 2017 року.

Вступила Україна в цей рік в стані ліквідації наслідків масової атаки на інформаційну інфраструктуру держави.

Саме проти України ворог - Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

На початку року Україна ще оговтувалася від масової кібератаки, що запровадилаРосійська Федерація у грудні 2016 р. Такими діями ворог вкотре намагався дестабілізувати ситуацію в Україні.З стану майже зупинення діяльності виходила низка державних установ України (Міноборони, Міносвіти, Мінінфраструктури, Укрзалізниця, морський порт «Південний» та НАК «Укренерго»). Але найбільш резонансними стали наслідки цієї атаки на Міністерство фінансів України, Держказначейство, Пенсійний фонд України та виконавчу службу. Унаслідок цієї кібератаки на державні фінансові установи протягом майже трьох днів були ускладнені сплати до бюджету податків та інших платежів, не працювала електронна система адміністрування ПДВ, спостерігалися збої в роботі митниці.

Слід відзначити, що за останній рік політика держави у сфері захисту її інформаційного простору та забезпечення інформаційної безпеки загалом стала більш комплексною й ефективною.

В інформаційній сфері за минулий рік відбулися по-справжньому знакові події.

Можна констатувати, що після особливо складних 2014–2016 рр. держава почала формувати в 2017 р. комплексну систему протидії інформаційному складнику гібридної війни. У 2017 р. приймаються узгоджені рішення, додержується досить вдалий баланс між обмежувальними і стимулюючими заходами як стосовно захисту інтересів громадян, суспільства та держави, так і для подальшого розвитку її інформаційного простору.

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»найшли своє відображення в Доктрині інформаційної безпеки України, затвердженій Указом Президента Українивід 25 лютого 2017 року № 47/2017, яким було введено в дію Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року«Про Доктрину інформаційної безпеки України».

Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Доктрина інформаційної безпеки, визначаючи розвиток системи стратегічних комунікацій пріоритетом, покладає на Міністерство інформаційної політики України завдання з розроблення стратегічного наративу і його імплементації.

Практичне виконання завдань, визначених цією Доктриною, відображено в планах дій Уряду України, а саме, вРозпорядженні Кабінету Міністрів України «Про затвердження середньострокового плану пріоритетних дій Уряду до 2020 року та Плану пріоритетних дій Уряду на 2017 рік» від 3 квітня 2017 р. № 275-р. За ініціативи Міністерства інформаційної політики України планується створити Координаційну раду з питань стратегічної комунікації. Продовжується реалізація Дорожньої карти Україна – НАТО зі стратегічних комунікацій.

На зухвалі дії інформаційно-пропагандистської машини Російської Федерації наслідувавУказ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 15 квітня 2017 р. № 133/2017

І хоча цей крок викликав неоднозначні оцінки експертів та широкої громадськості, проте потрібно усвідомлювати, що блокування сайтів і сервісів належить до сфери забезпечення безпеки держави, а не свободи слова, що і було визнано нашими партнерами з ЄС та міжнародних організацій. У НАТО, до речі, підтримали блокування російських сервісів в Україні.

Велике значення має, винесений на обговорення, Проект Закону про ратифікацію Адміністративних домовленостей щодо охорони інформації з обмеженим доступом між урядом України та Організацією Північно-атлантичного договору від 18 квітня 2017 р. № 0144.

Найбільш масштабні в Україні наслідки мало поширення вірусу NotPetya, який 27 червня 2017 р. атакував численні комп'ютерні системи вітчизняних державних і комерційних установ. Загалом, за підрахунками спеціалістів Microsoft та ESET, кібератака зачепила щонайменше 65 країн. Проте встановлено, що першою й основною метою кібератаки була саме Україна. У вітчизняних комп'ютерних мережах раніше за все була зафіксована активність вірусу, на яку, зрештою, припало понад 75 % усіх випадків ураження За попередніми підрахунками, у результаті атаки на території України станом на 7 липня 2017 р. було виведено з ладу до 10 % приватних, урядових і корпоративних комп'ютерів.

Урядові та недержавні агентства продовжують аналіз вірусу й тих можливостей, які він надавав його авторам. Але можна припустити, що основною метою вірусу було все ж кібершпигунство (зважаючи на те, що системи, які постраждали, належать переважно до державних установ чи об'єктів критичної інфраструктури), а атака 27 червня мала на меті завдання шкоди і приховання шпигунської частини вірусу.

На кібератаку, що відбулася 27 червня 2017 року, без затримки відреагували Рада національної безпеки і оборони України та Президент України. ВийшовУказ Президента України від 30 серпня 2017 року № 254/2017«Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32». Цім Указом були поставлені завданнявідповідним державним органам:

а) забезпечити в установленому порядку фінансування видатків на модернізацію ситуаційних центрів з кібербезпеки Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України;

а) забезпечити фінансування видатків на проектування захищеного центру обробки даних для розміщення державних електронних інформаційних ресурсів;

в) вжити заходів щодо створення Національного центру оперативно-технічного управління мережами телекомунікацій України та забезпечення його функціонування;

3) забезпечити модернізацію та розширення функціональних можливостей системи інформаційного обміну про кіберзагрози;

4)підготувати та винести в установленому порядку на розгляд Кабінету Міністрів України пропозиції щодо підготовки та перепідготовки фахівців з питань кіберзахисту.

Протягом короткого часу налагоджено системну роботу Національного координаційного центру кіберзахисту при РНБО України. Завдяки діяльності Центру були розроблені організаційно-координаційні рішення щодо співпраці суб'єктів кібербезпеки стосовно ліквідації наслідків кібератак на державні інформаційні ресурси фінансового сектору, подолання наслідків атаки вірусу NotPetya, налагоджено процес розроблення та впровадження узгодженого протоколу спільних дій суб'єктів забезпечення кібербезпеки та власників об'єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та інших кіберінцидентів, а також при подоланні їхніх наслідків.

Надзвичайно важливим завданням для захисту кібербезпеки держави є продовження робіт з формування Переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави (значного прогресу було досягнуто щодо включення до цього документа операторів мобільного зв'язку). Істотного вдосконалення потребує система кіберзахисту державних інформаційних ресурсів.

Ця обставина, зокрема, вимагає невідкладного розвитку національної системи кібероборони, що передбачає вжиття комплексузаходів щодо підготовки інформаційної інфраструктури сил оборони держави для набуття необхідних спроможностей із забезпечення обороноздатності в кіберпросторі.

При цьому силами Служби безпеки України за І півріччя 2017 р. було попереджено 137 випадків можливого витоку інформації, у т. ч. з обмеженим доступом, яка обробляється в ІТ-системах органів державної влади та місцевого самоврядування. У 2016–2017 рр. українськими правоохоронними органами (спільно з іноземними колегами та фахівцями з приватного сектору) було знешкоджено кілька потужних бот-мереж (наприклад, Pony та Linux/Mumblehard).

Відбувається стратегічний процес – кардинально оновлюються системні механізми реалізації Національної програми інформатизації, яка тривалий час фактично не виконувалася. Здійснюється контроль за формуванням завдань Національної програми інформатизації на 2018–2020 рр. та поданням відповідних пропозицій на розгляд Верховної Ради України разом із проектом Закону України «Про Державний бюджет України на 2018 рік». Незважаючи на масштабні дії державних структур в сфері забезпечення кібербезпеки на рівні інтересів суспільства та держави, перманентно важливим залишається фактор посилення обізнаності громадян про кіберзагрози. Як слушно зазначають дослідники, «забезпечення національної кібербезпеки неможливе без підвищення загальної обізнаності громадян про основні норми та правила поведінки в

кіберпросторі, адже систематичні порушення елементарних правил комп'ютерної безпеки працівниками ключових державних установ та об'єктів критичної інфраструктури можуть звести весь комплекс заходів, здійснюваних в рамках національної системи кібербезпеки, нанівець»

Лише при вирішенні кібербезпекових питань на всіх трьох рівнях (людини, суспільства та держави) ми зможемо дійсно створити ефективну та дієву національну систему кібербезпеки.

Найважливіша подія 2017 року прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (від 5 жовтня 2017 року № 2163-VIII).

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

У цьому Законі визначеніважливі терміни, відсутність офіційного тлумачення яких, затримувало конкретні дії з реагування на кіберінциденти. Це, зокрема, такі: кібератака, кібербезпека, кіберзагроза, кіберзлочин, кібероборона, кіберпростір, кібертероризм, критична інформаційна інфраструктура, національні електронні інформаційні ресурси, об'єкт критичної інформаційної інфраструктури та інші. Визначені об'єкти кібербезпеки та кіберзахисту, суб'єкти забезпечення кібербезпеки, принципи кібербезпеки, національна система кібербезпеки України. В законі визначені завдання суб'єктам національної системи кібербезпеки України. Найбільш знаковими на думку редактора є: "здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії" та "проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі". Національна безпека України розглядається нерозривно від інформаційної безпеки кібербезпеки та кіберзахисту.

Таким чином 2017 рік ввійде в історію України як прорив в розвитку та захисту інформаційної сфери існування суспільства та держави.

В наступному 2018 році слід очікувати суттєвих реальних дій з боку держави та суспільства в напряму виконання рішень національних державних структур та міжнародної спільноти.

Поздоровляю Вас, колеги, з наступаючим Новим 2018 роком, та бажаю великої наснаги в відтворюванні своїх мрій.

З повагою до Вас,
Головний редактор журналу «Сучасний захист інформації»
Довбешко Станіслав Володимирович

Засновник: Державний університет телекомунікацій
Зареєстровано Міністерством юстиції України
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ №20254-10654ПР від 10 червня 2014 р.

Наказом МОН України № 1021 від 07.10.2015 (Додаток 11, п. 110) Журнал включено до Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття науковихступенів доктора та кандидата наук в галузі технічних наук

Адреса редакційної колегії

03110, УКРАЇНА, м. Київ
вул. Солом'янська, 7
Державний університет телекомунікацій
Тел.: +38 (044) 249-29-17
Ел.пошта: szi.journal@dut.edu.ua
Web-сайт: http://www.dut.edu.ua

Редакція не може поділяти думок авторів. Відповідальність за зміст наданих матеріалів несуть автори.
Рекомендовано до друку Вченою радою Державного університету телекомунікацій
(протокол №9 від 13 листопада 2017 р.)
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру.
Серія ДК №2539 від 26.06.2006 р. Формат 64x90/8

Кількість примірників: 300.

Editorial Address

03110, Kyiv, UKRAINE
st. Solomenskaya 7
State University of Telecommunications
Tel.: +38 (044) 249-29-17
e-mail: szi.journal@dut.edu.ua
Web-site: http://www.dut.edu.ua

Copies: 300.