Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 1 (січень)

Київ - 2018

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В. І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники: О. Довгань, Л.Литвинова, С. Дорогих. Дизайн обкладинки С.Дорогих.

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К.: Видавничий дім «АртЕк», 2018. – №1 (січень) . – 56с.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

«…Військові хакери з Росії в 2017 році здійснили кібератаку проти України в спробі підірвати фінансову систему держави на тлі війни з проросійськими бойовиками, пише The Washigton Post з посиланням на звіт Центрального розвідувального управління (ЦРУ) США.

…видання зазначає, що в американській розвідці з високою часткою ймовірності впевнені в тому, що вірус Petya.A (згодом названий NotPetya) був створений військовою розвідкою Головного розвідуправління Росії…

Наголошується, що в ЦРУ відмовилися прокоментувати WP цю інформацію…» ***(ЦРУ підозрює військових хакерів Росії в кібератаці на Україну – WP // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/cru-pidozryuye-viyskovih-hakeriv-rosiyi-v-kiberataci-na-ukrayinu-wp-266006_.html). 13.01.2018).***

***

«По факту вмешательства в работу серверов Главного территориального управления юстиции в Одесской области и установки вредоносного программного обеспечения открыто уголовное производство по ст.361 Ч 1. Уголовного кодекса Украины…

Санкция статьи, по которой открыто уголовное производство, предусматривает наказание в виде штрафа от шестисот до тысячи необлагаемых минимумов доходов граждан или ограничение свободы на срок от двух до пяти лет, или лишение свободы на срок до трех лет, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет с конфискацией техсредств.

…Уязвимости портала ГТУ Юстиции в Одесской области обнаружили белые хакеры Украинского киберальянса в рамках акции #FuckResponsibleDisclousure рано утром 6 января. Сообщалось об утечке сотен гигабайт документов.

С 6 января сайт одесского управления Минюста был закрыт и только сегодня вновь стал доступен…» ***(Владимир Кондрашов. В Минюсте открыли уголовное дело из-за слива данных, но забыли закрыть уязвимость // Internetua (http://internetua.com/v-minuaste-otkrli-ugolovnoe-delo-iz-za-sliva-dannh-no-zabli-zakrt-uyazvimost).- 10.01.2018).***

***

«Белые хакеры из объединения Украинский киберальянс (УКА) в рамках акции #FuckResponsibleDisclosure обнаружили в сети научно-исследовательского института Министерства обороны Украины уязвимость, благодаря которой в открытом доступе оказались личные данные военнослужащих МО…

Речь идет о Государственном научно-исследовательском институте авиации, учредителем которого является Министерство обороны Украины…

…хактивистами обнаружен компьютер с именем PRIVAT, на котором были открытые на запись файлы с базами данных и двумя подключенными принтерами. В базах данных содержатся личные данные военнослужащих и сведения о

денежном довольствии военных. Кроме того, на устройстве обнаружена подробная инструкция по настройке удаленного доступа…

…на данный момент проверяют опубликованную информацию, однако… прокомментировать её не могут…». ***(Владимир Кондрашов. Личные данные военнослужащих Минобороны обнаружили в сети // Internetua (http://internetua.com/licsne-danne-voennoslujasxih-minoboron-obnarujili-v-seti).- 10.01.2018).***

***

«…в Украине уже определились первые претенденты на вручение национальной антипремии в сфере кибербезопасности…

6 января на официальной странице ГТУ Юстиции в Одесской области появилось сообщение о временном отключении собственного веб-сайта «в связи с установлением обстоятельств, которые могли повлечь технические сбои в его работе».

Под заковыристой формулировкой… пресс-служба областной юстиции завуалировала утечку в открытый доступ сотен гигабайт документов Минюста.

Уязвимость в рамках #FuckResponsibleDisclousure обнаружил Украинский кибералья́нс…

В ГТУЮ Одесской области среагировали довольно оперативно на информацию, опубликованную в 7 утра, – спустя 6 часов на официальной странице ведомства в Facebook появилось сообщение, что сайт временно закрыт. Также было объявлено, что при поддержке работников Управления Службы безопасности Украины и Причерноморского управления киберполиции «ведется работа по установлению причин данного инцидента».

Однако уже сейчас можно говорить точно об одной из главных причин «инцидента» – наплевательское отношение к собственной безопасности и отсутствие реакции на многочисленные сообщения об угрозе…

8 января Украинский кибералья́нс (УКА) обнаружил «дырявый» сайт, принадлежащий структуре Министерства регионального развития, строительства и ЖКХ Украины, а именно – Государственному фонду регионального развития…

…на главной странице этого же сайта был обнаружен встроенный скрипт для майнинга криптовалют. Криптомайнер Coinhive «заточен» под добывание Монеро – криптовлюты…

В воскресенье, 8 января, УКА также опубликовал скриншоты ряда документов «Укрзализныци»: «Перечень стрелочных переводов по структурному подразделению «Константиновская дистанция пути» по состоянию на первое января 2018 года», «Ведомость наличия изолирующих стыков по главным колиям структурного подразделения «Константиновская дистанция пути» по состоянию на 19.06.17», схемы путей и множество других документов, относящихся к работе железнодорожных узлов вблизи зоны АТО. Эти документ член УКА также обнаружил в открытом доступе в сети…

Также в открытом доступе найдены документы частной компании, занимающейся отделкой авиа- и водного транспорта, в том числе и для первых лиц государства и ГСЧС…

Количество документов, доступных для просмотра, зашкаливает за 200 Гиг…

Вчера, 8 января, к #FuckResponsibleDisclousure присоединилась группировка хакеров #CYBER_BABAK: в официальном твиттер-аккаунте команды появилась информация об уязвимости портала Конотопского авиаремонтного завода «Авиакон», входящего в государственный концерн «Укроборонпром». Завод специализируется на капитально-восстановительном ремонте и переоборудовании вертолетов Ми-24, Ми-35, Ми-8, Ми-17, Ми-26, Ми-2 всех модификаций…» ***(Владимир Кондрашов. Дыры в Минюсте и криптовалюты Минрегиона: первые провалы в кибербезопасности 2018 года // Internetua (http://internetua.com/dr-v-minuaste-i-kriptovaluat-minregiona-perve-proval-v-kiberbezopasnosti-2018-goda).- 09.01.2018).***

***

«…За словами голови Кіберполіції Сергія Демедюка, Департамент кіберполіції — новий підрозділ Національної поліції, який тільки формується. Проте з кожним роком набуває більшого досвіду, напрацьовує методологію, отримує знання від зарубіжних партнерів…

«Щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисяч. У 2017 році ми супроводжували близько 7 тис кримінальних проваджень, з них 4,5 тис — винятково кіберзлочини. За одинадцять місяців 2017 року ми направили до суду обвинувальні акти щодо 726 осіб», - озвучив статистику Демедюк». ***(Кількість кіберзлочинів збільшується на 2,5 тисячі в рік – голова Кіберполіції // Економічна правда (https://www.epravda.com.ua/news/2018/01/15/633010/). 15.01.2018).***

***

«…По словам главы киберполиции Сергея Демедюка, большинство киберпреступников совершают преступления, находясь в местах лишения свободы…

Демедюк указал, что пока в колониях и тюрьмах не будет побеждена коррупционная составляющая, преступления там будут происходить и дальше.

«Группа мошенников, которую мы задерживали последней, имела в сутки более миллиона гривень оборота…», — сказал он.

Глава киберполиции сообщил, что преступники построили целую империю мошенничества, где есть свои «воры в законе», организовывающие данные схемы.

«Мы отслеживаем эти схемы совместно с уголовным розыском, и в 2018 году будем проводить целевые тотальные операции по их искоренению», — сказал Демедюк…» ***(Большинство кибермошенников совершают преступления, уже находясь за решеткой // «Факты и комментарии®» (http://fakty.ua/255145-bolshinstvo-kibermoshennikov-sovershayut-prestupleniya-uzhe-nahodyas-za-reshetkoj). 15.01.2018).***

***

«…В прошлом году страна столкнулась с разрушительной кибератакой, которая на продолжительное время парализовала работу 80% госструктур,

некоторых СМИ и большинства банков. Украина оказалась абсолютно незащищенной перед интернет-агрессором…

Реальность такова, что в государственных структурах оплата труда системных администраторов настолько низкая, что хороший специалист никогда туда не пойдет. Вот и получается, что в организациях с миллионными счетами за кибербезопасность отвечает человек с зарплатой в 3 тысячи гривен…

В Украине отношение к хакерам очень лояльное и терпимое, поэтому в суде они отделываются штрафами и условными наказаниями. Как правило, украинские хакеры совершают преступления в других странах.

По информации кибер-силовика Сергея Демидюка, 80% украинских взломщиков находятся в розыске США. Украинское законодательство не позволяет привлечь их к ответственности, экстрадировать со страны их также невозможно. Более того, либеральное законодательство позволяет укрываться в Украине иностранным хакерам. Они практически без труда получают вид на жительство, потом гражданство и оседают здесь. А мы не можем выдавать своих граждан…

Большой опасностью для украинцев в недалеком будущем может стать кибершпионаж…

Почта и социальные сети в 2018-м будут и дальше использоваться хакерами для заражения компьютеров. По мнению экспертов отрасли, еще большее внимание злоумышленников привлекут электронные кошельки.

Киберстрахование становится одной из самых динамично развивающихся областей на рынке страхования, а специалисты по кибербезопасности станут самыми популярными и оплачиваемыми на рынке труда». ***(Галина Панкратьева. Кибергигиена для украинцев и хакерские тенденции 2018 // PERSONA.TOP (https://persona.top/2018/01/16/kibergigiena-dlya-ukraintsev-i-hakerskie-tendentsii-2018/). 16.01.2018).***

***

«Національний координаційний центр кібербезпеки при РНБО України 11 січня провів засідання, присвячене ринку криптовалют…

…На засіданні під головуванням Секретаря РНБО України було розглянуто результати випробувань на уразливість від кібератак інформаційно-телекомунікаційних систем органів державної влади та об'єктів критичної інфраструктури, найбільш важливих для безпеки і оборони держави; питання захисту інформації в системі біометричної верифікації та фіксації біометричних даних на пунктах пропуску через державний кордон України, а також інші питання кібернетичного захисту країни.

Окрім того, учасники засідання розглянули комплекс проблем, пов'язаних з неконтрольованим обігом криптовалют на території України…

Рішенням Національного координаційного центру кібербезпеки було доручено відповідним органам влади створити робочу групу за участю представників Національного банку України, Міністерства фінансів України, Національної комісії з цінних паперів та фондового ринку України, Служби безпеки України, Національної поліції України, Державної служби фінансового моніторингу України, Державної фіскальної служби України та Державної служби

спеціального зв'язку та захисту інформації України для напрацювання нормативно-правових пропозицій щодо регулювання цього питання…

Окрім того, доручено розробити механізм забезпечення доступу правоохоронних органів до даних криптовалютних бірж із зобов'язанням вказаних суб'єктів зберігати інформацію про всі транзакції протягом терміну, встановленого законодавством для фінансових організацій, та розкриття інформації про клієнта за вмотивованим запитом…» ***(Олександр Турчинов зацікавився крипто валютами // Агенція інформації та аналітики (http://galinfo.com.ua/news/oleksandr_turchynov_zatsikavyvsya_kryptovalyutamy_278465.html). 11.01.2018).***

***

«…Співробітники СБ України спільно з прокуратурою заблокували розповсюдження шкідливого програмного забезпечення, яке призначалося для віддаленого негласного отримання інформації з мобільних терміналів.

…За інформацією СБУ, програма запускалася автоматично при включенні мобільного телефону, не виявляла ознак активності під час роботи та діяла приховано від власника. «Можливості хакерського забезпечення дозволяли перехоплювати телефонні розмови, СМС- та ММС-листування, фіксувати місцезнаходження абонента, «знімати» спілкування через популярні месенджери та електронну пошту, надавали доступ до фото- і відеофайлів, що зберігаються на мобільному пристрої. Усі отримані дані зберігалися для клієнта в «особистому кабінеті» на веб-ресурсах зловмисників. Для постійного користування «сервісом» замовник повинен здійснити оплату на необхідний йому термін через електронні платіжні системи», - повідомили в СБУ. Співробітники Управління СБУ у Харківській області провели низку обшуків в офісах та за місцями мешкання учасників групи, під час яких вилучили докази їх протиправної діяльності.

…Кримінальне провадження здійснюється за ознаками злочинів, передбачених ч. 2 ст. 359 (незаконне використання спеціальних технічних засобів негласного отримання інформації) та ч. 1 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України…» ***(СБУ заблокувала поширення шпигунської програми для мобільних пристроїв // Є! «ЄДНІСТЬ-ІНФОРМ» (https://www.ednist.info/news/77378). 15.01.2018).***

***

«Служебное расследование установило виновного в утечке данных Национальной гвардии Украины.

Об этом InternetUA сообщил руководитель группы информации и коммуникации Восточного ОТО НГУ Дмитрий Образцов…

– На сегодняшний день должностное лицо… по результатам служебного расследования будет привлечено к строгой дисциплинарной ответственности, – сообщил представитель НГУ…» ***(Владимир Кондрашов. Виновного в утечке данных Нацгвардии нашли и обещают наказать // Internetua***

(http://internetua.com/-vinovnogo-v-utecske-dannh-nacgvardii-nashli-i-obesxauat-nakazat). 19.01.2018).

***

«В результате халатности скомпрометированными оказались персональные данные более 45 тысяч абонентов компании «ВОЛЯ».

Об этом на своей странице в Facebook сообщил консультант по кибербезопасности Егор Папышев…

Данные об абонентах включают ФИО, актуальный адрес, контактный телефон, тариф и сведения по некоторым платежам.

Кроме личных данных абонентов, в общей сети, утверждает Папышев, оказались документы, касающиеся финансов, зарплат, продаж и планов, а также рабочая документация и отчетности провайдера...

…эксперт уточнил, что речь идет о халатности сотрудника компании-партнера «Воля» в одном из регионов, имеющего доступ к служебным данным, реестрам и прочей «внутренней» информации провайдера. Сотрудник открыл полный доступ к своему персональному компьютеру (без авторизации и каких-либо механизмов защиты)…

Папышев отметил, что «Воля» достаточно оперативно отреагировала на инцидент…

…Дыра явно закрыта на текущий момент, что, впрочем, никак не уменьшает объема вытекшей информации в течение всего того времени, пока доступ к ней существовал…» ***(Владимир Кондрашов. Персональные данные десятков тысяч абонентов «Воли» ушли в сеть // Internetua (http://internetua.com/persolalnye-danne-desyatkov-tsyacs-abonentov-voli-ushli-v-set). 16.01.2018).***

***

«Фахівці кібербезпеки КП "Благоустрій" виявили махінації в електронній базі підприємства. Про це на своїй сторінці у Facebook заявив директор департаменту реклами і торгівлі Дніпровської міської ради…

"31 грудня 2017 року о 23:00 невідомі підключилися до бухгалтерської бази підприємства по віддаленому доступу та згенерували заднім числом кілька нових договорів на кіоски з комунальним підприємством на невідомого контрагента Вадима Богданова. Самих кіосків в природі немає…", - розповів Руслан Мороз.

Список віддаленого проникнення в базу і послідовності вироблених дій збережені. В КП "Благоустрій" заявили про відкриття кримінального впровдження щодо махінацій в базі…» ***(Дарина ТВАРА. Кіберзпека КП "Благоустрій" виявила електронні махінації в базі // Дніпроград (http://dniprograd.org/2018/01/20/kiberzpeka-kp-blagoustriy-viyavila-elektronni-makhinatsii-v-bazi_64242). 20.01.2018).***

***

«…Хакери атакували сайт ДП «Антонов». Про це 17 січня підприємство повідомило на власній сторінці у Facebook.

Зазначається, що хакери розмістили на новинному розділі так званий відкритий лист до уряду…

Станом на ранок 18 січня сайт підприємства не працює…» (***Концерн «Антонов» заявив про атаку хакерів на свій сайт // Громадсько-правовий портал «Ракурс» (http://racurs.ua/ua/n99809-koncern-antonov-zayavyv-pro-ataku-hakeriv-na-sviy-sayt). 18.01.2018).***

***

Правове забезпечення кібербезпеки в Україні

«Кабмин одобрил Концепцию создания госсистемы защиты критической инфраструктуры…

…Целью Концепции является определение основных направлений, механизмов и сроков комплексного правового урегулирования вопроса защиты критической инфраструктуры и создание системы государственного управления в этой сфере.

Реализация Концепции рассчитана на десятилетний срок (с 2017 по 2027 годы) и предусматривает краткосрочные, среднесрочные, долгосрочные задачи.

Так, предусмотрена категоризация объектов инфраструктуры, относящихся к государственной системе защиты критической инфраструктуры…

Также предусмотрено, что госсистема защиты критической инфраструктуры работает в таких режимах:

– штатный режим функционирования (проведение оценки возможных угроз и анализ рисков, информирование о возможных угрозах);

– защиты и реагирования на случай реализации угрозы (привлечение к ликвидации последствий ресурсов субъектов госсистемы защиты и владельцев объектов критической инфраструктуры);

– функционирования в кризисной ситуации (привлечение ресурсов с целью обеспечения устойчивости функционирования объектов);

– восстановления штатного режима работы и ликвидации последствий кризисной ситуации.

Кроме того, Минэкономразвития совместно с заинтересованными центральными органами исполнительной власти, другими госорганами и учреждениями должно в двухмесячный срок разработать и представить на рассмотрение Кабмина законопроект «О критической инфраструктуре и ее защите»…

Концепция утверждена распоряжением Кабмина от 6 декабря 2017 года № 1009-р.» (***Законопроект о защите критической инфраструктуры разработают до марта // Інформаційне агентство "ЛІГА:ЗАКОН (http://jurliga.ligazakon.ua/news/2018/1/11/167707.htm).- 11.01.2018).***

***

«Решением СНБОУ от 10 июля прошлого года, Кабинет министров Украины должен был в трехмесячный срок урегулировать вопрос о запрете

госучреждениям и организациям государственной формы собственности закупать услуги (заключать договоры) по доступу к сети Интернет у операторов (провайдеров) телекоммуникаций, в которых отсутствуют документы, подтверждающие соответствие системы защиты информации установленным требованиям в области защиты информации…

…Государственной службы специальной связи и защиты информации… на данный момент только осуществляются мероприятия по разработке проекта НПА…, который опубликован на сайте Госспецсвязи только в случае, если Государственная регуляторная служба примет решение о признании этого проекта регуляторным…» (***Владимир Кондрашов. В Украине могут запретить госорганам подключаться к «незащищенным» провайдерам // Internetua (http://internetua.com/v-ukraine-mogut-zapretit-gosorganam-podkluacsatsya-k-nezasxisxennm-provaideram-). 11.01.2018).***

***

Національна система кібербезпеки

«Загалом шість провайдерів станом на кінець 2017 року мають атестати відповідності комплексної системи захисту інформації, які відповідно до рішення Ради національної безпеки і оборони України (РНБО) «Про загрози кібербезпеці держави і невідкладні заходи з їх нейтралізації» надають їм право надавати послуги з доступу до Інтернету держорганам, підприємствам, установам та організаціям державної форми власності…

Так, на кінець 2017 року відповідні документи мають: адміністратор реєстру електронних декларацій, ДП "Українські спеціальні системи" (дійсний до 11 липня 2018 року), Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку (дійсний до 27 травня 2021 року), ПАТ "Укртелеком" (до 22 березня 2021 року), ПрАТ "Датагруп" (до 13 вересня 2022 року), ТОВ "Інфоком" (до 22 липня 2020 року) і ТОВ "Адамант" (до 23 червня 2020 року)…» (***Вимогам РНБО в частині захищеності інтернет-підключення для держорганів відповідають лише 4 приватні провайдери // Інтерфакс-Україна (http://ua.interfax.com.ua/news/economic/476862.html). 15.01.2018).***

***

«Система безпеки та захисту даних Секретаріату Кабінету міністрів України від несанкціонованого втручання складається з кількох підсистем, ...зокрема захисту периметру мережі, захисту мережевих ресурсів ззовні та в периметрі, антивірусного захисту, захисту від DDoS-атак тощо. Обладнання та програмне забезпечення системи безпеки та захисту даних від несанкціонованого втручання постійно оновлюється…

Що стосується витрат на систему захисту, то в Секретаріаті Кабміну запевнили, що до середини березня ця інформація обов'язково буде оприлюднена на Урядовому веб-порталі у розділі «Інформація про бюджет» (***В уряді зробили висновки з попередніх кібератак і посилюють захист // Укрінформ***

(https://www.ukrinform.ua/rubric-technology/2383033-v-uradi-zrobili-visnovki-z-poperednih-kiberatak-i-posiluut-zahist.html). 16.01.2018).

***

«**У Києві Голова СБ України Василь Грицак відкрив Ситуаційний центр забезпечення кібернетичної безпеки, створений на базі Департаменту контррозвідувального захисту інтересів держави в сфері інформаційної безпеки СБУ**…

СБ України у 2017 році отримала технічне обладнання та програмне забезпечення для роботи Центру в рамках виконання першого етапу Угоди про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки.

Ключовими можливостями Центру стануть система виявлення та реагування на кіберінциденти та лабораторія з комп'ютерної криміналістики. Вони дозволять попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії. За підтримки міжнародної спільноти в Україні буде створена мережа ситуаційних Центрів кібербезпеки, базовим з яких стане київський.

Принциповим аспектом роботи ситуаційного центру буде його відкритість для співпраці з усіма суб'єктами забезпечення кібербезпеки: установами, організаціями, підприємствами та профільними фахівцями…» ***(Дмитро Кропивницький. В Києві відкрився Ситуаційний центр забезпечення кібернетичної безпеки // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1711701-v-kiyevi-vidkrivsya-situatsiyniy-tsentr-zabezpechennya-kibernetichnoyi-bezpeki). 26.01.2018).***

***

О Департаменте киберполиции.

«…Среди задач департамента – «организация эффективного противодействия проявлениям киберпреступности и обеспечение действенного влияния на оперативную обстановку, а именно: предотвращение, выявление, прекращение и раскрытие уголовных правонарушений, механизм подготовки, совершение или сокрытие которых предполагает использование компьютеров, телекоммуникационных систем, компьютерных сетей и сетей электросвязи, а также других уголовных правонарушений, совершенных с их использованием», - рассказывают в департаменте…

На сегодня в киберполиции работают 329 человек, или 80% штатной численности.

Кроме того, на службе департамента состоят «белые» хакеры. Они работают в управлениях технологий и программирования, которые входят в состав департамента. Всего таких управлений четыре: в западном, южном, восточном и центральном регионе.

"Белые", или "этичные" хакеры, как правило, ищут уязвимости в компьютерных системах, взламывая их, не с целью украсть или совершить подлог данных, а для того, чтобы устранить уязвимость…

Сотрудники департамента киберполиции круглосуточно поддерживают связь с коллегами по всему миру, обеспечивая процесс немедленного обмена выявленными следами преступной деятельности по результатам реагирования на кибератаки и киберинциденты для оперативного анализа с дальнейшим обобщением полученных результатов и использования их для расследования и противодействию киберугроз…

«Большая часть уголовных правонарушений в платежной сфере происходит во время расчетно-кредитных операций. Одним из самых распространенных видов мошенничества с платежными картами как на территории Украины, так и во всем мире, является мошенничество, совершенное с помощью специальных устройств, таких как скиммер», - говорят в киберполиции…

Не менее распространенным в Украине является фишинг – вид мошенничества, целью которого является выманивание у доверчивых или невнимательных пользователей интернета реквизитов банковских карт…

Также сотрудники департамента ежедневно мониторят интернет на предмет продажи запрещенных в открытом пользовании препаратов и предметов: наркотиков, психотропов, прекурсоров, огнестрельного оружия, боеприпасов, взрывчатки…

Вместе с тем постоянно проводится анализ соцсетей, где на страницах подталкивают несовершеннолетних к самоубийству и телесным повреждениям. На протяжении 2017 года было выявлено 945 так называемых групп смерти, из которых 760 были заблокированы…» **(*Киберполиция: Чем занимаются украинские виртуальные копы // «Днепр Час» (https://dpchas.com.ua/zhizn/kiberpoliciya-chem-zanimayutsya-ukrainskie-virtualnye-kopy). 22.01.2018).***

***

Технічні аспекти кібербезпеки

«…Microsoft заявила, что компания временно приостанавливает работу патчей для защиты безопасности ПК от Meltdown и Specter для компьютеров с чипсетами AMD. Основанием для такого решения стали жалобы клиентов AMD на то, что обновления программного обеспечения заблокировали работу их ПК…

Meltdown и Spectre – это техники, которые позволяют хакерам обходить безопасность операционных систем и другого программного обеспечения для кражи паролей или ключей шифрования на большинстве типов компьютеров, телефонов и облачных серверов.

На прошлой неделе в AMD заявили, что различия между их чипсетами и чипсетами Intel означают, что микросхемы AMD были минимально подвержены атакам Meltdown - ошибку Spectre можно было решить с помощью обновлений программного обеспечения от Microsoft...» (***Ирина Фоменко. Microsoft приостановила работу патчей для защиты от Meltdown и Spectre // Internetua (http://internetua.com/microsoft-priostanovila-rabotu-patcsei-dlya-zasxit-ot-meltdown-i-spectre).- 10.01.2018).***

***

«Некоммерческая организация Wi-Fi Alliance готовит к выпуску новую версию защитного протокола WPA, давно ставшего стандартом для беспроводных сетей…

В частности, версия WPA3 предусматривает использование техники, способной предоставить пользователю надлежащую степень защиты даже в том случае, если тот выбрал пароль, по сложности не соответствующий типовым рекомендациям…

…Также будет облегчен выбор надежной конфигурации для устройств с ограниченным или отсутствующим дисплейным интерфейсом (к примеру, смарт-замков и лампочек)…

…Для усиления защиты критически важных сетей (правительственных, оборонных, промышленных) предлагается использовать алгоритмы шифрования 192-битным ключом из набора Commercial National Security Algorithm (CNSA), рекомендуемого американским Комитетом по национальным системам безопасности (Committee on National Security Systems)...» (***Maxim Zaitsev. WPA3 не за горами // Threatpost (https://threatpost.ru/wpa3-coming-soon-features-announced/23995/). 09.01.2018).***

***

«Исследователи Check Point обнаружили код LightsOut в 22 утилитах и приложениях для использования фонарика. В результате вредоносное ПО скачали от 1,5 млн до 7,5 млн раз. Цель его создателей — незаконное получение дохода от распространения рекламы…

Check Point уведомил Google об обнаруженных вредоносных приложениях, после чего Google оперативно удалил их из каталога Google Play.

LightsOut внедряет вредоносный код Solid SDK в с первого взгляда легитимные служебные программы и приложения-фонарики…» (***В Google Play обнаружен новый вид вредоносной рекламы // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5466968-V-Google-Play-obnaruzhen-novyj-vid.html#ixzz53sgbGVOf).- 10.01.2018).***

***

«Компанія Opera випустила 50-ю версію фірмового браузера. Апдейт включає відразу кілька важливих можливостей, в тому числі націлених на захист користувачів від нового типу зловмисників. …на даний момент Opera 50 знаходиться на стадії бета-тестування…

…Другим і більш значущим [з нововведень] Opera 50 є захист від зловмисників, що використовують комп'ютери користувачів для майнінгу криптовалют…

…В налаштуваннях Opera 50 з'явилася функція NoCoin, що знаходиться в розділі блокування рекламних оголошень…

Повний список змін можна знайти на офіційному сайті Opera» (***В Opera з'явився захист від кріптомайнеров // ООО "Центр інформаційної безпеки"***

(http://www.bezpeka.com/ua/news/2018/01/03/anti-cryptomining-in-Opera.html).- 03.01.2018).

***

«Експерти «Лабораторії Касперського» виявили прихований майнер NiceHash в піратських дистрибутивах популярних програм. Список продуктів включає як платні Adobe FineReader, Outlook, PowerPoint, так і вільне ПЗ на кшталт OpenOffice…

Зловмисники поширюють заражені файли через безліч однакових сайтів, які розрізняються лише назвою продукту, що просувається ПЗ: abby-finereader.ru, thecoreldraw.ru, thevisio.ru…

Автори звіту відзначають, що поширеність прихованих майнерів за останні чотири роки зросла в 8 разів. Тільки в перші три квартали 2017 року «Антивірус Касперського» виявив таке ПЗ майже на 1,7 млн. машин. До кінця року аналітики прогнозують зростання цього показника до 2 млн. комп'ютерів…

Приховані майнери піддають комп'ютер або мобільний гаджет більш серйозним загрозам, ніж проблеми з продуктивністю. Такі програми вміють відключати захисне ПЗ, відстежувати призначену для користувача активність, включаючи запуск додатків, проникати в автозавантаження і переустановлюватися, якщо їх видаляють…

Тим часом суди вже почали виносити перші вироки у справах про приховану установці таких програм. У законодавстві поки немає спеціальної статті, що обумовлює покарання за цей злочин, тому шахраї отримують термін за злом інформаційних систем. Якщо ж майнінг на корпоративних ресурсах вирішить зайнятися власний співробітник компанії, наприклад системний адміністратор, то його можуть звинуватити тільки в крадіжці електроенергії» (***Зловмисники використовують піратське ПЗ для прихованого майнінгу // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/01/03/mining-in-unlicensed-software.html). 03.01.2018).***

***

«Специалисты Facebook разместили на GitHub новый протокол шифрования для групповых чатов – Asynchronous Ratcheting Tree (ART).

…ART решает проблемы безопасности, которые присутствуют в Facebook Messenger, Signal, WhatsApp…

В протоколе используется модель asymmetric prekeys (асимметричные ключи), которая дает абонентам возможность получать защищенные групповые ключи. Кроме того, в ART применяется одноразовый асимметричный ключ настройки, используя который администратор чата при его создании может создавать закрытые ключи для всех участников.

Специалисты подчеркивают, что ART дает возможность ведения защищенной групповой переписки, даже если одного из участников чата скомпрометировали злоумышленники» (***Facebook выпустила новый протокол шифрования для групповых чатов // SecureNews (https://securenews.ru/facebook_art/).- 10.01.2018).***

***

«Ученые Принстонского университета провели эксперименты, чтобы узнать, можно ли на практике осуществить звуковую атаку на жесткий диск…

Специалисты провели эксперименты на жестких дисках систем видеонаблюдения и обычных компьютеров, работающих под управлением Fedora 27, Ubuntu 16 и Windows 10. Выяснилось, что звуковое воздействие на накопители с сигналом определенной частоты влечет временную потерю связи с жестким диском.

Если источник звука находится на очень близком расстоянии, то может понадобиться перезагрузка, при этом в процессе теряются последние данные. Это может стать критичным для камер видеонаблюдения, охранных систем и медицинских аппаратов.

В то же время специалисты подчеркивают, что организовать такие атаки крайне непросто. Так, злоумышленник должен воздействовать на устройство с небольшого расстояния и недолго. Кроме того, подходящие для атаки частоты уловимы для уха человека…» **(*Системы видеонаблюдения можно вывести из строя с помощью звука // SecureNews (https://securenews.ru/sound_attack/).- 08.01.2018).***

***

«Group-IB, международная компания, специализирующаяся на предотвращении кибератак, совместно с АМТ-ГРУП, системным интегратором и разработчиком, объявляют о выводе на рынок решения для обеспечения информационной безопасности и защиты от киберугроз внутри изолированных сегментов сетей крупных корпораций, промышленных предприятий, объектов ТЭК и финансовых организаций.

...Для защиты критической инфраструктуры экспертами компаний Group-IB и АМТ ГРУП было создано технологическое решение, позволяющее разделять сетевые сегменты, анализировать внутренние информационные потоки, «на лету» проверять любую подозрительную активность, выявлять и пресекать попытки проникновения в изолированные сегменты сети или компрометации данных на ранней стадии. Вердикт о степени опасности объекта выносится на основании классификатора, формируемого системой машинного анализа. Таким образом обеспечивается постоянный контроль реальной ситуации, что является необходимым условием при построении управляемой системы безопасности объектов критичной инфраструктуры…» **(*Олег Иванов. Group-IB и АМТ-ГРУП обеспечат безопасность сетевой инфраструктуры // ООО "АМ Медиа" (https://www.anti-malware.ru/news/2018-01-19-1447/25297). 19.01.2018).***

***

«Компании и организации намерены создавать планы по аварийному восстановлению данных, …где будут подробно описываться действия, которые необходимо предпринять для быстрого возобновления критически важных функций компании в случае катастрофы…

…Сам план должен включать следующее:

– Название, краткий обзор и основные цели плана.

– Контактную информацию для ключевых сотрудников и членов команды аварийного восстановления.

– Описание действий по реагированию на чрезвычайные ситуации сразу же после катастрофы.

– Схема всей IT-сети и сайта восстановления.

– Определение наиболее важных IT-активов и максимального времени отключения. Изучите термины «Целевая точка восстановления» (RPO) и «Время восстановления» (RTO). RTO - это время, за которое файлы должны быть восстановлены из резервного хранилища для нормального функционирования после катастрофы.

– Список программного обеспечения, лицензионных ключей и систем, которые будут использоваться в процессе восстановления.

– Техническая документация от поставщиков по программному обеспечению системы восстановления.

– Сводный документ страхового покрытия.

– Предложения по решению финансовых и правовых вопросов, а также информационно-пропагандистской деятельности в средствах массовой информации…

План должен быть под контролем членов команды, ответственных за критическую IT-инфраструктуру внутри компании. Кроме того, с планом должны быть ознакомлены генеральный директор или делегированный старший менеджер, директора, руководители отделов, сотрудники отдела кадров и связей с общественностью.

В плане должны быть указаны и перечислены компании, которые обеспечивают ПО и резервное копирование данных, владельцы объектов, управляющие недвижимостью, сотрудники правоохранительных органов и экстренные службы.

После того, как план будет создан и одобрен руководством, протестируйте его и при необходимости обновите. Обязательно укажите следующий период обзора и/или аудит функций аварийного восстановления…

Если катастрофа все таки случилась, пришло время реализовывать план. Убедитесь, что команда реагирования на инцидент (если она отличается от команды планирования аварийного восстановления) имеет копию плана аварийного восстановления.

Реагирование на инцидент включает в себя оценку ситуации, восстановление систем и последующие действия…» ***(Екатерина Шпачук. Что такое аварийное восстановление данных // Internetua (http://internetua.com/csto-takoe-avariinoe-vosstanovlenie-dannh). 25.01.2018).***

***

«Командою, що спеціалізується на інформаційній безпеці «Project Zero» компанії «Google» досліджено та опубліковано інформацію про надсерйозну апаратну вразливість центральних процесорів компаній виробництва Intel, AMD та процесорів працюючих на архітектурі ARM.

Вразливість дозволяє стороннім програмам отримувати несанкціонований доступ до певних даних в захищеній області пам'яті ядра. При цьому можливе отримання дампа системної пам'яті під час виконання JavaScript…

Данна вразливість, згідно припущень дослідників, не буде залишати жодних слідів після її використання зловмисниками.

…станом на 03 січня 2018 року вразливістю уражені продукти AMD, Apple, Arm, Google, Intel, Linux Kernel, Microsoft, Mozilla…

Департамент кіберполіції України наполегливо просить користувачів комп'ютерної техніки, уважно відслідковувати та негайно встановлювати всі критичні оновлення своїх операційних систем та браузерів…» (***Кіберполіція попереджає про глобальну вразливість, яка зачіпає практично всі процесори незалежно від операційної системи // Портал оперативних новин Varta1 (https://varta1.com.ua/kiberpolitsiya-poperedzhaye-pro-globalnu-vrazlyvist-yaka-zachipaye-praktychno-vsi-protsesory-nezalezhno-vid-operatsijnoyi-systemy/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+varta1news+%28VARTA1%29). 05.01.2018).***

***

«Компания Western Digital обновила прошивку своих портативных сетевых хранилищ (NAS-устройств), чтобы устранить обнаруженные еще в июне бреши. О проблемах стало известно благодаря исследователю компьютерной безопасности Джеймсу Бёрсегею (James Bercegay)…

Три самые значительные уязвимости представляют собой бэкдор на уровне прошивки, возможность несанкционированной записи через PHP-файл на встроенном сервере WM Cloud и брешь типа «подделка межсайтовых запросов», так называемую CSRF-уязвимость.

Любая из них грозит пользователям перехватом контроля над устройством или его настройками, а то и над всей локальной сетью, к которой оно подключено…

Уязвимости найдены в более 10 моделях Western Digital: MyCloud, MyCloudMirror, My Cloud Gen 2, My Cloud PR2100, My Cloud PR4100, My Cloud EX2 Ultra, My Cloud EX2, My Cloud EX4, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100…» **(*Anna Markovskaya. Исправлены критические уязвимости популярных NAS-хранилищ // Threatpost (https://threatpost.ru/western-digital-nas-backdoor-removed/24001/).- 10.01.2018).***

***

«Исследователи безопасности предупреждают, что недавно обнаруженные уязвимости в динамиках, подключенных к интернету, позволяют злоумышленникам определять точки входа в корпоративные сети.

Старший специалист Trend Micro Стивен Хилт объяснил, что сотрудники компании с помощью Shodan обнаружили от 4000 до 5000 динамиков Sonos, а также сотни динамиков Bose, к которым любой человек может получить доступ через интернет…

На практике это значит, что хакеры могут сделать гораздо больше, чем просто получить контроль над устройством. Они могут даже собирать информацию с устройства, находящихся в той же сети, что и динамики…

Другие сценарии атак включают в себя использование раскрытой информации о музыкальных пристрастиях пользователей для создания фишингового письма, предназначенного для отправки на электронный почтовый адрес, прикрепленный к аккаунту в потоковом сервисе.

Эксперты Trend Micro также предупреждают о том, что хакеры могут проводить мониторинг точек беспроводного доступа, к которым устройство пытается подключиться, чтобы отслеживать пользователей и фиксировать, когда они спят или находятся вне дома, чтобы злоумышленники могли совершить ограбление.

Также киберпреступники могут использовать раскрытую информацию для того, чтобы нарушить работу устройства пользователя, и отправить вредоносное письмо, замаскированное под «обновление от разработчика»…

Хотя количество затронутых устройств составляет небольшой процент от общего числа гаджетов, Sonos быстро исправила проблемы, обнаруженные Trend Micro, в то время, как в Bose еще никак не отреагировали на уязвимости» (***«Умные» динамики могут компрометировать корпоративные сети // SecureNews (https://securenews.ru/smart_speakers/).- 04.01.2018).***

***

«Специалисты из компаний IOActive и Embedi выявили 147 уязвимостей в 34 приложениях в Google Play, которые используются вместе с системами SCADA. Используя их, хакер может нарушить производственный процесс, осуществив взлом инфраструктуры предприятия или принудить оператора SCADA неумышленно выполнять действия, которые могут навредить системе…

Всего исследователям было выделено пять самых распространенных уязвимостей: изменение кода для вредоносных целей (94% программ), механизм авторизации, не имеющий должной защиты (59%), реверс-инжиниринг (53%), небезопасные хранилища данных (47%) и незащищенные коммуникации (38%).

IOActive и Embedi сообщили производителям продукции о выявленных проблемах и вместе с некоторыми из них подготовили патчи для приложений» (***Эксперты обнаружили свыше 100 уязвимостей в приложениях для SCADA-систем // SecureNews (https://securenews.ru/scada_vulnerabilities/). 15.01.2018).***

***

«В BitTorrent-клиенте Transmission найдена серьезная уязвимость, которая дает хакерам возможность дистанционно выполнять произвольный код и получать доступ к компьютерам пользователей. По мнению специалиста из Google Project Zero Тэвиса Орманди, …пользователи в большинстве своем не устанавливают пароли, так как считают, что доступ к JSON RPC интерфейсу может быть лишь у того, кто имеет физический доступ к компьютеру с работающим Transmission…

…злоумышленник может поменять каталог загрузки в Transmission на домашнюю папку пользователя и запустить скачивание торрент-файла .bashrc, который автоматически выполняется каждый раз, когда запускается командная оболочка Bash. Также хакер может дистанционно менять настройки Transmission и выполнять любую команду после того, как загрузка будет завершена. По словам эксперта, уязвимостью можно легко воспользоваться.

Орманди сообщил разработчикам о проблеме в конце ноября прошлого года, добавив в свой отчет готовый патч. Но разработчики Transmission не выпустили официальное обновление…

По словам представителей Transmission, официальный патч должен выйти в ближайшее время, но при этом не сообщается о каких-либо сроках его выхода. Как утверждают разработчики, уязвимость можно использовать лишь, если разрешен удаленный доступ и отключена парольная защита» **(*Опасная уязвимость выявлена в BitTorrent-клиенте Transmission // SecureNews (https://securenews.ru/transmission_2/). 16.01.2018).***

***

«…Гуан Гун (Guang Gong), один из ведущих экспертов по кибербезопасности в китайской ИБ-компании Qihoo 360, обнаружил две дыры в системе безопасности Android…

Первая уязвимость — ошибка безопасности движка V8 в браузере Chrome (CVE-2017-5116). Киберпреступники могли эксплуатировать эту брешь для выполнения произвольного кода в процессе system_server. Вредоносный код, таким образом, попадал на устройство через зараженный URL.

Вторую брешь (CVE-2017-14904) специалист нашел в библиотеках Gralloc. В блоге разработчиков Android писали, что ее, вероятнее всего, могли использовать для обхода песочницы.

Обеим брешам присвоен высокий уровень серьезности в рамках общей системы оценки уязвимостей.

Гуну удалось заработать $105 000 в рамках программы вознаграждений за брешь, найденную в Android, и еще $7500 в качестве бонуса по программе поиска уязвимостей в Chrome…» (***Egor Nashilov. Google вручила самую большую награду за поиск багов // Threatpost (https://threatpost.ru/google-awards-record-112500-bounty-for-android-exploit-chain/24190/). 22.01.2018).***

***

«Создатели фреймворка Electron обнаружили в нем уязвимость, которая позволяет запустить в приложениях удаленное выполнение кода.

Под угрозой оказались Skype, Visual Studio Code, GitHub, интернет-браузер Brave, мессенджеры Signal и Slack, интернет-ресурсы Basecamp, WordPress.com, Twitch и другие программы…

Обнаруженная уязвимость CVE-2018-1000006 затрагивает программы, которые в Windows указаны для использования по умолчанию…

Создатели Electron не раскрывают подробностей об уязвимости, но уточняют, что приложения для macOS и Linux остаются в безопасности. Разработчикам, которые работают с Windows, рекомендуется обновить версию фреймворка до 1.8.2-beta.4, 1.7.11 и 1.6.16…

Компания Microsoft уже сообщила, что последняя версия Skype не подвержена уязвимости…» ***(Egor Nashilov. Уязвимый фреймворк угрожает безопасности Windows-приложений // Threatpost (https://threatpost.ru/electron-framework-vulnerability-threatens-windows-apps/24295/). 26.01.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«**Компания Acronis выпустила бесплатное решение, основанное на собственной уникальной технологии, которая помогает пользователям отражать атаки программ-вымогателей с помощью искусственного интеллекта в режиме реального времени и восстанавливать данные без выплаты выкупа.**

…Технология Acronis Active Protection осуществляет мониторинг процессов и приложений в режиме реального времени, что позволяет автоматически выявить и отразить атаки, с которыми не справляются другие решения. В случае атаки программы-вымогателя Acronis Ransomware Protection блокирует вредоносный процесс и уведомляет об этом пользователя через сообщение во всплывающем окне. Если во время атаки будут повреждены какие-либо файлы, решение Acronis поможет пользователям за считанные секунды восстановить эти данные.

Вместе с Acronis Ransomware Protection пользователи получают бесплатное облачное хранилище объемом 5 Гб, для резервного копирования и защиты важных данных не только от вредоносных программ, но и от аппаратных сбоев, стихийных бедствий и иных событий, вызывающих потерю данных.

Acronis Ransomware Protection не потребует от пользователей каких-либо усилий в установке, но поможет избежать множества проблем. Решение занимает всего 20 Мб и практически не требует системных ресурсов, благодаря чему может работать в фоновом режиме, никак не влияя на производительность защищаемой системы…

Для того, чтобы загрузить бесплатную версию Acronis Active Protection, нужно зайти на сайт www.acronis.com и пройти по ссылке для загрузки. На данный момент решение доступно только для ОС Windows.» ***(Искусственный интеллект защитит от программ-вымогателей // ООО "ИКС-МЕДИА"***

(http://www.iksmedia.ru/news/5470786-Iskusstvennyj-intellekt-zashhitit.html#ixzz55a0xwE4I). 25.01.2018).

***

Світові тенденції в галузі кібербезпеки

«Експерти в сфері кібербезпеки та інформаційних систем визначили тренди сфери на 2018 рік…

За даними експертів, У 2018 році …кібератаки з метою розкрадання інформації стануть ще більш масовими.

…Гаджети та мобільні пристрої містять безліч «поломок-лазівок», які є точками входу для кіберзлочинців в хмарний сервіс або інфраструктуру…

Всі сучасні і майбутні атаки будуть проходити від імені легітимних облікових записів, так звана «загроза атаки інсайдера» в новому виконанні, коли зловмисник діє від імені підконтрольного йому облікового запису користувача або технічної служби.

…в Україні збільшиться кількість кібератак, спрямованих на розробників програмного забезпечення, провайдерів IT-сервісів і інших компаній, які надають інформаційні, консалтингові та фінансові послуги.

…Системи онлайн-платежів цікавлять шахраїв, які розробляють способи обходу захисту недосконалих програм.

У зв'язку з цим кількість fraud-атак зростає з геометричною прогресією. За словами експертів, це той канал загроз, на який варто звернути особливу увагу.

Небезпеку становить також таємний майнінг…» ***(У новому році буде більше кібератак — ISSP // Мінфін (https://minfin.com.ua/ua/2018/01/14/31873635/). 14.01.2018).***

***

«…Кибербезопасность 2018: общие тенденции

Для интернета вещей уязвимости станут более критическими и опасными. Несмотря на это, в законодательство США не будет внесено никаких изменений для урегулирования таких устройств. Конгресс сейчас не в состоянии принять даже непротиворечивые законы…

…Общий регламент защиты данных ЕС начнет действовать весной, и Европейские регуляторы начнут вводить его. В регламенте есть положение о безопасности и конфиденциальности, но до сих пор неизвестно, как они будут применяться. Если Европа начнет применять нормы безопасности в интернете со штрафами, которые существенно меняют ситуацию, мы увидим постепенные улучшения безопасности IoT. Если же нет, риски продолжат расти. Талантливые злоумышленники будут использовать подробные метаданные, похищенные изломами в Equifax, OPM и Anthem. И это будет точная целевая атака, которая будет опираться на демографические и психографические алгоритмы Big Data, с участием машинного обучения и искусственного интеллекта...

Демографические и психографические метаданные позволят выполнять передовые операции по фишингу в отношении руководителей критически важных инфраструктур и широкомасштабные операции влияния на население…

…Европа в течение последних двух лет уже претерпела ряд нападений на энергосистемы и производственные мощности. Поэтому в 2018-м, скорее всего, мы столкнемся с мощной атакой на критические инфраструктуры Америки…

Фейковые новости стали главной проблемой 2017 года и, вероятно, ситуация ухудшится в 2018-м. С CGI, фотошопом, технологиями голосового контроля, определить настоящим или поддельным есть фото или видео практически невозможно…

…В условиях фальшивых новостей, промышленность разовьет схему управления репутацией. Это позволит людям подтверждать свою личность через операцию, которая фиксирует взаимодействие только с конкретным человеком, и будет… следить за лицом во всех платформах, доменах и интерактивных форумах. Схема будет работать, даже если человек захочет сохранять анонимность…

То, как хорошие и плохие люди используют искусственный интеллект, в 2018 году изменится… Компании и организации используют машинное обучение и AI, чтобы укрепить свои позиции в области кибербезопасности. То же самое будут делать и …злоумышленники …использовать машинное обучение для ускорения процесс поиска уязвимостей в коммерческих продуктах…

Анализ биометрических поведенческих данных, основанной на AI, станет следующей основной тенденцией в области кибербезопасности и защиты данных. Сложные алгоритмы машинного обучения способны создавать профиль типичного поведения пользователя, определять необычные закономерности деятельности и освещать потенциальные угрозы в режиме реального времени, прежде чем злоумышленники смогут реализовать их…

В 2018-м основная уязвимость уничтожит ценность одной из популярных криптовалют, что повлечет ее эффективное «умирание». Криптовалюты, включая Bitcoin, Ethereum, Litecoin и Monero, сохранят общий рыночный капитал более $ 1 млрд. Это делает их более привлекательной мишенью для хакеров, поскольку их рыночная стоимость ежедневно растет…

…Другой серьезный недостаток обмена криптовалют приведет к существенному снижению стоимости Bitcoin и других основных криптовалют. Также прогнозируется вмешательства правительства в виде положений, которые уже начинают разрабатываться с целью устранения некоторых основных принципов анонимности для уменьшения мошеннического использования.

…Общий ландшафт безопасности в этом году будет сосредоточен вокруг двух вещей: облачных сервисов и IoT. В 2018-м все больше компаний будут принимать принцип «безопасность превыше всего» (security-first thinking). Также компании начнут обучать своих работников того, что представляет собой кибербезопасность…» **(*Какой будет кибербезопасность в 2018 году // ProstoTECH.com (https://prostotech.com/mobilzone/6069-kakoy-budet-kiberbezopasnost-v-2018-godu.html). 21.01.2018).***

***

«**Компания Experian выпустила очередной прогноз по противодействию утечке данных, где определены ключевые тенденции этого года…**

…киберпреступники станут расширять атаки на физические цели, включая критическую инфраструктуру. Первыми ощутят на себе это развитые страны. …угроза реальна на всех уровнях, от властей до рядовых граждан…

В России, по мнению экспертов, наиболее очевидной целью являются объекты энергетической и нефтяной отраслей. Попытки взлома ядерных объектов маловероятны, поскольку их IT-системы не связаны с глобальными сетями… А военные объекты уже подвергаются нападениям со стороны киберармий других стран, но пока в рамках учений…

…Для защиты бизнеса, государства и личности эксперты по-прежнему рекомендуют только использовать максимально продвинутые системы кибербезопасности…» ***(Как киберпреступления угрожают жизни // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3522047?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 17.01.2018).***

***

«…Опрос руководителей ИТ-служб государственных учреждений, проведенный аналитической фирмой Gartner, показал, что на 2018 год увеличение расходов ими планируется в первую очередь в сферах облачных технологий, кибербезопасности и аналитики…

Главной задачей опрошенные считают цифровую трансформацию. За ней по важности следуют безопасность и контроль…

…Важнейшими для выполнения этих задач технологиями руководители считают облачные сервисы и бизнес-аналитику. Технологии искусственного интеллекта по итогам опроса оказались лишь на 19-м месте, тогда как в частном секторе они находятся в десятке самых важных…» ***(Gartner: в 2018 году госсектор повысит расходы на облака, кибербезопасность и аналитику // «Открытые системы» (https://www.computerworld.ru/news/Gartner-v-2018-godu-gossektor-povysit-rashody-na-oblaka-kiberbezopasnost-i-analitiku). 26.01.2018).***

***

«Израильская компания кибербезопасности VDOO сегодня собрала $13 миллионов стартового капитала. Это позволит старпапу, основанному в городе Герцлия, создавать системы, которые защитят так называемый «интернет вещей» (Internet of Things, IoT).

…Система будет анализировать устройства пользователей, обеспечивать их необходимыми условиями для безопасной работы и контролировать права доступа…» (***VDOO: Израильская компания кибербезопасности собрала $13 млн. стартового капитала // ISRAland (http://www.isra.com/news/210306). 17.01.2018).***

***

«…На днях BlackBerry представила облачный сервис под названием Jarvis, который и будет искать слабые места в системах управления

беспилотными автомобилями. Как заверяют авторы, новая программа будет сканировать и определять слабые места в системе кибербезопасности самоуправляемых авто за несколько минут…

С системой Jarvis смогут работать абсолютно все автопроизводители… BlackBerry уже начала тестирование нового продукта, а одним из первых партнеров компании стал Jaguar Land Rover.» (***BlackBerry займется поиском уязвимостей в самоуправляемых авто // 1NEWS.INFO (https://www.1news.info/blackberry-%d0%b7%d0%b0%d0%b9%d0%bc%d0%b5%d1%82%d1%81%d1%8f-%d0%bf%d0%be%d0%b8%d1%81%d0%ba%d0%be%d0%bc-%d1%83%d1%8f%d0%b7%d0%b2%d0%b8%d0%bc%d0%be%d1%81%d1%82%d0%b5%d0%b9-%d0%b2-%d1%81%d0%b0%d0%bc-420726). 18.01.2018).***

***

«…В Женеве будет открыт новый Глобальный центр кибербезопасности, призванный помочь противостоять киберугрозам и объединить бизнесменов и представителей власти для сотрудничества по различным вопросам безопасности, а также обмену передовым опытом. О создании центра было объявлено в рамках Всемирного экономического форума в Давосе.

Центр будет работать как автономная международная организация, действующая под покровительством Всемирного экономического форума. Учреждение планирует начать свою работу в марте 2018 года. Основной задачей центра станет формирование каналов обмена информацией между правительствами и частными компаниями на добровольной основе…

…помимо предоставления канала связи для влиятельных фигур, центр будет эффективно консолидировать некоторые из других инициатив ВЭФ, связанных с кибербезопасностью…

Глобальный центр кибербезопасности уже получил поддержку нескольких известных компаний и правоохранительных организаций, в том числе британского телекоммуникационного гиганта BT Group, производителя микрочипов Qualcomm, российского «Сбербанка» и Интерпола…» ***(ВЭФ анонсировал создание Глобального центра кибербезопасности // SecurityLabRu (https://www.securitylab.ru/news/491033.php). 25.01.2018).***

***

«…24 января 2018 года стало известно об очередном приобретении ИТ-гиганта [Cisco] - им стал калифорнийский стартап Skyport Systems, разработавший платформу для особо защищенных серверов SkySecure Server.

Финансовые условия сделки не разглашаются…

«Благодаря приобретению Cisco сможет использовать интеллектуальную собственность Skyport и опыт в области программных и сетевых решений для ускорения развития своих приоритетных направлений», - написал в блоге компании вице-президент Cisco по корпоративному развитию Роб Сальваньо» ***(Cisco покупает разработчика платформы сверхзащищенных серверов Skyport Systems // ChannelForIT (http://channel4it.com/publications/Cisco-pokupaet-***

razrabotchika-platformy-sverhzashchishchennyh-serverov-Skyport-Systems-29272.html#). 29.01.2018).

***

«**Google запустила новое подразделение, которое будет продавать компаниям из списка Fortune 500 программное обеспечение для обеспечения кибербезопасности.**

Новая инициатива должна помочь американскому интернет-гиганту укрепить позиции в секторе корпоративных ИТ.

Новое подразделение под названием Chronicle вышло из экспериментального подразделения Google X и теперь является отдельной компанией в составе материнского холдинга Alphabet. Chronicle сделает ставку на софт, которое базируется на машинном обучении и позволяет анализировать большие массивы данных на предмет кибербезопасности оперативнее и точнее, чем это делают традиционные системы.

Chronicle начал предлагать два сервиса: платформу безопасности и аналитики для предприятий и онлайн-сканер вирусов и вредоносного ПО VirusTotal. Новая платформа работает на основе инфраструктуры Alphabet и будет использовать машинное обучение и расширенные возможности поиска для помощи компаниям в анализе безопасности…

Представители Google пока не готовы делиться подробной информацией о работе нового подразделения и количестве компаний, участвующих в альфа-тестировании проекта…» ***(Google запустила подразделение кибербезопасности // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5470968-Google-zapustila-podrazdelenie-kibe.html#ixzz55a3K3SRS). 26.01.2018).***

***

«…Group-IB проанализировала основные риски информационной безопасности для криптоиндустрии и составила рейтинг основных угроз для ICO (первичное размещение криптовалюты).

…Согласно данным Group-IB, каждое ICO атакуют в среднем около 100 раз в течение месяца...

Подводя итоги года по направлению защиты проектов, связанных с криптовалютами, в Group-IB составили рейтинг наиболее опасных угроз для индустрии:

I место. Фишинг. Этот вид мошенничества по-прежнему представляет самый опасный тип угроз. На его долю приходится более 50% всех похищенных средств. По данным Group-IB, крупная фишинговая группировка похищает от $30,000 до $1,500,000 в месяц… Под угрозой не только проекты, выходящие на ICO, но также трейдеры, крипто-энтузиасты и другие владельцы криптовалют.

2 место. Дефейс или целенаправленные атаки. Ошибки в конфигурации серверов веб-приложений, компрометации паролей от хостинга или же использование уязвимого программного обеспечения являются одними из самых распространенных причин взлома. Злоумышленникам удается подменить адрес кошелька, на который производится сбор средств…

3 место. Атаки с «социальным вектором». В эту категорию в Group-IB включили атаки на членов команд проектов и воровство монет у представителей комьюнити через социальные сети, тематические форумы и медиа-ресурсы. В последние месяцы 2017 года и в начале 2018 специалисты Group-IB фиксируют всплеск мошенничеств в социальных сетях…

Эксперты Group-IB подтвердили… ажиотаж вокруг блокчейна и криптовалют вызвал повышенное внимание к ним со стороны киберпреступников. В ушедшем году произошли десятки крупных успешных атак на криптовалютные сервисы, показавших, что злоумышленники адаптировали схемы атаки на банки и используют тот же инструментарий для взлома криптобирж, кошельков и атак на пользователей…

…Основываясь на данных собственных проектов и изучении мирового опыта, в компании прогнозируют следующие векторы развития угроз для криптовалютных проектов:

– Мошеннические фишинг-схемы с использованием крипто-брендов будут усложняться…

– Социальные векторы атак будут развиваться: мишенью хакеров все чаще будут сами фаундеры, члены команды проектов и участники сообществ.

– Увеличится число хищений у владельцев монет…

– Android-трояны будут атаковать владельцев криптовалют…

Общий вывод: хакеры считают проекты, выходящие на ICO, легкой наживой, тогда как эта модель привлечения средств теперь привлекает миллиарды долларов. Некоторые проекты, как указывается в отчете, привлекали в ходе ICO по $300,000 в секунду» ***(В среднем в ходе каждого ICO совершается более 100 атак // ООО "ИКС-МЕДИА"(http://www.iksmedia.ru/news/5470613-V-srednem-v-xode-kazhdogo-ICO-sover.html#ixzz55a038OSI). 25.01.2018).***

***

Сполучені Штати Америки

«Инициативная группа законодателей заподозрила китайские смартфоны Huawei Mate 10 в возможности вести слежку за пользователями… и направила письмо в Федеральную комиссию по связи США…

В этой связи один из крупнейших американских операторов мобильной связи AT&T отказался от продаж смартфонов Huawei Mate 10…

Американские законодатели и ранее озвучивали подобные обвинения. К примеру, в отчете 2012 году комитета Палаты представителей по разведке от 2012 года указывается, что две китайские компании, в том числе Huawei, представляют угрозу нацинальной безопасности США. В свою очередь, руководство Huawei неоднократно категорически опровергало обвинения подобного характера…» **(*В США китайские смартфоны заподозрили в шпионаже // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120658). 11.01.2018).***

***

«…2018 рік і прогрес, який відбувається в теорії штучного інтелекту, а також у кібербезпеці, вказує на те, що необхідно бути готовим до неочікуваного повороту подій. Більше 50% фахівців з інформаційної безпеки компанії Cylance вважають, що вже починаючи з цього року, хакери безсумнівно почнуть використовувати штучний інтелект, як кіберзброю…» (***Грицина Вікторія. Штучний інтелект керуватиме хакерськими атаками // Pingvin.Pro (https://pingvin.pro/gadgets/news-gadgets/shtuchnyj-intelekt-keruvatyme-hakerskymy-atakamy.html).- 02.01.2018).***

***

«У 2017 році спеціалісти ФБР США не змогли отримати доступ до більш ніж половини електронних пристроїв, які використовувались для планування терористичних або кримінальних дій, через використання на них різних інструментів шифрування інформації

ФБР США не змогло дослідити інформацію на понад 7,8 тис. пристроях. Про це заявив директор Федерального бюро розслідувань Крістофер Рей під час виступу на міжнародній конференції з питань кібербезпеки…

Очільник ФБР також додав, що ФБР підтримує шифровку даних, але зауважив, що програми забезпечення безпеки інформації мають створюватись так, щоб не підривати здатність Бюро забезпечувати безпеку США» (***ФБР не змогло отримати доступ до майже 8 тис. пристроїв підозрюваних через шифрування інформації // «Ракурс» (http://racurs.ua/ua/n99650-fbr-ne-zmoglo-otrymaty-dostup-do-mayje-8-tys-prystroyiv-pidozruvanyh-cherez-shyfruvannya). 14.01.2018).***

***

«В Сети обнаружена фотография, на которой один из сотрудников Гавайского агентства по чрезвычайным ситуациям позирует на фоне мониторов…

… К одному из экранов прикреплена заметка с написанным на ней паролем. На другом мониторе можно увидеть еще одну заметку, напоминающую пользователю как выйти из учетной записи.

По словам представителя ведомства, пароль настоящий и использовался для «внутреннего приложения», которое, насколько ему известно, больше не используется…

…фотография вызвала у пользователей ряд вопросов по поводу серьезности подхода агентства к организации информационной безопасности» (***Гавайское агентство по чрезвычайным ситуациям хранило пароль в открытом доступе // SecurityLab.ru (https://www.securitylab.ru/news/490858.php). 17.01.2018).***

***

«Великі технологічні компанії SAP, Symantec і McAfee дозволили російським властям вишукувати уразливості в ПЗ американського уряду

Це встановило розслідування, проведене агентством Reuters…

Ця практика створила потенційну загрозу для безпеки комп'ютерних мереж щонайменше десятка федеральних відомств, відзначають американські законодавці і експерти з безпеки…

Щоб забезпечити собі можливість працювати на російському ринку, технологічні компанії дозволяли російському оборонному відомству переглядати вихідні коди деяких своїх продуктів. Російська влада наполягає, що це необхідно для виявлення дефектів, якими можуть скористатися хакери.

Однак ті ж продукти використовуються і деякими американськими відомствами, пов'язаними з підвищеною секретністю - Пентагоном, Державним департаментом, ФБР і розвідувальними службами, - для захисту від хакерських атак з боку таких супротивників, як Росія…

…не менше восьми агентств використовують продукти SAP, Symantec і McAfee, з кодами яких ознайомилися російська влада. У деяких відомствах використовували більше одного з чотирьох продуктів.

McAfee, SAP, Symantec і британська фірма Micro Focus, якої тепер належить ArcSight, відзначають, що перегляд вихідних кодів проводився під наглядом виробника ПО на безпечних об'єктах, де код неможливо було видалити або змінити. Вони наполягають, що цей процес не компрометує безпеку продукту.

На тлі наростаючого занепокоєння з приводу цього процесу Symantec і McAfee вирішили припинити цю практику, а Micro Focus збирається різко обмежити її в кінці наступного року…

Агентство Reuters не виявило випадків, коли вихідний код зіграв якусь роль в кібератаки» ***(SAP, Symantec і McAfee розкрили вихідні коди російській владі, - Reuters // Espreso.tv (https://espreso.tv/news/2018/01/26/sap_symantec_i_mcafee_rozkryly_vykhidni_kody_rosiyskiy_vladi_reuters). 26.01.2018).***

***

«Власти США рассматривают возможность создания внутри страны защищенной сверхскоростной мобильной сети 5G для предотвращения возможной киберугрозы со стороны Китая…

Проект предусматривает создание централизованной сети 5G в течение трех лет. В ближайшие шесть-восемь месяцев, в частности, будет обсуждаться финансирование проекта.

Рассматриваются два варианта реализации - создать подобную сеть силами правительства или поручить это американским сотовым операторам…

По мнению американского руководства, создание подобной сети необходимо для того, чтобы обезопасить использование перспективных технологий, таких как беспилотные автомобили и виртуальная реальность, а также противостоять угрозе со стороны Китая в экономической и кибернетической сферах…» ***(США планируют создать безопасную сеть 5G для защиты от китайской киберугрозы // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5471348-SSHA-planiruyut-sozdat-bezopasnuyu.html#ixzz55a63rujV). 29.01.2018).***

***

«Європейська комісія оголосила про плани інвестування спільно з державами-членами ЄС у створення європейської інфраструктури суперкомп'ютерів світового рівня…

Нова фінансова та юридична структура - спільне підприємство EuroHPC - реалізує і розгорне в ЄС інфраструктуру розрахунків високого ступеня ефективності світового рівня.

EuroHPC буде також підтримувати програму досліджень і інновацій з метою розвитку технологій і інформаційної техніки, а також програмного забезпечення для суперкомп'ютерів.

Внесок ЄС у EuroHPC складе близько 486 млн євро до 2020 року з чинного в даний час багаторічного фінансового плану Євросоюзу. Аналогічну суму додадуть держави-члени та асоційовані з ЄС країни» (***ЄС інвестує 1 млрд євро у створення інфраструктури суперкомп'ютерів // Європейська правда (http://www.eurointegration.com.ua/news/2018/01/11/7075936/).- 11.01.2018).***

***

«Государственные структуры Литвы и информационные системы особой важности отказались от программного обеспечения российского производителя антивирусов «Лаборатории Касперского»…

Распоряжение, требующее отказаться от этой продукции, во второй половине декабря 2017 года приняло правительство Литвы. По утверждению властей, программы «Касперского» несут «потенциальную угрозу национальной безопасности и пользующимся им информационным инфраструктурам особой важности». Их должны заменить в течение 90 дней.

Антивирусами «Касперского» пользовалось около 5% госучреждений…

Как отметили в самой «Лаборатории», они продолжат оказывать услуги своим клиентам в Литве, несмотря на введенные властями ограничения» ***(Госструктуры Литвы отказались от программ «Лаборатории Касперского» // ЖурДом (http://jourdom.ru/news/99896). 29.01.2018).***

***

Російська Федерація

«…Государство пригласит исследователей поискать уязвимости в IT-системах — это отражено в плане мероприятий по информационной безопасности программы «Цифровая экономика Российской Федерации». Минкомсвязь, ФСБ и ФСТЭК по инициативе Сбербанка и компании InfoWatch разработали план до 2020 года, а первые проверки начнутся в апреле 2018 года.

…На поиск уязвимостей до конца 2020 года планируется выделить 800 миллионов рублей, в том числе 500 миллионов рублей из бюджета. Отвечать за поиск уязвимостей, начать который планируется в апреле, будет Центр

компетенций по импортозамещению в сфере информационно-компьютерных технологий.

Предполагается два вида проверок — с предварительным уведомлением разработчика системы и без него…

…тестироваться будут государственные IT-системы и IT-продукты вендоров…

Принять участие в тестах смогут как компании, так и частные лица, вроде хакеров…» ***(Хакерам заплатят из бюджета в рамках программы «Цифровая экономика» // РосКомСвобода (https://roskomsvoboda.org/35084/).12.02.2018).***

***

«Закон «О критической информационной инфраструктуре» (КИИ), вступивший в силу 1 января 2018 года, полноценно пока не заработал. Причина - в отсутствии подзаконных актов.

…Часть документов уже принята, а ряд проектов еще находится в финальной стадии подготовки, говорит руководитель операционного направления центра мониторинга и реагирования на кибератаки Solar JSOC Антон Юдаков. Среди них — документы, касающиеся категорирования, требований к защите и контролю безопасности объектов критической информационной инфраструктуры (КИИ)…

…на рассмотрении находится проект постановления правительства о порядке госконтроля за обеспечением безопасности значимых объектов КИИ, разработанный Федеральной службой по техническому и экспортному контролю (ФСТЭК). В нем указано, что госконтроль осуществляется путем плановых и внеплановых выездных проверок со сроками проведения до 20 и 10 рабочих дней соответственно…

Можно ожидать появления в разработке и новых документов, прежде всего в направлении предупреждения атак, а также более широкого использования существующей на рынке экспертизы в рамках государственно-частных партнерств…» (***Защите от кибератак не хватает подзаконных актов // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5469326-Zashhite-ot-kiberatak-ne-xvataet.html#ixzz54vqpPDTf). 19.01.2018).***

***

«Все служебные компьютеры Минобороны РФ могут быть переведены с операционной системы Microsoft на отечественную Astra Linux…

…за внедрение операционных систем отвечают два главных управления ведомства — связи и развития информационных технологий. Если новая ОС будет соответствовать требованиям военных, ее установят на все компьютеры в министерстве…

…система Astra Linux на протяжении нескольких лет используется Вооруженными силами РФ, в частности, на ней базируется информационная система Национального центра управления обороной РФ…» (***Компьютеры Минобороны могут перевести на российское ПО // РИА Новости (https://ria.ru/defense_safety/20180109/1512265092.html - 09.01.2018)***

***

«Центр компетенций по кибербезопасности при Сбербанке провел «диагностику» актуальных проблем в области кибербезопасности в России, после чего был выработан план действий.

Сбербанк определил 500 мероприятий для обеспечения кибербезопасности в рамках госпрограммы «Цифровая экономика»…

…этот план был направлен в правительство» ***(Сбербанк разработал план из 500 мероприятий для национальной кибербезопасности // «Открытые системы» (https://www.computerworld.ru/news/Sberbank-razrabotal-plan-iz-500-meropriyatiy-dlya-natsionalnoy-kiberbezopasnosti). 24.01.2018).***

***

«**Власти могут заставить компании страховаться от утечки персональных данных**. … к середине лета Минфин, Минкомсвязи и Роскомнадзор должны решить, нужно ли оговаривать это законодательно. Подобное требование может коснуться огромного количества игроков рынка — от онлайн-магазинов до кредитных организаций…

Руководитель Агентства кибербезопасности Евгений Лифшиц считает, что защититься от них с помощью подобной меры невозможно, а дополнительную финансовую нагрузку бизнес переложит на потребителей…

Идея страхования от утечки персональных данных, в принципе, правильная, но на сегодняшний день нереализуемая, считает генеральный директор агентства разведывательных технологий «Р-Техно» Роман Ромачев...

Пока страховой рынок не определился, будет ли страхование рисков утечек персональных данных перспективным или нет. Но, скорее всего, желающие занять эту нишу найдутся, убежден заместитель генерального директора страховой компании «Ресо Гарантия» Игорь Иванов…

По данным InfoWatch, в России чаще всего утечки персональных данных происходят из государственных органов, компаний высокотехнологичного сектора, образовательных учреждений и банков» ***(Андрей Загорский. Персональным данным «выпишут» страховку // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3520927?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82% D1%8C). 15.01.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«**Анатолий Аксаков, председатель комитета Госдумы по финансовому рынку, планирует предложить президенту Америки Дональду Трампу создать общий штаб по кибербезопасности в рамках G-20. ..**в ходе визита господина Аксакова в Соединенные Штаты появится возможность обсудить двусторонние отношения с американскими конгрессменами. «У нас есть много поводов для

беседы. Особенно по теме кибербезопасности, если учесть, что американские власти обвиняют российских хакеров в кибератаках. Я считаю, что должен быть единый штат в рамках "двадцатки" по кибербезопснсти и общими подходами к регулированию вопросов, реакции на действия хакеров», — говорит Аксаков…» ***(Олег Иванов. Госдума предложит Трампу создать штаб по кибербезопасности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-01-25-1447/25357). 25.01.2018).***

***

Кіберзахист критичної інфраструктури

«За результатами досліджень спеціалістів ESET, у 2018 році слід очікувати атаки на об'єкти критичної інфраструктури та електронні системи голосування, нові виклики безпеці конфіденційних даних та подальше поширення програм-вимагачів.

…На думку спеціалістів ESET, атаки на ланцюг постачання продовжаться і в 2018 році.

«Попри те, що сьогодні багато великих компаній більш відповідально ставляться до власної кібербезпеки, а IT-спеціалістам виділяються значно більші бюджети для захисту корпоративної мережі, залишається велика кількість малих підприємств, які постачають товари та послуги великим організаціям і не мають таких можливостей, як наслідок, саме такі невеликі компанії є привабливою ціллю для кіберзлочинців»,— розповідають спеціалісти ESET.

Від технічного прогресу відстає також безпека електронних систем голосування. Технологічне втручання у виборчий процес може спричинити серйозні проблеми для забезпечення легітимності виборів у майбутньому. З цією метою всі аспекти виборчої системи повинні розглядатися як частина найважливішої інфраструктури кожної країни і мають бути захищені належним чином.

Ще однією поширеною проблемою у наступному році може стати конфіденційність даних звичайних користувачів. Постачальники програмного забезпечення збирають усе більше особистої інформації власних споживачів, використовуючи її з метою наживи. Фактично сьогодні дані стали новою «валютою» для користувачів за використання дешевого або безкоштовного програмного забезпечення. У наступному році проблема захисту конфіденційної інформації може стати актуальною також для пристроїв Інтернет-речей, здатних збирати інформацію про різні сфери життя користувача…» (***Стало відомо, хто стане жертвою хакерів у 2018 році // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/stalo-vidomo-hto-stane-zhertvoyu-hakeriv-u-2018-rotsi.html).- 02.01.2018).***

***

«Експерти допускають, що уразливості в системах управління ядерними арсеналами можуть призвести до катастрофічних наслідків.

Достатньо розумна кібератака проти Великої Британії чи будь-якої іншої ядерної країни може призвести до того, що помилково буде завданий ядерний удар…

За гіршим сценарієм, на думку експертів аналітичного центру Chatham House, кібератака може призвести до умисної дезінформації і випадкового застосування ядерної зброї…

Експерти зауважують, що ядерні сили країни будували ще до того, як з'явився інтеренет і сучасні передові технології. Тож не рідко питання кіберзахисту цифрових систем в структурі ядерних арсеналів не отримує потрібної уваги» ***(Кібератака може стати причиною ядерної війни - The Times // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/kiberataka-mozhe-stati-prichinoyu-yadernoyi-viyni-the-times-265845_.html). 11.01.2018).***

***

«Приложение для занятий спортом Strava (оно при помощи трекера дает возможность бегунам, велосипедистам и лыжникам записывать свой маршрут и делиться им в Сети) случайно "рассекретило" военные базы на всей планете.

Компания выложила в Сеть карту мира со всеми маршрутами, которые пользователи приложения пробежали или проехали за два года его существования (таких маршрутов примерно 1 млрд.). Как оказалось, на карту попали не только маршруты обычных любителей спорта, но также американских солдат, которые пользуются трекерами и часто не снимают их целый день…

…Пресс-секретарь Пентагона (военного командования США) Одрисия Харрис заявила, что американские военные крайне серьезно относятся к ситуации с картами и намерены определить, нужно ли усилить безопасность в связи с использованием фитнес-трекеров.

Представители Strava в ответ на это заявили, что …опубликованную карту маршрутов они считают в достаточной степени "анонимизированной".

Всего на Strava, по данным компании, зарегистрированы 27 млн. бегунов, велосипедистов, лыжников и других любителей спорта» (***Фитнес-приложение для бега "рассекретило" военные базы по всему миру (https://www.currenttime.tv/a/29004462.html) 29.01.2018).***

***

Кіберзлочинність та кібертероризм

«…Исследование под названием «Глобальные риски – 2018» было представлено на Всемирном экономическом форуме в Женеве…

Авторы исследования призывают правительства разных стран кооперироваться в борьбе с международными хакерскими группировками, а также подключить к процессу технологические компании, специализирующиеся на изучении и предотвращении атак. Эксперты предупреждают, что ошибочное определение источника кибератак может привести к удару по непричастным странам, а в крайнем случае – к применению обычного вооружения.

В этой связи специалисты настаивают на выработке правовых норм для кибервойн по аналогии с вооруженными конфликтами…

Кроме того, специалисты ВЭФ призывают подумать над международным запретом на применение отдельных классов кибератак» (***Эксперты предрекли Интернету скорое разрушение // ООО «Медиахолдинг «Репортер» (http://reporter-ua.com/2018/01/18/326167_eksperty-predrekli-internetu-skoroe-razrushenie). 18.01.2018).***

***

«…Растущая популярность кибератак изменила всю картину корпоративной преступности в мире. К такому выводу пришли эксперты нью-йоркской исследовательской и консалтинговой компании Kroll… Уровень киберпреступности непрерывно растет с 2012 года, однако в минувшем году число тех, кто хоть раз подвергся кибератаке, достигло рекордного уровня — 86% опрошенных компаний по всему миру… При этом более половины компаний, опрошенных исследователями Kroll, считают, что их компании «подвержены или очень подвержены» краже информации.

4 из 10 опрошенных руководителей считают, что их компании в минувшем году подвергались атаке вирусов, второй по популярности вид атак с применением вредоносных программ — фишинговые атаки по электронной почте…» ***(Евгений Хвостик. Кибератаки вывели корпоративную преступность на новый уровень // АО«Коммерсантъ»(https://www.kommersant.ru/doc/3527218?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 22.01.2018).***

***

«Издание The Tribune в ходе журналистского расследования смогло получить незаконный доступ к системе биометрических данных Агентства Индии по уникальной идентификации (UIDAI), заплатив за это всего 500 рупий, то есть около $8.

Журналистам понадобилось 10 минут, чтобы найти в тайном чате в мессенджере WhatsApp дилера, который продал им логин и пароль для входа на сайт UIDAI, где находятся персональные данные пользователей. За дополнительные 300 рупий, то есть около $5, дилер предоставил софт для изготовления биометрической ID-карты пользователя UIDAI.

Система UIDAI закрепляет за каждым жителем Индии уникальный двенадцатизначный номер под названием Aadhaar. К нему привязаны имена, фамилии, адреса, телефонные номера и банковские данные физических лиц, а также их биометрические параметры — отпечатки пальцев и сканы радужной оболочки глаза. Всего в систему Aadhaar занесено более миллиарда граждан…

Исследователи безопасности, изучившие инцидент, полагают, что журналисты The Tribune получили доступ к сайту UIDAI на правах администрирования, а именно — для обработки обращений от пользователей, заметивших опечатку в своем имени или адресе. Администратор имеет право

устранить такую опечатку, однако доступа к биометрическим данным при этом не получает.

Таким образом, приобретенные за $8 логин и пароль оказываются бесполезны для фальсификации денежных транзакций, поскольку банки требуют их биометрического подтверждения. Сама UIDAI также утверждает, что доступа к биометрии получено не было, поэтому заключенная в WhatsApp сделка не опасна для системы Aadhaar. Тем не менее, UIDAI пожаловалась на The Tribune в правоохранительные органы за приобретение нелегального доступа к базе.

Однако The Tribune пишет, что представители UIDAI в Чандигархе, с которыми связалось издание, были «шокированы», когда узнали, что приобретенные логин и пароль дают доступ к уникальным двенадцатизначным номерам, именам, адресам, телефонным номерам, адресам электронной почты и фотографиям граждан Индии…

Отследить дилера, действовавшего на условиях анонимности, пока что не удалось…» (***Крупнейший в мире банк биометрических данных взломан за $8 и 10 минут // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5467221-Krupnejshij-v-mire-bank-biometriche.html#ixzz53si0rb00).- 11.01.2018).***

***

«…в Бюро расследований Министерства юстиции Тайваня признали, что раздавали USB-накопители, зараженные вредоносной программой, в ходе конференции по безопасности, которая проходила 11-15 декабря прошлого года.

Устройства выдавались в качестве призов для победителей викторины по кибербезопасности. Всего было выдано 250 накопителей объемом в 8 гигабайт. 54 из них были заражены вредоносным ПО XtbSeDuA.exe.

Программа осуществляла сбор персональных данных пользователей и передавала их на IP-адрес в Польше…

Как утверждают в Бюро, накопители были приобретены у подрядчиков. Несмотря на то, что часть устройств были произведены в материковом Китае, ведомство исключает версию шпионажа со стороны властей КНР. 54 накопителя были заражены после того, как их подключили к инфицированному компьютеру, который сотрудник компании-подрядчика задействовал для того, чтобы перенести операционную систему на устройства и проверить их емкость.

После жалоб пользователей 12 декабря Бюро расследований прекратило раздавать «призы», однако в итоге удалось вернуть лишь 20 из 54 накопителей» (***Полиция Тайваня раздавала на конференции по безопасности USB-накопители с вирусами // SecureNews (https://securenews.ru/taiwan/).- 10.01.2018).***

***

«Эксперты из Rhino Labs описали новую методику хищения учетной информации Windows с применением малоизвестного функционала в Microsoft Word – subDoc, который дает возможность загружать документ в тело другого документа. Кроме того, эта функция может быть использована для

дистанционной загрузки файлов в основной документ, что дает возможность применять его в криминальных целях.

Новая методика основана на атаке типа Pass-the-hash, позволяющей хакеру пройти авторизацию на удаленном сервере, где аутентификация производится с помощью протокола NTLM или LM. Эта методика может быть использована на любом сервере и сервисе, который работает с протоколом аутентификации NTLM или LM, вне зависимости от операционной системы на компьютере жертвы...

Как утверждают специалисты, в настоящее время описанная ими методика атаки пока не получила широкой известности, поэтому антивирусы не могут распознать ее…» (***Малоизвестный функционал Microsoft Word может применяться для хищения паролей // SecureNews (https://securenews.ru/subdoc/).- 09.01.2018).***

***

«Жителя Огайо Филлипа Дурачински в среду обвинили в незаконной слежке и сборе данных с компьютеров граждан и организаций США…

В ходе следствия было установлено, что 28-летний хакер в течение 13 лет собирал информацию из систем, принадлежащих частным лицам, школам, полиции и даже Министерству энергетики США.

Установлено, что мужчина собирал широкий спектр информации с компьютеров, включая банковские рекорды, фотографии, поисковые запросы в Интернете и потенциально смущающие сообщения.

Чтобы получить доступ к конфиденциальной информации хакер удаленно подключался к камерам и микрофонам, установленным на компьютеры его жертв…» (***Американский хакер 13 лет следил за людьми через компьютеры // Украинское рейтинговое агентство "УРА" (http://ura-inform.com/ru/society/2018/01/11/amerikanskij-khaker-13-let-sledil-za-ljudmi-cherez-kompjutery). 11.01.2018).***

***

«15-летний подросток из Британии, притворившись главой ЦРУ, получил доступ к планам разведывательных операций в Афганистане и Иране…

Молодой человек Кейн Гэмбл… использовал «социальную инженерию» (манипулятивный метод получения необходимой информации), чтобы получить доступ к личным и рабочим аккаунтам глав авторитетных разведывательных структур США.

В частности, Гэмбл …назывался министром Национальной безопасности США и главой Национальной разведки при президентстве Барака Обамы.

В ходе судебных заседаний стало известно, что подросток …публиковал личную информацию жертв, терроризировал их звонками и сообщениями, скачивал порнографию на их компьютеры и контролировал их планшеты и телевизоры…

Сам Гэмбл признал себя виновным в совершении десяти преступлений. Среди которых – получение доступа к интернет-счету Verizon главы ЦРУ Джона

Бреннана. Сначала подросток представился сотрудником компании, затем самим Бреннаном…

Еще одной жертвой школьника стал старший советник по науке и технологиям Барака Обамы Джон Холдрен. Гэмбл передал личные данные чиновника своему соратнику. Последний вызвал полицию, заявив, что в доме Холдрена произошел насильственный инцидент.

Эти восемь месяцев хаоса для американских чиновников завершились в феврале 2016 года. Тогда Гэмбл в течение нескольких дней получил доступ к сети Департамента юстиции США. В частности, доступ к данным 20 000 сотрудников ФБР и дела о взрыве на нефтяной платформе Deepwater Horizon.

ФБР и секретная служба США немедленно связались с полицией Великобритании, и подросток был арестован. Он находился дома…» ***(Екатерина Шпачук. Подросток из Британии получил доступ к секретной информации США, притворившись главой ЦРУ // Internetua (http://internetua.com/podrostok-iz-britanii-polucsil-dostup-k-sekretnoi-informacii-ssha-pritvorivshis-glavoi-cru). 22.01.2018).***

***

«…Фонд электронных рубежей (Electronic Frontier Foundation, EFF) совместно с компаний Lookout, специализирующейся на безопасности мобильных устройств, выявили новую кампанию кибершпионажа, охватившую тысячи устройств в более чем двадцати странах. Сотни гигабайт данных были украдены в основном с мобильных устройств, на которые были установлены шпионские приложения…

Данная киберугроза, получившая название «Темного каракала»(Dark Caracal), вероятно, была разработана государственными хакерами, которые используют соответствующую инфраструктуру. В совместном докладе EFF и Lookout утверждается, что эта киберугроза может быть связана с Главным управлением общей безопасности – национальной разведывательной службой Ливана…

«Темный каракал» атаковал цели в США, Канаде, Германии, Ливане и Франции. Кибератаке оказались подвержены военнослужащие, гражданские активисты, журналисты и юристы. Украденные данные весьма разнообразны – от записей телефонных переговоров до документов и фотографий. Очевидно, что это глобальная кампания, направленная именно на мобильные устройства…» (Комментарий Директора EFF по кибербезопасности Евы Гальперин)…

«Одной из особенностей данной атаки было то, что она не требовала ресурсозатратного и дорогостоящего выявления уязвимостей программного обеспечения. Для успешной атаки было достаточно лишь разрешения самих пользователей на установку приложений, которые, как оказалось, содержали вредоносное ПО…». (Комментарий технического специалиста EFF Купера Квинтина)***» (Dark Caracal: новая кампания по кибершпионажу, охватившая тысячи устройств по всему миру // РосКомСвобода (https://roskomsvoboda.org/35408/). 21.01.2018).***

***

«Канадське трансагентство Metrolinx зазнало атаки з боку хакерів з КНДР…

За словами представниці компанії Анни-Марі Ейкінс, кібератака на сервери трансагентства сталася раніше в січні, але «не привела до порушення конфіденційності і не порушила роботу будь-яких систем безпеки». Подробиці вона наводити не стала…

Трансагентство Metrolinx займається забезпеченням роботи систем громадського транспорту та аеропортів Торонто, всіх його передмість, а також міста Гамільтон…» ***(Тарас Джміль. Канадське трансагентство зазнало атаки хакерів з КНДР // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1711262-kanadske-transagentstvo-zaznalo-ataki-khakeriv-z-kndr). 24.01.2018).***

***

«Администрация одной из самых крупных бирж криптовалюты в Японии – Coincheck – признала, что у нее была похищена крупная сумма денег, а именно около 400 миллионов долларов в криптовалюте NEM (XEM).

…По данным сайта Coinmarketcap.com, курс NEM 26 января снизился на 14,5%. Руководитель NEM Foundation Лон Вонг называет эту кражу криптовалюты самой масштабной за всю историю.

Оказалось, что администрация Coincheck не прислушалась к рекомендациям по использованию технологии MultiSi. Это система, состоящая из нескольких ключей-паролей, которые необходимы для того, чтобы снять деньги со счета. Кроме того, клиентские счета хранились на компьютере, не изолированном от сети Интернет.

…хакеры украли лишь криптовалюту NEM, однако не рассказали никаких подробностей о самих киберпреступниках» ***(Хакеры украли около 400 миллионов долларов у крупной японской биржи криптовалют // securenews.ru (https://securenews.ru/nem/). 29.01.2018).***

***

«Японская криптовалютная биржа Coincheck сообщила, что возместит из собственных средств потери клиентов от хакерской атаки. В ходе кибератаки 26 января было похищено криптовалюты NEM на $400 млн, от кражи пострадали 260 тыс. пользователей.

Биржа обещает выплатить им компенсацию по ставке $81 за каждую монету. Всего было похищено 523 млн монет. Дата выплат не называется…» ***(Биржа Coincheck возместит клиентам потери криптовалюты от хакерской атаки // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3533301?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0)/. 28.01.2018).***

***

«…эксперты по кибербезопасности объясняют, что майнеры нашли способ встраивать код в рекламу на YouTube через платформу DoubleClick от Google.

Написанный на JavaScript код позволяет авторам объявлений добывать криптовалюту Monero с помощью сервиса CoinHive.

Для этих целей используются мощности компьютеров пользователей, которые просматривают видео…» ***(Майнеры начали использовать рекламу на YouTube для добычи криптовалют // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/217871-majnery_nachali_ispoljzovatj_reklamu_na_youtube_dlja_dobychi_kriptovaljut). 28.01.2018).***

***

«Число атак с помощью зловредов-шифровальщиков, направленных против рядовых пользователей, выросло в 2017 году на 93% по сравнению с 2016 годом, а против систем предприятий и организаций – на 90%.

Такие данные опубликовала в годовом отчете компания Malwarebytes.

…Стоит отметить, что в 2017 появились «гибридные» зловреды, сочетающие в себе функционал шифровальщиков и традиционных вирусов, способных воспроизводить себя, продолжая цепочку заражений. Тем не менее, главными способами инфицирования остались традиционные для хакеров массированные спам-рассылки, вредоносная реклама и наборы эксплойтов.

Также интересно отметить, что к концу 2017 года все эти каналы распространения зловредов показали снижение активности шифровальщиков. А наиболее активно стали распространяться другие типы вредоносного ПО – как традиционные (банковские троянцы и шпионские программы), так и совсем новые (программы для тайного майнинга криптовалют)» ***(2017 стал «звездным» годом для зловредов-шифровальщиков // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5471300-2017-stal-zvezdnym-godom-dlya-zlovr.html#ixzz55a5d8LbV). 29.01.2018).***

***

Діяльність хакерів та хакерські угруповування

«Компания из США по кибербезопасности ThreatConnect заподозрила хакеров Fancy Bears в регистрации доменов, имитирующих сайты Всемирного антидопингового агентства (WADA), Антидопингового агентства США USADA и Олимпийского совета Азии (OCASIA)…

Адреса якобы были зарегистрированы в декабре 2017 года. В ThreatConnect заявили, что они могут быть использованы для спланированных кибератак против этих или сторонних организаций….

В среду, 10 января, группа Fancy Bears выложила подтверждающие документы и переписку высшего руководства Международного олимпийского комитета (МОК) и WADA, в которых говорится, что целью комиссии Макларена

было отстранение россиян от участия в Олимпиадах в Рио-де-Жанейро и Пхенчхане, дискредитация МОК и всего олимпийского движения, а также борьба за власть и деньги в мировом спорте» ***(Мария Коваленко. Хакеров Fancy Bears подозревают в атаках по заказу РФ // Ведомости-Украина (http://vedomosti-ua.com/84451-hakerov-fancy-bears-podozrevayut-v-atakah-po-zakazu-rf.html). 12.01.2018).***

***

«Специалисты ESET обнаружили новый метод компрометации рабочих станций, который использует кибергруппа Turla. Данная техника применяется в атаках, нацеленных на сотрудников посольств и консульств стран постсоветского пространства.

…Специалисты ESET предполагают, что подобная атака может производиться следующими способами:

– Одна из машин в корпоративной сети жертвы может быть взломана, чтобы использоваться в качестве плацдарма для локальной атаки Man-in-the-Middle (MitM). Далее в ходе атаки трафик компьютера жертвы будет перенаправлен на скомпрометированную машину в локальной сети.

– Атакующие могут скомпрометировать сетевой шлюз организации для перехвата входящего и исходящего трафика между корпоративной сетью и интернетом.

– Перехват трафика может производиться на уровне интернет-провайдера (ISP) – тактика известна из недавнего исследования ESET, посвященного кибершпионажу. Известные жертвы находятся в разных странах и, по данным ESET, используют услуги минимум четырех провайдеров.

– Хакеры могут выполнить атаку на BGP-маршрутизаторы (Border Gateway Protocol hijacking) для перенаправления трафика на контролируемый ими сервер, хотя эта тактика, скорее всего, привлекла бы внимание систем мониторинга…

Новый инструмент используется в атаках минимум с июля 2016 года. Связь с Turla установлена на основании нескольких признаков, включающих использование бэкдора Mosquito и нескольких IP-адресов, ранее отнесенных к данной кибергруппе…» ***(Группа Turla распространяет бэкдор вместе с установщиком Flash Player // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5466976-Gruppa-Turla-rasprostranyaet-bekdor.html#ixzz53sh3NJvN).- 10.01.2018).***

***

«Хакери використовували сайт українського розробника бухгалтерського програмного забезпечення Crystal Finance Millennium (CFM) для поширення банківського трояна ZeuS…

…вірус поширюється… через сайт компанії CFM. Жертв заражали по електронній пошті. У листах містився ZIP-архів з файлом JavaScript, який працював як завантажувач, через який шкідливий вірус надходив в систему з домену, пов'язаного з сайтом CFM…

Атака трояна відбулася в період святкування Дня Незалежності України в кінці серпня 2017 року. Їй було піддано понад 3 тис. комп'ютерів, переважно, компаній з США і України. Найбільше поширення трояну відбулося серед абонентів "Укртелекому"…» ***(Хакери поширили троян через український сайт бухгалтерських програм // Espreso.tv (https://espreso.tv/news/2018/01/10/khakery_poshyryly_troyan_cherez_ukrayinskyy_sayt_bukhgalterskykh_program). 10.01.2018).***

***

«Хакери намагалися викрасти конфіденційні дані від груп, які будуть брати участь у зимових Олімпійських іграх, що відбудуться у лютому цього року…

…під час останнього місяця електроні листи, заражені шкідливими програмами, були відправлені організаціям, пов'язаним з іграми, що відбуватимуться у корейському місті Пхьончхан.

…встановити відповідальних не вдалося…

Е-мейли зі зловмисними програми надходили на електронні пошти компаній із сінгапурської IP-адреси. У тексті таких повідомлень отримувачам пропонували відкрити програми в тестовому режимі. Відправники листів видавали себе за працівників Національного центру протидії тероризму Південної Кореї, який у цей час проводив антитерористичні навчання в регіоні…» ***(Віта Підлубна. Зимову Олімпіаду-2018 атакують хакери // (http://www.unn.com.ua/uk/news/1708533-zimovu-olimpiadu-2018-atakuyut-khakeri).- 08.01.2018).***

***

«Неизвестные киберпреступники осуществили взлом DNS-сервера сервиса BlackWallet.co, который предоставляет веб-кошельки для криптовалюты Stellar Lumen (XLM)…

Инцидент произошел 13 января, когда злоумышленники перехватили DNS-запись домена BlackWallet.co и осуществили ее переадресацию на собственный сервер. Как утверждает администратор BlackWallet, деньги со счетов пользователей начали пропадать после того, как хакеры заполучили доступ к аккаунту хостинг-провайдера…

Всего киберпреступники украли около 669000 XLM (400000 долларов). Вскоре после взлома работа BlackWallet.co была остановлена администрацией…

Хакеры 14 января начали перевод денег со своего аккаунта XLM на биржу криптовалюты Bittrex. Скорее всего, преступники хотели замести следы путем обмена XLM на другую криптовалюту. Сейчас администрация BlackWallet ведет переговоры с Bittrex по вопросы блокировки аккаунта киберпреступников…» ***(Хакеры украли 400000 долларов в криптовалюте из кошельков сервиса BlackWallet // SecureNews (https://securenews.ru/blackwallet/). 15.01.2018).***

***

«Правоохоронні органи та спецслужби Болгарії проводять перевірку за фактом злому сторінки президента країни Румена Радєва в Facebook…

Злам стався 21 січня. Вранці на сторінці президента Болгарії з'явилася стаття турецькою мовою з посиланням на турецький сайт, який займається кредитуванням.

Після появи статті користувачі соціальних мереж відразу ж почали попереджати один одного, що, найімовірніше, сторінка була зламана хакерами. Болгарські правоохоронці порекомендували користувачам соціальної мережі не відкривати посилання на статтю, бо воно може містити віруси…» ***(Facebook-сторінку президента Болгарії зламували хакери // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/facebookstorinku_prezidenta_bolgarii_zlamuvali_khakeri/). 22.01.2018).***

***

«…В декабре 2017 года эксперты FireEye опубликовали отчет, посвященный распространению вируса Triton. Он маскируется под легитимное ПО для Triconex, предназначенное для рабочих станций под управлением Windows, и задействует проприетарный протокол TriStation…

По сообщению Schneider Electric, хакеры использовали ранее неизвестную уязвимость старых версий прошивок Triconex. Брешь в системе безопасности позволила злоумышленникам осуществить удаленную загрузку трояна, которая стала «частью сложного сценария заражения вредоносным ПО». Schneider Electric обещает выпустить инструменты для выявления и удаления вируса в феврале 2018 года.

По данным компании Dragos, специализирующейся на кибербезопасности, через уязвимость Triconex была атакована компания на Ближнем Востоке — предположительно, в Саудовской Аравии» ***(Хакеры использовали уязвимость в ИТ-системе для ядерных и нефтегазовых объектов // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5469359-Xakery-ispolzovali-uyazvimost-v-ITs.html#ixzz54vq1dhnd). 19.01.2018).***

***

«…персональные данные более чем 100000 клиентов самой крупной в Канаде телекоммуникационной компании Bell Canada были украдены киберпреступниками.

Представители компании признали, что хакеры смогли украсть сведения об именах, электронных почтовых адресах и телефонных номерах клиентов. Банковские данные, включая номера кредитных карт, не были похищены злоумышленниками.

Bell Canada сообщила клиентам об инциденте и принесла свои извинения. Сейчас канадские правоохранители занимаются расследованием данной утечки…» ***(Произошла утечка данных свыше 100000 клиентов канадского оператора связи Bell // securenews.ru (https://securenews.ru/bell_canada_2/). 25.01.2018).***

***

«Агенти нідерландської спецслужби AIVD стежили за російським хакерським угрупованням Cozy Bear, яке підозрюють у зломі серверів Демократичної партії США під час президентської кампанії

Про це ідеться у розслідуванні нідерландської газети deVolkskrant та програми новин Nieuwsuur…

Журналісти стверджують, що нідерландська спецслужба AIVD стежила за роботою Cozy Bear фактично у прямому ефірі. Повідомляється, що AIVD мала доступ до комп'ютерів російських хакерів з 2014 по 2017 роки. Отриману інформацію нідерландські агенти передавали ЦРУ та АНБ.

…Угрупування Cozy Bear ще з 2010 року атакувала корпорації, урядові установи та чиновників різних країн, в тому числі нідерландських.

В певний момент російське хакерське угрупування отримало доступ до емейл сервера з перепискою Барака Обами, на той момент президента США. Вони не змогли дістатись до його особистого Блекбері, але отримали доступ до переписки з посольствами та дипломатами.

Саме за допомогою доступу до камер безпеки у офісі хакері вдалось довести, що група Cozy Bear контролюється Службою Зовнішньої Розвідки РФ.

За даними ЗМІ доступ нідерландської розвідки до мережі CozyBear тривав 1-2.5 роки…

AIVD відстежувала кожен крок російських хакерів, включно із стеженням через веб-камери…

Завдяки проникненню нідерландська спецслужба довідалась, що хакерами керує Служба зовнішньої розвідки Росії…» ***(Нідерландські спецслужби шпигували за російськими хакерами, які зламали штаб Клінтон, - ЗМІ // Espreso.tv (https://espreso.tv/news/2018/01/26/niderlandski_specsluzhby_shpyguvaly_za_rosiyskymy_khakeramy_yaki_zlamaly_shtab_klinton_zmi). 26.01.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«Эксперты из Trend Micro выявили новую вредоносную программу FakeBank, которая дает хакерам возможность перехвата SMS-сообщений с кодами безопасности банка. С помощью кодов злоумышленники могут сбросить пароли в банковских аккаунтах жертв…

Как утверждают исследователи, вредоносная программа маскируется под приложения для управления SMS/MMS. FakeBank осуществляет перехват SMS-сообщений, чтобы затем похищать денежные средства пользователей.

Программа, прежде всего, атакует клиентов российских банков, включая «Сбербанк», «Лето Банк» и «ВТБ24». Кроме того, факты инфицирования устройств программой FakeBank выявлены в Германии, Китае, Румынии и Украине…

Также эксперты выяснили, что FakeBank похищает и передает на командный сервер пользовательскую информацию, включая данные о телефонных номерах,

установленных банковских приложениях, балансе на платежных картах и сведения о местоположении…

Как сообщают специалисты, большая часть командных серверов FakeBank расположена на территории Польши и России…» ***(Банковская троянская программа FakeBank атакует пользователей из России // SecureNews (https://securenews.ru/fakebank/). 12.01.2018).***

***

«Исследователь информационной безопасности unixfreaxjp из команды MalwareMustDie …нашел первую в истории вредоносную программу для Linux, которая заражает процессоры ARC, – Mirai Okiru…

Mirai Okiru – это первая вредоносная программа, которая предназначена именно для атак на процессоры ARC. И ее появление может иметь катастрофические последствия. В MalwareMustDie утверждают, что каждый год в мире производится более миллиарда устройств «Интернета вещей» (IoT), снабженных чипами ARC. Таким образом, число систем, которые могут быть заражены программой, огромно. Гигантский ботнет, который хакеры могут потенциально создать с помощью Mirai Okiru, подойдет для выполнения целого спектра вредоносных задач…» ***(Обнаружена первая в истории вредоносная программа для процессоров ARC // SecureNews (https://securenews.ru/arc/). 15.01.2018).***

***

«Специалисты по кибербезопасности компании AlienVault сообщили о приложении, устанавливающем на зараженный компьютер программу для добычи криптовалюты, перенаправляемой затем в КНДР…

По словам экспертов, приложение было создано в конце декабря 2017 года, в данный момент адрес сервера не доступен, что может говорить либо о прекращении работы программы, либо о том, что сервер в КНДР использовался для маскировки реального источника приложения…» ***(Дмитрий Зубарев. Эксперты обнаружили «работающую на КНДР» программу для майнинга // ООО «Деловая газета Взгляд» (https://vz.ru/news/2018/1/9/902718.html).- 09.01.2018).***

***

«Специалисты по кибербезопасности из компаний Check Point, Ixia и Certego обнаружили, что более 700 серверов на Windows и Linux заражены вредоносным программным обеспечением RubyMiner, используемым для скрытого майнинга криптовалюты. Первые атаки были замечены ещё на прошлой неделе, но массовый характер эпидемия приобрела лишь на днях.

Тем не менее эксперты кибербезопасности уверены, что хакеры только начали разворачивать свою массированную деятельность, а это значит, что в будущем может быть подвержено атаке гораздо больше серверов.

Так как майнер работает на серверах под Windows и Linux, хакеры используют для определения типа серверного программного обеспечения утилиту p0f. Если ПО старое, то взломщики запускают специальные эксплоиты, которые

заражают сервер вредоносным майнером, добывающим криптовалюту за счёт чужих мощностей и без ведома их владельцев…

Пока масштаб невелик: кошельки, которые подключены к RubyMiner, содержат криптовалюты всего на 540 долларов, но хакеры, атакующие сервера WebLogic, за несколько месяцев смогли намайнить несколько сотен тысяч долларов» ***(Сервера на Linux и Windows массово поражает вирус-майнер // Hi-News.ru (https://hi-news.ru/technology/servera-na-linux-i-windows-massovo-porazhaet-virus-majner.html). 18.01.2018).***

***

«Обнаружен новый троянец Mezzo, способный подменять реквизиты в файлах обмена между бухгалтерскими и банковскими системами.

По данным экспертов «Лаборатории Касперского», в настоящий момент зловред просто отправляет собранную с зараженного компьютера информацию на сервер злоумышленникам, и, по мнению аналитиков, это может говорить о том, что создатели троянца готовятся к будущей кампании. Количество жертв Mezzo пока исчисляется единицами, при этом большинство заражений зафиксировано в России.

Распространяется Mezzo с помощью сторонних программ-загрузчиков…

Основной интерес для Mezzo представляют текстовые файлы популярного бухгалтерского ПО, созданные менее двух минут назад. Функционал троянца предполагает, что после обнаружения таких документов он ждет, последует ли открытие диалогового окна для обмена информаций между бухгалтерской системой и банком. Если это произойдет, зловред может подменять реквизиты счета в файле непосредственно в момент передачи данных. В противном случае (если диалоговое окно так и не будет открыто) Mezzo подменяет весь файл поддельным…» ***(Троянец охотится за реальными и криптовалютами // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5470929-Troyanecz-oxotitsya-za-realnymi-i.html#ixzz55a246Gdt). 25.01.2018).***

***

«**Эксперт из Bitdefender Богдан Ботезату рассказал о новом IoT-ботнете, который состоит, прежде всего, из незащищенных IP-камер.**

Ботсеть Hide 'N Seek (HNS) появилась впервые 10 января, но несколько дней спустя прекратила свою работу. 20 января ботнет возобновил свою активность увечился с 12 инфицированных устройств до 14000…

Боты HNS способны принимать и выполнять несколько команд, в том числе, похищать информацию, выполнять кода и вмешиваться в работу устройства. У ботсети отсутствует функционал для организации DDoS-атак.

…Как и другие подобные вредоносные программы для IoT-устройств, HNS автоматически удаляется после перезагрузки устройства» ***(Появилась новая опасная IoT-ботсеть HNS // securenews.ru (https://securenews.ru/hns/). 25.01.2018).***

***

«…12 января глава Управления оборонных информационных систем минобороны США генерал-лейтенант Алан Линн заявил, что Пентагон готовится к отражению очередной хакерской атаки.

…На сегодняшний день в ведомство Пентагона постоянно поступают сообщения о возможности хакерского взлома, так называемого "террабайта смерти". В настоящее время военному ведомству приходится отражать атаки масштабом 600 гигабайт, однако ранее масштабы атак были гораздо меньше. Линн утверждает, что ежегодно, а точнее каждые восемь-девять месяцев, офицеры ведомства прибегают к помощи ИТ-специалистов для замены оборудования для борьбы с вирусными атаками…» ***(Пентагон готовится к масштабной кибератаке // Украинское рейтинговое агентство "УРА" (http://ura-inform.com/ru/society/2018/01/12/pentagon-gotovitsja-k-masshtabnoj-kiberatake). 12.01.2018).***

***

«Национальный центр кибербезопасности Литвы расследует хакерскую атаку против новостного интернет-портала tv3.lt, сообщило минобороны страны.

Редактор портала Артурас Анужис сообщил, что …хакеры «распространили ложную информацию о министре обороны Литвы Раймундасе Кароболисе и ведущем программы радиостанции Ziniu radijas Ридасе Ясюленисе»…

Анужис утверждает, что, «по предварительным данным», за атакой стоят «российские программисты», но никаких доказательств он не предъявил…

Вице-министр обороны Эдвинас Керза заявил, что …согласно предоставленной редакцией информации, можно считать, что хакерский взлом был осуществлен с российского IP-адреса. При этом Керза обвинил Москву в неготовности сотрудничать в расследовании кибернетических инцидентов.» ***(Антон Антонов. «Российских программистов» заподозрили во взломе литовского новостного портала // ООО «Деловая газета Взгляд» (https://vz.ru/news/2018/1/19/904194.html). 19.01.2018).***

***

«У Німеччині недооцінюють і намагаються не помічати ступінь загрози, яку представляють з себе російські кібератаки…

Про це сказав німецький публіцист, експерт з Росії, який багато років пропрацював у Москві журналістом, автор цілої низки книг про цю країну Борис Райтшустер, виступаючи в Берліні на подіумній дискусії, присвяченій кібер-безпеці.

А от експерт з питань безпеки і міжнародних відносин Німецького інституту міжнародної політики і безпеки Аннегрет Бендік поглядів Райтшустера багато в чому не розділяла. За її твердженнями, сьогодні говорити про кібер-війну було б не

коректно, слід говорити про окремі атаки, пов'язані з різними мотивами, зокрема, криміналом, шпигунством…

Експерт визнає, що кібер-атаки «супроводжують міжнародні конфлікти». Такий зв'язок підтвердили, зокрема, конфлікти в Грузії та навколо України, зазначила Бендік.

Також вона навела витримки з доповіді берлінського Фонду науки і політики, співавтором якого є, зокрема, про те, що Росія все більше намагається розширити своє авторитарне розуміння інформаційного суверенітету. Китай все більше закриває свій інтернет-простір, а США прагнуть розвивати військово-наступальний кібер-захист…» ***(Німці недооцінюють загрозу російських кібератак – експерт // Укрінформ (https://www.ukrinform.ua/rubric-world/2383504-nimci-nedoocinuut-zagrozu-rosijskih-kiberatak-ekspert.html). 17.01.2018).***

***

«Останні десять років Москва проводила «мілітаризацію» своїх кібертехнологій, натомість НАТО почало серйозно розглядати це питання лише у 2013 році… Про це заявив колишній помічник генерального секретаря Альянсу з питань безпеки Сорін Дукару…

Небажання західних держав займатися "мілітарізацією" Інтернету призвело до того, що Росія та Китай отримали кіберперевагу. Ці країни активно вводять обмеження у цифровому просторі, тому їм простіше захищатися від кібератак, а також здійснювати їх, залишаючись при цьому анонімними, пояснив експерт. За словами екс-чиновника НАТО, у цій сфері атакуючі дії ефективніші, адже той, хто обороняється повинен закрити всі "діри та проґалини", а тому нападнику досить знайти одну "лазівку"…» ***(НАТО не готове до протистояння з Росією в кіберпросторі, – екс-чиновник Альянсу // 7dniv.info (http://7dniv.info/politics/98449-nato-ne-gotove-do-protistoiannia-z-rosieiu-v-kberprostor-eks-chinovnik-aliansu.html). 17.01.2018).***

***

«…Пентагон предлагает расширить список случаев, когда США может применить ядерное оружие…

В соответствии с новым документом под названием Nuclear Posture Review ("Обзор ядерной позиции") Минобороны предлагает разрешить применение оружия, если враг совершает разрушительные кибератаки на энергосистемы или коммуникационную связь США.

Теперь документ направили на согласование в Белый дом. Конечная публикация отчета планируется на ближайшие недели и определит дальнейшую ядерную позицию США» ***(Пентагон предлагает применять ядерное оружие в ответ на кибератаки // Espreso.tv (https://ru.espreso.tv/news/2018/01/17/pentagon_predlagaet_prymenyat_yadernoe_oruzhye_v_otvet_na_kyberataky). 17.01.2018).***

***

«**Согласно заявлению министра обороны Великобритании Гэвина Уильямсона изданию The Telegraph, в настоящее время Россия изучает британскую критическую инфраструктуру**, в частности, как она связана с электростанциями на материке. Это нужно для осуществления атак с целью посеять в стране «панику» и «хаос». В случае удара по критической инфраструктуре и электростанциям Великобритании могут погибнуть «тысячи, тысячи и тысячи», предупредил министр…

Такого же мнения придерживается бывший статс-секретарь лорд Алан Уэст (Alan West). По его словам, он «совершенно уверен» в том, что Россия ищет способ добраться до британской критической инфраструктуры…» ***(Минобороны Великобритании: РФ готовит атаки на критическую инфраструктуру // Internetua (http://internetua.com/minoboron-velikobritanii-rf-gotovit-ataki-na-kriticseskuua-infrastrukturu). 27.01.2018).***

***

Анонси подій у галузі кібербезпеки

«**…столичный "Код ИБ ПРОФИ" 1-4 марта соберет более 200 участников - ИБ-руководителей из Москвы и других городов России и ближнего зарубежья.** Программа из 32 мастер-классов, куратором которой вновь выступает Алексей Лукацкий (Cisco), выстроена в логике цикла «Шухарта-Деминга» или PDCA, который часто расшифровывается как "Планируй .Делай. Контролируй. Совершенствуй". В первой секции "Планируй" ключевыми темами мастер-классов станут ИБ-стратегия, риск-менеджмент, непрерывность бизнеса, операционная устойчивость… Далее в секции "Делай" раскроют лучшие практики open security (Алексей Качалин, Сбербанк),построения bug bounty (Кирилл Ермаков, QIWI), управления инцидентами в корпоративном SOC (Дмитрий Кузнецов, Positive Technologies) и жизненным циклом инцидента ИБ (Дмитрий Мананников, бизнес-консультант по безопасности), научат раннему обнаружению шифровальщиков (Александр Скакунов, VolgaBlob). Спикеры секции "Контролируй" Рустем Хайретдинов (Атак Киллер) и Наталья Гуляева (Hogan Lovells) расскажут, как выстроить эффективные правила внутри корпорации и передавая ИБ на аутсорс. Мастер-классы блока "Совершенствуй" охватят темы внешних коммуникаций компании в случае взлома, лучших практик киберучений, возможностей SCRUM в ИБ, психологии ИБ и социальной инженерии, культуры ИБ и цифровой устойчивости, игрофикации в обучении ИБ и др…» ***(Олег Иванов. Стал известен полный состав спикеров Кода ИБ ПРОФИ в Москве // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-01-26-1447/25360). 26.01.2018).***

***

«17 и 18 мая в Киеве, в галерее «Лавра», пройдет первая практическая профессиональная конференция по кибербезопасности NoNameCon…

Цель мероприятия – акселерация развития индустрии кибербезопасности и, соответственно, сообщества профессионалов этой отрасли в Украине, через кооперацию всех направлений и разветвлений сферы кибербезопасности и ее потребителей…

Программа мероприятия формируется из выступлений и практических занятий:

– Практическая часть состоит из трех компонентов: CTF, hacking villages и воркшопы. На воркшопы смогут зарегистрироваться участники конференции, когда начнется общая регистрация на мероприятие. На villages сможет попасть любой участник – это будет открытая зона. На CTF competition попадут только победители отборочных туров, которые пройдут онлайн, – уточнил в комментарии для InternetUA соорганизатор NoNameCon…» ***(Владимир Кондрашов. В Украине состоится конференция профессионалов по кибербезопасности // Internetua (http://internetua.com/v-ukraine-sostoitsya-konferenciya-professionalov-po-kiberbezopasnosti). 13.01.2018).***

***

Нові надходження до Національної бібліотеки України імені В.І. Вернадського

IV Всеукраїнська конференція студентів, аспірантів та молодих вчених «Сучасні проблеми розвитку підприємств харчової промисловості: теорія та практика», 24-25 листопада 2016 рік : [програма і матеріали]. - Київ : НУХТ, 2016. - 431 с.

Зі змісту:

- Близнюк М.М. Організація системи забезпечення інформаційної безпеки підприємства.

Шифр зберігання НБУВ: ВС62898.

***

V Міжнародна науково-практична конференція «Математичні методи, моделі та інформаційні технології в економіці», 18-19 травня 2017 р. : [матеріали конф.]. - Чернівці : Друк Арт, 2017. - 182 с.

Зі змісту:

- Вовкодав О.В., Кіх Р.Ю. Інформаційна безпека підприємства;
- Ставницький О.В., Бабіч С.М. Захист інформації в інформаційних економічних системах.

Шифр зберігання НБУВ: ВА814780.

***

XV Всеукраїнська наукова конференція «Розвиток системи обліку, аналізу та аудиту в Україні: теорія, методологія, організація», 24 березня 2017 р. : тези доп. учасників. - Київ : НАСОА, 2017. - 326 с.

Зі змісту:

- Цаль-Цалко Ю.С. Процедури облікової політики в системі кібербезпеки підприємства.

Шифр зберігання НБУВ: ВА814823.

***

Актуальні задачі сучасних технологій : зб. тез доп. V Міжнар. наук.-техн. конф. молодих учених та студентів, 17-18 листоп. 2016 р. - Тернопіль, 2016. - Т. 2. - 433 с.

Зі змісту:

- Добжанський В.О. Найкращі способи захисту сайту від злому;
- Кащук О.М., Фриз М.С. Захист та шифрування даних в системах мобільного зв'язку GSM.

Шифр зберігання НБУВ: В356846/2.

***

Актуальні проблеми правового регулювання в Україні та країнах ближнього зарубіжжя (правові підходи до геополітичних реалій) = Actual problems of legal regulation in Ukraine and neighboring countries (legal approaches to geopolitical realities) : матеріали VI міжнар. наук.-практ. Інтернет конф., 23 груд. 2016 р. - Львів : Растр-7, 2016. - 251 с.

Зі змісту:

- Заїр Р.П. Інформаційні війни – загроза інформаційній безпеці держави;
- Похильська М.В. Захист персональної інформації в мережі Інтернет.

Шифр зберігання НБУВ: СО35370.

***

Живило Є.О. Напрями створення та розбудови національної системи кібербезпеки / Є. О. Живило, О. О. Черноног // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. - 2017. - Вип. 3. - С. 60-65.

Визначено пріоритети та шляхи вдосконалення державної політики забезпечення кібербезпеки України. Запропоновано загальнодержавна модель побудови Національної системи кібербезпеки, окреслено її функціональні елементи.

Шифр зберігання НБУВ: Ж71640.

***

Захист інформації і безпека інформаційних систем: матеріали VI Міжнар. наук.-техн. конф., 1-2 черв. 2017 р. - Львів : Вид-во Львів. політехніки, 2017. - 177 с.

Зі змісту:

- Хорошко В., Хохлачова Ю. Тимченко М. Забезпечення безпеки в кібернетичному просторі держави;
- Щербина Ю. Казакова Н., Фразе-Фразенко О. Аналіз методів та засобів оцінки ризиків інформаційної безпеки;

- Кобозєва А. Розвиток блоково-орієнтованого підходу до задачі виявлення клонування в цифровому зображенні;
- Толюпа С., Пархоменко І. Методи протидії впливу кібератак на інформаційну систему;
- Сокульський О., Богданенко М. Засоби захисту електронних докуметів на різних етапах його життя;
- Руда Х., Стахів М., Стахів Т. Використання методу аналітичної ієрархії у сфері кібербезпеки;
- Дудцкевич В., Микитан Г., Рубець А. Характеристики загроз та класифікація порушників у кіберфізичних системах;
- Яцків Н., Яцків С. Типи атак на інтернет речей.

Шифр зберігання НБУВ: СО35287.

***

Кец Д. Ідентифікація загроз несанкціонованого доступу до конфіденційних мережевих ресурсів / Кец Дмитро, Присяжний Дмитро, Салієва Ольга // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні : науково-технічний зб. – 2017.- Вип. 1 (33).- С. 59-70.

Розкрито існуючі атаки на конфіденційні мережеві ресурси та способи їх виявлення. Запропоновано метод і алгоритм ідентифікації загроз несанкціонованого доступу, що базується на аналізі фактичних даних об'єму мережевого трафіку.

Шифр зберігання НБУВ: Ж70508.

***

Корчак Ю. Актуальні проблеми інформаційної безпеки та способи їхнього вирішення / Ю. Корчак, Ю. Фургала // Електроніка та інформаційні технології. - 2017. - Вип. 7. - С.93-104.

Проаналізовано сучасний стан глобальної інформаційної безпеки. Описано нові кберзагрози, напрями та методи боротьби з ними.Особливу увагу звернено на шкідливе програмне забезпечення, як руткіти, які значно небезпечніші ніж віруси.

Шифр зберігання НБУВ: Ж29711.

***

Матеріали VII міжнародної науково-практичної конференції «Комплексне забезпечення якості технологічних процесів та систем», 24-27 квітня 2017 р., Чернігів. - Т. 2. - 2017. - 199 с.

Зі змісту:

- Ткач Ю.М. Загрози інформаційної безпеки вищого навчального закладу;
- Зайчук Я.І., Гуменюк Т.В., Ляхович І.Р. Аналіз безпеки програмного забезпечення з використанням нейромережі;
- Андрущенко Д.М., Козіна О.М., Програма для захисту цифрових зображень;

- Лахно В.А., Петренко Т.А. Система интеллектуальной поддержки принятия решений в слабо формализуемых задачах обеспечения кибербезопасности;
- Гур'єв В.І., Фірсова І.В. Кібербезпека хмарних технологій;
- Ігнатенко П.Л., Коваленко Ю.Б. Підвищення надійності цільового програмного забезпечення.

Шифр зберігання НБУВ: В356805/2.

***

Островий О.В. Деякі підходи до удосконалення державної політики забезпечення кібернетичної безпеки України / Островий О.В. // Збірник наукових праць Донецького державного університету управління. Сер. : Державне управління. - 2016. - Т. 17, Вип. 298. - С. 77-85.

Проаналізовано нормативно-правову базу регулювання системи кібернетичної безпеки в Україні. Надано оцінку рівня державного забезпечення кібернетичної безпеки. Визначено проблемні питання, що перешкоджають забезпеченню кібернетичної безпеки в державі.

Шифр зберігання НБУВ: Ж70751/Держ. упр.

***

Публічне адміністрування у сфері обігу наркотиків: правове регулювання та напрямки оптимізації : зб. наук. пр. І Міжнар. наук.-практ. конф. (15 берез. 2017 р., м. Харків). - Харків, 2017. - 246 с.

Зі змісту:

- Баранов Р.Р. Особливості норм поліцейського права у сфері міжнародного співробітництва в боротьбі з кібернаркозлочинністю.

Шифр зберігання НБУВ: ВА814417.

***

Сігайов А. Ботнети: методи виявлення та протидії / Сігайов Андрій, Воловик Андрій // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні : науково-технічний зб. – 2017.- Вип 1 (33).- С. 22-30.

Розглянуто історію ботнетів, їх типову архітектуру, тенденції розвитку. Надано рекомендації щодо їх виявлення та знешкодження.

Шифр зберігання НБУВ: Ж70508.

***

Сопілко І. М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет / І. М. Сопілко // Юридичний вісник. Повітряне і космічне право. - 2017. - № 3. - С. 61-69.

Виокремлено новий вид загроз, пов'язаних з Інтернетом, а саме ризики, що пов'язані із захистом об'єктів авторського права в мережі Інтернет, що потребують належного реагування держави. Проаналізовано напрямки вдосконалення захисту авторських прав у мережі Інтернет. Підтримано позицію щодо необхідності

впровадження програми з підвищення медіа-грамотності населення, професійних стандартів онлайнової журналістики, продовження реформ щодо прозорості власності, недопущення концентрації на медійному ринку і незалежності редакційної політики ЗМІ від впливу політично-фінансових груп.

Шифр зберігання НБУВ: Ж73401.

***

Сучасна війна: гуманітарний аспект. Науково-практична конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба, 30 червня 2017 року: тези доп. - Харків, 2017. - 207 с.

Зі змісту:

- Нарчук Ю.В. Правові аспекти інформаційної безпеки в Україні;
- Дзьобань О.П., Соснін О.В. Інформаційна безпека у сфері комунікацій.

Шифр зберігання НБУВ: ВА814784.

***

Сучасні проблеми інформаційної безпеки на транспорті. СПІБТ-2016 : матеріали VI Всеукр. наук.-техн. конф. з міжнар. участю, 13-14 груд. 2016 р. - Миколаїв : НУК, 2016 . - Ч. 1. - 2016. - 131 с.

Зі змісту:

- Баранов О.А. Особливості правової підготовки спеціалістів з кібербезпеки;
- Мельник С.В. Актуальні питання професійної підготовки фахівців з кібербезпеки для системи правоохоронної діяльності в Україні;
- Турти М.В. Підготовка кадрів у галузі інформаційної безпеки до розв’язку аналітичних задач.

Шифр зберігання НБУВ: В356827/1.

***

Традиції та інновації розвитку приватного права в Україні: освітній вимір : матеріали V Всеукр. наук.-практ. конф. (м. Полтава, 3 черв. 2016 р. - Полтава : ПУЕТ, 2017. - 142 с.

Зі змісту:

- Кульчій О.О. Інформаційна безпека в мережі Інтернет: особливості правового регулювання.

Шифр зберігання НБУВ: ВА814662.

***

Фізико-технологічні проблеми передавання, обробки та зберігання інформації в інфокомунікаційних системах : матеріали V Міжнар. наук.-практ. конф., 3-5 листоп. 2016 р. - Чернівці : Місто, 2016. - 271 с.

Зі змісту:

- Войтович О.П., Хомін Д.М. Аналіз сучасних систем виявлення вторгнень як засобу боротьби з ботнео-кодом;

- Пислар І.В., Брасловський В.В., Єгорова Т.С., Рождественська М.Г. Модель потоків даних системи управління ризиком безпеки інформації.

Шифр зберігання НБУВ: СО35367.

***

Шевченко А.С. Метод оцінювання ризику інформаційної безпеки внаслідок обмеження пропускної спроможності міжмережними екранами наступного покоління при використанні додаткових активних систем захисту інформації / А.С. Шевченко, І.В. Самойлов, В.А. Толстих, С.Г. Артюх // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. - 2017. - Вип. 3. - С. 165-170.

Розглянуто метод оцінювання ризиків, який враховує додатковий ризик внаслідок порушення доступності інформації під час передачі через обмеження пропускної спроможності міжмережними екранами нового покоління NGFW при застосуванні таких систем захисту інформації, як: системи виявлення та попередження вторгнень IDS/IPS, систем контролю додатків (Application Control), систем попередження втрати даних DLP, систем веб-контролю (Web Control), контролю електронної пошти (Email proxy), віртуальних приватних мереж VPN тощо.

Шифр зберігання НБУВ: Ж71640.

***

Виготовлено в друкарні
ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, вул. Мельникова, буд. 63
Тел.. 067 440 11 37
artek.press@ukr.net
www.artek.press

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції –
серія № ДК №4779 від 15.10.14р.