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

№ 7 (липень)

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. Дизайн обкладинки С.Дорогих.

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

«Текст скандально известного законопроекта №6688, устанавливающего внесудебную блокировку сайтов, набирали в пиратской версии Microsoft Word…

Об этом на своей странице в Facebook пишет львовский блогер Петр Нек…

– Я зашел на сайт Верховной Рады и загрузил законопроект, чтобы самому его почитать и попробовать вникнуть. Ну, и по привычке посмотрел, кто создавал документ, кто редактировал. (Word по умолчанию пишет данные, указанные при установке программы). Так вот оказалось, что документ набирали на пиратском Microsoft Word …» ***(Владимир Кондрашов. Законопроект о цензуре в Интернете писали в пиратском Word // Internetua (http://internetua.com/zakonoproekt-o-cenzure-v-internete-pisali-v-piratskom-word). 05.07.2018).***

***

«**Год назад Украину потрепала сама известная и самая масштабная кибератака в истории нашего государства – так называемая «атака вируса Petya».** Урокам, которые вынесли бизнес и государство из инцидента, был посвящен круглый стол, организованный вчера в «Лига: Закон»…

Экономический ущерб от произошедшего основатель компании «Октава Киберзащита» Александр Кардаков оценивает в сумму до 450 миллионов долларов.

– Произошла фактически остановка части экономики Украины: примерно трети на три дня, – рассказал Кардаков…

Цифра в 450 миллионов долларов, уточнил Кардаков, не учитывает убытки, которые понес бизнес от потери информации, и затраты на восстановление информационных систем…

Участники круглого стола назвали атаку «переломным моментом»: именно после неё и в госсекторе, и в бизнесе наконец-то начали всерьез рассматривать киберугрозы…» ***(Владимир Кондрашов. Чему нас научил вирус Petya // Internetua (http://internetua.com/csemu-nas-naucsil-virus-petya). 04.07.2018).***

***

«Служба безопасности Украины постоянно фиксирует кибератаки, которые поддерживаются государством-агрессором.

Об этом на круглом столе, посвящённом урокам от атаки вируса Petya A, сообщил сотрудник ситуационного центра обеспечения кибербезопасности СБУ Андрей Окаевич…

По словам сотрудника СБУ, часто такие атаки происходят с использованием так называемых "zero day"-уязвимостей, то есть ранее неизвестных уязвимостей.

То, что атаки "поддерживаются" РФ, как утверждает Окаевич, стимулирует СБУ больше внимания уделять вопросам кибербезопасности.

Андрей Окаевич также отметил, что СБУ фиксирует тенденцию атакующих к компрометации инфраструктуры производителей программного обеспечения…» ***(Владимир Кондрашов. СБУ регулярно фиксирует российские кибератаки //***

Internetua (http://internetua.com/sbu-regulyarno-fiksiruet-rossiiskie-kiberataki). 03.07.2018).

***

«…Вперше у Військовому інституті телекомунікацій та інформатизації імені Героїв Крут, серед цивільних та військових вишів на кафедрі військової підготовки відкрили підготовку за військово-обліковою спеціальністю «Організація захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах» (державне замовлення)…

Під час навчання майбутні фахівці кіберзахисту отримають знання з організації та забезпечення кібербезпеки на тактичному рівні, проведення пошуку та оцінки вразливості в кіберпросторі, застосування комплектів для реалізації розслідування кібернетичних інцидентів…» ***(Альона Душенко. Кременчужан запрошують долучитися до захисту кіберпростору // "Кременчуцький ТелеграфЪ" (https://www.telegraf.in.ua/kremenchug/10071221-kremenchuzhan-zaproshuyut-doluchitisya-do-zahistu-kberprostoru.html). 12.07.2018).***

***

«Суддя Шевченківського районного суду Києва Вікторія Світлицька запропонувала розробити інструкцію, що вбереже суддів від кібератак на їхні електронні інформаційні ресурси.

Так, суддя повідомила Вищу раду правосуддя про отримання невстановленими особами файлів з інформацією про її телефонні дзвінки, отримані телекомунікаційні послуги, …що, на думку судді, є порушенням таємниці її телефонних розмов, а також несанкціонованим доступом до електронних скриньок, акаунтів у соціальних мережах…

З аналогічним скаргами звернулася суддя Дзержинського районного суду міста Харкова Ганна Подус.

За словами судді, на адресу її особистої електронної пошти почали надходити повідомлення з поштового сервісу mail.ru від невідомих осіб з погрозами застосувати насильство щодо Подус та членів її сім'ї у разі, якщо вона продовжить розглядати справу, яка зараз перебуває у її провадженні…» ***(Судді просять розробити інструкцію, що вбереже їх від кібератак // "Українське право" (http://ukrainepravo.com/news/ukraine/suddi-prosyat-rozrobyty-instruktsiyu-shcho-vberezhe-yikh-vid-kiberatak-/). 12.07.2018).***

***

«…eHealth – не має сертифіката відповідності на комплексну систему захисту інформації і мало того, що не пройшла державну експертизу…

Держслужба спецзв'язку і захисту інформації пояснює, що таке положення справ може сприяти витоку персональних даних громадян внаслідок кібератак, а також конфіденційної інформації, як історія хвороби і діагноз…» ***(МОЗ незаконно збирає ваші дані, — журналіст // Українська служба швидких новин (https://sumynews.online/moz-nezakonno-zbiraye-vashi-dani-zhurnalist/). 07.07.2018).***

***

«Украинский киберальянс» объявил флешмоб против безответственной, как они говорят, политики кибербезопасности украинских государственных структур…

Около двух месяцев назад активисты начали флешмоб #FuckResponsibleDisclosure…

Суть флешмоба заключается в обнародовании в социальных сетях несекретных документов из служебных компьютеров, демонстрации ненадежности сайтов отдельных министерств и служебных баз данных предприятий и объектов критической инфраструктуры. Активисты не используют чисто хакерские методы — обычно достаточно только поиска в Google, пишет спикер УКА под ником Шон Таунсенд в своей колонке об итогах флешмоба.

Впрочем, после их «проверок» правоохранители открыли как минимум два уголовных производства. Им удалось прорваться на почтовый сервер МВД…» ***(Вадим Петров. Украинские хакеры обнародовали служебные документы украинских военных, энергетиков и чиновников // Bad Android (https://bad-android.com/news/36228-ukrainskie-khakery-obnarodovali-sluzhebnye-dokumenty-ukrainskikh-voennykh-energetikov-i-chinovnikov). 11.07.2018).***

***

«Первый в Украине коммерческий SOC (Security Operation Center) запустил IT- бизнесмен и основатель компании Октава Киберзахист Александр Кардаков...

Новый Центр располагается в UNIT.City и предоставляет ряд услуг: управление средствами кибербезопасности, автоматизированное обнаружение и блокирование кибератак в реальном времени, расследование инцидентов, анализ рисков кибербезопасности…

Новая площадка также является лабораторией и Центром компетенций, где можно демонстрировать и моделировать любые решения в области кибербезопасности…

В компании "Октава Киберзахист" отмечают, что при необходимости они готовы взаимодействовать с Государственным центром кибербезопасности, профильными подразделениями СБУ, Госспецсвязи и Киберполицией.» ***(В Киеве открылся первый коммерческий Центр управления кибербезопасностью // DsNews (http://www.dsnews.ua/society/v-kieve-otkrylsya-pervyy-kommercheskiy-tsentr-upravleniya-02072018173300). 02.07.2018).***

***

«Центральна виборча комісія напередодні президентських та парламентських виборів вживає заходів з оновлення та розвитку IT-інфраструктури й впровадження сучасних програмних засобів захисту інформації для підвищення стійкості перед сучасними кіберзагрозами…

У ЦВК зазначили, що відповідні заходи вживаються відповідно до Стратегії кібербезпеки України та закону "Про захист інформації в інформаційно-телекомунікаційних системах"…» ***(Олександр Сивачук. ЦВК працює щодо***

запобігання можливим кібератакам під час виборів в Україні // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/exclusive/1742875-tsvk-pratsyuye-schodo-zapobigannya-mozhlivim-kiberatakam-pid-chas-viboriv-v-ukrayini). 23.07.2018).

***

«12 июля состоялась первая всеукраинская конференция «Основные принципы обеспечения кибербезопасности в нотариальной деятельности», организованная Нотариальной палатой Украины.

…На необходимости сотрудничества с Минюстом касаемо разработки способов защиты как нотариусов, так и баз данных, акцентировали внимание и президент НПУ Владимир Марченко, и заместитель Министра юстиции Елена Сукманова…

Непосредственно о мерах, которые могут предпринять нотариусы для защиты от кибератак, говорил Максим Литвинов, руководитель Ситуационного центра обеспечения кибербезопасности Департамента контрразведывательной защиты интересов государства в сфере информационной безопасности СБУ. Так, нотариусам может быть полезен ресурс, созданный для раздачи идентификаторов компрометации, которые позволяют блокировать опасные IP-адреса…

При этом в ходе дальнейшего обсуждения была обнаружена истинная проблема - реестры ГП «НАИС» доступны только на Windows 7, которую компания Microsoft перестала сопровождать с 2014 года.

Исходя из опыта других стран, практически полную защиту реестров можно обеспечить только организовав локальную сеть нотариусов, без доступа к Интернету… из-за дороговизны такое решение вряд ли будет реализовано в Украине…

Советы нотариусам дали и представители киберполиции…

Ну а в целом, поскольку нотариат является частным институтом, обеспечить кибербезопасность всех государство технически не в состоянии. Поэтому нотариусам советуют стать «параноиками» и помнить, что надежная защита влечет за собой неудобства в работе.» ***(Марина Ясинская. Как нотариусам защититься от кибератак, обсуждали в Нотариальной палате // Інформаційне агентство "ЛІГА:ЗАКОН" (http://jurliga.ligazakon.ua/news/2018/7/13/171148.htm). 13.07.2018).***

***

Національна система кібербезпеки

«Урядом затверджено план заходів на 2018 рік з реалізації Стратегії кібербезпеки України. Це передбачено постановою Кабінету Міністрів України від 11 липня 2017 року № 481-р.

Зокрема, передбачається розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, вчинені щодо державних та

інших інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

Також планується підвищення рівня відповідальності посадових осіб державних органів, установ та організацій за порушення вимог щодо інформування в установленому порядку про несанкціоновані дії (кібератаки) стосовно державних інформаційних ресурсів.

Окрім того, Держспецзв'язок визначений органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів.

Державним органам, підприємствам, установам та організаціям державної форми власності, крім закордонних дипломатичних установ України, забороняється закуповувати послуги (укладати договори) з доступу до Інтернету в операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації.

…Одним з пунктів Стратегії є проектування захищеного дата-центру (центру обробки даних) для потреб державних органів, насамперед суб'єктів сектору безпеки і оборони, фінансового, енергетичного, транспортного секторів і утворення Національного центру оперативно-технічного управління телекомунікаційними мережами України.» ***(Кримінальну відповідальність за кіберзлочини щодо державних органів розмежують // "Українське право" (http://ukrainepravo.com/news/ukraine/kryminalnu-vidpovidalnist-za-zlochyny-shchodo-derzhavnykh-resursiv-rozmezhuyut-/). 17.07.2018).***

***

«В Днепровском горсовете появилось новое современное оборудование и программное обеспечение…

Об этом сообщила и.о. заместителя мэра Днепра Яника Мерило на своей странице в Фейсбук:

«Днепровский горсовет и Государственный центр киберзащиты и противодействия киберугрозам государственной службы специальной связи и защиты информации Украины расширили сотрудничество.

В рамках договора о сотрудничестве CERT-UA передает горсовету в использование специальное оборудование и программное обеспечение для повышения уровня защиты информационных систем. Данная система позволит более эффективно мониторить информационные системы и блокировать системы, которые заражены или представляют угрозу для других систем…» ***(Днепру больше не страшны кібератаки // "Днепр Час" (https://dpchas.com.ua/politika/dnepru-bolshe-ne-strashny-kiberataki). 04.07.2018).***

***

«Правлением Интернет Ассоциации Украины было принято решение о создании Комитета ИнАУ по вопросам кибербезопасности…

Как сообщается, в ближайшее время состоятся учредительное собрание по созданию этого Комитета…

По словам Главы Правления Интернет Ассоциации Украины Александр Федиенко, комитет будет открытым для тех, кому небезразличны вопросы кибербезопасности:

– Идея в том, чтобы максимально привлечь технических специалистов для выработки решений, для тех же операторов и провайдеров, для защиты их клиентов от воздействия атак, – подчеркнул Федиенко. – Комитет возьмет на себя консультативные функции, в том числе и технические, функции анализа законодательного поля, работы с правоохранительными органами…» ***(Владимир Кондрашов. Интернет Ассоциация Украины создает комитет по кибербезопасности // Internetua (http://internetua.com/internet-associaciya-ukrain-sozdaet-komitet-po-kiberbezopasnosti). 19.07.2018).***

***

Правове забезпечення кібербезпеки в Україні

«Министерство экономического развития и торговли Украины разработало и готовит к обнародованию на сайте МЭРТ законопроект «О критической инфраструктуре и её защите»…

…целью проекта Закона является создание государственной системы защиты критической инфраструктуры, внедрение единых подходов к организации управления объектами системы на государственном и местном уровнях, определение основ взаимодействия привлеченных к защите критической инфраструктуры государственных органов и субъектов хозяйствования, общества и граждан.

– Отдельно в проекте Закона будут закреплены порядок и критерии отнесения объектов инфраструктуры к объектам критической инфраструктуры, что будет охватывать предприятия, учреждения, организации независимо от формы собственности, которые осуществляют деятельность в различных отраслях, в том числе и в информационно-коммуникационной сфере, – обещают в МЭРТ…» ***(Владимир Кондрашов. МЭРТ готовит к публикации законопроект о критической инфраструктуре // Internetua (http://internetua.com/mert-gotovit-k-publikacii-zakonoproekt-o-kriticseskoi-infrastrukture). 12.07.2018).***

***

«В среду, 4 июля, Комитет Верховной Рады Украины по вопросам национальной безопасности и обороны единогласным решением рекомендовал народным депутатам принять в первом чтении скандальный законопроект №6688.

…законопроект под соусом информационной безопасности предлагает ряд «новшеств», самым обсуждаемым из которых является возможность блокировки без решения суда на 48 часов любого ресурса в сети Интернет, а по решению следственного судьи, суда, прокурора или СНБО – на более длительные периоды за размещение «запрещенной информации»…

Среди других опасных тезисов законопроекта, на которые указывает коалиция «За свободный Интернет»:

– продолжение практики произвольной и непрозрачной блокировки доступа к информационным ресурсам;

– наделение СБУ неконтролируемыми полномочиями в сфере надзора за выполнением требований по блокированию сайтов;

– усиление ответственности операторов телекоммуникаций и других субъектов за невыполнение каких-либо требований о предоставлении телекоммуникационных услуг или блокировки ресурсов, независимо от серьезности нарушений;

– наложение чрезмерных финансовых обязательств на операторов и провайдеров телекоммуникаций за собственные средства закупать и устанавливать определенные государством технические средства для блокировки доступа…» ***(Владимир Кондрашов. Законопроект №6688: цензура в Интернете, тоталитаризм и российский след // Internetua (http://internetua.com/zakonoproekt-6688-cenzura-v-internete-totalitarizm-i-rossiiskii-sled). 05.07.2018).***

***

«Розроблений Державною службою спеціального зв'язку та захисту інформації проект постанови Кабінету Міністрів України, що встановлює вимоги до проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, не відповідає міжнародним стандартам кібербезпеки і містить значні корупційні ризики.

До таких висновків прийшов експерт з кібербезпеки, Голова ГО «Українська група інформаційної безпеки» Костянтин Корсун, проаналізувавши проект авторства ДССЗІ…

У ключовому для української кібербезпеки Законі, «Про основні засади забезпечення кібербезпеки України», поміж іншого, визначено поняття об'єкту критичної інфраструктури та закладено вимогу про регулярне (не рідше разу на рік) проведення незалежного аудиту інформаційної безпеки таких об'єктів. Обов'язок розробити вимоги щодо проведення такого аудиту законом були покладено на Державну службу спеціального зв'язку та захисту інформації…

Як зазначає Костянтин Корсун, використана в проекті Вимог термінологія не відповідає ключовим міжнародним стандартам інформаційної безпеки ISO/IES 27000…

Мова йде про такі визначення, як «ризик», «вразливість» та ряд інших термінів проекту…

Однак набагато серйозніші проблеми у запропонованого проекту – з корупцією. Корсун звертає увагу на вимогу Держспецзв'язку до компаній, які матимуть право проводити аудити ОКІ: такі підприємства має очолювати лише «аудитор ІБ», а частка у статутному капіталі такої фірми має належати «аудиторам ІБ» не менш, ніж на 70%. Така норма, переконаний експерт, з'явилася завдяки корупційним зв'язкам між авторами документу та певними компаніями, які пролобіювали дивну вимогу в проекті постанови Кабміну…

– Корупція та войовнича некомпетентність у сфері регулювання інформаційної галузі та кібербезпеки набувають в Україні критичних форм. Якщо це не зупинити, матимемо чергову порцію мертвонародженої регуляції, яка працюватиме виключно на кишені окремих чиновників та близьких до них компаній, але жодним чином не сприятиме підвищенню кібербезпеки об'єктів критичної інфраструктури та інших не менш важливих інформаційних ресурсів країни, – підсумовує Костянтин Корсун…» ***(Експерти кепкують із «фахівців» Держспецзв'язку // Goodnews.ua (http://goodnews.ua/technologies/eksperti-kepkuyut-iz-faxivciv-derzhspeczvyazku/). 27.07.2018).***

***

«В Організації з безпеки і співробітництва в Європі закликали Раду переглянути законопроект, який дозволяє блокувати сайти без рішення суду.

Про це повідомляється в заяві представника ОБСЄ з питань свободи засобів масової інформації Арлема Дезіра…

Представник ОБСЄ зазначив, …що цей законопроект повинен містити чіткі заходи метою яких буде захист принципів прозорості, пропорційності та необхідності. В ОБСЄ закликали Україну уникнути застосування надмірних заходів, які можуть вплинути на поширення інформації в інтернеті…» ***(В ОБСЄ занепокоєні українським законопроектом про кібербезпеку // 7dniv.info – інформаційно-аналітичне інтернет видання (http://7dniv.info/events/103540-v-obsye-zanepokoien-ukraiinskim-zakonoproektom-pro-kberbezpeku.html). 07.07.2018).***

***

«У Раді зареєстровано проект закону Кабінету Міністрів № 8608 про внесення змін до деяких законів України, щодо вирішення питання збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів на випадок кібератак…

"З метою виконання заходів щодо нейтралізації чинників, які можуть призвести до реалізації загроз кібербезпеці... передбачено визначити Державну службу спеціального зв'язку та захисту інформації України органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів, а також встановлення порядку передачі, збереження і доступу до цих копій", — йдеться у пояснювальній записці до проекту закону…

"Одночасно, з метою усунення різночитання в термінології, що вже використовується в чинному законодавстві, в понятійний апарат законопроекту вводиться новий термін „державні електронні інформаційні ресурси"…» ***(Дмитро Кропивницький. Кабмін пропонує створити резервне сховище держінформації на випадок кібератак // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1741940-kabmin-proponuye-stvoriti-rezervne-skhovische-derzhinformatsiyi-na-vipadok-kiberatak). 18.07.2018).***

***

«В условиях проведения РФ гибридной войны против Украины украинским специалистам удалось установить общие черты у всех крупных кибератак и причастность к их проведению хакерских групп, действующих под контролем спецслужб РФ…

«В апреле 2018 года была обнаружена и локализована кибератака на объекты оборонно-промышленного комплекса государства, направленная на дискредитацию Украины на международной арене и распространение в информационном пространстве недостоверной информации относительно ряда объектов критической инфраструктуры, в частности ненадежности украинской стороны в сотрудничестве в научной и инженерной сферах», — отметил начальник Департамента контрразведывательной защиты интересов государства в сфере информационной безопасности СБУ Александр Климчук.

В то же время, специалисты ситуативного центра кибербезопасности СБУ обнаружили и своевременно отреагировали на кибератаку, направленную на информационные системы сектора безопасности и обороны Украины, в первую очередь, СБУ, Минобороны, ГПСУ и подразделений, которые привлечены к выполнению заданий в рамках Операции объединенных сил. Целью этой кибератаки было поражение компьютерных сетей этих ведомств и персональных компьютеров сотрудников для получения отдаленного доступа и похищения служебной информации.

По данным СБУ, данная кибератака была осуществлена хакерской группировкой, которая находится в аннексированном Крыму, с применением вредного программного обеспечения, известного как "Armagedon". Ранее данное программное обеспечение применялось спецслужбами РФ.

Кроме того, в мае Службой безопасности Украины во взаимодействии с представителями международных IT-компаний было предотвращено проведение масштабной кибератаки с использованием вредного программного обеспечения VPNFilter на государственные структуры и частные компании с целью дестабилизации ситуации во время проведения в Киеве финала Лиги Чемпионов УЕФА.

"Результаты проведенных исследований, в том числе во взаимодействии с ведущими IT-компаниями, указывают на общие черты всех кибератак, и причастности к их проведению известных СБУ хакерских групп, которые действуют под контролем спецслужб РФ…, — пояснил он.» ***(В СБУ объяснили, как вычисляют «почерк» кибератак из РФ // Goodnews.ua (http://goodnews.ua/technologies/v-sbu-obyasnili-kak-vychislyayut-pocherk-kiberatak-iz-rf/). 12.07.2018).***

***

«Правоохоронці блокували спробу російських спецслужб здійснити втручання у роботу мережевого обладнання товариства “Аульська хлороперелівна станція”, яке є об’єктом критичної інфраструктури країни…

Фахівці спецслужби у сфері кібербезпеки встановили, що протягом декількох хвилин системи управління технологічними процесами та системи виявлення ознак аварійних ситуацій підприємства були умисно уражені комп'ютерним вірусом VPNFilter з території РФ.

За даними спецслужби, продовження кібератаки могло призвести до зриву технологічних процесів та можливої аварії.

Співробітники СБУ у взаємодії із працівниками провайдера та "Аульської хлороперелівної станції" визначили місцезнаходження шкідливого програмного забезпечення VPNFilter та знешкодили його…» ***(Іра Огнєва. СБУ попередила кібератаку на стратегічно важливий об'єкт // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1740623-sbu-poperedila-kiberataku-na-strategichno-vazhliviy-obyekt). 11.07.2018).***

***

«Агресор і надалі використовуватиме кібератаки як один з інструментів геополітичного впливу. Про це заявив заступник Голови СБУ Олег Фролов під час 1-ї Конференції високого рівня керівників антитерористичних відомств держав-членів ООН у Нью-Йорку…

"Низка потужних та складних кібератак, цинічних за задумом та катастрофічних за можливими наслідками, на комп'ютерні мережі енергетичного, банківського, транспортного секторів, галузі зв'язку вкотре засвідчили намір агресора використовувати кібератаки як один з інструментів геополітичного впливу", — йдеться у заяві…» ***(Іра Огнєва. Кібератаки РФ як інструмент гібридної війни триватимуть і надалі – СБУ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1739052-kiberataki-rf-yak-instrument-gibridnoyi-viyni-trivatimut-i-nadali-sbu). 02.07.2018).***

***

«…експерт з питань кібербезпеки ряду урядових організацій США Клет Стівенс прокоментував агресивну інформаційну політику російських спецслужб в сегменті українського Інтернету…

Клет Стівенс підкреслив той факт, що поширення пропаганди не обмежується інформаційними і новинними ресурсами, а основна частина маніпуляції суспільною свідомістю відбувається на популярних платформах з піратською музикою і відео-контентом. Компанії, які монетизують інтернет-трафік, такі як "Adwise.agency", використовують велику кількість технічних пасток, що дозволяють збирати персональні дані користувачів, а після – передавати їх для тіньових політичних компаній і бізнес операцій.

…На думку Стівенса, діяльність таких компаній як "Adwise.agency" відкрито рекламує в Україні заборонений Yandex.ru і інші інструменти російської пропаганди, повинна жорстко регулюватися з боку українського уряду…

Стівенс бачить велику перспективу в об'єднанні зусиль українського та американського уряду в боротьбі з тіньовими платформами і наполягає на необхідності створення міжурядової органу з кібербезпеки, здатного зупинити діяльність подібних компаній.» ***(Україна – яскравий приклад: американський***

експерт розсекретив пропагандистську мережу // Телеканал новин «24» (https://24tv.ua/ukrayina__yaskraviy_priklad_amerikanskiy_ekspert_rozsekretiv_propagandistsku_merezhu_n993228?utm_source=rss). 03.07.2018).

***

«Російські хакери заражають комп'ютери українських компаній шкідливим ПЗ, що забезпечує несанкціонований доступ до них ("back doors") для масштабної координованої атаки.

Про це заявив керівник кіберполіції України Сергій Демедюк в інтерв'ю Reuters.

За його словами, хакери націлені на компанії, банки та енергетичну інфраструктуру через активацію шкідливого програмного забезпечення.

Так, з початку року поліція виявляє віруси в фішингових листах, відправлених з доменів державних установ, системи яких були зламані, та підроблені веб-сторінки, що імітують реальні сайти державних органів.

Демедюк повідомив, що, намагаючись уникнути виявлення, хакери впроваджують шкідливе програмне забезпечення у мережі компаній, розбивши його на окремі файли.

«Аналіз вже виявленого шкідливого ПЗ і націленість атаки на Україну свідчать про те, що все це готується на певний день», – сказав він…

«Все, що ми бачимо, все, що ми перехопили в цей період: 99% слідів ведуть до Росії», – додав Демедюк. Він додав, що українська поліція працює з іноземними урядами для виявлення хакерів…» ***(Маштабну кібератаку готують проти України російські хакери: назвали приблизну дату // «Урядовий кур'єр» (http://ukurier.gov.ua/uk/news/mashtabnu-kiberataku-gotuyut-proti-ukrayini-rosijs/). 03.07.2018).***

***

«На інформаційні ресурси Центральної виборчої комісії постійно здійснюються дрібні кібератаки, але протягом 2018 року не зафіксовано жодного випадку DDoS-атаки…

Водночас, як наголосили у відомстві, ЦВК разом із Держспецзв'язку та СБУ постійно "здійснюють заходи, спрямовані на посилення безпеки функціонування інформаційних ресурсів"….» ***(Олександр Сивачук. У ЦВК заявили, що на них постійно здійснюються дрібні кібератаки // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/exclusive/1742877-u-tsvk-zayavili-scho-na-nikh-postiyno-zdiysnyuyutsya-dribni-kiberataki). 23.07.2018).***

***

Боротьба з кіберзлочинністю в Україні

«С апреля 2017 по апрель 2018 неизвестные лица, используя электронно-цифровые ключи государственных исполнителей семи отделов государственной исполнительной службы ГТУЮ во Львовской области…, без

ведома последних, несанкционированно вмешались в работу Автоматизированной системы исполнительных производств, Государственного реестра прав на недвижимое имущество и Государственного реестра обременений движимого имущества, и самовольно сняли обременение с ряда объектов движимого и недвижимого имущества физических и юридических лиц. В список «жертв»-госисполнителей попали не только рядовые сотрудники ГИС, но даже и.о. начальника одного из отделов.

…общая сумма ущерба может превышать 350 миллионов гривен…

Среди объектов, с которых неизвестные сняли обременения, – имущество компании ПАО «Компания Росток» (долг компании перед кредиторами из правопреемника «Укринбанка», ПАО «Укр/Ин/Ком», по данным СМИ, составляет 350 миллионов гривен); комплекс нежилых помещений на 4 304,8 кв.м. в Николаеве (сумма, которую должен его собственник, «Николаевский бизнес-центр Александровский», кредиторам из ПАО «Укр/Ин/Ком» – более 16,6 миллионов гривен); квартира в Киеве; 98 единиц различной сельскохозяйственной техники, средней стоимостью 10 тысяч долларов каждая; десятки легковых автомобилей премиум и бизнес-сегмента, автобусов и многое другое…

Следствию удалось установить, где находились неизвестные, совершившее вмешательство в работу госисполнителей, и даже определить IP адреса и номера мобильных устройств, с которых неизвестные выходили в сеть. Однако, исходя из данных в судебном реестре, дальше следствие в поиске злоумышленников пока не продвинулось…». ***(Владимир Кондрашов. Арестованное имущество украли через интернет у исполнительной службы // Internetua (http://internetua.com/arestovannoe-imusxestvo-ukrali-cserez-internet-u-ispolnitelnoi-slujby). 13.07.2018).***

***

«Житель Одесской области заплатит в общей сложности 13 632 гривны за пользование интернетом местного провайдера с марта прошлого года по январь 2018-го за одну гривну в месяц.

Соответствующий приговор был вынесен Суворовским районным судом Одессы…

Как стало известно, первого марта прошлого года житель Лиманского района Одесской области зашел на сайт своего провайдера ООО «ТРК «Бриз» и в личном кабинете, перейдя на страницу изменения пакета услуг, «используя уязвимости в свойствах страницы личного кабинета сайта и работы системы установления тарифного плана, совершил несанкционированное вмешательство в работу автоматизированной системы ООО ТРК «Бриз»». В суде доказали, что обвиняемый «на языке web-программирования отправил серверу «Apache» Интернет-провайдера модифицированный «POST» запрос, в результате работы которого сервер получил команду об изменении стандартного тарифного плана и присвоении абоненту скрытого пакета услуг с идентификатором «100». Данный пакет услуг значится в ООО ТРК «Бриз» как «Безлимитный-30», который доступен исключительно сотрудникам компании. Стоимость пользования такой услугой составляет 1 гривну в месяц.

Таким образом. говорится в приговоре, обвиняемый причинил провайдеру материальный ущерб на общую сумму 3577,80 гривен…» ***(Владимир Кондрашов. Житель Одесской области заплатит 13 тысяч за интернет по 1 гривне // Internetua (http://internetua.com/jitel-odesskoi-oblasti-zaplatit-13-tsyacs-za-internet-po-1-grivne). 10.07.2018).***

***

«За перші шість місяців 2018 року працівники Департаменту кіберполіції супроводжували більше чотирьох тисяч кримінальних правопорушень у сфері протидії кіберзлочинності, з них - 2,3 тисячі – викрито протягом 2018 року…

За словами начальника Департаменту кіберполіції Сергія Демедюка, серед основних напрямків діяльності підрозділу слід відмітити позитивну роботу з протидії злочинам у сфері кібербезпеки, платіжних систем, електронної комерції та боротьбу зі злочинами у сфері поширення протиправного контенту. Водночас, він відмітив стрімке збільшення кількості кримінальних правопорушень у сфері платіжних систем та кібербезпеки у літній період…» ***(Кіберполіція відмічає збільшення кількості правопорушень у сфері платіжних систем та кібербезпеки // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vidmichaye-zbilshennya-kilkosti-pravoporushen-u-sferi-platizhnyx-system-ta-kiberbezpeky-1519/). 14.07.2018).***

***

«Бухгалтерська програма M.E.Doc – стала першим IT-продуктом, що знаходиться під захистом Ситуаційного центру забезпечення кібербезпеки СБУ.

…Результатом такої синергії став Меморандум, який Служба безпеки України підписала з компанією Linkos Group з метою розвитку ефективної системи кібербезпеки держави. …Портфель Linkos Group включає в себе такі бренди як: M.E.Doc, СОТА, АЦСК «Україна», Звіт Корпорація, FlyDoc, ISpro, ПТАХ, Твій Час.

В рамках Меморандуму Ситуаційний центр забезпечення кібербезпеки СБУ підключив Linkos Group до платформи MISP-UA…

MISP-UA виконує функцію інформаційного щита в режимі реального часу, що знаходиться попереду IT-інфраструктури компанії та забезпечує не лише захист, а й протидію, реакцію і нейтралізацію кіберінцидентів. Ця платформа є сенсором кіберзагроз. Вона працює з 59 світовими каналами, що ведуть постійний обмін інформацією про кіберподії, має саме актуальне наповнення бази ідентифікаторів компрометації. Постійно оновлюється та наповнює світові системи захисту інформації даними про підозрілу поведінку інформаційних систем. Проводить аудит та аналіз, що здатні передбачити шляхи атаки та загрози…» ***(M.E.Doc під захистом СЦ кібербезпеки СБУ // МЕТА (http://pr.meta.ua/read/55060). 11.07.2018).***

***

«СБУ для розбудови ефективної системи кібербезпеки держави підписала Меморандум з державним підприємством «Антонов».

Документ має забезпечити обмін у режимі реального часу технологічними даними щодо кіберінцидентів з використанням платформи MISP-UA…» ***(СБУ і "Антонов" підписали меморандум щодо обміну даними про кібератаки в режимі реального часу // Goodnews.ua (http://goodnews.ua/technologies/sbu-i-antonov-pidpisali-memorandum-shhodo-obminu-danimi-pro-kiberataki-v-rezhimi-realnogo-chasu/). 11.07.2018).***

***

«Следственное управление ГУ Национальной полиции в Черновицкой области занимается делом киберпреступника, который в сети продавал вредоносное компьютерное обеспечение и даже обучал менее опытных коллег методикам проведения DDoS-атак…

Согласно материалам досудебного расследования, житель, предположительно, Черновцов, зарегистрированный на «хакерских форумах» под логином Ytka, с 2017 года выставлял на продажу учетные записи, «стиллеры» (вредоносные программы, позволяющие похищать сохраненные в системе логины и пароли), частные ботнеты и скрытые майнеры криптовалют. Кроме того, Ytka предлагал и услуги по частному обучению проведения DDoS-атак…

Пока не установлено, кто именно покупал «товары», предлагаемые Ytka, и кого подозреваемый обучал проведению DDoS-атак…» ***(Владимир Кондрашов. Полиция вычислила "киберпреступника-учителя" // Internetua (http://internetua.com/kiberpoliciya-vychislila-kiberprestupnika-ucsitelya). 23.07.2018).***

***

«ПриватБанк попередив клієнтів про нову схему шахрайства з використанням підробленого сайту "Приват24"…

За даними фахівців банку, вже зафіксовані випадки, коли клієнтам через різноманітні канали комунікацій (месенджери, електронну пошту) приходить повідомлення про поповнення карти невідомою особою на кілька тисяч гривень. Далі шахраї пропонують перейти по посиланню на фальшиву квитанцію з фішинговим сайтом "Приват24".

У банку застерегли від відкриття таких повідомлень від шахраїв…» ***(Юлія Шрамко. Шахраї придумали нову схему з "Приват24" // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1741934-shakhrayi-pridumali-novu-skhemu-z-privat24). 18.07.2018).***

***

«…Працівники Слобожанського управління Департаменту кіберполіції Національної поліції України викрили двох студентів коледжу, які збували шкідливе програмне забезпечення для прихованого видобутку криптовалют.

За даним фактом було розпочато кримінальне провадження за ч.2 ст.361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України.

Оперативники кіберполіції встановили, що шкідливе програмне забезпечення спільники придбали на одному з хакерських форумів. Змінивши його, студенти пропонували купити це програмне забезпечення іншим зацікавленим особам.

Окрім збуту вірусу, студенти використовували його і для власних потреб. Вони розміщували на форумах та інших інтернет-ресурсах посилання на фейкове програмне забезпечення, вражене цим вірусом, та, з його допомогою, видобували криптовалюту…» ***(Кіберполіція викрила студентів технічного вишу у поширенні шкідливої програми для прихованого майнінгу крипто валют // Кіберполіція (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-studentiv-texnichnogo-vyshu-u-poshyrenni-shkidlyvoyi-programy-dlya-pryxovanogo-majningu-kryptovalyut-234/). 18.07.2018).***

***

«Хакеру, который в июле и сентябре 2017 года взламывал сайт Министерства образования Украины и размещал там обнаженные фото своей знакомой, грозит штраф в размере 1000 необлагаемых налогом доходов граждан (17 тысяч гривен).

Об этом свидетельствует определение Шевченковского районного суда города Киева…

Согласно материалам дела, в июле 2017 подозреваемый, "с целью унижения и публичного освещения личной жизни своей знакомой", зная, что последняя работала в Министерстве образования и науки Украины, спланировал осуществить несанкционированное вмешательство в компьютерную сеть (официальный интернет-сайт Министерства образования и науки Украины), и заблокировать доступ к основным функциям сайта и к информации, которая на нем находится, "путем размещения на главной странице сайта www.mon.gov.ua фотоснимков обнаженной знакомой и нецензурных выражений о последней"…» ***(Владимир Кондрашов. Хакер опубликовал фото обнаженной подружки на сайте Минобразования // Internetua (http://internetua.com/haker-opublikoval-foto-obnajennoi-podruzgki-na-saite-minobrazovaniya). 30.07.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«…Спільну декларацію про співробітництво підписали президент Єврокомісії Жан-Клод Юнкер, президент Європейської ради Дональд Туск та генеральний секретар НАТО Єнс Столтенберг…

Документ передбачає посилення співпраці ЄС та НАТО у таких сферах як військова мобільність, спільна підготовка до кібератак та гібридних атак, боротьба

з тероризмом та нелегальною міграцією у Середземному морі…» ***(ЄС і НАТО домовились про співпрацю // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/yes-i-nato-domovilis-pro-spivpratsyu.html). 11.07.2018).***

***

«Учасники 20-го саміту Україна - Євросоюз домовилися координувати кроки з протидії загрозам втручання у вибори, зокрема кібератакам і кампаніям з дезінформації, повідомив український президент Петро Порошенко…

"Без сумніву, Кремль спробує знову втрутитися, але на цей раз ми будемо готові. Ми погодилися координувати і робити спільні заходи для протидії загрозам втручання будь-якого характеру, незалежно від того, це кампанія з дезінформації або кібератаки", - сказав глава Української держави …» ***(Україна і ЄС домовилися координувати кроки з протидії загрозам втручання у вибори // Інтерфакс-Україна (https://ua.interfax.com.ua/news/political/516906.html). 09.07.2018).***

***

«В ряде городов Донецкой и Луганской областей специалисты проекта «Team 4 Ukraine» из Чехии проводят встречи с общественностью, направленные на обучение населения основам кибербезопасности…

Эксперты уже посетили Авдеевку, Славянск и Краматорск. Петр Пойман отметил, что основным вопросом, который волнует жителей прифронтового Донбасса, является защита личных данных в социальных сетях и противостояние российской пропаганде в интернете…» ***(Европейские специалисты обучат жителей Донбасса основам кибербезопасности // Информационное агентство «Вчасно» (https://vchasnoua.com/donbass/56944-evropejskie-spetsialisty-obuchat-zhitelej-donbassa-osnovam-kiberbezopasnosti). 13.07.2018).***

***

«Выявлять угрозы и лидеров, их генерирующих, предупреждать и противостоять дестабилизации обстановки в регионе будут сами жители. Таков основной смысл проекта «Стійка Україна», направленный на усиление национальной безопасности страны. На первом этапе специалисты Международного центра безопасности и обороны при поддержке правительства Эстонии провели масштабные социологические исследования в трех областях, прилегающих к зоне военных действий.

…Около 2000 социологических опросов, психолингвистический анализ более 600 миллионов профилей в социальных сетях, фокус-группы и глубинные интервью на территории Харьковской, Донецкой и Луганской областей показали: в нацбезопасности Украины есть три главных пробела, говорит руководитель проекта, исполнительный директор аналитического центра по обороне и безопасности Эстонии Дмитрий Теперик.

«Это область коммуникационной безопасности, вторая область – информационная безопасность (это работа с медиа-пространством, с каналами

информации и инфраструктурой). И третья область – кибербезопасность, все, что связано с IT-системами, с программированием, с кодами», – уточнил он.

Это три области, в которых в Эстонии есть определенная компетенция, и она пригодится Украине…

«Есть лига кибер-безопасности Эстонии, которая имеет полномочия от лица государства помогать отражать кибер-атаки. В нее входят добровольцы – специалисты, которые каждый день ходят на работу, связанную с IT-областью, но на выходных или в свободное время, по вечерам могут помогать государству отражать кибер-атаки или мониторить кибер-пространство», – рассказал эксперт…

Не смотря на то, что за спиной Эстонии есть мощный военный союзник в лице НАТО, эта страна осознает все риски информационных атак, учится действовать привентивно, создает инструменты для такой борьбы и намерена помочь Украине….

До 2020 года инициаторы проекта планируют устранить все пробелы в эффективном сотрудничестве государства и гражданского общества…» ***(Ірина Горбасьова. Как добровольцы помогают защищать государство: опыт Эстонии // Радіо Свобода (https://www.radiosvoboda.org/a/donbass-realii/29343073.html). 05.07.2018).***

***

«Палата представників Конгресу США ухвалила проект закону про «Бюджет США на 2019 року на потреби національної оборони»…

До документа включено основні положення проекту «Закону про співпрацю з Україною з питань кібербезпеки». Він передбачає допомогу Україні у посиленні власних спроможностей щодо захисту від кібератак.

Зокрема, Державному департаментові доручили подати до Конгресу доповідь про стан співробітництва з Україною у сфері кібербезпеки, щоб шукати нові напрями взаємодії і підтримки…» ***(США можуть виділити $250 млн на безпеку України // "Українські медійні системи" (https://glavcom.ua/news/ssha-mozhut-vidiliti-250-milyoniv-na-bezpeku-ukrajini-515944.html). 27.07.2018).***

***

«Белый дом собирается поддержать проект оборонного бюджета США, в котором говорится о предоставлении Украине помощи в размере $250 млн, сообщила пресс-секретарь администрации президента США Сара Сандерс…

Отмечается, что документ включает положения о продолжении сотрудничества с Украиной в вопросе кибербезопасности, который предусматривает помощь Киеву в усилении собственных возможностей по защите от кибератак.

Также в разделе об "усилении сдерживания российской агрессии в Европе" говорится об усилении политики безопасности в помощи Украине и поддержку реформ оборонного сектора…» ***(Белый дом готов поддержать оборонный бюджет, в котором предусмотрена помощь Украине // Фокус (https://focus.ua/world/402864/). 30.07.2018).***

***

«У понеділок протокол про намір створити сили швидкого кібернетичного реагування підписали в Люксембурзі міністри оборони Литви, Естонії, Хорватії, Нідерландів і Румунії. Франція, Іспанія, Польща та Фінляндія до ініціативи долучаться до кінця року…

Країни ЄС передбачають створення кібернетичних команд з ротацією кожні шість місяців…

За словами міністра оборони Литви Раймундаса Каробліса, з інститутами ЄС буде обговорена можливість використання в рамках проекту коштів бюджету Співтовариства для закупівель устаткування і програмного забезпечення. До проекту на правах спостерігачів приєднаються ще чотири країни - Бельгія, Греція, Словенія та Німеччина…» ***(Анастасія Ткачук. П'ять країн ЄС створять кібернетичні сили // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1737962-pyat-krayin-yes-stvoryat-kibernetichni-sili). 25.07.2018).***

***

Світові тенденції в галузі кібербезпеки

«Согласно исследованию, проведенному консалтинговой компанией Juniper Research, стало известно, что решения по кибербезопасности для индустрии Интернета вещей (IoT) достигнут $6 млрд к 2023 году…

По данным исследования, главными двигателями решений по кибербезопасности для рынка IoT станут растущие бизнес-риски и нормативно-правовые стандарты. Так, расходы на обеспечение безопасности объектам смарт-жилья в 2023 году будут составлять менее 17%. Ожидается, что расходы на безопасность умных сетей энергоснабжения достигнут $1 млрд через пять лет…

Что касается проблем в отношении IoT, то по мнению 54% респондентов, повышенные риски, связанные с внедрением экосистем IoT, представляют собой серьезную проблему…» ***(IoT и проблемы безопасности: чего ожидать через 5 лет — исследование // PaySpaceMagazine «доступно о платежах» (https://psm7.com/news/iot-i-problemy-bezopasnosti-chego-ozhidat-cherez-5-let-issledovanie.html). 12.07.2018).***

***

«ESET подписала технологическое соглашение по кибербезопасности – договор между крупными компаниями технологического сектора, которые обязуются защищать от киберпреступности пользователей во всем мире.

Технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord) объединяет больше 40 компаний. Среди участников альянса – Facebook, Microsoft, SAP, Oracle, Cisco, HP, Dell, VMware и другие….

Создание соглашения стало ответом на масштабные инциденты прошлых лет, включая эпидемию шифратора WannaCry в 2017 г. Альянс открыт для частных компаний с безупречной репутацией и высокими стандартами кибербезопасности, готовых соблюдать принципы соглашения…». ***(Владимир Смирнов. ESET вместе***

с Cisco, Microsoft, Oracle и SAP защитит от киберугроз // ChannelForIT (http://channel4it.com/publications/ESET-vmeste-s-Cisco-Microsoft-Oracle-i-SAP-zashchitit-ot-kiberugroz-31005.html#). 04.07.2018).

***

«Аналитики компании InfoWatch …проанализировали около 70 случаев утечек данных из российских и иностранных компаний в течение прошлого года, а также публичные сообщения о подобных деструктивных действиях бывших сотрудников компаний в отношении информационных активов работодателя.

…чаще всего деструктивным действиям подвержены медицинские учреждения и госструктуры. Почти каждый второй (60%) увольняемый неправомерно копировал и передавал (54%) конфиденциальную информацию третьим лицам, в том числе конкурентам и преступникам.

…в половине случаев (52,8%) передача данных повлекла за собой прямой ущерб для работодателя. Чаще всего речь идет о том, что конкурент получил сведения о разработках или необходимость компенсировать затраты третьих лиц, чья информация обрабатывалась компанией и была скомпрометирована.

В исследовании говорится, что причиной подобных утечек становятся нелояльные сотрудники. В основном это рядовые сотрудники (81% нарушений), а на топ-менеджеров или системных администраторов приходятся остальные 19% случаев. Главным мотивом для рядовых сотрудников является личная выгода: работа на конкурента или вред из мести.» ***(Валерий Вискалин. Исследование: эксперты назвали причину утечек информации в компаниях // Rusbase (https://rb.ru/news/utechki-prichina/). 17.07.2018).***

***

«Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) объявил о решении с 1 августа 2018 года прекратить использование 11 устаревших специальных публикаций из серии NIST SP 800. Документы по-прежнему будут доступны, однако более не будут подвергаться пересмотру или замене…

Документы NIST SP 800 концентрируются вокруг кибербезопасности и содержат руководства, технические спецификации, рекомендации и годовые отчеты. Публикации направлены на обеспечение и поддержку нужд государственных структур в сфере кибербезопасности и конфиденциальности, но нередко используются и частными компаниями. В настоящее время на сайте института размещены более 180 документов SP 800, включая проекты и финальные версии.» ***(С 1 августа NIST отзовет 11 рекомендаций по кибербезопасности // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=124093). 19.07.2018).***

***

«…в исследовании SANS Institute "Обзор защиты конечных точек и реагирования на киберинциденты" (Survey on Endpoint Protection and Response)… указывается, что примерно 50% коммерческих организаций,

представителей которых опрашивали в рамках исследования, инвестировали в nextgen-технологии, но 37% так и не внедрили их в полной мере. У 49% компаний есть средства выявления бесфайловых кибератак, но 38% также не используют их для защиты своих систем …

Исследователи опросили 277 ИТ-экспертов на тему того, какие угрозы волнуют их больше всего. 42% респондентов ответили, что ключевой угрозой они считают эксплойты для конечных точек. Годом ранее основной эту проблему называли 53% респондента. При этом уже 20% респондентов заявили, что не имели понятия о случившихся в их инфраструктуре инцидентах…

В то время как бизнес-структуры все активнее вкладываются в самые передовые технологии киберзащиты, они испытывают серьезные проблемы с их внедрением и использованием. Между тем, традиционные инструменты теряют эффективность: по данным исследования, только в 47% случаев антивирусы для конечных точек смогли идентифицировать взлом; в 32% сигнал тревоги подали автоматизированные SIEM-системы, еще в 26% случаев — продвинутые платформы обнаружения и реагирования на киберугрозы…

На сегодняшний день, как указывается в исследовании, большая часть атак на конечные точки по сути нацелена на их пользователей, а не на уязвимости в ПО. Более чем половина респондентов отметили атаки типа drive-by, 53% — фишинговые атаки и прочие примеры социальной инженерии. Также 50% респондентов отметили, что им приходилось иметь дело с шифровальщиками-вымогателями. В 40% инцидентов фигурировали украденные реквизиты доступа.

Эксперты отмечают, что в 84% случаев кибератаки на конечные точки затрагивают более одного устройства. В то время как чаще всего атакуют настольные компьютеры и ноутбуки, в прицел злоумышленников нередко попадают серверы, облачные устройства, SCADA-системы и промышленные устройства интернета вещей…» ***(SANSInstitute: сверхпродвинутые антивирусы на три четверти не используются // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=124076). 18.07.2018).***

***

«Совет по финансовой стабильности (Financial Stability Board, FSB) опубликовал краткий словарь терминов по кибербезопасности под названием Cyber Lexicon. Словарь включает набор из 50 основных терминов, связанных с защитой от киберугроз в финансовом секторе.

…Приведенная в словаре лексика может быть полезной для обеспечения защиты от киберугроз, оценки и мониторинга рисков финансовой стабильности и кибербезопасности, а также для обмена важной информацией.

…В дальнейшем Совет по финансовой стабильности планирует дополнить словарь и внести некоторые правки…» ***(Совет по финансовой стабильности обнародовал словарь по кибербезопасности // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=124035). 17.07.2018).***

***

«Страховые компании Lexington Insurance Company и Beazley Insurance Company подали в суд на фирму по кибербезопасности Trustwave с целью возмещения средств, выплаченных клиентам. Trustwave обвиняется в неспособности обнаружить вредоносное ПО в сети Heartland Payment Systems в течение нескольких месяцев, что привело к одной из самых серьезных утечек данных в 2000-х годах…

В январе 2009 года Heartland Payment Systems, предоставляющая услуги процессингового центра для обработки данных с пластиковых банковских карт, сообщила о крупной утечке данных. По словам представителей компании, услугами которой пользуются масса западных коммерческих банков, злоумышленникам удалось проникнуть в сети фирмы и получить доступ к информации о банковских картах.

В рамках страховых соглашений Lexington Insurance Company и Beazley Insurance Company заплатили Heartland Payment Systems $30 млн. Однако, как следует из гражданского иска, страховые компании пытаются возместить данные расходы, утверждая, что фирма Trustwave, с которой Heartland заключила контракт на обслуживание, не выполнила свою часть договора.

В частности, Trustwave не смогла выявить атаку 24 июля 2007 года, а также допустила установку вредоносного ПО на серверы своего клиента 14 мая 2008 года. Согласно иску, Trustwave не обнаружила признаков подозрительной активности во время проверок безопасности, которые она предоставляла Heartland в течение двух лет в рамках контракта. В свою очередь представители Trustwave направили встречный иск против страховщиков, а также назвали их требования необоснованными.» ***(На ИБ-компанию Trustwave подали в суд за неспособность обнаружить вредоносное ПО // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123932). 10.07.2018).***

***

«Объем продаж аппаратных и программных средств, а также услуг, связанных с информационной безопасностью, в 2018 году вырастет в мире на 10,2% и достигнет 91,4 млрд долл.

Больше 27 млрд долл. в сумме потратят на закупки технологий безопасности банки, компании отрасли дискретного производства (в первую очередь высокотехнологичного) и государственные структуры. По 5 млрд долл. и более приходится еще на четыре отрасли (непрерывное производство, профессиональные услуги, потребительский рынок и телекоммуникации).

Больше 18 млрд долл. в 2018 году уйдет на оплату управляемых сервисов безопасности (арендных систем, управляемых сторонними провайдерами, но располагающихся на платформе клиента). Второй по величине сектор технологий — аппаратные средства сетевой безопасности. За ними следуют услуги интеграции и ПО для защиты устройств пользователей.

К 2020 году, полагают аналитики, 30% рынка технологий безопасности займут поставщики, предлагающие интегрированные платформы безопасности (Unified Threat Management, UTM)…» ***(IDC: мировой рынок технологий***

безопасности в 2018 году превысит 91 миллиард долларов // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123831). 04.07.2018).

***

«Немецкий корпоративный cloud- и хостинг-провайдер Colobridge подготовил аналитический обзор ключевых проблем корпоративной кибербезопасности за 2013-2017 гг…

Документ содержит 39 графиков, подготовленных на основе анализа статистических данных авторитетных источников (Verizon, Symantec, Ponemon Institute, Infowatch, Gemalto и др.). Графики подробно иллюстрируют количество утечек или скомпрометированных учетных записей, типы скомпрометированных данных, стоимость утечек и их последствия, источники киберугроз и другие причины потери данных, мишени киберпреступников…» ***(Выяснилось, кто чаще всего стоит за утечкой корпоративной информации // Goodnews.ua (http://goodnews.ua/technologies/vyyasnilos-kto-chashhe-vsego-stoit-za-utechkoj-korporativnoj-informacii/). 27.07.2018).***

***

Сполучені Штати Америки

«…Согласно докладу De Correspondent и Bellingcat, через фитнес-приложение и трекер физической активности Polar Flow можно найти информацию о тренировках и использовать ее для идентификации сотрудников, работающих на военных базах и в правительственных зданиях.

Технология включала доступ к API разработчика Polar. Через API можно не только изучить общедоступные данные, но и получить приватную информацию. API также не ограничивал количество запросов, поэтому возможно, что кто-то мог собрать данные о миллионах пользователей.

…По информации De Correspondent, достаточно найти государственное или военное сооружение, затем поискать данные о тренировках в этой локации, а потом изучить другие тренировки пользователя…

В Polar признали проблему и заявили, что в ближайшее время ее решат…» ***(Ирина Фоменко. Интернет вещей не подходит для шпионов // Internetua (http://internetua.com/internet-vesxei-ne-podhodit-dlya-shpionov). 10.07.2018).***

***

«С октября прошлого года Twitter вдвое больше заблокировал фейковых аккаунтов в рамках постоянной борьбы с поддельными учетными записями, в том числе ботами и интернет-троллями…

Компания продолжает обеспечивать контроль после президентских выборов в США в 2016 году, спровоцировавших скандалы, связанные с пропагандой, дезинформацией и преследованиями в социальных сетях.

… компания блокирует до 1 миллиона фейковых профилей в день, а в мае и июне заблокировала 70 миллионов аккаунтов. Существенная часть процесса автоматизирована.

Автоматизированные системы идентифицируют около 10 миллионов учетных записей в месяц. …Как заявляют в Twitter, компания блокирует создание 50 000 подозрительных учетных записей в день.

Большинство экспертов уверены, что значительное количество профилей – фейковые. …"чистка" может привести к снижению идентификации пользователей Twitter во втором квартале этого года. Идентификация, демонстрирующая медленный рост и фактическое снижение числа пользователей, может негативно повлиять на акции компании…» ***(Ирина Фоменко. Твиттер наносит удар по ботам // Internetua (http://internetua.com/twitter-nanosit-udar-po-botam). 09.07.2018).***

***

«Американские СМИ обратили внимание на то, что в тот день, когда президент США Дональд Трамп в шутку призвал Россию помочь в поисках 30 тысяч писем, удаленных кандидатом в президенты от демократов Хиллари Клинтон, на аккаунты ее офиса проводилась кибератака…

Журналисты BuzzFeed обратили внимание на то, что Трамп именно в этот день призывал российских хакеров найти электронные письма Клинтон…

Трамп также призывал Россию «или любую другую страну или человека» опубликовать электронные письма Клинтон. Впрочем, на следующий день он признал, что «это был сарказм»…» ***(Алексей Ласнов. «Русские хакеры» атаковали почту Клинтон «по просьбе Трампа» // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/13/932421.html). 13.07.2018).***

***

«***9 компаній, що відповідають за кібербезпеку США***

…CyberArk Software (акції торгуються на біржі NASDAQ під індексом CYBR)

…Ця компанія займається питаннями привілейованого доступу та захисту даних. Серед запропонованих нею рішень — безліч функцій, включаючи захист та управління обліковими записами, ізоляція сеансів користувача та моніторинг змін даних.

Cisco (торгує акціями на NASDAQ під індексом CSCO)

…Серед продуктів цієї компанії є низка сервісів для хмарних технологій, електронної пошти, локальних мереж, роутерів. Опікується сектором захисту від загроз та мережевими рішеннями для компаній і державних установ.

IBM (акції продаються на Нью-Йоркській фондовій біржі під індексом IBM)

…Компанія відома своїми корпоративними рішеннями щодо IT-безпеки, які охоплюють мобільні, дані, мережі та кінцеві рішення. IBM використовує штучний інтелект, а також хмарні платформи для захисту та виявлення загроз.

Microsoft (на біржі NASDAQ під індексом MSFT)

…Корпорація надає численні інструменти для протидії кіберзлочинності, починаючи від свого головного продукту Windows Defender до своїх хмарних центрів відповідності безпеки Azure та офісного продукту Office 365.

Amazon (Amazon Web Services) (на біржі NASDAQ, має індекс акцій AMZN)

…головною її спеціалізацією є хмарні дата-центри та рішення для захисту даних, а також інфраструктура, платформенні рішення та міграція сервісів і компаній під час DDoS-атак на їхні власні ресурси.

FireEye (акції на NASDAQ мають індекс FEYE)

…Компанія відома за своїми передовими службами захисту від кіберзагроз. Пропонує численні рішення для формування служб захисту від хакерів на корпоративному рівні — від електронного листування до локальних мереж та інтелектуальних систем.

Lockheed Martin (акції у лістингу Нью-Йоркської фондової біржі, індекс LMT)

…Американська компанія, яка має свої інтереси у аерокосмічній, оборонній галузі, також займається технологіями кіберзахисту та …на ринку онлайн-технологій відома завдяки рішенням та послугам для кібербезпеки, Також займається дата-центрами та обробкою даних.

Check Point Software (на NASDAQ під індексом CHKP)

…Займається питаннями єдиного захисту та уніфікованих рішень при пошуку та блокуванні кіберзагроз. Ця компанія пропонує низку продуктів для захисту як мобільних, так і наземних мереж, хмарних сервісів та налаштування рівня доступу до файлів і даних.

Symantec (біржа NASDAQ, індекс SYMC)

…Компанія є лідером у різних сферах кібербезпеки — як для кінцевих, так і для корпоративних споживачів у США та за межами Сполучених Штатів…» ***(Олександр Мельник. На сторожі незалежності — 9 компаній, що відповідають за кібербезпеку США // Na chasi (https://nachasi.com/2018/07/04/na-storozhi-nezalezhnosti/). 04.07.2018).***

***

«Недавно в сфере военно-воздушной промышленности США произошел невиданный ранее инцидент – специальная мониторинговая группа Instinkt Group, принадлежащая компании Recorded Future, отыскала на просторах даркнета украденный набор военных документов относительно технических характеристик беспилотного военного дрона USAF MQ-9, который был зарегистрирован в ВВС США не так давно. …Таким образом, специалисты из Instinkt Group сумели отыскать те самые документы, которые продавались неким англоговорящим хакером…

Специалистам из компании Recorded Future удалось отследить следы попадания секретных военных документов на летательный беспилотный дрон MQ-9, все еще находящийся на стадии тестирования и проверки, и они выявили, что некий злоумышленник продавал их всего за 200 долларов США …техническая информация в документах главным образом касалась таких тем, как расположение топлива и груза…» ***(Роман Розенталь. В Даркнете найдены утерянные***

документы на военный дрон USAF MQ-9 // Faina Idea (http://www.fainaidea.com/technologii/transport/v-darknete-najdeny-uteryannye-dokumenty-na-voennyj-dron-usaf-mq-9-146909.html). 12.07.2018).

***

«Три ведущих сотрудника по кибербезопасности ФБР уходят в отставку…

Дэвид Реш, глава отдела кибербезопасности в подразделении агентства, которое занимается расследованием финансовых преступлений и организованной преступности; Скотт Смит, помощник директора ФБР и глава киберподразделения; и депутат Говард Маршалл - либо уже ушли, либо уйдут в течение месяца.

Карл Гаттас и Джеффри Триколи, старшие агенты, ответственные за расследования национальной безопасности, включая безопасность выборов, ушли из ФБР в начале этого года…» ***(Ирина Фоменко. Лучшие сотрудники по кибербезопасности бегут из ФБР // Internetua (http://internetua.com/lucsshie-sotrudniki-po-kiberbezopasnosti-begut-iz-fbr). 26.07.2018).***

***

«США принесли официальные извинения Москве за срыв консультаций по кибербезопасности, сообщил спецпредставитель президента по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям Андрей Крутских…

Российско-американская встреча по кибербезопасности на уровне экспертов должна была пройти в Женеве в феврале. Однако американская сторона в последний момент отказалась от участия…» ***(США официально извинились за срыв переговоров по кибербезопасности // «Парламентская газета» (https://www.pnp.ru/politics/ssha-oficialno-izvinilis-za-sryv-peregovorov-po-kiberbezopasnosti.html). 19.07.2018).***

***

«…Согласно исследованию компании по кибербезопасности Coronet, многие сети Wi-Fi не зашифрованы, небезопасны и настроены ненадлежащим образом.

…в Coronet изучили данные 45 самых загруженных американских аэропортов за 5 месяцев этого года. Затем каждому из них присвоили оценку индекса угрозы на основе уязвимости устройств и риска использования сетей.

…есть три основных вещи, которыми пользователь рискует, подключаясь к публичной сети Wi-Fi…

Многие вредоносные общедоступные сети Wi-Fi выглядят, как любая другая сеть. Но когда пользователь нажимает "принять условия", чтобы подключиться, так можно установить вредоносное ПО на свое устройство…

Если пользователь подключен к опасной сети, он может стать целью фишинга. По данным Федеральной торговой комиссии, хакер создает веб-страницу, которая выглядит точно так же, как и другая, например, для входа в чужую

электронную почту. Когда пользователь вводит свой логин и пароль, он фактически вводит свою информацию на сайт хакера…

Третий пункт особо важен для бизнесменов, работающих во время поездок. Если пользователь подключен к опасной сети и передает данные кому-либо из коллег, они проходят через устройства злоумышленника…» ***(Войдите в сеть через Wi-Fi аэропорта и будете взломаны // Goodnews.ua (http://goodnews.ua/technologies/vojdite-v-set-cherez-wi-fi-aeroporta-i-budete-vzlomany/). 19.07.2018).***

***

«Вокруг подаренного Путиным Трампу футбольного мяча раздавался хор предостережений, дескать, в сувенире ЧМ могут быть жучки…

"Метки на мяче указывают на то, что в нем есть чип с крошечной антенной, которая передает сигнал на телефоны неподалеку. Но это не шпионское устройство, а рекламируемая Adidas функция мяча", - сообщает журналист Bloomberg Вернон Сильвер.

При изготовлении мяча внутрь него помещают чип NFC - под логотипом, напоминающим иконку WiFi. "Благодаря чипу фанаты, поднося свои мобильные устройства к мячу, могут получить доступ к видеозаписям с игроком, матчам и другому контенту", - поясняет журналист.

В Adidas отказались комментировать, может ли чип стать средством хакерской атаки…» ***(В футбольном мяче, который Путин подарил Трампу, есть чип с передатчиком // Украинское рейтинговое агентство "УРА" (http://ura-inform.com/ru/interesno/2018/07/26/v-futbolnom-mjache-kotoryj-putin-podaril-trampu-est-chip-s-peredatchikom). 27.06.2018).***

***

Країни ЄС

«Комітет міністрів Ради Європи опублікував нові рекомендації для країн-членів спільноти з метою захисту прав дітей у цифровому середовищі - Інтернеті, мобільних пристроях, соціальних мережах…

В Організації закликають держави вжити конкретних заходів для захисту дитини від передчасного впливу цифрового середовища. Зокрема, дітям слід роз'яснити їх права і свободи, існуючі обмеження, а також прищепити повагу до чужої гідності і виробити протидію до розпалювання ворожнечі. Крім того, слід підвищувати їх юридичну грамотність з тим, щоб запобігати у майбутньому порушенню прав інтелектуальної власності.

Крім того, в Раді Європи порекомендували готувати дітей до активної участі у "цифровому громадянстві". З іншого боку, держави зобов'язуються забезпечити захист персональних даних і недоторканність приватного життя майбутнього громадянина…

Крім того, для дітей і їхніх представників повинні бути забезпечені доступні засоби правового захисту і подачі скарг - як судових, так і несудових…» ***(Ira***

Огнєва. Рада Європи роз'яснила права дітей у цифровій сфері // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1739544-rada-yevropi-rozyasnila-prava-ditey-u-tsifroviy-sferi). 04.07.2018).

***

«Вероятность распространения кибернетических атак и возможное их воздействие на финансовую систему Литвы является крупнейшим риском, свидетельствуют результаты новейшего опроса финансовых учреждений, проведенного Центробанком (Банк Литвы)…

Согласно результатам опроса, в первом полугодии четыре из 29 опрошенных финансовых учреждений сталкивались с риском, который представляют кибернетические преступления, а одно из них понесло убытки, сообщил Центробанк…» ***(Банк Литвы: кибератаки остаются крупнейшим риском для финансовой системы // mResearcher (https://mresearcher.com/2018/07/bank-litvy-kiberataki-ostayutsya-krupnejshim-riskom-dlya-finansovoj-sistemy.html). 15.07.2018).***

***

«Подозрения о вмешательстве России в ход выборов в бундестаг Германии, прошедших в 2017 году, не оправдались, сообщила контрразведка ФРГ.

…«по мере приближения выборов в бундестаг в конечном итоге был зафиксирован спад российской кибератвности с возможной привязкой к выборам»…» ***(Анна Инсарова. В Германии отвергли подозрения о вмешательстве России в выборы в бундестаг // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/24/933976.html). 24.07.2018).***

***

«…Експерт «UkraineWorld» поговорив з Тоомасом Гендріком Ільвесом, який з 2006 по 2016 рік був президентом Естонії…

«500 урядових послуг в Естонії доступні онлайн. 98% медичних приписів робляться по інтернету. 98% податків сплачують онлайн. Естонці отримують чип, який діє як сімкарта, тому можуть робити ці операції з телефону, – каже Ільвес. – Є тільки три речі, які естонці не можуть зробити онлайн: одружитися, розлучитися і фізично передати нерухомість…».

Естонія почала перехід до цифрового суспільства, об’єднавши людей засобами комунікації. До 1998 року всі естонські школи були підключені до інтернету. Країну вкрила мережа вайфай, а літніх людей навчили користуватися комп’ютером.

Водночас Естонія почала розв’язувати проблему, яка досі гостро стоїть у багатьох країнах, йдеться про цифрову безпеку…

«Ми маємо чип і номер, – пояснює він. – Чип дає нам шифрування на всіх етапах так, що ніхто не може вкрасти [ідентифікаційний номер] посередині. Маємо номер, що відповідає коду чипа, а далі у нас є шифрування, яке веде туди, куди нам треба».

Ільвес також підкреслює, що уряд тримає всі дані окремо і за категоріями. «Поліція може переглянути тільки ваше кримінальне досьє або адресу, – каже він. – Вони не мають доступу до вашої медичної карти. Тільки ваш лікар, і ніхто інший, може переглядати дані про ваше здоров'я».

Цифрування допомогло Естонії кардинально скоротити корупцію. «Дані з поліцейського радара записуються в комп'ютер, тому навіть, якщо поліціянт хоче, він не може взяти хабар, – каже Ільвес. – На вищому рівні корупції це також працює, тому що ви зобов'язані проводити тендери … ви повинні подавати заявки по інтернету, і є часова позначка»…» ***(Цифрове суспільство, кібербезпека та протидія дезінформації – інтерв'ю з Тоомасом Гендріком Ільвесом // kherson-news.info (http://kherson-news.info/interview/cifrove-syspilstvo-kiberbezpeka-ta-protidiia-dezinformaciyi-interv-u-z-toomasom-gendrikom-ilvesom/). 25.07.2018).***

***

Російська Федерація та країни ЄАЕС

«Участники заседания Временной комиссии Совета Федерации по развитию информационного общества обсудили вопросы обеспечения кибербезопасности детей.

…По словам главы комиссии Людмилы Боковой, в этот раз участники также сконцентрировались на вопросах развития законодательства в сфере защиты детей, проведения исследований в сферах информатизации школ и работы школьных психологов, а также разработке рекомендаций для школ по организации обучения детей информационной безопасности…

Представители профильных ведомств договорились, что подготовят предложения до октября…» ***(Дмитрий Гончарук. Школы получат новые рекомендации по обучению детей информационной безопасности // «Парламентская газета» (https://www.pnp.ru/politics/shkoly-poluchat-novye-rekomendacii-po-obucheniyu-detey-informacionnoy-bezopasnosti.html). 12.07.2018).***

***

«Россия создаст автоматизированную систему обмена информацией о киберугрозах между разными компаниями и правоохранительными органами. Она позволит координировать действия при реагировании на киберугрозы, заявил Президент России Владимир Путин…

Также предстоит выработать новые комплексные решения по предупреждению и пресечению правонарушений против граждан в цифровой среде…» ***(Россия создаст автоматизированную систему обмена информацией о киберугрозах // «Парламентская газета» (https://www.pnp.ru/politics/rossiya-sozdast-avtomatizirovannuyu-sistemu-obmena-informaciey-o-kiberugrozakh.html). 06.07.2018).***

***

«Президент Владимир Путин на международном конгрессе Сбербанка по кибербезопасности назвал борьбу с кибератаками задачей государственного масштаба.

«В первом квартале этого года по сравнению с аналогичным периодом прошлого года число кибератак на российские ресурсы увеличилось на треть. Убежден, их нейтрализация и в целом обеспечение кибербезопасности – это государственная задача», – заявил президент…

Президент подчеркнул, что нейтрализовать масштабы киберугроз можно только вместе, объединив усилия мирового сообщества. Кроме того, он заявил о необходимости выработать новые комплексные решения по предотвращению преступлений в сфере кибербезопасности…

При это президент отметил, что вся инфрастуктура связи должна основываться на российских технологиях, прошедших сертификацию.

..Также Путин призвал выработать единые международные правила игры в цифровой сфере, учитывающие права и интересы всех государств…» ***(Алина Назарова. Путин назвал борьбу с кибератаками государственной задачей // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/6/931279.html). 06.07.2018).***

***

«…Ни одна кредитная организация в России не соответствует нормам по кибербезопасности, установленным Центробанком РФ. Об этом сообщил исполняющий обязанности директора департамента информационной безопасности ЦБ Артем Сычев…

По словам чиновника, банки проходят серьезные проверки кибербезопасности и, хотя у регулятора есть замечания, они не носят критического характера…» ***(Ни один банк в РФ не соответствует требованиям по кибербезопасности в полной мере // SecurityLabRu (https://www.securitylab.ru/news/493849.php). 09.07.2018).***

***

Інші країни

«Согласно отчету Агентства по кибербезопасности Сингапура (Cyber Security Agency of Singapore, CSA) …за 2017 год …было атаковано более 20 тыс. веб-сайтов, большинство из которых принадлежали предприятиям малого и среднего бизнеса. В минувшем году было обнаружено почти 23 тыс. URL-адресов для фишинга (phishing). Эти мошеннические веб-сайты использовались для хищения личной информации (пароли и данные кредитных карт).

По данным Singapore Police Force, несмотря на общее снижение уровня преступности в стране, в 2017 было зарегистрировано 5430 случаев кибер-преступлений, что составляет 16,6% от общего количества преступлений.

Агентство обратилось к предприятиям и частным лицам с призывом повышать осведомленность о кибербезопасности с помощью различных

информационных кампаний и платформ…» ***(Сингапур: рост киберугроз на фоне снижения общего уровня преступности // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/singapur-rost-kiberprestupeniy-na-fone-snizheniya-urovnya-prestupnosti). 13.07.2018).***

***

«Израильский производитель программного обеспечения для кибербезопасности Check Point Software Technologies подвел итоги второго квартала 2018 года.

За этот период компания выручила 468 млн долларов, что на 2% больше, чем годом ранее…

В апреле-июне 2018 года Check Point получила чистую прибыль в размере 198 млн долларов, что на 10 млн долларов больше показателя годичной давности.

…по итогам второй четверти компания заработала 125,7 млн долларов на продаже продуктов и лицензий, на обновлении ПО и услугах поддержки — 210 млн долларов. Подписки на системы информационной безопасности принесли вендору 132 млн долларов выручки…» ***(Доходы Check Point выросли и оказались выше ожиданий рынка // Goodnews.ua (http://goodnews.ua/technologies/doxody-check-point-vyrosli-i-okazalis-vyshe-ozhidanij-rynka/). 26.07.2018).***

***

Протидія зовнішній кібернетичній агресії

«Когда журналисты прибыли в Сингапур на исторический саммит президента США Трампа и северокорейского лидера Ким Чен Ына в прошлом месяце, эксперты по безопасности встревожились тем, что ожидало репортеров. Помимо бутылок с водой и путеводителя в "welcome bag" обнаружили подозрительную вещь: миниатюрный вентилятор, который подключается к USB-порту комп’ютера…

По словам экспертов, никогда нельзя использовать USB-устройства, не зная, откуда они. Хакеры и шпионы могут использовать их, как троянского коня - устройства на первый взгляд безобидные, но с вредоносными программами, предназначенными для управления компьютером и кражи информации…

Как считают аналитики, чаще всего именно через USB-устройства хакеры собирают информацию или заражают девайсы…

Сергей Скоробогатов, исследователь безопасности оборудования в Кембриджском университете, проверил один из вентиляторов с саммита. Эксперт не обнаружил никаких вредоносных программ на USB. "Тем не менее, это не исключает возможности вредоносных или троянских компонентов, установленных в USB-разъем в вентиляторах, лампах и других USB-устройствах пользователей", - написал Скоробогатов в своем отчете. По его словам, только один USB-вентилятор точно безопасен – тот, который он проверил. Остальные могут оказаться носителями вредоносных программ…» ***(Ирина Фоменко. USB устройства с саммита Трампа и Ким Чен Ына оказались шпионскими // Internetua***

(http://internetua.com/usn-ustroistva-s-sammita-trampa-i-kim-csen-na-mogut-okazalis-shpionskimi). 05.07.2018).

***

«Спецпрокурор США Роберт Мюллер предъявил обвинения в хакерстве 12 россиянам, связанным с якобы вмешательством России в американские выборы 2016 года.

…они якобы взломали компьютерную сеть Демократического комитета и украли имена пользователей и пароли сотрудников избирательного штаба Хиллари Клинтон.

Обвинения против россиян включают в себя «заговор с целью совершения преступления против США», кражу личных данных и «заговор с целью отмывания денег». Граждан России обвиняют в опубликовании электронных писем на сайте dcleaks.com.

Заместитель главы министерства юстиции США Род Розенстайн заявил, что российские спецслужбы взломали сайт американского избиркома и украли информацию на 500 тыс. избирателей…

Представители Мюллера также назвали имена обвиняемых, все они якобы являлись офицерами частей 26165 и 74455 ГРУ…». ***(Алексей Ласнов. США обвинили во «вмешательстве» в выборы 12 «кадровых сотрудников ГРУ» // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/13/932408.html). 13.07.2018).***

***

«Twitter заблокував 2 акаунти, пов'язані з 12 росіянами, викритими у втручанні у вибори в США…

У керівництві соцмережі Twitter повідомили, що облікові записи @DCLeaks_ і @ Guccifer_2 заблоковані. Ці акаунти були названі в обвинувальному висновку 12 співробітникам військової розвідки РФ…» ***(Twitter заблокував 2 акаунти, які "зливали" вкрадені російськими хакерами дані // 7dniv.info – інформаційно-аналітичне інтернет видання (http://7dniv.info/politics/103769-twitter-zablokuvav-2-akaunti-iak-zlivali-vkraden-rosyskimi-hakerami-dan.html). 15.07.2018).***

***

«Посол США в Російській Федерації Джон Хантсман заявив, що Вашингтон буде працювати над запитом про видачу 12 офіцерів російської розвідки, проти яких висунуті звинувачення в причетності до кібератаки під час президентських виборів у США 2016 року.

За його словами, офіс ФБР і посольство США в Москві будуть працювати над екстрадицією обвинувачених росіян…» ***(Вашингтон працюватиме над екстрадицією 12 росіян, - посол // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/150718-vashyngton-pracyuvatyme-nad-ekstradyciyeyu-12-rosiyan-posol). 15.07.2018).***

***

«Росія посіла друге місце в рейтингу головних загроз Європейського союзу

Про це повідомляє Главред з посиланням на доповідь Європейської ради з міжнародних відносин (ECFR).

У рейтингу загроз Росія стоїть відразу після радикальних ісламістських угруповань. Третє місце займає Північна Корея.

За даними дослідження, дій Росії найбільше побоюються в Фінляндії, Естонії, Румунії, Литві та Польщі. Велика Британія і Німеччина теж відчувають тривогу з цього приводу. Тим часом Кіпр, Італія, Греція, Угорщина і Португалія не вважають Росію небезпечною…» ***(Росія потрапила до головних загроз Євросоюзу // Espreso.tv (https://espreso.tv/news/2018/07/15/rosiya_potrapyla_do_golovnykh_zagroz_yevrosoyuzu). 15.07.2018).***

***

«…Директор національної розвідки США Ден Коутс заявив про загрозу масштабної атаки на системи США…

Коутс зазначив, що хакери з Росії, Китаю, Ірану та Північної Кореї щоденно здійснюють кібератаки на США. Цілями таких нападів є американські підприємства, урядові установи, наукові організації, фінансовий сектор, а також об'єкти інфраструктури.

Директор національної розвідки США наголосив, що Москва діє найбільш агресивно серед іноземних сил, намагаючись зруйнувати американську систему демократії. Водночас китайський уряд, за словами Коутса, має найбільш здібних хакерів, які цікавляться крадіжками інформації та прогресі у сфері технологій…» ***(Американська розвідка назвала чотири країни, відповідальні за щоденні кібератаки на США // Racurs.ua® (http://racurs.ua/ua/n108005-amerykanska-rozvidka-nazvala-chotyry-krayiny-vidpovidalni-za-schodenni-kiberataky-na-ssha). 15.07.2018).***

***

«Уривки із лекції Томаша Флідра, координатора програм із кібербезпеки громадської організації «Team 4 Ukraine», розказаної в Харкові під час проекту «Кібербезпека України – поширення позитивного досвіду на країни «Вишеградської четвірки» (B4):

– Ефективність роботи кіберзлочинців із Росії – результат злиття кіберзлочинності в Росії зі спецслужбами, та підпорядкування цих злочинців владі в Москві…

– …У Росії експерти з кіберзлочинності та кіберзлочинці …зливаються в одну єдину спільноту і підпорядковуються, в кінцевому підсумку, російським спецслужбам...

– Кіберлочинцям, які працюють на Москву, влада Росії дозволяє безкарно заробляти злочинним шляхом гроші. Москві ж це дає професіоналів, які на них працюють…

– Спектр атак широкий – від проникнення в ваші приватні дані до шкідливих програм, які шифрують дані на вашому комп'ютері і вимагають виплат за їх розшифрування, аж до атак на об'єкти інфраструктури інших держав…

– Як каже британський експерт із питань Росії Марк Джелеотті, Росія віддавна воює з «Заходом». Її сила в централізованому авторитаризмі. Росія значно слабша на технологічному, фінансовому та багатьох інших рівнях, проте значно швидше мобілізується та має синергію різних методів війни. Це теж стосується і кіберзлочинності…

– Кібератаки для Росії дуже вигідні, бо це дешево і завдає значної шкоди противнику…

– У гібридній війні Росія використовує поєднання інформаційної пропагандистської атаки з кібератакою…» ***(Ігор Тимоць. «Росія поєднує кібератаки з пропагандою», – експерт із кібербезпеки Томаш Флідр // Portal Polsko-Ukrainski (http://www.polukr.net/uk/blog/2018/07/kibervezpieczenstwo/). 11.07.2018).***

***

«…У Великобританії висловили побоювання, що після закінчення Чемпіонату світу з футболу, який проводиться в Росії, Російська Федерація може провести нові атаки на західні країни, причому першою під удар потрапляє Британія…

Британські розвідувальні агентства проводять підготовчі заходи на той випадок, якщо Росія дійсно атакує Великобританію…» ***(Розвідка Британії попередила про ймовірність нових атак РФ після ЧС-2018 - The Times // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/rozvidka-britaniyi-poperedila-pro-ymovirnist-novih-atak-rf-pislya-chs-2018-the-times-282497_.html). 07.07.2018).***

***

«…Практика применения Россией информационного оружия привела к тому, что Запад фактически оказался перед необходимостью включить в военные доктрины механизмы противодействия атакам "ниже уровня боевых действий", считает американский политолог и специалист по международной безопасности Джозеф Най в новой статье "Is Cyber the Perfect Weapon?".

…пока что информационные атаки представляются более действенными для дезинформации и возбуждения беспорядков, чем для физического воздействия на противника. По его мнению, это делает такие атаки скорее вспомогательным оружием, нежели главным средством достижения победы…

Именно физический ущерб, пишет далее Най, является критерием нанесения ответного удара согласно действующей военной доктрине США. Америка считает себя вправе ответить на кибератаку применением любого вида оружия пропорционально нанесенному ей противником физическому ущербу. Другим принципом этой доктрины является то, что международное право на самооборону применимо и к кибератакам…

Но, возможно, продолжает эксперт, мы смотрим совсем не в ту сторону, и реальную угрозу для безопасности представляет не только заметный физический

ущерб, но и расширение конфликтов в "серую зону", которая находится вне сферы внимания традиционных войн. Именно в этом ключе начальник российского Генштаба Валерий Герасимов сформулировал доктрину "гибридной войны", в которой сочетаются традиционное оружие, экономическое принуждение, информационные операции и кибератаки…

Это приводит его к следующему выводу: если президент России Владимир Путин считает, что его страна ведет борьбу с США, но от масштабного применения силы его удерживает угроза ядерной войны, тогда, похоже, кибератаки становятся для него "абсолютным оружием"…

Най считает, что сетевое вмешательство России в президентские выборы в США в 2016 году было инновационным по своему характеру. "…Гениальность российских инноваций в этой информационной войне заключается в том, что в них сочетались доступные технологии с возможностью отрицания ответственности, поскольку предпринятые действия находились чуть ниже порога безусловной агрессии".

…Противодействие этому новому виду оружия, пишет Най, требует стратегической организации национальных ресурсов с участием всех государственных ведомств и с упором на более эффективное сдерживание.

...Главное же средство достижения успеха, по мнению Ная, заключается в том, что США должны обеспечить для кибератак и манипулирования социальными сетями такие высокие издержки, чтобы такие атаки перестали быть "абсолютным оружием" для боевых действий ниже уровня вооруженного конфликта.» ***(Абсолютное цифровое оружие в гибридной кибервойне России // Информационное агентство ЛІГАБізнесІнформ (http://www.liga.net/politics/opinion/absolyutnoe-tsifrovoe-orujie-v-gibridnoy-kibervoyne-rossii). 11.07.2018).***

***

«…угруповання, яке називала себе Dragonfly або Energetic Bear зуміло зламати мережі електричних компаній в США, що вважалися захищеними, зазначає Міністерство внутрішньої безпеки. Як вважають у відомстві, угруповання пов’язане з російською владою.

Зламати мережі хакерам вдалося завдяки атакам на партнерів електричних компаній. В результаті вони обманом дістали необхідні паролі і отримали доступ до комп’ютерів диспетчерських служб, з яких могли влаштовувати перебої з подачею електрики.

Раніше Міністерство внутрішньої безпеки неодноразово говорило про погрози з боку хакерів, проте цього разу воно вперше повідомило про те, що реально зробили кіберзлочинці. При цьому назви компаній у відомстві згадувати не стали, розповівши лише про “сотні жертв”…» ***(Олексій Супрун. The Wall Street Journal повідомила про злам російськими хакерами електромереж в США // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1743009-the-wall-street-journal-povidomila-pro-zlam-rosiyskimi-khakerami-elektromerezh-v-ssha). 24.07.2018).***

***

«Директор Агентства національної безпеки США Пол Накасоне на щорічному форумі з питань безпеки в Аспені заявив про створення спеціального підрозділу для боротьби з російськими загрозами в кіберпросторі…

"Росія має великі можливості, на які ми, безумовно, будемо відповідати. Я створив російську групу –Russia Small Group. Це відповідає тому, що розвідувальна спільнота робило після 2016 - 2017 року", - сказав Накасоне.

Він додав, що США необхідно мати який спосіб, для захисту від Росії у кіберпросторі…» ***(Анастасія Ткачук. У США створили підрозділ для боротьби з російськими кібератаками // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1742942-u-ssha-stvorili-pidrozdil-dlya-borotbi-z-rosiyskimi-kiberatakami). 23.07.2018).***

***

«Іран підготував необхідну комп'ютерну інфраструктуру для того, щоб зробити масовані кібератаки щодо систем США. З таким твердженням виступила телекомпанія NBC, яка посилається на неназваних представників американських владних структур…

За їхніми даними, Іран готовий до того, щоб почати вчинення таких атак щодо державної інфраструктури і приватних компаній США і ряду країн Європи, проте до цього моменту немає будь-яких свідчень того, що дана кібероперація може статися в найближчому майбутньому. У зв'язку з цим Вашингтон посилює захист проти кібернападів, попереджає своїх союзників, а також вивчає можливі заходи реагування, зазначає телеканал…

Телеканал наводить заяву прес-секретаря іранського постійного представництва при ООН Алірези Мірусефі, який заявив, що "Іран не має намірів вступати в яку-небудь кібервійну з США". За його словами, Вашингтон може використовувати свої підозри про нібито наміри Тегерана зробити хакерські напади проти США в якості виправдання можливого початку власних кібератак щодо Ірану…» ***(Олексій Супрун. Іран готовий до здійснення масованих кібератак проти США // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1742564-iran-gotoviy-do-zdiysnennya-masovanikh-kiberatak-proti-ssha). 21.07.2018).***

***

«Троє кандидатів на вибори в Конгрес США, які відбудуться цієї осені, піддалися кібератаці з використанням підробленої сторінки Microsoft. Про це заявив віце-президент компанії з питань безпеки Том Берт на форумі Aspen…

"Раніше в цьому році ми виявили, що фейковий домен Miscrosoft використовували як майданчик для фішингових атак", - зазначив віце-президент. За його словами, діяли хакери, імовірно, пов'язані з російською розвідкою. …Разом з тим назвати імена кандидатів Берт відмовився. Він підкреслив, що це люди, які могли бути "цікавими цілями для шпигунства у зв'язку з їх посадами". Віце-президент заявив про видалення фейкового домену і фішингових повідомлень…»

(На трьох політиків, які хочуть потрапити у Конгрес США, напали кіберзлочинці з підробленої сторінки Microsoft // ТзОВ "Редакційні системи" (http://expres.ua/news/2018/07/21/302313-troh-politykiv-hochut-potrapyty-kongres-ssha-napaly-kiberzlochynci). 21.07.2018).

***

«Дональд Трамп за два тижні до вступу на посаду президента США в січні 2017 року був ознайомлений з цілком таємними розвідувальними даними, що вказують нібито на те, що президент Росії Володимир Путін особисто віддав вказівку про кібератаки з метою вплинути на вибори в США в 2016 році

…на зустрічі з Трампом 6 січня 2017 року, серед наданих йому розвідувальних відомостей були "тексти і електронні послання від російських військових і інформація, отримана від цілком таємного джерела, близького до Путіна, який виклав Центральному розвідувальному управлінню, яким чином Кремль прийняв рішення про кампанії кіберзламів і дезінформації".

…Трамп "з небажанням переконався" в тому, що йому говорили, однак згодом "спробував поставити під сумнів всі ясні свідчення", отримані ним на брифінгу і схвалені всіма керівниками розвідки США…» ***(Олексій Супрун. Трампу в 2017 році представили дані від секретного джерела, близького до Путіна - The New York Times // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1742318-trampu-v-2017-rotsi-predstavili-dani-vid-sekretnogo-dzherela-blizkogo-do-putina-the-new-york-times). 20.07.2018).***

***

«…В ОБСЄ прокоментували інформацію про ймовірний витік внутрішньої інформації та її потрапляння до спецслужб РФ.

…спостерігачі запевняють, що вживали всіх необхідних "заходів щодо захисту даних, а також для протистояння різним кібератакам на місію".

У повідомленні також зазначається, що робота місії, попри все, і надалі залишатиметься "прозорою"…» ***(В ОБСЄ прокоментували "злив" даних моніторингової місії ФСБ Росії // 5 канал (https://www.5.ua/polityka/v-obsye-prokomentuvaly-zlyv-danykh-monitorynhovoi-misii-fsb-rosii-173928.html). 18.07.2018).***

***

«Сенатор от штата Миссури Клэр Маккаскил …в специальном заявлении рассказала о предполагаемой атаке российских хакеров на компьютерную сеть Сената.

«Россия продолжает вести кибервойну против нашей демократии. Я продолжу откровенно высказываться и оказывать давление с целью привлечь их к ответственности. В то время как это нападение не увенчалось успехом, возмутительно, что они считают, что им может сойти это с рук», – передает ТАСС слова Маккаскил, добавившей, что «не позволит себя запугать».

…Маккаскил ведет кампанию по переизбранию в Сенат, промежуточные выборы состоятся в ноябре 2018 года…» ***(Дмитрий Зубарев. Американский сенатор обвинила «российских хакеров» в кибератаке // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/27/934435.html). 27.07.2018).***

***

«…Пентагон уповноважив Кібернетичне командування Сполучених Штатів (United States Cyber Command) застосовувати більш агресивний підхід щодо захисту від кібератак. Зміна стратегії може збільшити ризик конфлікту з іноземними державами, які фінансують кіберзлочинців.

..нова стратегія передбачає постійну підривну діяльність "на межі війни" в іноземних комп'ютерних мережах. За словами чиновників, вона створювалась протягом більш як десятиліть антитерористичних операцій, в яких Сполучені Штати навчились, що найкращим способом перемогти "Аль-Каїду" чи "Ісламську державу" є знищення бойовиків всередині їхніх баз або житлових приміщень.

Мета… полягає в тому, щоб "боротись із небезпечними діями противника, перш ніж вони посягнуть на нашу національну міць".

Американська оборона стає "якомога ближчою до походження діяльності супротивника, що розширює наш потенціал для виявлення слабких сторін противників, вивчення їхніх намірів і можливостей та протидії нападам", — говориться в документі.

Але, на думку нинішніх і колишніх чиновників, існують ризики ескалації — дії США в іноземних мережах можуть привести до ударів у відповідь проти американських банків, дамб, фінансових ринків або комунікаційних мереж…» ***(Саша Картер. Кіберкомандування США отримало повноваження здійснювати рейди на іноземні мережі // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1736605-kiberkomanduvannya-ssha-otrimalo-povnovazhennya-zdiysnyuvati-reydi-na-inozemni-merezhi). 18.07.2018).***

***

«Нові гібридні загрози роблять життєво важливим посилення кіберзахисту ЄС зі швидкою командою кібер-реагування і більш тісне співробітництво з НАТО. Про це заявили в середу депутати Європарламенту…

Резолюція кіберзахисту була підтримана 476 голосами "за" проти 151 голосу "проти". Ще 36 депутатів утримались від голосування.

В резолюції йдеться, що Росія, Китай і Північна Корея, а також недержавні суб'єкти, здійснюють зловмисні кібер-атаки на критичні інфраструктури ЄС, займаються кібер-шпигунством та масовим спостереженням за громадянами ЄС…

Європейські депутати підкреслюють, що фрагментована стратегія та можливості оборони Європи зробили її вразливою для кібер-атак. Тому вони настійно закликають держави-члени ЄС посилити здатність своїх збройних сил працювати разом і зміцнювати кібер-співробітництво на рівні ЄС з НАТО та іншими партнерами.

Це може призвести до збільшення кількості спільних кібер-вправ, навчань і обміну між військовослужбовцями, залучення експертів з кібер-криміналістиці, а також вдосконалення досвіду місій і операцій в області кіберзахисту.

Європейські депутати віддають перевагу двом кібер-проектам, що мають бути запущені в межах Постійної структурної співпраці (PESCO): платформи для обміну інформацією для кібер-інцидентів та групи швидкого реагування…» ***(Саша Картер. Європарламентарі хочуть посилити зв'язки з НАТО щодо кіберзахисту // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1735917-yevroparlamentari-khochut-posiliti-zvyazki-z-nato-schodo-kiberzakhistu-yes). 13.07.2018).***

***

«Пентагон планує відмовитися від послуг компаній, що використовують розроблене в Росії і Китаї програмне забезпечення. Про це заявила заступник міністра оборони США з питань закупівель Еллен Лорд…

За її словами, Пентагон вже півроку працює над формуванням списку компаній, що використовують російський або китайський програмний код. Таким чином відомство хоче запобігти закупівлі "проблемного коду, що не відповідає оборонним стандартам США".

Лорд додала, що …Пентагон також хоче зміцнити здатність своїх постачальників протистояти кібератакам…» ***(Пентагон готує "чорний список" компаній, що використовують російське ПО // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/pentagon-gotuye-chorniy-spisok-kompaniy-scho-vikoristovuyut-rosiyske-po-284270_.html). 28.07.2018).***

***

Кіберзахист критичної інфраструктури

«…Специалисты из компании по кибербезопасности Record Future обнаружили, что как минимум два человека, связанные с американскими военными, получили доступ к секретным файлам, в том числе к руководству для основного боевого танка США и беспилотников Reaper. Это произошло из-за того, что военные не сменили имя пользователя и пароль на своих роутерах, которые были по умолчанию на них установлены и указаны на сайте производителя маршрутизаторов…

Хакеру оставалось просто изучить настройки по умолчанию для маршрутизаторов в открытом доступе в интернете, а затем использовать их для кражи данных с компьютеров, подключенных к этим роутерам…» ***(Сергей Гурьянов. Стало известно, как хакеры украли информацию о дроне Reaper у военных США // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/11/931987.html). 11.07.2018).***

***

«На прошлой неделе появились отчеты, подтверждающие, что сторонние разработчики приложений могли читать электронные письма, принадлежащие миллионам учетных записей Gmail…

Комитет энергетики и торговли Конгресса США направил 10 июля письма как Apple, так и Alphabet, задав множество вопросов о конфиденциальности. Большинство из них адресованы генеральному директору Alphabet Ларри Пейджу касательно отчета The Wall Street Journal, сбора аудиозаписей и отслеживания местоположения.

Несмотря на обещание Google перестать проверять электронные сообщения пользователей для повышения эффективности целевой рекламы, компания по-прежнему разрешает третьим сторонам читать электронные письма…

Также законодатели заинтересовались, может ли информация, которая хранится непосредственно на устройстве, быть передана Google, Apple или сторонним разработчикам, даже если пользователи отключили службы определения местоположения. Кроме того, республиканцы обеспокоены возможностью записи аудио с устройств, когда функция "Okay, Google" отключена. Комитет попросил ответить компании на все вопросы до 23 июля» ***(Ирина Фоменко. Предпочитаете Gmail? Тогда прочтите это // Internetua (http://internetua.com/predpocsitaete-gmail-togda-procstite-eto). 11.07.2018).***

***

«…Google официально объявила о том, что приняла новые стандарты безопасности и профессиональной этики, а потому запрещает своим сотрудникам читать письма других пользователей – однако это не останавливает третьих лиц.

Именно третьи лица, предоставляющие пользователям сервиса Google Mail различные приложения и плагины как раз могут читать чужую почту – из этого не делается большого секрета, к примеру, в стенах компании Return Path Inc., которая отмечает, что это остается единственным способом бороться с потенциальными угрозами кибербезопасности…

Стоит отметить, что на этой волне стремления защитить пользовательские данные вместе с компанией Google некоторые другие корпорации – такие как Microsoft и Yahoo – также заявили о введении новых стандартов кибербезопасности...» ***(Роман Розенталь. Googe принимает новые меры безопасности в отношении данных пользователей // Faina Idea (http://www.fainaidea.com/interesnoe/neobychnoe/googe-prinimaet-novye-mery-bezopasnosti-v-otnoshenii-dannyh-polzovatelej-146417.html). 03.07.2018).***

***

«…Минтранс России выложил на общественное обсуждение проект приказа Правительства РФ «Об утверждении требований к автоматизированной информационной системе оформления воздушных

перевозок, базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования»…

Минтранс предлагает с 1 января 2020 года персональные данные авиапассажиров должны начать хранить на территории России. Речь идет о переносе серверов и баз данных компаний, обеспечивающих бронирование и продажу внутрироссийских авиаперевозок, регистрацию пассажиров и взаиморасчеты.

Контролировать обработку персональных данных будет Роскомнадзор. Провайдер системы бронирования должен быть также зарегистрирован в России. Минтранс отмечает, что новые требование призваны обеспечить суверенитет России, безопасность персональных данных пассажиров и противодействие терроризму…» ***(Данные российских авиапассажиров перенесут в Россию // РосКомСвобода (https://roskomsvoboda.org/40219/). 06.07.2018).***

***

«…У пошуковій видачі «Яндекса» виявилися документи користувачів сервісу Google Docs, що містять приватну інформацію.

…Документи, які потрапляють у видачу «Яндекса», не були захищені налаштуваннями приватності - це означає, що їх автор дозволив перегляд (або навіть редагування) всім, у кого є потрібне посилання. Google і сам індексує доступні всім документи з Google Docs. Однак в пошуку Google відсутня принаймні частина текстових файлів і таблиць з приватною інформацією, які були у видачі «Яндекса»…» ***(«Яндекс» видав користувачам доступ до приватних файлів сервісу Google Docs // "Українські медійні системи" (https://glavcom.ua/news/yandeks-vidav-koristuvacham-dostup-do-privatnih-fayliv-servisu-google-docs-510173.html). 0507.2018).***

***

«…предустановленные вредоносные приложения на бюджетных Android-смартфонах, продающихся в развивающихся странах, были обнаружены экспертами в сфере кибербезопасности.

Как выяснилось, эти программы собирают информацию о моделях телефонов, а заодно и об их владельцах. Затем все эти сведения они отправляют рекламным компаниям, а те начинают атаковать пользователей предложениями на основе их предпочтений.

В качестве передаваемой информации выступают такие данные, как местоположение человека, номера IMEI и MAC-адреса.

Как оказалось, приложения-шпионы найдены на гаджетах, которые продает сингапурская компания Singtech в Мьянме и Камбодже. Также активность программы обнаружили в Бразилии, Индии и Китае.

…данные собирают сразу несколько компаний - например сингапурская GMobi с китайской Adups, а также индийская MoMagic.

Заметим, что среди партнеров на сайте GMobi числятся Huawei и Xiaomi, но производители отрицают сотрудничество с ней.» ***(СМИ: дешевые Android-смартфоны шпионят за пользователями // informing.ru (http://informing.ru/2018/07/14/smi-deshevye-android-smartfony-shpionyat-za-polzovatelyami.html). 14.07.2018).***

***

«…11 липня, керівниця британського Управління комісара з питань інформації Елізабет Денхем повідомила про те, що її відомство стягне з Facebook штраф у розмірі в 500 тисяч фунтів стерлінгів (565 тисяч євро)…

Співробітники відомства виявили в діях компанії Facebook порушення британського закону про захист даних. За словами представниці Управління, американський інтернет-велетень не зумів гарантувати безпеку особистої інформації своїх користувачів, а також виявився не досить прозорим у питанні збору даних користувачів третіми особами…» ***(Валерій Сааков.Великобританія оштрафує Facebook через витік даних користувачів // Deutsche Welle (https://www.dw.com/uk/%D0%B2%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%96%D1%8F-%D0%BE%D1%88%D1%82%D1%80%D0%B0%D1%84%D1%83%D1%94-facebook-%D1%87%D0%B5%D1%80%D0%B5%D0%B7-%D0%B2%D0%B8%D1%82%D1%96%D0%BA-%D0%B4%D0%B0%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D1%96%D0%B2/a-44626293). 11.07.2018).***

***

«Роскомнадзор направил запросы в «Яндекс», «Сбербанк» и ВТБ в связи с ситуацией вокруг утечки данных пользователей сервисов в поисковой выдаче «Яндекса»…

Компании должны ответить на запрос в течение 30 дней…

Ранее SEO-специалист Павел Медведев обнаружил, что через поисковик «Яндекса» можно получить личные данные клиентов сервисов РЖД, «Сбербанка», ВТБ, московских муниципальных служб и сервисов бронирования билетов.

«Сбербанк» по результатам проверки опроверг информацию об утечке персональных данных клиентов из «Яндекса»…

В «Яндексе» также прокомментировали …информацию об утечке, заявив, что поисковый робот индексирует документы, если это не запрещено в настройках, которые устанавливает владелец сайта или вебмастер…» ***(Екатерина Симикян. Роскомнадзор потребовал от «Яндекса», «Сбербанка» и ВТБ разъяснить ситуацию вокруг утечки даннях // Rusbase (https://rb.ru/news/rkn-yandex-sber-vtb-data/). 17.07.2018).***

***

«Конфиденциальная информация клиентов международного телекоммуникационного холдинга Telefonica оказалась под угрозой из-за ошибки разработчиков…

Telefonica занимает восьмое место в мире по числу абонентов и обслуживает 325 млн человек. Организация подвергла риску платежную информацию, номера телефонов, адреса, записи звонков и другие данные клиентов. На возможность утечки обратил внимание пользователь платного телевидения Movistar, предоставляемого Telefonica, и сообщил в FACUA — испанскую организацию по защите прав потребителей.

Всему виной ошибки в настройках ресурса для клиентов платного сервиса. Проблема была связана с тем, что идентификатор просмотра счетов отображался в URL-адресе и был виден любому посетителю сайта. Хотя нет доказательств, что конфиденциальная информация попала в руки мошенников, подобная неосторожность могла привести к массовому сбору сведений об абонентах…

Оповещение клиентов и все последующие действия компании должны быть выполнены в соответствии с Общим регламентом по защите данных (GDPR). К тому же Telefonica должна выплатить штраф в размере от 10 до 20 миллионов евро или сумму, эквивалентную 2–4% годового оборота…» ***(Dmitry Nazarov. Абоненты Telefonica могли просматривать данные друг друга // Threatpost (https://threatpost.ru/telefonica-abonents-can-see-each-other-personal-data/27295/). 18.07.2018).***

***

«…Европейский парламент принял резолюцию, призывающую Европейскую комиссию не продлевать действие договора о передаче личных данных между ЕС и США, заключенного в 2016 году…

Вступившая одновременно с этим в силу директива ЕС о защите данных (GDPR) разрешает передавать личные данные граждан ЕС только в страны с надлежащим уровнем охраны личных данных. В договоре между ЕС и США (Privacy Shield) определены условия, позволяющие обрабатывать личные данные граждан ЕС в США. Однако, как говорится в резолюции, не все из них выполнены — в частности, сенат США все еще не утвердил трех членов комитета по защите личных данных и гражданских свобод (PCLOB), что препятствует его работе. Не назначен также омбудсмен по договору Privacy Shield, а правила министерства торговли США не предусматривают проверок американских компаний на выполнение условий Privacy Shield.

Резолюция Европарламента не имеет обязательной силы. Решение о приостановке действия договора может принять только Еврокомиссия или Европейский суд…» ***(Европарламент требует приостановить действие договора о передаче личных данных между ЕС и США // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=124044). 17.07.2018).***

***

«Німецькі медіакомпанії і організація зі сфери хімічних досліджень стали метою кібератак…

Наявна інформація свідчить про хвилю атак, здійснених, імовірно, з метою шпигунства...

Відомство з охорони конституції уточнює, що за атаками, імовірно, стоїть російська спецслужба. Мова йде …про так звану атаку спрямованого фішингу, з високою точністю здійснену проти конкретних об'єктів.

Електронною поштою надсилалися листи від імені відправника, що заслуговує на довіру, з зараженим текстовим документом в форматі Word. Коли користувач відкривав його, надходила рекомендація дозволити виконання макросів. Якщо дати такий дозвіл, то відкривається можливість стеження за мережевою інфраструктурою або навіть управління нею.

Існує ймовірність того, що в Німеччині, крім медіакомпаній і організації, що займається хімічними дослідженнями, виявилися зачеплені і інші підприємства…» ***(Олексій Супрун. Спецслужба ФРН розповіла про кібератаки на німецьку пресу // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1741040-spetssluzhba-frn-rozpovila-pro-kiberataki-na-nimetsku-presu). 13.07.2018).***

***

«Согласно последнему отчёту американской компании CipherTrace, занимающейся кибербезопасностью, в первой половине 2018 года преступники похитили с криптовалютных бирж более $750 млн. — в три раза больше, чем за весь 2017-й.

…Похищенные криптовалюты преступники впоследствии отмывают, что позволяет им скрывать свою личность и избегать ареста. В криптовалютном секторе работают многочисленные сервисы по отмыванию денег (их называют миксерами, прачечными и прочими прижившимися терминами). Сервисы работают по одному принципу: получают средства от множества разных клиентов, смешивают их путём разбития общей суммы на множество произвольных адресов, а затем снова распределяют на адреса клиента-получателя. Обычно такие сервисы берут от 1 до 3% за транзакцию.

Помимо специализированных сервисов, преступники часто используют сайты азартных игр… В сети доступны от 100 до 200 сайтов азартных игр с упором на криптовалюты. Преступники открывают на них аккаунты, после чего переводят деньги с целью легализации. В онлайн-казино они делают самые простые ставки или даже просто выводят средства на новый адрес, не принимая участия в играх.

…в отчёте CipherTrace упоминается деятельность международной Группы по противодействию легализации преступных доходов и финансированию терроризма (FATF). Текущие правила обязывают биржи иметь регистрацию или лицензию, верифицировать личности клиентов, предотвращать отмывание денег и сообщать надзирающим органам о подозрительной торговле и транзакциях. …сейчас

сотрудники FATF активно обсуждают вопрос о том, как заставить криптовалютные биржи соблюдать правила.

Аналогичную задачу ставит перед собой американская Сеть по борьбе с финансовыми преступлениями (FinCEN). Её внимание обращено в первую очередь на сервисы по отмыванию денег, биржи, предлагающие исключительно криптовалютные торговые пары (без фиатных валют), и конфиденциальные монеты.» ***(С начала 2018 года преступники похитили с криптобирж более $750 млн. // BIGFIN (https://bigfin.net/05/07/2018/s-nachala-2018-goda-prestupniki-pohitili-s-kriptobirzh-bolee-750-mln/). 05.07.2018).***

***

«Многочисленные кражи криптовалюты осуществлялись через рассылку фейковых электронных писем на японском языке пользователям крупных криптовалютных бирж.

…у FSA есть претензии к шести лицензированным японским криптовалютным биржам. Связаны они с тем, что предприятия не уделили должного внимания безопасности и не пересмотрели свою политику управления бизнесом. На днях стало понятно почему было проявлено недоверие к ним. Согласно данным отчетов, в ноябре прошлого года в Японии производились кибератаки с целью кражи криптовалюты.

Киберпреступники использовали фишинг, дабы получить логины и пароли пользователей крупных криптовалютных бирж. Они делали рассылку фейковых электронных писем на японском языке пользователям данных предприятий. Таким образом, они получали доступ к их аккаунтам и крали их виртуальные активы. Это стало известно намного раньше, но криптовалютные предприятия, к которым недавно и были предъявлены претензии, вовремя не предприняли контрмер против онлайн-мошенничества и фишинга…» ***(Каролина Узун. В Японии киберпреступники использовали фишинг для кражи криптовалюты // Qled (https://www.qled.com.ua/news/%d0%ba%d0%b8%d0%b1%d0%b5%d1%80%d0%bf%d1%80%d0%b5%d1%81%d1%82%d1%83%d0%bf%d0%bd%d0%b8%d0%ba%d0%b8-%d0%ba%d1%80%d0%b0%d0%b6%d0%b8-%d0%ba%d1%80%d0%b8%d0%bf%d1%82%d0%be%d0%b2%d0%b0%d0%bb%d1%8e%d1%82%d1%8b/). 03.07.2018).***

***

«Завершившийся в России XXI чемпионат мира по футболу – FIFA World Cup 2018 – не обошелся без компрометации конфиденциальных данных.

Аналитический центр InfoWatch собрал наиболее интересные примеры утечек с крупнейшего футбольного форума.

За время проведения XXI чемпионата мира не было зафиксировано серьезных утечек, связанных в активностью киберпреступников. Однако хакеры вовсю старались использовать центральное спортивное событие лета. Так, отмечены случаи использования фальшивых сайтов и мошеннических приложений, эксплуатирующих тему Кубка мира, о чем предупреждали эксперты InfoWatch. Например, десятки израильских военнослужащих пострадали от вредоносной

программы, загрузив из Google Play приложение, которое предлагало отслеживать статистику чемпионата мира. Шпионская программа могла записывать разговоры пользователей и похищала контент с их устройств. Израиль обвинил в данной атаке группировку ХАМАС.

Бренд чемпионата мира также был использован для маскировки хакерской атаки при компрометации сайта Ammyy Admin – популярной в России программы для удаленного управления компьютером. В доменном имени управляющего сервера киберпреступники прописали «fifa2018start». По данным ESET, пользователи, скачавшие Ammyy Admin 13-14 июня, получили «в нагрузку» многоцелевой троян. Вредоносная программа была заточена на кражу паролей к криптовалютным кошелькам и аккаунтам…» ***(Как теряли информацию во время Кубка мира // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5514999-Kak-teryali-informaciyu-vo-vremya.html). 16.07.2018).***

***

«В конце июня в Детройте (США) киберпреступники буквально среди бела дня похитили с автозаправочной станции 600 галлонов (около 2270 литров) топлива.

…около 13 часов оператор АЗС обнаружил, что не может прекратить подачу топлива на одной из колонок. Компьютерная система управления колонкой вышла из строя и не реагировала на команды. На протяжении полутора часов оператор пытался решить проблему. За это время не менее 10 автомобилей заправились у неисправной колонки и покинули АЗС, ничего не заплатив. Общий финансовый ущерб составил порядка 1800 долларов.

Отчаявшийся оператор вызвал полицию и смог, наконец, воспользоваться системой аварийного прекращения подачи топлива. Прибывшие на место офицеры предположили, что колонка подверглась кибератаке.

Расположившимся неподалеку от АЗС хакерам удалось дистанционно подключиться к системе. Предположительно, они перевели колонку в так называемый диагностический режим, в котором она может продолжать подачу топлива, но не сообщает об этом на терминал оплаты и не реагирует на команды оператора.» ***(Хакеры взломали заправку // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5514113-Xakery-vzlomali-zapravku.html). 11.07.2018).***

***

«Интерес киберпреступников к незаконному майнингу постепенно ослабевает в результате снижения цен на криптовалюту, следует из опубликованного MalwareBytes Labs отчета.

…Согласно отчету, после массового всплеска активности в конце 1-го квартала 2018 года, количество майнеров для Android-устройств также пошло на спад. При этом во втором квартале было зафиксировано почти в 2,5 раза больше случаев обнаружения майнеров для мобильных устройств.

…активность, связанная с сервисом Coinhive, позволяющим майнить криптовалюту в браузере пользователя, остается сравнительно высокой. Помимо этого, появляются и другие схожие сервисы, такие как Cryptoloot. По словам

специалистов, злоумышленники все чаще "используют браузерные майнеры с открытым исходным кодом и адаптируют их для своих потребностей".» ***(Киберпреступники утрачивают интерес к майнингу криптовалюты // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=124095). 19.07.2018).***

***

«…От 30% до 40% киберпреступлений совершаются подростками в возрасте от 14 до 16 лет — к таким выводам пришли авторы исследования "Threat Zone 17/18: новые вызовы цифрового мира", осуществленного Сбербанком совместно с дочерней компанией BI.ZONE.

…исследование показало, что мишенями примерно половины атак становятся компании финансового сектора. При этом общественность узнает только о 20% инцидентов, в частности, потому, что компании не желают раскрывать эту информацию. Из всех киберугроз в мире наиболее распространены вирусы-шифровальщики типа WannaCry.

Исследователи подсчитали, что по итогам 2018 г. ущерб, нанесенный экономике России киберпреступниками, превысит 1,1 трлн руб. Ущерб от действий хакеров для мировой экономики Всемирный экономический форум (ВЭФ) оценивает более чем в $1 трлн. К 2022 г. этот показатель может вырасти до $8 трлн…

Кроме того, исследование показало, что более 80% хакерских атак включают в себя применение социальной инженерии...» ***(Исследование Сбербанка: почти половину кибератак в России совершают подростки // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123875). 06.07.2018).***

***

«Эксперты по кибербезопасности из «Лаборатории Касперского» опубликовали отчет о DDoS-атаках во втором квартале 2018 года...

По словам специалистов, в ходе атак хакеры эксплуатируют уже известные уязвимости, например, обнаруженную в 2001 году проблему в протоколе Universal Plug-and-Play, а также уязвимость в протоколе CHARGEN, который используется преимущественно принтерами и копировальными аппаратами.

В течение второго квартала 2018 года злоумышленники атаковали с помощью ботнетов ресурсы в 74 странах. Первое место по количеству атак занимает Китай (59,03%), второе – Гонконг (17,13%), третье – США (12,46%).

…активность ботнетов, состоящих из устройств под управлением ОС Windows сократилась почти в 7 раз, в то время как активность ботнетов из устройств под управлением Linux выросла на 25%.

Популярным методом монетизации DDoS-атак являются атаки на криптовалютные биржи…

Помимо этого, хакеры атакуют киберспортивные площадки, совершая нападения как на игровые серверы, так и на отдельных игроков…» ***(Активность DDoS-ботнетов из устройств под управлением Linux выросла на 25% // Goodnews.ua (http://goodnews.ua/technologies/aktivnost-ddos-botnetov-iz-ustrojstv-pod-upravleniem-linux-vyrosla-na-25/). 28.07.2018).***

***

«…11 июля появились доказательства проникновения китайской команды хакеров в компьютерные системы, принадлежащие избирательной комиссии Камбоджи, лидерам оппозиции и средствам массовой информации накануне выборов 29 июля.

…после отказа Евросоюза и США поддержать выборы, Китай вложил 20 млн долларов в Национальную избирательную комиссию Камбоджи…

Начальник киберразведки FireEye Бенджамин Рид сообщил, что его команда отследила вредоносные файлы на незащищенном сервере китайской организации TEAM.Periscope.

На сервере хакеров аналитики FireEye обнаружили записи, свидетельствующие о том, что группа хакеров скомпрометировала избирательную комиссию Камбоджи и несколько камбоджийских министерств. Журналы доступа к серверам в одном экземпляре прослеживаются по IP-адресу на юге острова Хайнань на юге Китая.

"Это государственная организация, поскольку хакеры ищут информацию, которая принесет пользу китайскому правительству", - утверждают в FireEye…

В МИД Китая заявили, что они не знают о TEAM.Periscope и решительно выступают против кибератак…

Камбоджийская избирательная комиссия была осведомлена о взломе, и подала жалобу правительству…» ***(Ирина Фоменко. Китайские хакеры пытаются повлиять на выборы Камбоджи // Internetua (http://internetua.com/kitaiskie-haker-ptauatsya-povliyat-na-vbor-kambodji). 12.07.2018).***

***

«Сервіс для створення «спогадів» з соцмереж Timehop 4 липня піддався хакерській атаці. Взлом відбувся за аккаунта в хмарному сервісі, не захищеного двофакторної аутентифікацією.

Команда сервісу зреагувала на ситуацію по ходу її розвитку, однак на момент закриття дірки, дані 21 млн користувачів вже витекли…

При цьому ключі, що дозволяли Timehop читати і відображати усередині додатку пости, теж провалилися, але їх оперативно дезактивували… Підтверджень про те, що якісь акаунти постраждали від рук хакерів, поки немає.

…Timehop проводить внутрішній аудит, а також працює над поліпшенням протоколів безпеки.

Сервіс також залучив для взаємодії сторонню команду з кібербезпеки, зв'язався з провайдером хмарних і поспілкувався з місцевими і федеральними властями США, повідомивши всі відомості про інцидент…» ***(21 мільйон користувачів популярного мобільного застосування постраждав від витоку даних // Українська служба швидких новин (https://sumynews.online/21-miljon-***

koristuvachiv-populyarnogo-mobilnogo-zastosuvannya-postrazhdav-vid-vitoku-danix/). 09.07.2018).

***

«Хакеры получили доступ к системам безопасности одного из крупных международных аэропортов и выставили данные на продажу за $10…

Логины и пароли, которые получили киберпреступники, открывают доступ к управлению системами безопасности и автоматизации воздушной гавани через протокол удаленного рабочего стола.

…Несмотря на то, что проблема устранена, название воздушной гавани не раскрывается.

Каким образом взломщикам удалось получить доступ к конфиденциальным данным, достоверно неизвестно.» ***(Хакеры пытались продать международный аэропорт за $10 // Goodnews.ua (http://goodnews.ua/technologies/xakery-pytalis-prodat-mezhdunarodnyj-aeroport-za-10/). 13.07.2018).***

***

«В Тюмени на центр нейрохирургии была совершена хакерская атака, во время которой удалось отключить медицинское оборудование прямо во время операции

…глава Сбербанка России Герман Греф рассказал, что на днях получил письмо от главврача Тюменского федерального центра нейрохирургии Альберта Суфианова, который попросил помощи в связи с кибератакой на центр.

"Он делал очень сложную операцию на головном мозге тринадцатилетней девочке. И в середине этой операции клинический центр подвергся кибератаке, и все компьютерные системы, все приборы, которые сопровождали эту операцию, были отключены", - сообщил Греф на Международном конгрессе по кибербезопасности.

…благодаря опытности профессора ему и его коллегам удалось "довести эту операцию до завершения практически без показаний приборов".» ***(В России хакеры атаковали больницу // DsNews (http://www.dsnews.ua/world/v-rossii-hakery-atakovali-bolnitsu-09072018123100). 09.07.2018).***

***

«**Неизвестные хакеры успешно атаковали официальный сайт VSDC – популярного бесплатного инструмента для конвертации и редактирования аудио- и видеофайлов…**

По данным китайской компании Qihoo 360, под видом редактора VSDC устанавливались шпионская программа-инфостилер, клавиатурный шпион и троянец удаленного доступа (remote access trojan - RAT).

Шпионская программа в состоянии похищать логины и пароли учетных записей в Telegram и Steam, а также перехватывать переписку в Skype и данные цифрового кошелька Electrum. Клавиатурный шпион передает на серверы киберпреступников все вводимую пользователем с клавиатуры информацию, а

троянец потенциально позволяет установить удаленный контроль над инфицированным устройством.

Атакой оказались затронуты пользователи как минимум из 30 стран. В настоящий момент администрации VSDC удалось обнаружить и ликвидировать проблему…» ***(Шпион вместо редактора // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5514390-Shpion-vmesto-redaktora.html). 12.07.2018).***

***

«Під час найгіршої кібератаки у Сінгапурі хакери вкрали особисті дані 1,5 мільйонів пацієнтів, включаючи амбулаторні рецепти 160 000 осіб…

В ході атаки, хакери проникли в комп'ютери SingHealth - найбільшої групи медичних закладів Сінгапуру, що має чотири лікарні, п'ять національних спеціальних центрів та вісім поліклінік…

Немедичні персональні дані пацієнтів, які були незаконно відкриті та скопійовані, містили їхні імена, номери документів, адреси, стать, расу та дати народження…» ***(Саша Картер. У Сингапурі наймасштабніша в історії кібератака: викрадено особисті дані 1,5 млн людей // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1742410-u-singapuri-naymasshtabnisha-v-istoriyi-kiberataka-vikradeno-osobisti-dani-1-5-mln-lyudey). 20.07.2018).***

***

«По мнению эксперта по вопросам кибербезопасности, виновники крупной кибератаки в Сингапуре, в результате которой было похищено 1,5 млн учетных записей клиентов медицинских клиник SingHealth, вероятно, действовали по указанию неких государственных субъектов…

Президент регионального подразделения компании FireEye Эрик Хох отмечает существенные различия этого инцидента и типичных хакерских атак. Если последние целью ставят продажу (требование выкупа) похищенных данных, то в данном случае утечка медицинских данных видных чиновников может использоваться для принуждения в выполнении требований иного характера...

Премьер-министр Сингапура предположил, что хакеры искали компромат. «Мои данные о лекарствах не то, о чем я обычно рассказываю людям…», — добавил он.» ***(Заказчиками хакерской атаки в Сингапуре могли быть государственные лица // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/zakazchikami-hakerskoy-ataki-v-singapure-mogli-byit-gosudarstvennyie-litsa). 24.07.2018).***

***

«…Журналисты The Guardian изучили работу одного из крупнейших хакерских форумов в Интернете – FreeHacks. Это российское сообщество, цель которого – объединить все ресурсы для максимизации эффективности и распространения знаний.

Он работает так же, как любой обычный форум… с различными подфорумами, разделенными на категории…

Весь форум на русском языке - и насчитывает около 5 000 активных членов…

При попытке зарегистрироваться на сайте пользователь должен ознакомиться с определением миссии – своего рода обоснованием для незаконной деятельности…

По словам журналистов The Guardian, удивительно, как сообщество работает вместе, чтобы уничтожить "западные" системы и получить от этого прибыль. Как правило, хакеры в странах первого мира боятся работать вместе из-за высоких рисков. Однако в России власти, похоже, не заботятся о том, что эти хакеры наносят ущерб другим странам. Большинство пользователей на этом форуме - постоянные члены уже более шести лет.» ***(Ирина Фоменко. Что представляет из себя крупнейший российский хакерский форум // Internetua (http://internetua.com/csto-predstavlyaet-iz-sebya-krupneishii-rossiiskii-hakerskii-forum). 26.07.2018).***

***

«Серверы Oracle WebLogic подвергаются атакам со стороны хакеров, пытающихся перехватить контроль над уязвимыми устройствами, на которых еще не установлен недавний патч для критической уязвимости CVE-2018-2893. Об этом сообщили исследователи безопасности из компаний ISC SANS и Qihoo 360 Netlab.

Уязвимость CVE-2018-2893 представляет собой проблему в компоненте программного обеспечения Oracle WebLogic, позволяющую удаленному злоумышленнику получить контроль над сервером без необходимости знать его пароль и, потенциально, выполнить произвольный код на устройстве.

…Oracle выпустила исправления 18 июля 2018 года, однако, спустя три дня несколько PoC-кодов были опубликованы различными пользователями в Сети. По меньшей мере два из них все еще доступны в интернете.

Первые попытки эксплуатации начались 21 июля 2018 года, после того, как сообщения о существовании PoC-кодов распространились через социальные сети. С тех пор число атак постепенно начало увеличиваться.

По словам исследователей, существует как минимум две отдельные группы хакеров, которые, предположительно, смогли автоматизировать процедуру эксплуатации.

Владельцам серверов рекомендуется как можно скорее установить обновления от Oracle за июль 2018 года…» ***(На серверы Oracle WebLogic совершен ряд кібератак // Goodnews.ua (http://goodnews.ua/technologies/na-servery-oracle-weblogic-sovershen-ryad-kiberatak/). 25.07.2018).***

***

«Телеканалы WDR и ZDF из ФРГ были атакованы российской хакерской группой Sandworm…

Кибератака, по информации источников, произошла в начале июня… Телеканал ZDF сообщил, что нападение хакеров якобы действительно было, в результате него пострадали менее 10 компьютеров.

Посольство России в ФРГ прокомментировало сообщение об атаках. «Бундестаг, МИД, теперь WDR и ZDF. Кто еще? Сгораем от любопытства», – написали российские дипломаты в Twitter.

Хакерскую группу Sandworm, которую Запад связывает с Россией, ранее уже обвиняли в «блэкауте» на Украине, случившемся в декабре 2015 года. Тогда пятая часть Киева оказалась без света из-за аварии на подстанции…» ***(Алексей Ласнов. Немецкие телеканалы обвинили российских хакеров в кибератаке // Деловая газета «Взгляд» (https://vz.ru/news/2018/7/27/934558.html). 27.07.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«Компания Check Point в отчёте Global Threat Impact Index за июнь отмечает, что за последние четыре месяца атаки банковских троянов выросли на 50%. В десятку самых активных угроз вошло два семейства троянов.

Банковский троян Dorkbot, ворующий конфиденциальную информацию и запускающий DDoS-атаки, затронул 7% организаций по всему миру. Так, зловред поднялся с восьмого на третье место в списке самых опасных вредоносных программ по версии Check Point. Также в июне появился троян Emotet, способный похищать банковские данные пользователей и распространяться с помощью уже инфицированных компьютеров. Новый вредонос стремительно распространяется последние два месяца — он переместился с 50 места апрельского отчета на 11 позицию текущего. Вместе с Dorkbot в топ-10 киберугроз вошел троян Ramnit, ворующий банковские данные и FTP-пароли…

Исследователи Check Point также проанализировали наиболее эксплуатируемые уязвимости. На первом месте — уязвимость CVE-2017-7269 с глобальным охватом 46%, затем CVE-2017-10271 (40%), на третьем месте — уязвимость типа «внедрение SQL-кода», затрагивающая 16% организаций во всем мире.

Этот список показывает, что злоумышленники успешно используют как современные методы (две уязвимости, опубликованные в 2017 г.), так и классические векторы атак, такие как внедрение SQL-кода.» ***(Банковские трояны стали активнее в полтора раза // «Компьютерное Обозрение» (https://ko.com.ua/bankovskie_troyany_stali_aktivnee_v_poltora_raza_125298).*** 12.07.2018).

***

«Эксперты в области кибербезопасности обнаружили новый вирус, поражающий компьютеры на macOS. Создатель специализированного сайта Objective-See Патрик Вардл (Patrick Wardle) в своем блоге назвал его «дураком» (OSX.Dummy).

Вредоносное ПО распространялось киберпреступниками через мессенджеры Discord и Slack. Притворяясь известными криптовалютными инвесторами или

администраторами каналов, посвященных цифровым средствам, они рекомендовали жертвам ввести некоторые команды в терминале macOS.

Такие команды приводили к загрузке файла, который самостоятельно закреплялся в системе и разрешал преступникам доступ к ней. Эксперты предполагают, что вредное программное обеспечение было предназначено для воровства криптовалюты у майнеров…» ***(Обнаружен компьютерный вирус-«дурак» // Goodnews.ua (http://goodnews.ua/technologies/obnaruzhen-kompyuternyj-virus-durak/). 07.07.2018).***

***

«Исследователь в области кибербезопасности из Болгарии под ником VessOnSecurity сообщил в своем Twitter об обнаружении нового опасного вируса.

По словам эксперта, действия вредоносного ПО схожи с поведением ботнета Mirai, который в 2016 году отключил несколько стран мира от интернета в ходе DDoS-атаки…

Спустя несколько дней исследователь опубликовал карту распространения вируса. …По его данным, количество атак с помощью неизвестного вируса увеличивается с каждым часом, — по данным на 1 июля вредное ПО совершало нападение каждые 1,2 секунды.

Судя по URL-адресам, с которых чаще всего подгружаются вредоносные файлы, вирус действительно как-то связан с уже известным мощным ботнетом: указатели содержат упоминания Mirai и его модификации Sora…». ***(У самого опасного интернет-оружия появился конкурент // Goodnews.ua (http://goodnews.ua/technologies/u-samogo-opasnogo-internet-oruzhiya-poyavilsya-konkurent/). 05.07.2018).***

***

«В конце мая нынешнего года эксперты в области кибербезопасности предупредили общественность о новой вредоносной кампании, в рамках которой злоумышленники заразили высокотехничным ПО VPNFilter по меньшей мере 500 тыс. маршрутизаторов и устройств хранения данных по всему миру…

Специалисты компании Symantec разработали бесплатный online-инструмент VPNFilter Check, позволяющий быстро проверить маршрутизаторы на предмет компрометации вредоносным ПО VPNFilter. В частности, инструмент анализирует входящий трафик в домашних и корпоративных сетях и определяет, был ли он модифицирован.

Как пояснил эксперт Весселин Бонтчев (Vesselin Bontchev), инструмент не детектирует присутствие VPNFilter на маршрутизаторе, а определяет манипуляции с HTTPS-соединением…» ***(Представлен инструмент для проверки на предмет заражения вредоносом VPNFilter // Goodnews.ua (http://goodnews.ua/technologies/predstavlen-instrument-dlya-proverki-na-predmet-zarazheniya-vredonosom-vpnfilter/). 04.07.2018).***

***

«ESET выполнила анализ вредоносной программы Win32/Glupteba, известной как компонент масштабной киберкампании «Операция Windigo»…

Специалисты ESET наблюдают за Win32/Glupteba с 2011 года…

Согласно новому исследованию ESET, в настоящее время Glupteba больше не использует инфраструктуру Windigo. Вредоносная программа стала частью собственного ботнета и распространяется посредством MSIL/Adware.CsdiMonetize.AG – программы, доставляющей различные семейства вредоносного ПО с оплатой за число установок (Pay-Per-Install).

Анализ новых образцов Glupteba установил, что малварь была переписана с нуля. Если прежде Glupteba была сравнительно небольшой и простой, то сейчас это объемная и сложная программа. Ранее Glupteba поддерживала около 70 функций, а сейчас – больше 3600.

Изменилась область применения вредоносной программы. В составе своего ботнета Glupteba не только генерирует спам, но и используется в качестве прокси различными автоматизированными системами. …Кроме того, Glupteba замечена в атаках, основанных на повторном использовании пароля – малварь обеспечивает некоторую анонимность злоумышленникам.

По данным телеметрии ESET, с начала 2017 года активность Glupteba зафиксирована в 180 странах. 25% обнаружений вредоносной программы приходится на Россию, Украину и Турцию…» ***(На Россию, Украину и Турцию приходится 25% обнаружений Win32/Glupteba // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5515970-Na-Rossiyu-Ukrainu-i-Turciyu-prixod.html). 19.08.2018).***

***

«Специалисты ESET обнаружили новую киберкампанию, в которой используются сертификаты для подписи кода, украденные у компании D-Link Corporation.

Вредоносная компания была зафиксирована ESET после обнаружения нескольких подозрительных файлов. Они были подписаны действительным сертификатом D-Link Corporation. Тот же сертификат использовался в легитимном ПО D-Link.

…В ходе исследования в ESET нашли также вредоносные образцы, подписанные сертификатом другой тайваньской технологической компании – Changing Information Technology Inc., которая специализируется на продуктах для безопасности…

С помощью украденных сертификатов распространялись два семейства вредоносных программ: бэкдор для удаленного управления зараженным компьютером Plead и связанный с ним инструмент для сбора паролей, сохраненных в Google Chrome, Internet Explorer, Microsoft Outlook и Mozilla Firefox.

По мнению экспертов, за атакой стоит кибершпионская группа BlackTech, атакующая цели в Восточной Азии…» ***(Хакеры подписывали вредоносное ПО сертификатом D-Link // ООО "ИКС-МЕДИА"***

(http://www.iksmedia.ru/news/5513706-Xakery-podpisyvali-vredonosnoe-PO.html). 10.07.2018).

***

«Несколько дней назад команда Digital Shadows сообщила о публикации на одном из форумов файлов и исходного кода ПО, предположительно связанных с кампаниями хакерской группировки Carbanak (также известной как Anunak и Cobalt)…

Carbanak представляет собой бэкдор, предназначенный для внедрения в сети финансовых организаций и кражи средств.

…исследователи поставили под сомнение принадлежность опубликованного кода группировке Carbanak и оказались правы.

Эксперты "Лаборатории Касперского" провели анализ исходного кода и выяснили, что речь идет о другом финансовом вредоносном ПО, известном под названиями Karamanak, Ratopak и Pegasus (не следует путать с шпионским ПО Pegasus для iOS). Судя по временным меткам, код был создан в 2015-2016 годах. По словам исследователей, вирусописатели определенно являются русскоговорящими, их цель – финансовые организации в России…» ***(Утекший "исходный код Carbanak" оказался совсем другим трояном // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123988). 13.07.2018).***

***

«Зловмисники перетворили опублікований минулого місяця PoC-код на реальний експлоїт для атак на ПК під управлінням Windows 10.

Автори шкідливого ПЗ несамовито накинулись на новий вектор атак, представлений на початку минулого місяця. Даний спосіб передбачає використання файлів SettingContent-ms для виконання коду на ПК під управлінням Windows 10.

…кілька днів тому зловмисники вперше створили ланцюжок експлойтів, що використовує файл SettingContent-ms для завантаження і установки реального шкідливого ПЗ. Зокрема, один з використовуваних зловмисниками файлів SettingContent-ms завантажував троян для віддаленого доступу Remcos.

…поява робочих експлойтів для завантаження реального шкідливого ПЗ свідчить про серйозні наміри кіберзлочинців використовувати даний вектор атак.» ***(Хакери використовують файли SettingContent-ms для завантаження шкідливого ПЗ // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/07/04/SettingContent-ms.html). 04.07.2018).***

***

«Користувачі по всьому світу виявили на своїх комп'ютерах шкідливу програму All-Radio 4.27 Portable, яку неможливо видалити.

…вперше пости про вірус з'явилися на форумі Malwarebytes. Зараженими виявилися комп'ютери з операційною системою Windows. При цьому видалити шкідливу програму жодному з користувачів не вдалося. Оригінальна програма All-Radio 4.27 Portable являє собою універсальний плеєр, що дозволяє слухати музику і

дивитися ТБ. Невстановлені хакери підробили програму і видали заражене ПЗ за оригінал…

Експерти застерегли від використання програм-активаторів, тому що вони можуть містити цей вірус, що не видаляється.» ***(На Windows з'явився вірус, що не видаляється // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/07/04/All-Radio-virus.html). 04.07.2018).***

***

«**До этого времени вредоносное ПО Pegasus было в дарквебе, теперь появилось в общем доступе**

Данный инструмент позволяет вывести денежные средства через автоматизированное рабочее место банка. При этом для осуществления атаки на любые кредитные организации не требуются специальные знания, так как вместе с Pegasus идет инструкция по использованию программы.

…образец выложенной в сеть программы Pegasus немного устарел, т.к. датируется 2015 годом, однако для киберпреступника не составит труда адаптировать ее под современные условия.» ***(В открытый доступ выложили инструмент для кибератак на банки // SecureNews (https://securenews.ru/a-tool-for-cyber-attacks-on-banks-was-posted-openly/). 16.07.2018).***

***

«Дослідники компанії ESET виявили кібершпигунську кампанію, націлену на українські держустанови…

Зловмисники заражають комп'ютери жертв вірусами Quasar RAT, Sobaken і Vermin зі схожим вихідним кодом, за допомогою яких викрадають дані і аудіозаписи розмов з комп'ютерів жертв.

Віруси розповсюджуються за допомогою фішингових листів і вже вразили комп'ютерні мережі кількох сотень жертв з різних держустанов України…

Примітно, що віруси модифіковані таким чином, щоб працювати тільки при російській або українській розкладці з IP-адресами в межах Росії або України. Якщо ці умови не дотримані, вірус самостійно видалиться…» ***(На українські держустанови відбулася кібератака // Varta1 (https://varta1.com.ua/na-ukrayinski-derzhustanovy-vidbulasya-kiberataka/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+varta1news+%28VARTA1%29). 24.07.2018).***

***

«Хакеры скрывают вредоносный код внутри полей метаданных изображений, размещенных в официальной CDN (сеть доставки контента) компании Google – googleusercontent.com. Об этом сообщил исследователь безопасности из компании Sucuri Денис Синегубко.

На данном домене, как правило, размещаются изображения и фотографии, загруженные на сайтах Blogger.com и в социальной сети Google+.

По словам исследователя, ему удалось обнаружить одну рекламную кампанию по распространению вредоносного ПО, в которой CDN

GoogleUserContent использовалась для размещения одного из вредоносных изображений.

Обнаруженное исследователем изображение содержало вредоносную программу, предназначенную для хищения токенов безопасности PayPal. Злоумышленники поместили зашифрованный вредоносный код в поле комментария в метаданных изображения.

Примечателен метод хранения файла, не позволяющий сообщить о вредоносе. В Google предусмотрена отправка сообщений о нарушении изображением авторских прав, однако не о проблемах с безопасностью…

Помимо этого, исследователь заявил о невозможности идентификации автора изображения…» ***(Сеть распределения контента от Google используется для хранения вредоносного ПО // Goodnews.ua (http://goodnews.ua/technologies/set-raspredeleniya-kontenta-ot-google-ispolzuetsya-dlya-xraneniya-vredonosnogo-po/). 21.07.2018).***

***

«Стало известно, что количество вирусов-майнеров превысило долю ранее популярных троянов-вымогателей. Об этом сообщается в отчете компании Skybox Security, занимающейся информационной безопасностью.

…на данный момент 32% всех кибератак составляют крипто-майнеры, в то время как вирусы-вымогатели занимают всего 8% рынка компьютерных атак. Хакеры встраивают программный код на сайты, либо пишут вирусы, которые используют ресурсы компьютеров пользователей для добычи криптовалют...» ***(Вирусы-майнеры стали одной из главных угроз в интернете // Goodnews.ua (http://goodnews.ua/technologies/virusy-majnery-stali-odnoj-iz-glavnyx-ugroz-v-internete/). 22.07.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«На прошлой неделе прокуратура Израиля обвинила бывшего сотрудника компании NSO Group в краже программного кода продукта…

Экс-сотрудник NSO попытался продать украденный код конкурентам за 50 миллионов долларов в криптовалюте, но потенциальный покупатель предупредил компанию…

NSO, сотрудничающая с израильскими военными, известна своим программным обеспечением, которое используют для взлома шифрования на смартфонах…

Ситуация с NSO уникальна тем, что программный код создан экспертами по безопасности. ПО NSO используется для наблюдения, прежде всего государственными клиентами, и для взлома таких устройств, как iPhone. Программное обеспечение контролирует израильское правительство…» ***(Ирина***

Фоменко. Израильскую компанию по кибербезопасности обокрал собственный сотрудник // Internetua (http://internetua.com/izrailskuua-kompaniua-po-kiberbezopasnosti-obokral-sobstvenni-sotrudnik). 12.07.2018).

***

«…В период чемпионата мира нейтрализовано почти 25 миллионов кибератак и иных преступных воздействий на информационную инфраструктуру России, так или иначе связанную с проведением чемпионата мира по футболу», — заявил Президент РФ Владимир Путин на встрече с представителями штаба по обеспечению безопасности ЧМ-2018.

Путин добавил, что власти, готовясь к соревнованиям, проверили более 2 млн человек, задействованных в строительстве объектов ЧМ и организации турнира...

Российский лидер подчеркнул важность реализации системы идентификации футбольных болельщиков с изготовлением персонифицированных карт зрителей, а также интегрированной с ней системы контроля доступа на стадионы…» ***(Путин: за время ЧМ2018 на Россию было совершено 25 млн кибератак // РосКомСвобода (https://roskomsvoboda.org/40422/). 16.07.2018).***

***

«Правоохранительные органы Ливана арестовали трех человек, подозреваемых в осуществлении крупнейшей в истории страны кибератаки, в ходе которой были взломаны множество ливанских компаний и организаций.

В ходе операции правоохранители задержали хакера, одного из его сообщников и местного бизнесмена.

По словам представителей властей, хакер взломал ИТ-системы агентств безопасности, правительственных ведомств и частных компаний, таких как две сотовые телекоммуникационные компании и крупный интернет-провайдер Ogero Telecom, контролируемый государством.

…в большинстве случаев хакеры похищали данные взломанных компаний и позднее попытались продать их. Как полагают ливанские СМИ, третий арестованный подозреваемый, местный бизнесмен, может являться покупателем данных и нанимателем хакеров.

Инцидент был выявлен Ogero Telecom в конце июня…» ***(В Ливане хакеры провели крупнейшую в истории страны кибератаку // Goodnews.ua (http://goodnews.ua/technologies/v-livane-xakery-proveli-krupnejshuyu-v-istorii-strany-kiberataku/). 13.07.2018).***

***

«Житель штата Кентукки на суде признал, что является автором LuminosityLink — коммерческой программы удаленного доступа, которую покупатели использовали для захвата контроля над чужими компьютерами.

В заявлении о признании вины, которое подписал 21-летний Колтон Граббс (Colton Ray Grubbs) и заслушал суд, сказано, что LuminosityLink появился на рынке в апреле 2015 года. За два с лишним года этот RAT-инструмент купили более 6 тыс. пользователей.

…этот инструмент можно устанавливать удаленно и без предупреждения — то есть без ведома владельца компьютера. Широкий набор функций LuminosityLink, согласно рекламе, позволяет ему регистрировать нажатия клавиш, вести наблюдение с помощью веб-камеры и микрофона, просматривать и выгружать файлы, похищать учетные данные для доступа к сайтам, добывать криптовалюту, проводить DDoS-атаки и обходить антивирусную защиту…

По совокупности Граббсу грозит до 25 лет лишения свободы со штрафом в размере 750 тыс. долларов…» ***(Maxim Zaitsev. Создателю LuminosityLink RAT грозит тюремный срок // Threatpost (https://threatpost.ru/luminositylink-rat-author-signs-plea-agreement/27292/). 18.07.2018).***

***

«Вчера в Роттердаме состоялось заседание суда, на котором было заслушано дело братьев Мелвина и Денниса ван де Б., обвиняемых в создании и распространении шифровальщиков CoinVault и Bitcryptor (он же CoinVault 2.0).

…Вымогательское ПО CoinVault появилось в Интернете в 2014 году; это был один из первых Windows-зловредов, шифрующих файлы и требующих плату за ключ расшифровки. Распространялся он преимущественно под видом “кряков” и за полтора года умудрился проникнуть в 108 стран, хотя подавляющее большинство жертв CoinVault составили голландцы.

Предполагаемых авторов этой вымогательской кампании удалось выявить в результате расследования, проведенного киберполицией Нидерландов и “Лабораторией Касперского”…

По оценке прокуратуры, атаки CoinVault принесли инициаторам более 10 тыс. евро (с жертв взимали по 1 биткойну, курс которого в те годы составлял примерно 220 долларов). Голландская полиция зарегистрировала около 1,3 тыс. жалоб; некоторые заявители дали показания в суде. Одна из жертв даже попыталась вернуть свой биткойн, который отдала за ключ расшифровки в 2015 году, — в надежде подзаработать на разнице: 1 биткойн сейчас эквивалентен почти 6,24 тыс. долларов США.

Один из представших перед судом братьев, Мелвин, предположительно является автором вредоносной программы, второй (Деннис) занимался ее распространением. По заявлению защиты, Мелвин в настоящее время трудоустроен и на своем месте “незаменим”, Деннис учится в Техническом университете Эйндховена.

Вынесение приговора подсудимым запланировано на 26 июля.» ***(Maxim Zaitsev. В Нидерландах судят создателей CoinVault // Threatpost (https://threatpost.ru/coinvault-authors-on-trial-in-the-netherlands/27161/). 13.07.2018).***

***

«Чотири людини затримані в Бразилії за підозрою в хакерських атаках на смартфони відомих політичних діячів…

…у числі постраждалих опинилися 25 осіб, у тому числі глава цивільної канцелярії президента Елісеу Паділья, секретар у справах уряду Карлуш Марун, а також колишній міністр соціального розвитку Озмар Терра. Після злому мобільних пристроїв хакери отримували доступ до контактів політиків і під різними приводами починали просити грошей у їх знайомих. Багато з тих, із ким спілкувалися злочинці, не наважувалися відмовити співрозмовникам, яких вважали впливовими чиновниками. Тому зловмисники легко отримували банківські перекази на запитані суми.

За даними правоохоронних органів, у цілому учасники угруповання змогли збагатитися на 76 тис. реалів (майже 20 тис. доларів). Зараз слідчі намагаються встановити, чи встигли зловмисники продати кому-небудь конфіденційну інформацію зі смартфонів чиновників…» ***(Самуїл Проскуряков. У Бразилії затримали хакерів, які зламали смартфони соратників президента // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1741904-u-braziliyi-zatrimali-khakeriv-yaki-zlamali-smartfoni-soratnikiv-prezidenta). 19.07.2018).***

***

«Два года назад хакер по имени Voksi нашел способ взломать проблемную DRM-защиту Denuvo. Он продолжал воевать с Denuvo до последнего времени, но вчера к нему постучалась полиция.

Voksi всего 21 год, он живет в Болгарии и противостоял Denuvo из принципа: по его словам, «раздутому софту нет места в играх».

…Denuvo замедляет ПК и понижает количество кадров в секунду в игре. Иногда она выдает ошибки при запуске. …То есть, она попросту портит компьютеры пользователей, а потому является не столько проблемой пиратов, сколько наказанием для игроков, которые покупают игры честно…

Опасаясь за свою свободу, Voksi предложил Denuvo пойти на мировое разрешение конфликта, однако компания отказалась решать вопрос мирно и сказала, что с делом будет разбираться прокуратура.

…Юный хакер, хотя и был весьма умелым, являлся лишь частью хакерского сообщества Revolt. …Кроме того, Revolt - не единственное сообщество, ведущее борьбу за свободу от Denuvo. К примеру, с вредоносной системой защиты также довольно успешно борются китайские хакеры.» ***(Болгарский хакер Voksi, взломавший защиту Denuvo, арестован // IGate (http://igate.com.ua/lenta/22337-bolgarskij-haker-voksi-vzlomavshij-zashhitu-denuvo-arestovan). 26.07.2018).***

***

Технічні аспекти кібербезпеки

«На международном конгрессе по кибербезопасности ICC в Москве компания Bi.zone продемонстрировала сценарий атаки на систему управления автомобилем.

Специалисты компании собрали и запрограммировали небольшое устройство, которое дает возможность постороннему управлять машиной. Устройство можно незаметно установить за пару минут. Например, вскрыть на автомойке панель, подключить маленькое плато к диагностическому разъему и закрыть её обратно. Пользователь ничего не заметит, а у злоумышленника появится доступ к автомобилю через Интернет из любой точки мира.

Для демонстрации возможностей была выбрана серийно выпускаемая машина Tesla Model 3. Удаленно специалисты компании управляли детищем Илона Маска – освещением салона, ремнями безопасности, открывали и закрывали двери.

..Отчет о выявленных уязвимостях поступил в Tesla и в настоящее время они закрыты – демонстрация проводилась на старых прошивках. Но сам подход может быть использован на других автомобилях, что наглядно показывает новые риски, появляющиеся в современном цифровом мире.» ***(Николай НОСОВ. Кто управляет вашим автомобилем? // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5512885-Dochka-Sberbanka-nauchilas-vzlamyva.html). 06.07.2018).***

***

«…В шоу-руме концерна «Автоматика» прошла демонстрация возможностей киберзащищенной системы видеоконференцсвязи IVA AVES-S. На глазах у потенциальных заказчиков была проведена серия массированных DDOS-атак на систему, а также смоделированы ситуации выхода из строя сетевого оборудования и серверов. Однако IVA AVES-S продемонстрировала «живучесть», сохранив полную работоспособность всех сервисов.

Система IVA AVES-S представляет собой универсальную программно-аппаратную платформу для организации многоточечных защищенных видеоконференций с разрешением Full HD…

В ходе демонстрации DDOS-атаки проводились как изнутри системы, так и извне…» ***(Киберзащищенный аналог «Скайпа» выдержал массированные хакерские атаки // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5513027-Kiberzashhishhennyj-analog-Skajpa.html). 06.07.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«В 2017 году государственные и частные программы поиска уязвимостей помогли обнаружить более 78 тыс. брешей в компьютерных системах. Такая информация содержится в отчете сервиса Hacker One, опубликованном 11 июля...

Основываясь на информации о более чем 1000 конкурсов bug bounty, размещенных на платформе, специалисты сделали вывод, что этичные хакеры способны обнаружить самые серьезные баги. Доля критических и опасных уязвимостей среди найденных брешей составила 24%...

Программы вознаграждения добровольных исследователей в 2017 году помогли обнаружить на 22% больше уязвимостей, нежели годом ранее. Возможно, это связано с резким увеличением активности государственных органов. Они объявили на 125% больше конкурсов по поиску брешей, чем в 2016-м.

Количество программ bug bounty, объявленных компаниями из Европы, Ближнего Востока и Африки, выросло за год на 22%. Азиатско-Тихоокеанский регион показал рост на 37%, Северная Америка — на 38%. Наилучшую динамику продемонстрировали организации и правительственные учреждения Латинской Америки. В 2017-м здесь объявили на 143% больше конкурсов, чем годом ранее.

Объем вознаграждений, выплаченных ИТ-специалистам, вырос в 2017 году на 157%. Microsoft, Google и другие крупные компании предлагают до $250 тыс. за помощь в поиске уязвимостей…

Самые щедрые из организаторов программ bug bounty — государственные учреждения. Средняя выплата за одну уязвимость в 2017 году здесь составила $3,9 тыс. На втором месте технологические компании с результатом $3,6 тыс., на третьем — организации телекоммуникационного сектора, готовые выделить около $3 тыс…

Больше всего денег на bug bounty заработали американские специалисты. На их долю пришлось 17% всех полученных наград за поиск уязвимостей. На втором месте — Индия с 13% призовых денег. Третью строчку занимают ИБ-эксперты из России, получившие 6% от общего объема вознаграждения. В пятерку лучших вошли также представители Великобритании и Германии.

Данные отчета позволяют сделать вывод, что в мире сформировано высококвалифицированное сообщество независимых специалистов, готовых участвовать в программах bug bounty…» ***(Dmitry Nazarov. Компании готовы платить до $250 тыс. за информацию о багах // Threatpost (https://threatpost.ru/companies-offer-up-to-250k-for-bug-reports/27228/). 16.07.2018).***

***

«Команда специалистов из Политехничского университета Виргинии (США), исследовательской группы Microsoft Research и Китайского Университета науки и технологий разработала метод атаки, позволяющий осуществить подмену GPS-сигнала (GPS-спуфинг) автомобильных навигаторов и заставить владельцев машин ехать по неверному маршруту.

…Новый метод позволяет осуществлять спуфинг-атаки с учетом схемы маршрута. Для этой цели исследователи разработали специальный алгоритм, работающий в режиме почти реального времени, и портативное устройство для трансляции сигнала GPS, которое может крепиться к автомобилю жертвы или машине злоумышленника, следующего за объектом на расстоянии до 50 метров.

С помощью алгоритма атакующий может выбрать любую локацию, куда нужно заманить жертву. Алгоритм создает и передает GPS-сигналы на целевой навигатор, который затем отображает маршруты, соответствующие физической карте дорог. В реальном мире жертва, следующая таким указаниям, поедет по неверному маршруту или окажется в другом месте, пояснили ученые. По их словам, алгоритм способен создавать некорректные маршруты для 99,8% поездок.

Ученые протестировали алгоритм в лабораторной среде и в реальных условиях на дорогах США и Китая. Как отмечается, из 40 участников эксперимента удалось обмануть 38 (95%)…» ***(Эксперты разработали метод, позволяющий осуществить подмену GPS-сигнала // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=124014). 16.07.2018).***

***

«Група вчених із США і Німеччини опублікувала результати дослідження вразливостей стандарту передачі даних LTE, також відомого як 4G…

Міжнародна команда дослідників розповіла про три варіанти атак, заснованих на вразливості LTE. Дві з них є пасивними, тобто не дозволяють зловмисникам управляти трафіком мобільного пристрою. В одному випадку мова йде про доступ до метаданих переданих пакетів інформації, а в іншому - про відстеження сайтів, які відвідує жертва.

Третя атака отримала назву aLTEr. Експлуатуючи недоліки стандарту LTE, кіберзлочинці можуть перехоплювати і підміняти DNS-пакети, перенаправляючи користувача на власні ресурси…

Всі три атаки експлуатують уразливості 4G, пов'язані з недостатнім захистом інформації…

Стандарт 5G, який прийде на зміну LTE, передбачає більш надійний захист інформації, однак теж є вразливим. Як підкреслили дослідники, новою технологією передбачені посилене шифрування і контроль цілісності даних, однак вони не є обов'язковими…» ***(Аналітики навчилися перехоплювати і змінювати трафік мереж 4G // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/07/04/scientists-can-intercept-and-change-4g-traffic.html). 04.07.2018).***

***

«…В браузере Microsoft Edge перестал работать XSS-фильтр - механизм безопасности, предотвращающий межсайтовое выполнение сценариев (XSS-атака) в браузерах. На проблему обратил внимание специалист компании PortSwigger Гарет Хэйес (Gareth Heyes).

Впервые данная функция появилась в Internet Explorer 8, а позже была реализована в Edge и других интернет-обозревателях, таких как Google Chrome и Apple Safari. Функционал также известен как X-XSS-Protection…

В последние три года Edge по умолчанию проверял код любой загружаемой страницы вне зависимости от того, сконфигурирован заголовок X-XSS-Protection или нет. Однако несколько дней назад Хэйес обнаружил, что настройки XSS-фильтра не работают привычным образом. По его словам, теперь функция по умолчанию отключена…

Специалист проинформировал Microsoft о проблеме, однако инженеры компании не предоставили пояснений по данному вопросу…» ***(В Microsoft Edge «сломалась» одна из функций безопасности // SecurityLabRu (https://www.securitylab.ru/news/494579.php). 22.07.2018).***

***

«…Эксперты «Лаборатории Касперского» проанализировали более десятка мобильных приложений от каршеринговых компаний (сдающих в аренду автомобили), и обнаружили серьезные уязвимости, с помощью которых злоумышленники могут похитить персональную информацию и даже угнать автомобиль.

…приложения от каршеринговых компаний могут заинтересовать киберпреступников по целому ряду причин. К примеру, они могут взломать учетную запись легитимного пользователя и ездить на машине за его счет, угнать машину или использовать ее в преступных целях. Кроме того, злоумышленники могут следить за передвижениями пользователя и получить доступ к его персональным данным.

Вышеописанные сценарии возможны пока только в теории, однако, как отметили в ЛК, киберпреступники уже продают взломанные учетные записи клиентов каршеринговых компаний. Продавцы рекламируют свой товар, уверяя, что с его помощью покупатель получит целый ряд возможностей, в том числе возможность водить автомобиль без водительских прав…» **.** ***(Приложения от каршеринговых компаний позволяют угнать автомобиль // SecurityLabRu (https://www.securitylab.ru/news/494634.php). 26.07.2018).***

***

«Експерти в області кібербезпеки склали список найнебезпечніших мобільних додатків, які можуть викликати загрозу для корпоративних клієнтів. Про це йдеться в дослідженні компанії Appthority за другий квартал 2018 року.

Найбільш ризикованими додатками для iOS-пристроїв фахівці назвали месенджери WhatsApp і Facebook Messenger. Крім того, в трійку лідерів антирейтингу потрапила навігаційна програма Waze.

Додатки WhatsApp і Facebook також отримали найвищі бали за рівнем ризику на смартфонах під управлінням Android. Однак на третьому місці тут розташувався месенджер Telegram. Дослідники відзначили, що і Waze, і Telegram потрапили в списки вперше.

Месенджери Facebook і WhatsApp отримали по 7 балів з 10. Висока оцінка означає, що додатки можуть відправляти на сервери дані, пов’язані з підприємством, або ж не відповідають політиці безпеки…» ***(Названо найнебезпечніші додатки для смартфонів // ВСВІТІ (http://vsviti.com.ua/news/87035). 23.07.2018).***

***

«Разработчики компании Apple исправили криптографическую ошибку, которая возникает в протоколе Bluetooth и позволяет злоумышленникам перехватывать трафик, вторгаясь в соединение между сопряженными устройствами.

…уязвимость может возникать вследствие недостаточно тщательной проверки устройствами с поддержкой Bluetooth параметров шифрования при установке соединения друг с другом. Это в свою очередь позволяет злоумышленникам, находящимся вблизи жертвы (на расстоянии до 30 м), получать доступ к ее конфиденциальным данным.

…Несмотря на то что публично о существовании уязвимости было сообщено только 23 июля, Apple выпустила обновления фирменных ОС с исправлением бага почти месяц назад...» ***(Apple еще раз доказала, что не стоит пренебрегать обновлениями // Goodnews.ua (http://goodnews.ua/technologies/apple-eshhe-raz-dokazala-chto-ne-stoit-prenebregat-obnovleniyami/). 26.07.2018).***

***

«…Эксперт по кибербезопасности Мэтт Грэбнер (Matt Graebner) обнаружил довольно элегантный способ обходить «белые списки» авторизованных приложений Windows и осуществлять запуск произвольного неподписанного кода.

Согласно описанию, которое приводит Грэбнер, используемый в Windows скрипт winrm.vbs (располагается в папке System32) способен обрабатывать и запускать «контролируемый злоумышленником XSL», который не подпадает под ограничения enlightened script host, что позволяет запускать произвольный код.

«Если снабдить winrm.vbs параметрами “-format:pretty” или “-format:text”, он вызывает WsmPty.xsl или WsmTxt.xsl из каталога, в котором находится cscript.exe, — пишет исследователь. — Это означает, что если злоумышленник скопирует cscript.exe в область, находящуюся под его контролем и в которой располагается его вредоносный XSL, ему удастся добиться запуска произвольного кода. По факту эта проблема практически идентична методу Кейси Смита (Kasey Smith) с использованием wmic.exe»…

Грэбнер указывает, что не существует надежных способов блокировать угрозу иначе как посредством активации принудительной проверки целостности кода в пользовательском режиме (User Mode Code Integrity) в модуле контроля приложений Windows Defender (WDAC). Однако, по словам Грэбнера, большинство организаций не использует WDAC.

В любом случае, пишет исследователь, присутствие на диске неподписанных WsmPty.xsl и WsmTxt.xsl должно немедленно вызывать подозрения…». ***(Найден способ взломать «белые списки» приложений Windows // Goodnews.ua (http://goodnews.ua/technologies/najden-sposob-vzlomat-belye-spiski-prilozhenij-windows/). 18.06.2018).***

***

«Консультант по кибербезопасности компании Asterisk Питер Хэнней рассказал о том, что любой смартфон можно использовать как прослушивающее устройство…

Специалист отметил, что приложения могут реагировать на слова-триггеры, включать запись звука и передавать полученные данные разработчикам. Далее эти данные могут обрабатываться специальными алгоритмами. Это может быть

сделано, к примеру, для того, чтобы показывать пользователю рекламу товаров, которыми он интересуется.

Распознавание слов может производиться приложением непосредственно на смартфоне при условии, что разработчики предусмотрели такую функциональность.

И при этом отследить их будет крайне непросто. В большинстве популярных сервисов данные шифруются и невозможно отследить, какую именно информацию собирают приложения и по каким триггерам срабатывает запись голоса…» ***(Ирина Черныш. Эксперты назвали слова, которые запускают слежку в мобильных приложениях // Голосиа (https://golos.ua/i/626914). 30.07.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Блокчейн-стартап Oasis Labs объединяет светил академического мира и исследователей кибербезопасности из различных научных центров, включая Массачусетский технологический институт и Калифорнийский университет в Беркли.

9 июля компания сообщила, что ей удалось привлечь $45 млн. в ходе закрытой предварительной продажи токенов, в которой приняли участие крупнейшие инвесторы криптовалютного сектора. Средства пойдут на разработку и запуск децентрализованной блокчейн-платформы (решения облачного вычисления) с акцентом на приватности.

Представители Oasis Labs полагают, что платформа сумеет обойти ограничения в области производительности, надёжности и приватности, которые испытывают многие блокчейн-приложения. Они рассчитывают, что за счёт этого она сможет конкурировать с такими популярными платформами облачных вычислений, как, например, Amazon Web Services. Платформа, по их мнению, сможет обслуживать сервисы, чувствительные к аспекту конфиденциальности — например, из сферы машинного обучения…» ***(A16z и Binance помогли Oasis Labs собрать $45 млн. на закрытом токенсейле // BIGFIN (https://bigfin.net/10/07/2018/a16z-i-binance-pomogli-oasis-labs-sobrat-45-mln-na-zakrytom-tokensejle/). 10.07.2018).***

***

«Распространение цифровых технологий и внедрение автоматизированного вождения приводит к тому, что автомобили становятся потенциальным объектом для хакерских атак. В поддержку концепции безаварийного вождения Vision Zero, компания Continental использует технологии кибербезопасности для защиты цифровых систем…

Для расширения возможностей в разработке технологий автомобильной безопасности, Continental приобрели израильскую компанию Argus Automotive

Cyber Security, мирового лидера в сфере автомобильной безопасности, который предоставляет комплексные и проверенные решения для защиты от хакерских атак.

…Компания Continental будет внедрять криптографическую функцию создания ключей безопасности во все будущие продукты. Ключи безопасности уникальны для каждого продукта, обеспечивает максимальную защиту от хакерских атак, так как их невозможно прочитать снаружи, так же как и PIN-код от телефона. Однако кибербезопасность автомобильных систем необходимо обеспечивать не только после интеграции, но и во время загрузки программного обеспечения и цифровых ключей. Именно поэтому на предприятиях по всему миру внедряется специальная концепция производственной безопасности, основанная на анализе рисков с целью выявления уязвимых мест. Автопроизводители также выигрывают, получая возможность передавать собственные ключи в систему с помощью безопасной сети Continental.

Специалисты Continental постоянно отслеживают десятки систем для выявления уязвимого места еще до того, как на него могли бы напасть хакеры. Для оперативного устранения слабых мест, Continental внедрили систему быстрого реагирования на инциденты - дополнительный уровень безопасности, обеспечивает мгновенную реакцию в случае реальной атаки. …Специалистами было разработано комплексное решение для беспроводного обновления программного обеспечения. Миллионы автомобилей моментально получат новую версию системы безопасности без необходимости посещения сервисного центра…» ***(Continental внедряет защиту авто от хакерских атак // AUTO-Consulting (http://www.autoconsulting.com.ua/article.php?sid=41818). 05.07.2018).***

***

«Команда программистов Apple, Mozilla, Cloudflare и Fastly разработала новый механизм передачи идентификатора хоста через HTTPS. Это произошло в ходе хакатона, состоявшегося на 102-м Инженерном совете Интернета (IETF) 14–15 июля в Монреале. Специалисты создали Encrypted Server Name Indication (ESNI) — зашифрованный вариант TSL-расширения, содержащего имя веб-ресурса…

В рамках очередной сессии хакатона сборная команда инженеров четырех компаний предложила решение проблемы и даже представила два тестовых сайта, использующих ESNI…

Бета-версия ESNI уже поддерживается библиотеками браузера Firefox, а также движком Chromium, на котором работают Opera, Яндекс.Браузер и другие интернет-обозреватели.

Хакатоны предоставляют возможность совместной работы специалистов из разных компаний и областей программирования. Обычно в рамках интенсивной сессии группа фокусируется на решении одной проблемы…» ***(Egor Nashilov. Протокол HTTPS станет надежнее благодаря шифрованию SNI // Threatpost (https://threatpost.ru/esni-to-the-rescue-of-https-protocol/27277/). 18.07.2018).***

***

«Международная команда исследователей нашла способ устранения ключевого недостатка сетевого протокола NTP…

Протокол NTP отвечает за синхронизацию системного времени компьютера и позволяет избежать ошибок при передаче данных. Технологию разработали десятки лет назад, и за время существования в ней нашелся ряд уязвимостей. Одна из них — возможность манипуляции внутренними часами устройства при помощи отправки специально сконструированных пакетов на целевой компьютер.

Эту брешь можно задействовать в атаках на чувствительные ко времени приложения и системы, к примеру, биткойны, TLS и DNS. Протокол предусматривает шифрование данных, однако на практике оно применяется нечасто. Более того, по мнению специалистов, злоумышленники могут скомпрометировать даже защищенные пакеты NTP.

Исследователи из Marvell Semiconductor и Еврейского университета в Иерусалиме предложили методику, блокирующую атаки, связанные с манипуляцией системным временем. Они разработали Chronos — NTP-клиент, способный отсекать подозрительные пакеты от взаимодействия с часами устройства…

Программа совместима с актуальной версией NTP и не требует изменения режима работы серверов. Ожидается, что Chronos сделает бессмысленными атаки, основанные на сдвиге времени…» ***(Egor Nashilov. Ученые придумали, как закрыть давнюю брешь в NTP // Threatpost (https://threatpost.ru/chronos-devouring-ntp-time-security-flaw/26995/). 03.07.2018).***

***

«Стартап Rubrik с помощью нового сервиса Radar, запущенного им вчера, рассчитывает снизить риск потери информации в результате кибератак с использованием ransomware.

..Как и многие сегодняшние средства киберзащиты, Radar основывает свою способность устранять угрозы на техниках машинного обучения. Его алгоритмы анализируют каждодневное использование данных, чтобы научиться отличать аномальное поведение от нормальной активности. Автоматизация процесса позволяет организациям обнаруживать прорыв защиты ещё до того, как поступят жалобы пользователей. Это важно поскольку оставляет ransomware меньше времени на распространение.

Кроме того, Radar предоставляет диагностические функции, которые, в частности, позволяют выявить конкретные данные, пострадавшие в результате инцидента, и найти для них самые свежие «чистые» бэкапы.

Radar построен на облачной платформе Polaris, выпущенной Rubrik в апреле этого года.…» ***(Минимизацией ущерба от ransomware займётся интеллектуальный сервис Radar // «Компьютерное Обозрение» (https://ko.com.ua/minimizaciej_ushherba_ot_ransomware_zajmyotsya_intellektualnyj_servis_radar_125462). 27.07.2018).***

***

Shevchenko A. Identification of "zero day" threats in cybersecurity using taxonometric method / A. Shevchenko, M. Tkachenko, V. Shevchenko // Системи обробки інформації. - 2018. - Вип. 1. - С. 136-141.

Вивчено досвід медицини та біології, щодо упереджувальних дій проти вірусів та інфекцій. Встановлено аналогію підходів до боротьби проти атак «нульового дня» в кіберсистемах та підходів до боротьби з «хворобами брудних рук» в медицині. Досвід епідеміології розповсюджено на боротьбу проти кібернетичних загроз «нульового дня». Проаналізовано використання кластерного аналізу в різних галузях діяльності людства. Для ідентифікації кібернетичних загроз обрано таксонометричний метод, який дозволяє створювати еталони в умовах відсутності попередньої інформації щодо нових видів загроз. Доведено можливість реалізації запропонованого підходу на звичайних бюджетних персональних комп'ютерах. Побудовано графічні ілюстрації щодо обрання еталону та побудовано приклад дендрограми об'єктів взаємодії з інформаційною системою.

Шифр зберігання НБУВ: Ж70474.

***

Баглай Р. О. Загрози безпеки хмарних технологій для банків / Р. О. Баглай // Системи обробки інформації. - 2018. - Вип. 1. - С. 127-135.

Проведено аналіз загроз безпеки інформаційних технологій при впровадженні хмарних обчислень для забезпечення безперебійної та ефективної діяльності банківських установ. Запропоновано заходи щодо мінімізації цих загроз. Розглянуто проблеми та переваги хмарних технологій на різних рівнях архітектурного ландшафту банку для забезпечення конфіденційності, цілісності, автентичності та доступності даних.

Шифр зберігання НБУВ: Ж70474.

***

Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.07 / Діордіца Ігор Володимирович ; Запоріз. нац. ун-т. - Запоріжжя, 2018. - 32 с.

Досліджено чинне законодавство, історичні, сучасні вітчизняні та зарубіжні наукові джерела з метою визначення сутності, особливостей та системи адміністративно-правового регулювання кібербезпеки України, а також формулювання пропозицій та рекомендацій щодо удосконалення її функціонування.

Охарактеризовано поняття та правовий зміст кіберзагроз на сучасному етапі. Визначено особливості класифікації та легітимації загроз кібербезпеці у нормативно-правових актах України. Окреслено правову природу національної системи кібербезпеки як складової системи національної безпеки. Визначено

напрями оптимізації адміністративно-правового регулювання формування кіберосвіти в Україні.

Шифр зберігання НБУВ: РА434303.

***

Діордіца І.В. Детермінованість кібербезпекової політики кібернетичною функцією / Діордіца І.В. // Науковий вісник Херсонського державного університету. Сер. : Юридичні науки. - 2017. - Вип. 6(2). - С. 61-62.

Розглянуто формування та реалізація кібернетичної функції. Доведено необхідність розвитку кібернетичної функції шляхом формування окремого напряму державної політики – кібербезпекової політики. Визначено зміст кібернетичної функції держави.

Шифр зберігання НБУВ: Ж73149/пр.

***

Панаско О. М. Забезпечення захисту паролів користувачів в процедурах аутентифікації / О. М. Панаско, М. В. Хроленко // Вісник Черкаського державного технологічного університету. Серія : Технічні науки. - 2017. - № 4. - С. 111-117.

Досліджено підходи щодо забезпечення захисту паролів користувачів, які відіграють визначальну роль при реалізації процедури аутентифікації, авторизації та аудиті систем захисту із використанням парольної інформації хашування із додаванням так званої «солі» - рядка випадкових даних, що подається на вхід хеш-функції одночасно із вихідними даними. Проведено аналіз відомих способів атак на систему аутентифікації, що пов’язані із отриманням паролів при зламі системи за їх хеш-значеннями, до яких, зокрема, відносяться метод повного перебору, пошук за словником, застосування спеціальних структур даних таблиць пошуку.

Шифр зберігання НБУВ: Ж69418.

***

Титарчук Є. О. Захист персональної інформації користувачів комп'ютерних систем при використанні публічних хмарних сервісів : автореф. дис. ... канд. техн. наук : 05.13.05 / Титарчук Євгеній Олександрович ; Вінниц. нац. техн. ун-т. - Вінниця, 2018. - 24 с.

Запропоновано та розроблено нову математичну модель сервісу деперсоналізації користувачів, яка на відміну від існуючих, використовує метод частково гомомоофного шифрування на основі еліптичних кривих, що дозволяє захистити інформацію користувача від несанкціонованого доступу до неї зі сторони провайдера хмарного сервісу, враховуючи необхідність її обробки. Реалізовано програмне забезпечення, що реалізує ядро системи деперсоналізації користувачів при використанні інформаційної системи, яка виконує обчислення на стороні хмарного сервісу публічного типу.

Шифр зберігання НБУВ: РА434113.

***

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.