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

№ 4 (квітень)

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

«Единый веб-портал использования публичных средств "E-data" (spending.gov.ua) и официальный сайт Министерства финансов Украины оказались недоступными для пользователей сети на протяжении нескольких часов.

О проблемах в работе spending.gov.ua на своей странице в Facebook сообщил руководитель проекта "e-Data" Александр Щелоков…

Он уточнил, что "падение" сайта в период подачи бухгалтерской отчетности может утруднить работу более 40 тысяч бухгалтеров…

Также стало известно, что недоступен и официальный сайт Министерства финансов…

– Произошел сбой у одного из провайдеров интернета. Минфину предоставляют услуги несколько провайдеров, поэтому произвели смену маршрутизации ресурсов Минфина, то есть перестроили доступ к ресурсам через другого провайдера, а это заняло некоторое время. Когда провайдер исправил проблемы в своей работе, мы вернули стандартную маршрутизацию. Сейчас все работает в штатном режиме, – объяснили нашему изданию в Министерстве финансов…» ***(Владимир Кондрашов. Сайт Минфина и портал публичных средств «легли» из-за проблем у одного из провайдеров // Internetua (http://internetua.com/sait-minfina-i-portal-publicsnh-sredstv-legli-iz-za-problem-u-odnogo-iz-provaiderov). 03.04.2018).***

***

«…Как свидетельствуют последние отчеты аналитиков из компании Malwarebytes, пик активности хакеров, использующих скрытый майнинг, пришелся на октябрь 2017 года, достигнув рекордных 25 млн попыток несанкционированного привлечения оборудования пользователей к добыче криптовалют. В марте 2018 года специалисты компании зафиксировали 16 млн таких попыток…

Как утверждают специалисты компании Eset.ua, наибольшей популярностью среди хакеров-майнеров пользуется вредоносные скрипты HTML/ScrInject и JS/CoinMiner, которые злоумышленники размещают как на фальшивых ресурсах, так и на зараженных официальных сайтах.

Пик активности использования наиболее популярных хакерских скриптов был зафиксирован в январе 2018 года. С начала года до марта уровень распространения JS/CoinMiner в Украине незначительно снизился с 15.49% до 11.36%...

По статистике компании eset.ua, доля российских посетителей ресурсов со встроенными майнинг-скриптами в 2017 году составила 65,29%. Процент украинцев — 21,95%. Замыкает тройку лидеров Беларусь — доля жителей этой страны среди жертв составляет 6,49%.

От майнинга не защищены ни пользователи macOS, ни смартфонов. Свою роль в этом сыграло появления ряда крипто-валют, которые можно добывать на средних по мощности компьютерах, чем и воспользовались злоумышленники.

Страдает от скрытого майнинга и бизнес. Количество попыток добычи криптовалюты на мощностях компаний достигло пика в феврале 2018 года — 550 тыс. обнаружений. После этого наступил мартовский спад, который может быть вызван изменением стратегии атак…» ***(Хворостяный Виталий. Майнеры атакуют бизнес // Internetua (http://internetua.com/mainer-atakuuat-biznes). 11.04.2018).***

***

«В сети разгорелся скандал вокруг одного из популярнейших сайтов поиска работы в Украине – rabota.ua. Причиной стало утверждение о том, что портал якобы хранит пароли учетных записей пользователей в открытом виде или используя шифрование, не дающее надлежащей защиты данных.

Первым о проблеме на своей странице в Facebook сообщил Георгий Исаченко. Отсутствие должного внимания к безопасности со стороны портала подтвердили эксперт по кибербезопасности и операционный директор Berezha Security Владимир Стыран и консультант по кибербезопасности Егор Папышев…

Хранение паролей пользователей в открытом виде, по его мнению Георгий Исаченко, может означать, что любая утечка базы данных сайта позволит злоумышленникам увидеть пароли пользователей…

Однако особую опасность, по его мнению, представляет возможная утечка информации о паролях к корпоративным аккаунтам…

Лидер OWASP Kyiv Владимир Стыран отметил, что в общем случае пароли в базе должны храниться в виде, из которого чрезвычайно трудно (а для большинства людей – невозможно) воспроизвести их первоначальную форму. Например, в форме криптостойких хэшей (SHA512, Argon2 etc.)…

В цивилизованном мире, отмечет эксперт, факт хранения паролей в чистом виде – это уже признак инцидента…

«Хорошим примером неправильных выводов и последующего нагнетания ситуации на основе неполных данных» назвал ситуацию директор по маркетингу rabota.ua Константин Павлов, отписавшись на своей странице в Facebook.

– На самом деле, не смотря на то, что пароли приходят в открытом виде в письме, в базе они хранятся в зашифрованном виде по уникальному алгоритму, который расшифровывается специальной процедурой, – сообщил Павлов…

В комментарии для издания AIN Павлов также предложил 3 тысячи долларов тому, кто сможет расшифровать пароли на скриншоте базы данных Rabota.ua…» ***(Владимир Кондрашов. Скандал с паролями rabota.ua: что известно и насколько всё серьёзно // Internetua (http://internetua.com/skandal-s-parolyami-rabota-ua-csto-izvestno-i-naskolko-vse-serezno). 12.04.2018).***

***

«Підписання декларації про вибір лікаря передбачає внесення персональних даних пацієнтів в електронну систему охорони здоров’я. Дані пацієнтів, так само як і медиків, надійно захищені, — запевняють у Міністерстві охорони здоров’я (МОЗ) України…

Персональні дані пацієнтів збираються за їх письмової згоди — вона є частиною декларації про вибір лікаря, затвердженої Порядком вибору лікаря, що надає первинну медичну допомогу. Тож ставлячи підпис у декларації, людина погоджується на обробку своїх даних у системі «Електронне здоров'я».

Найближчим часом в електронній системі охорони здоров'я будуть обробляти лише так звані «нечутливі» персональні дані — паспортні дані, індивідуальний податковий номер, адресу проживання…

Зараз у центральному компоненті системи немає медичних даних або інших так званих «чутливих» даних.

Центральна база даних електронної системи охорони здоров'я знаходиться на території України, у захищеному дата-центрі в місті Києві. Цей дата-центр має комплексну систему захисту інформації (КСЗІ). Дата-центр відповідає міжнародним стандартам (сертифікат відповідності ISO 27001:2013, сертифікат виданий Bureau Veritas № IND17.0398/U) та українським стандартам (атестат відповідності ДССЗЗІ № 14162 від 22.07.16 р.) у сфері захисту даних.

У процесі розробки компонентів електронної системи охорони здоров'я були залучені фахівці з кібербезпеки декількох незалежних компаній, включаючи одну з «Великої четвірки» (найбільші у світі компанії, що надають аудиторські й консалтингові послуги). Проведено низку аудитів кібербезпеки…» ***(Устінов О.В. Вибір лікаря 2018: чи захищені персональні дані? // «Український медичний часопис» (https://www.umj.com.ua/article/123477/vibir-likarya-2018-chi-zahishheni-personalni-dani). 04.04.2018).***

***

«…Злам нового сайту міністерства енергетики та вугільної промисловості України "був випадковим". Так пояснив хакерську атаку, що сталась 24 квітня, спікер Українського кіберальянсу – спільноти кіберактивістів з різних міст України, – відомий під псевдонімом Sean Brian Townsend. За його словами, сайт знаходився на одному сервері з іншими комерційними сайтами і особа, ймовірно, з Марокко зламала один із них, "зламавши міненерговугілля за компанію"…

Атака й справді виглядала дещо дивно: на головній веб-сторінці міненерговугілля містилося залишене хакерами повідомлення і не було жодного доступу до інших його сторінок. А для розблокування сайту кіберзлочинці вимагали 0,1 біткоіна, що відповідає сумі у приблизно 24 тисяч гривень…

Зважаючи навіть на таку ніби примітивну атаку, Sean Brian Townsend досить скептично відгукується про державні зусилля у сфері захисту кіберпростору. "Якщо арабський школяр, що декілька слів англійською зв'язати не може, ламає сайт міністерства навіть не цілеспрямовано, а просто тому, що він трапився під руку, це свідчить про те, що, схоже, не змінилося нічого", – каже хакер…» ***(Чому сайти українських держструктур так легко зламати хакерам // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/chomu-sayti-ukrayinskih-derzhstruktur-tak-legko-zlamati-hakeram.html). 27.04.2018).***

***

«Минулий 2017 для України став роком так званої "чорної кібербезпеки", незважаючи на те, що фактично прийняття Закону України "Про основні засади забезпечення кібербезпеки України", повинно було почати процес широкого впровадження методів і засобів захисту кіберпростору. Положення закону набудуть чинності тільки з 9 травня 2018 року…

Ці та інші питання визначили під час широкої дискусії в Київській торгово-промисловій палаті за участю керівництва Держспецзв'язку, провідних київських експертів, представників приватного сектора і громадянського суспільства.

…керівники Держспецзв'язку представили на розгляд порядок формування переліку об'єктів критичної інформаційної інфраструктури, а також вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Партнер юридичної фірми "Астерс" Юрій Котляров запропонував державі сформувати і прийняти новий підхід до державно-приватного партнерства, в якому повинен бути задіяний науковий потенціал і фірми, що спеціалізуються в сфері інформаційної безпеки…

Директор Інституту комп'ютерних інформаційних технологій Національного авіаційного університету Олександр Юдін запропонував створення полігонів, які мають технологічний і кадровий інструментарій для формування практичних навичок фахівців з моделювання та відбиття кіберзагроз. Він зазначив критичну відсутність міжнародно-сертифікованих фахівців з відбиття кіберзагроз, хоча в Україні існує 30 вузів, які готують кадри з кібербезпеки і необхідність більш тісної співпраці з Міністерством освіти України в цьому питанні.

…Було також схвалено рішення сформулювати і направити пропозиції до державних органів для створення підзаконних актів протягом найближчих трьох місяців» ***(Столичні бізнесмени запропонували нові підходи для посилення кібербезпеки // "Хрещатик" (http://www.kreschatic.kiev.ua/ua/5096/news/1524834616.html). 27.04.2018).***

***

«…Кількість кіберзлочинів збільшується щороку. Якщо в 2014 році Департамент кіберполіції України зафіксував 4800 злочинів в галузі IT, а в 2015 — 6025, то у 2017 ця цифра загрожує бути ще більшою. Тож як же захистити свої дані пересічному українцю?

Суттєвим чинником, який значно полегшує хакерські атаки на комп’ютери користувачів є те, що в нашій державі надзвичайного поширення набуло використання неліцензійного програмного забезпечення. Згідно з дослідженням міжнародної асоціації BSA, на кінець 2015 року в Україні його обсяг становив близько 82%... Тож, варто замислитися над використанням альтернативи пропріє тарного (патентованого) програмного забезпечення вільних операційних системи, офісних пакетів тощо…

У сучасному світі особливу увагу потрібно надати захисту електронної пошти… Тобто, щоб увійти до скриньки, окрім логіну та паролю потрібно ввести

ще спеціальний код, який зазвичай надсилають у вигляді SMS. Двокрокова верифікація є одним з найефективніших методів посилення захисту даних…

Таємничі протоколи https та http досі залишаються містикою для пересічних громадян... За протоколом http дані передаються незахищеними, тоді як https забезпечує криптографічний захист… Тому краще нівелювати загрозу відраз — використовувати ресурси, які підтримують протокол https, а не http.

…Для тих, хто переймається своєю онлайн-анонімністю, гарним помічником може стати браузер Tor. Програмне забезпечення Tor маршрутизує трафік через всесвітню мережу добровільно встановлених серверів, щоб приховати місцезнаходження користувача…

Мало хто знає, як просто і швидко хакер може зібрати дані про користувача за допомогою публічного Wi-Fi… Приєднуючись до хакерського Wi-Fi, людина дає злочинцю відомості не лише про весь трафік, а також про всі логіни, паролі та дані, які вводить.

Та усі ці поради, як вберегтися від кіберзлочинів, можуть виявитися марними, якщо злочинець заволодіє носієм інформації користувача. Щоб завадити цьому, можна зашифрувати сам жорсткий диск. Тоді у разі втрати фізичного носія (комп'ютера, ноутбука тощо) інформація не буде скомпрометована…» ***(Яна Собецька. Коротко про кібербезпеку, або Кому належать ваші дані // Otiumportal (http://otiumportal.com/korotko-pro-kiberbezpeku-abo-komu-nalezhat-vashi-dani). 25.04.2018).***

***

Національна система кібербезпеки

«В прошлом году в Украине был принят закон о кибербезопасности. Документом, среди прочего, предусмотрена обязанность государственных стратегических объектов до лета этого года обеспечить безопасность своих компьютерных сетей.

…эксперт по вопросам экономики Андрей Вигиринский отметил, что на данный момент Украина крайне уязвима в контексте кибербезопасности. Главная проблема – недостаток финансирования и отсутствие соответствующей статьи в госбюджете. Особенно это опасно на фоне предстоящих выборов…» ***(Украина безумно уязвима в контексте кибербезопасности, - Вигиринский // Украинское рейтинговое агентство "УРА (http://ura-inform.com/ru/society/2018/04/10/ukraina-bezumno-ujazvima-v-kontekste-kiberbezopasnosti-a-vigirinskij). 10.04.2018)***.

***

«…Укрепление устойчивости против российских гибридных угроз. Мы должны переосмыслить наши подходы к гибридной безопасности, к фейковым новостям и пропаганде», - подчеркнул Петр Порошенко на открытии 11-го Киевского форума.

Глава государства отметил, что это те сферы, в которых российский потенциал чрезвычайно значителен, гораздо больше, чем в Украине, Соединенных Штатах Америки, в Канаде, Франции, Германии…

«Подчеркиваю, что цифровая эра требует от нас взять на вооружение новые и эффективные законодательные предохранители для защиты достижений свободного выбора наших обществ, одновременно обеспечив деликатный баланс между демократическими свободами и требованиями кибербезопасности», - сказал Порошенко…» ***(Президент хочет законодательно защититься от киберугроз со стороны РФ // ForUm (http://for-ua.com/article/1152655). 12.04.2018).***

***

«Львів – Депутат Львівської міськради від Всеукраїнського об'єднання «Свобода», вчитель історії львівської школи №100 Мар'яна Батюк заперечує, що написала на своїй сторінці у Фейсбук пост із привітанням до дня народження Адольфа Гітлера і розмістила фотографію нацистського диктатора. Тим часом управління освіти Львівської міськради проводить розслідування цього інциденту і якщо підтвердиться факт, що вчителька поширила пост, то вона може бути звільнена з роботи.

Зранку на сторінці у Фейсбук Мар'яни Батюк з'явився пост із фотографією Гітлера і кількома компліментарними словами на адресу нацистського злочинця. За словами Мар'яни Батюк, вона проводила урок історії, а на перерві подивилась на свою сторінку в соцмережі і побачила пост.

«Я його одразу витерла… Думаю, що мені зламали сторінку. …можливо це напад на мене і мою політичну силу», – каже Мар'яна Батюк. …

Інцидент із дописом у соціальній мережі під іменем Мар'яни Батюк перевіряє управління освіти Львівської міськради…

«Це фейкова кібератака. Ми дізнались, що це вкрай важко з'ясувати, хто зламав сторінку. Люди, які ставали жертвами таких атак, довго відбілювали свою репутацію і доводили свою правоту…», – зауважив Любомир Мельничук.

…Після розслідування інциденту міське управління освіти оприлюднить своє рішення.

На сьогодні, кажуть фахівці, ніхто із громадян не захищений від того, що може стати жертвою кібератаки» ***(Галина Терещук. Львівська вчителька заперечує, що писала пост до дня народження Гітлера // Радіо Свобода (https://www.radiosvoboda.org/a/29182927.html). 20.04.2018).***

***

Правове забезпечення кібербезпеки в Україні

«Национальной полицией Украины был разработан проект Закона Украины «О внесении изменений в некоторые законодательные акты относительно имплементации отдельных норм Конвенции о киберпреступности»…

Законопроектом, помимо прочего, предполагалось временное ограничение доступа к информации без решения суда, которое заключается в блокировании (ограничении) провайдерами и операторами телекоммуникаций передачи информации с или на определенный (идентифицированный) информационный ресурс (информационный сервис), адреса сети Интернет, домена и тому подобное. Так, блокированию, согласно проекту документа, мог подлежать информационный ресурс (информационный сервис), адрес в сети Интернет, домен, а не запрещена информация. Такой подход может привести к блокированию законной информации или иного информационного ресурса с незапрещенными данными, который использует указанный IP-адрес (домен) совместно с возможным правонарушителем…

24 мая 2017 более двух десятков профильных организаций и активистов написали открытое письмо в Кабмин, МВД, Минюст, Нацполицию, Госспецсвязи, Генпрокуратуру и офис Уполномоченного по правам человека с требованием не согласовывать данный проект закона…

Также общественность обращала внимание властей на то, что в Конвенции о киберпреступности (положения которой якобы и имплементирует законопроект) вопросы относительно какой-либо блокировки отсутствуют в принципе.

27 февраля законопроект, разработанный в стенах Нацполиции, был снова согласован с замечаниями Национальной комиссии, осуществляющей госрегулирование в сфере связи и информатизации. Представители общественности вновь выступили против: во время заседания НКРСИ озвучивалась информация об игнорировании полицейскими совместной работы с активистами, длившейся около двух месяцев. Кроме того, законопроект как регуляторный акт не выносился на общественное обсуждение… Представители общественности также обратили внимание регулятора на тот факт, что в Конвенции о кибрепреступности нет норм о блокировке…

Первого марта этого года Интернет Ассоциация Украины направила письма Премьер-министру Украины, Главе Нацполиции, Министру юстиции, Генеральному прокурору Украины, главе СБУ, Первому Вице-премьер-министру, руководителю Госспецсвязи и в СНБОУ с просьбой не согласовывать и не подавать на рассмотрение в Верховную Раду Украины этот законопроект в редакции, предложенной Национальной полицией Украины.

В ИнАУ аргументировали свою позицию тем, что разработанный Нацполицией проект Закона Украины «О внесении изменений в некоторые законодательные акты Украины относительно имплементации положений Конвенции о киберпреступности» не соответствует его декларируемым целям и задачам и положениям Конвенции. Кроме того, отдельные положения проекта Закона прямо противоречат действующему законодательству, и, в случае их применения, могут привести к нарушению прав и законных интересов операторов, провайдеров телекоммуникаций, а также конституционных прав и свобод граждан. В ИнАУ просили положения проекта Закона привести в полное соответствие с ратифицированной Украиной Конвенцией о киберпреступности.

В Генеральной прокуратуре Украины, отвечая на письмо ИнАУ, открестились от судьбы законопроекта, отметив, что не могут повлиять на его

несогласование или неподачу в парламент. Доработкой законопроекта (как и самим вопросом о доработке), по словам представителей Генпрокуратуры, должны заниматься в профильных парламентских комитетах…» ***(Владимир Кондрашов. ГПУ рекомендовала полиции существенно доработать скандальный законопроект о цензуре в сети // Internetua (http://internetua.com/gpu-rekomendovala-policii-susxestvenno-dorabotat-skandalni-zakonoproekt-o-cenzure-v-seti). 03.04.2018).***

***

«Министерство юстиции Украины пока не получало разработанного Нацполицией законопроекта «О внесении изменений в некоторые законодательные акты Украины относительно имплементации положений Конвенции о киберпреступности».

Об этом говорится в ответе Минюста на обращение Интернет Ассоциации Украины…» ***(Владимир Кондрашов. Минюст не получал скандального законопроекта о цензуре в сети // Internetua (http://internetua.com/minuast-ne-polucsal-skandalnogo-zakonoproekta-o-cenzure-v-seti). 16.04.2018).***

***

«Во время доработки законопроекта будут учтены, в пределах компетенции, замечания и предложения Интернет Ассоциации Украины к скандальному законопроекту «О внесении изменений в некоторые законодательные акты Украины относительно имплементации положений Конвенции о киберпреступности».

Об этом говорится в ответе Департамента Киберполиции НПУ на обращение ИнАУ…

В Департаменте Киберполиции НПУ на обращение ИнАУ сообщили, что данный законопроект направлен на согласование в заинтересованные органы государственной власти и другие органы власти «для выражения отдельного мнения».

– Сегодня проект акта дорабатывается согласно полученным замечаниям. Также информируем, что во время доработки будут учтены, в рамках компетенции, замечания и предложения, полученные от Интернет Ассоциации Украины, – говорится в документе…» ***(Владимир Кондрашов. Киберполиция пообещала доработать скандальный законопроект о цензуре в сети // InternetUA (http://internetua.com/kiberpoliciya-poobesxala-dorabotat-skandalni-zakonoproekt-o-cenzure-v-seti). 27.04.2018).***

***

«…Кабінет міністрів пропонує посилити покарання за втручання в роботу об'єктів критичної інформаційної інфраструктури. …Відповідна ініціатива міститься в урядовому законопроекті №8304, зареєстрованому в парламенті…

Законопроект, зокрема, пропонує посилити покарання за несанкціоноване втручання в роботу об'єктів критичної інформаційної інфраструктури: змінити

термін позбавлення волі з колишніх 2-5 років до 6-8 років, а також збільшити термін позбавлення права займати певні посади або займатися певною діяльністю з 2 до 3 років.

При цьому за повторне вчинення таких дій або за аналогічні дії за попередньою змовою групою осіб, або якщо такі дії заподіяли істотну шкоду термін позбавлення волі пропонується збільшити до 10 років.

Пропонується також посилити відповідальність за створення, розповсюдження і збут шкідливого програмного забезпечення, збільшивши штраф з 0,5-1 тис до 3-5 тис неоподатковуваних мінімумів доходів громадян, а термін позбавлення волі з 2 до 4-6 років.

За повторні аналогічні дії, дії в групі за змовою або ж за заподіяння істотної шкоди пропонується встановити позбавлення волі на термін від 6 до 9 років.

Законопроект також пропонує встановити в якості міри відповідальності за несанкціонований збут або розповсюдження створеної та захищеної відповідно до чинного законодавства інформації з обмеженим доступом, яка обробляється на об'єкти критичної інформаційної інфраструктури, позбавлення волі на строк до 7 років.

При цьому за повторні аналогічні дії, дії в групі за змовою або ж за заподіяння істотної шкоди пропонується встановити позбавлення волі на строк від 6 до 10 років.

Крім того, законопроект посилює покарання за порушення правил експлуатації комп'ютерів і комп'ютерних систем, мереж електрозв'язку, а також правил захисту інформації, яка на них обробляється, вчинені щодо об'єктів критичної інформаційної інфраструктури.

Зокрема, такі дії пропонується карати штрафом від 1 тис. до 2 тис. неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від трьох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до 3 років…» ***(У Кабміні пропонують позбавлення волі на 8 років за кіберзлочини // «Дзеркало тижня. Україна» (https://dt.ua/ECONOMICS/u-kabmini-proponuyut-pozbavlennya-voli-na-8-rokiv-za-kiberzlochini-275994_.html). 23.04.2018).***

***

Кібервійна проти України

«Українських військових застерігають від використання російського мобільного додатку, який збирає персональну інформацію та відстежує пересування користувачів

Про це повідомляє Військове телебачення України.

…Найбільш популярним, вважають експерти, є "ДМБ Таймер".

…цей додаток отримує інформацію про активність користувача, який використовує на своєму мобільному пристрої службу геолокації, камеру, мікрофон, внутрішню пам'ять. Також програма може блокувати сплячий режим телефону.

…користувачами російського шпигунського додатку є багато українських військовослужбовців, зокрема й учасників бойових дій…» ***(Російський мобільний додаток збирає інформацію про українських військових // Espreso.tv (https://espreso.tv/news/2018/04/03/rosiyskyy_mobilnyy_dodatok_zbyraye_informaciyu_pro_ukrayinskykh_viyskovykh). 03.04.2018).***

***

«У листопаді 2014 року колишній депутат Держдуми РФ від "Единой России" Олексій Муратов надіслав у Кремль план із дестабілізації ситуації в Запорізькій області.

Про це йдеться у статті Тома Парфітта "Операція Троя: російський план поширення хаосу в Україні" у британському виданні The Times, опублікованій 2 квітня…

Виявлений хакерами план "звільнення від нацистсько-фашистських окупантів" передбачав підготовку населення регіону до проросійських протестів. Він був частиною масштабнішої стратегії із дестабілізації України…

Доповідь ґрунтується на витоку інформації з електронного листування радника російського президента Володимира Путіна Владислава Суркова…

Це третя доповідь за листуванням Суркова, яку в Кремлі назвали сфабрикованою, пише автор. Він зазначив, що отримані хакерами листи свідчать про спроби Москви впливати на українську політику на свою користь за допомогою пропаганди відділення та автономізації регіонів зі значною кількістю російськомовного населення…» ***(Росія готувала заколот в Запорізькій області // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/rosiya-gotuvala-zakolot-v-zaporizkiy-oblasti.html). 06.04.2018).***

***

«Украина должна быть готова предотвратить кибератаки со стороны Российской Федерации, которые возможны во время президентских и парламентских выборов 2019 года, считает председатель комитета Верховной Рады по иностранным делам Анна Гопко.

"…мы должны уже вводить профилактические меры для того, чтобы предотвратить, не допустить, в том числе кибератаки, для фальсификации или срыва голосования во время выборов 2019 года", - сказала А.Гопко в ходе "круглого стола" на тему "Реформирование системы национальной безопасности Украины. Роль парламента" в пятницу в Киеве…» ***(Украина должна подготовиться к кибератакам со стороны РФ во время выборов-2019 – Гопко // Интерфакс-Украина (https://interfax.com.ua/news/telecom/497311.html). 06.04.2018).***

***

«Департамент киберполиции Национальной полиции Украины объявил о задержании группы лиц, которые занимались продажей персональных данных украинских граждан. …речь идет о краденных базах данных клиентов «Нова пошта» и «ПриватБанк»…

Ведется расследование по ч.2 ст. 361 УК (незаконное вмешательство в работу компьютерных сетей). Полицейские провели обыск в помещении, откуда работала группа, изъяли компьютеры, где хранились базы данных, телефоны, флешки и деньги — 25 000 грн и $36 000.

В «ПриватБанке» отрицают, что это дело может касаться баз данных банка: «…за последние полтора года никаких утечек баз данных из банка не было…»

В компании «Нова пошта» заявили, что сообщение о преступлении компания подала в Киберполицию еще в феврале этого года… По нему внесли ведомости в Единый реестр досудебных расследований. «Никакой дополнительной информации об указанном уголовном производстве компания не получала», — сообщила пресс-служба «Нова пошта».

Сейчас полицейские устанавливают, как группа получила доступ к базам данных компаний и госструктур…» ***(Ольга Карпенко. Задержаны мошенники-продавцы баз данных — предположительно, клиентов «ПриватБанка» и «Нова пошта» // AIN.UA (https://ain.ua/2018/04/06/zaderzhany-prodavcy-baz-dannyx?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ain ua+%28AIN.UA%29). 06.04.2018).***

***

«…Департамент киберполиции Национальной полиции Украины объявляет набор «белых» хакеров в штат.

Официально конкурс на вакансии стартует 10 апреля, будут искать специалистов с хорошими знаниями в теории и практике кибербезопасности. Зарплаты специалистам обещают от 25 тыс. грн до 50 тыс. грн.

Подавать заявки в онлайне можно будет на сайте Национальной полиции…» ***(Киберполиция ищет хакеров на зарплату до 50 тыс. грн // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/231008-kiberpolitsija_ishchet_hakerov_na_zarplatu_do_50_tys._grn). 07.04.2018).***

***

«Сайт Державного підприємства "Антонов" в черговий раз був атакований хакерами.

"…Будь-які повідомлення, які поширюються з сайту www.antonov.com, починаючи з 19 квітня, є помилковими", - попередили в прес-службі державного концерну "Укроборонпрому".

В ДК "Укроборонпром" звернулися до представників ЗМІ з проханням "бути обережними і не йти на поводу у зловмисників, які цілеспрямовано намагаються дискредитувати провідне українське підприємство в галузі авіабудування".»

(Хакери атакували сайт українського підприємства "Антонов" // Gazeta.ua (https://gazeta.ua/articles/life/_hakeri-atakuvali-sajt-ukrayinskogo-pidpriyemstva-antonov/832880). 19.04.2018).

***

«20-летнего студента разоблачили сотрудники киберполиции во Львове…

Юноша изобрел вирус, который похищал данные из браузеров и запоминал нажатия на клавиатуру. Предназначен для похищения данных с браузеров и записей всех нажатий клавиатуры…

Юноша использовал IP-адреса университета, в котором учился. Брал по $5 с каждого клиента.

У парня изъяли компьютер и банковскую карточку, с помощью которой он получал наличные. Все это направили на экспертизу. По ее результатам примут решение об объявлении студенту о подозрении. Открыли уголовное производство…»***(Во Львове арестовали студента-хакера // Gazeta.ua (https://gazeta.ua/ru/articles/np/_vo-lvove-arestovali-studentahakera/834282). 27.04.2018).***

***

«Неизвестный мошенник выманил у граждан Танзании и Эстонии 11 374 доллара (почти 300 тысяч гривен), пообещав конвертировать их в криптовалюту Bitcoin. Позже он исчез вместе с сайтом, на котором предлагались услуги по конвертации.

Об этом говорится в решении Ровенского городского суда Ровенской области…

Как сообщается, Ровенский отдел полиции ГУНП в Ровенской области проводит расследование по материалам Полесского Управления Департамента Киберполиции по признакам уголовного преступления, предусмотренного ч. 3 ст. 190 УК Украины (мошенничество, совершенное в крупных размерах, или путем незаконных операций с использованием электронно-вычислительной техники).

В решении суда упоминается 2 эпизода данного расследования.

22 августа прошлого года гражданин Танзании перечислил на счет платежной системы advCash 8 394 доллара «с целью конвертирования их в соответствующую сумму в биткоинах». Биткоины танзанский криптоинвестор, конечно же, не получил.

Спустя ровно неделю, 27 августа, гражданин Эстонии решил поменять доллары с кошелька advCash на криптовалюту. Погуглив, он нашел «подходящий» сайт и перечислил на указанный администратором счёт 2 980 долларов…

В ГУ НП в Ровенской области отказались предоставить какие-либо детали расследования, сославшись на тайну следствия. Также неизвестно, почему делом занимается именно полиция города Ровно…» ***(Владимир Кондрашов. Украинская полиция ищет криптомошенника, который обокрал жителей Танзании и Эстонии // InternetUA (http://internetua.com/ukrainskaya-policiya-isxet-kriptomoshennika-kotori-obokral-jitelei-tanzanii-i-estonii). 27.04.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Японські поліцейські проведуть для українських колег тренінги з міжнародних розслідувань, кібербезпеки та протидії наркозлочинності. Про це йшлося під час зустрічі Голови Нацполіції Сергія Князєва та Міністра-радника Посольства Японії в Україні Мічіо Харада.

Під час зустрічі сторони обговорили співпрацю у реалізації проекту надання міжнародної допомоги в частині оснащення поліцейських підрозділів сучасними цифровими засобами радіозв'язку, зимовим форменим одягом та службовими автомобілями.

Міністр-радник Посольства Японії в Україні запросив українських поліцейських до участі у тренінгах, які відбудуться в Японії впродовж року…

Голова Нацполіції Сергій Князєв зазначив, що поліцейські приймуть запрошення. Він додав, що українські правоохоронці, в свою чергу, готові обмінятися з японськими колегами позитивними напрацюваннями у сфері протидії тероризму, кібербезпеки та боротьби з фінансовими махінаціями…» ***(Японці проведуть для українських поліцейських тренінги з міжнародних розслідувань // "Українське право" (http://ukrainepravo.com/news/ukraine/yapontsi-provedut-dlya-ukrayinskykh-politseyskykh-treningy-z-mizhnarodnykh-rozsliduvan/). 15.04.2018).***

***

«…Европейский союз и Украина должны углубить сотрудничество в вопросах кибербезопасности. Об этом во время пресс-конференции в Варшаве сказал депутат Европарламента Михал Бони…

Бони отметил, что Украина еще не является членом ЕС, но в системе кибербезопасности должна иметь схожий путь по достижению сертификатов и в формировании соответствующих стандартов.

Евродепутат подчеркнул, что сейчас "очень хорошая возможность", чтобы страны Восточного партнерства перенимали новые ЕС, строя новые стандарты и нормы кибербезопасности ЕС…» ***(Евродепутат инициирует углубление киберсотрудничества с Киевом // Информационное агентство ЛІГАБізнесІнформ (http://news.liga.net/politics/news/evrodeputat-initsiiruet-uglublenie-kibersotrudnichestva-s-kievom). 07.04.2018).***

***

«У Краматорську Донецької області військовослужбовцям Держприкордонслужби передали технічну допомогу від Уряду Канади.

Комп'ютерне обладнання на суму 500 тисяч доларів США вручив Надзвичайний і Повноважний Посол Канади в Україні Роман Ващук…

Отримані сервери та 150 автоматизованих місць на базі «тонких клієнтів», програмне та апаратне устаткування та радіостанції дозволять розгорнути інформаційну мережу, що захистить від кібератак.

Автоматизовані робочі місця «тонкий клієнт» забезпечать віддалену роботу з інформацією, оскільки вона буде зберігатися на спеціалізованому серверному вузлі в Києві.

Дане обладнання було придбане за кошти Канади за участі представників Управління ООН з обслуговування проектів (UNOPS)…» ***(«Ми зможемо протистояти кіберзагрозам», - краматорські прикордонники отримали новітнє ІТ-обладнання // ИА «Вчасно» (https://vchasnoua.com/donbass/55918-mi-zmozhemo-protistoyati-kiberzagrozam-kramatorski-prikordonniki-otrimali-novitne-it-obladnannya). 17.04.2018).***

***

«Міністр внутрішніх справ Арсен Аваков зустрівся з директором Федерального бюро розслідувань США Крістофером Реєм, після чого вони підписали Меморандум про взаємну співпрацю…

Згідно з документом, МВС і ФБР співпрацюватимуть у боротьбі з незаконним обігом наркотиків та кіберзлочинністю.

Аваков наголосив, що така угода між МВС та ФБР дозволить зробити радикальний прорив у питаннях, які стосуються обміну інформацією, доступу до тих чи інших технічних можливостей…

Він додав, що під час робочої зустрічі з директором ФБР обговорювалося затримання учасників міжнародної злочинної платформи, відомої як Avalanche, яка щодня інфікувала по всьому світу до півмільйона комп'ютерів…» ***(США разом боротимуться проти наркотиків та кіберзлочинності // ГО «Український інтерес» (https://uain.press/security/792214-792214). 18.04.2018).***

***

Світові тенденції в галузі кібербезпеки

«Компанії в усьому світі дедалі частіше страждають від кібератак. Як захистити дані і не зазнати фінансових збитків?

…Згідно із звітом про ризики кібербезпеки Cybersecurity Venturesreport, до 2019 року бізнес у світі буде стикатися з атаками кожні 14 секунд. До 2021 року збитки від загроз кібербезпеки будуть оцінюватися 6 трлн дол. Крім збільшення кількості кібератак, буде зростати й рівень складності кіберзлочинів…

Це означає, що зараз недостатньо мати в компанії ІТ-фахівця, який відповідає за кібербезпеку, як це було досі. Періодично слід проводити зовнішній аудит інформаційної безпеки…

Крім того, багато українських компаній мають невеликий штат ІТ, а деякі взагалі нічого не роблять у сфері кібербезпеки або не вважають її пріоритетом.

Однак чим сильніше бізнес "зав'язаний" на ІТ, тим вищим повинен бути пріоритет, тим частіше компанії мусять проводити аудит своїх систем, впроваджувати практики контролю за дотриманням правил інформаційної безпеки.

..Універсального рецепту аудиту не існує, це унікальний продукт, розроблений для потреб конкретного бізнесу. Як базовий мінімум до нього необхідно включити перевірку управління доступом і змінами програм, мережеву безпеку, управління безперервністю ведення бізнесу за настання форс-мажорних обставин.

…Внутрішні фахівці найчастіше є слабкою ланкою в системі управління інформаційною безпекою. Рівень контролю за їх обліковими записами, як і за тим, наскільки вони обізнані щодо питань безпеки, в компаніях часто досить низький.

Відсутні вимоги щодо регулярної зміни паролів, нема захищеної системи реєстрації та моніторингу дій адміністратора. Ці недоліки особливо актуальні на тлі технології фішингу, яка активно поширюється у всьому світі. Це вид інтернет-шахрайства, що використовується для крадіжки даних користувачів…

Неефективне управління оновленнями ПЗ робить системи уразливими до використання дірок у безпеці. Ще більшим ризиком є застаріле ПЗ, яке більше не підтримується розробниками і для якого не випускаються оновлення…

Впровадження технічних рішень для забезпечення інформаційної безпеки не повинно відбуватися окремо від розробки і впровадження супутніх процесів та регламентів, інакше інвестиції у впровадження рішень можуть бути втрачені…

Виявити проблему — 20% її вирішення, інші 80% залежать від роботи співробітників. У випадках проведення зовнішніх і внутрішніх аудитів безпеки критично важливий етап — виправлення недоліків працівниками компанії.

Якщо результати перевірки кібербезпеки з року в рік показують одні й ті ж проблеми, варто задуматися про ефективність роботи над помилками…» ***(Максим Батуренко. "Petya" — не останній. Як захистити бізнес від кібератак // Економічна правда (https://www.epravda.com.ua/columns/2018/04/2/635488/). 02.04.2018).***

***

«Понятие кибербезопасности постоянно расширяется вместе с диджитализацией общества…

Кибератаки и другие акции злоумышленников с целью получения конфиденциальной информации или активов пользователей стали частым явлением. Для этого злоумышленники используют все возможные источники, начиная с соцсетей и заканчивая интернетом вещей.

Еще одно относительно новое явление в области интернет-угроз — хактивизм…

Ради высоких целей хактивисты пытаются добраться к конфиденциальной информации крупных компаний и государственных структур. Но помимо авторитарных правительств и «злых корпораций» от их действий часто страдают обычные люди.

…Соцсети — это одновременно способ объединить людей и угроза персональным данным…

Чтобы защитить корпоративную сеть от злоумышленников, сотрудникам лучше не входить в учетные записи компании с домашних устройств и смартфонов. Не стоит использовать одинаковые пароли на личных и рабочих аккаунтах. Эффективным решением станет применение двухфакторной идентификации и менеджеров паролей…

Не стоит забывать и о фишинге — так называется похищение злоумышленниками конфиденциальных данных пользователей. Мошенники весьма находчивы при использовании этого метода.

Противодействовать фишингу просто. Пользователю нужно осторожнее относиться к приходящим на почту сообщениям, тщательно проверять информацию и не предоставлять личные данные посторонним людям.

…Еще одной уязвимой точкой стал интернет вещей. Проблема в том, что пока в нем недостаточно проработана система защиты. Пользователи часто даже не меняют пароли на подключенных к подобной сети устройствах. Злоумышленники могут легко получить контроль над системой. Выход из ситуации специалисты видят в использовании для защиты IoT искусственного интеллекта и машинного обучения.

Еще одним популярным оружием в руках хакеров стали ransomware-атаки. В них используются вирусы-вымогатели, блокирующие работу компьютеров и корпоративных сетей и требующие за восстановление доступа деньги…

Диджитализация общества привела к росту количества угроз для пользователей и компаний. Но главное оружие злоумышленников — не технологии, а низкий уровень знаний в области кибербезопасности. Именно потому, помимо использования специального ПО, каждому пользователю сети стоит изучать информацию о текущих угрозах, а также сохранять максимальную осторожность и бдительность.» ***(Как диджитализация меняет индустрию кибербезопасности // PaySpaceMagazine «доступно о платежах» (https://psm7.com/blogs/kak-povsemestnaya-didzhitalizaciya-menyaet-industriyu-kiberbezopasnosti.html). 14.04.2018).***

***

«34 глобальні технологічні компанії та організації домовилися спільно протидіяти кібератакам та зобов'язалися не допомагати урядам їх чинити.

Вони підписали про це угоду 17 квітня…

До угоди долучились такі великі компанії як Facebook, Microsoft, HP, Avast, Dell, Nokia та інші. Водночас, як відзначає DW, серед підписантів документу немає Amazon, Apple, Alphabet (Google) і Twitter…

Компанії домовилися посилити захист кожної людини від кібератак, незалежно від мотивації тих, хто їх скоює.

Підписанти угоди прогнозують, що загальні збитки від кібератак до 2022 року сягнуть позначки у вісім трильйонів доларів і негативно вплинуть на безліч компаній: від маленьких фірм до лікарень.

Представники цих 34 компаній планують провести першу зустріч вже цього тижня на конференції про кібербезпеку RSA Conference в Сан-Франциско…» ***(Facebook, Microsoft та інші компанії домовилися разом протидіяти***

кібератакам // MediaSapiens (http://ms.detector.media/web/cybersecurity/facebook_microsoft_ta_inshi_kompanii_domovilisya_razom_protidiyati_kiberatakam/). 18.04.2018).

***

«…Корпорация Oracle и KPMG провели глобальный опрос 450 ИТ-специалистов… Согласно результатам отчета Oracle и KPMG «Cloud Threat Report, 2018», 90% специалистов по информационной безопасности классифицируют более половины своих данных, хранимых в облаке, как конфиденциальные. Более того, 97% опрошенных разработали правила использования облаков, однако подавляющее большинство (82%) обеспокоены тем, соблюдают ли сотрудники эти правила.

…40% респондентов указывают, что выявление инцидентов, связанных с облачной безопасностью, и реагирование на них в настоящее время является главной задачей в области ИБ. Чтобы решить ее, 4 из 10 опрошенных компаний предпринимают такие меры, как найм архитекторов по облачной безопасности, а 84% респондентов для эффективной защиты от сложных угроз идут по пути повышения автоматизации…

Изменение ландшафта угроз создает новые проблемы: лишь 14% опрошенных сообщили, что могут эффективно анализировать события безопасности, касающиеся большей части (75-100%) своих данных, и эффективно реагировать на них.

Рост расходов на обеспечение кибербезопасности: 89% респондентов ожидают увеличения инвестиций в кибербезопасность в своей организации в следующем финансовом году.

Несогласованность в облачных политиках: 26% респондентов считают одной из главных проблем отсутствие единой политики в разветвленной инфраструктуре…» ***(Что предпринимают компании для защиты конфиденциальных данных в облаках // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5493139-Chto-predprinimayut-kompanii-dlya.html#ixzz5DDDyG6hD). 18.04.2018).***

***

«…Чтобы получить больше информации о современном ландшафте киберугроз, Check Point Software Technologies опросил 443 ИТ и ИБ-специалистов по всему миру о вызовах, с которыми они сталкиваются, отражая атаки «Пятого поколения». Результаты исследования 2018 Security Report показали, что защита большинства компаний отстаёт на 10 лет и как минимум на два поколения от современных кибератак Gen V. Это говорит о глобальной повсеместной уязвимости перед атаками «Пятого поколения». Эксперты Check Point подготовили 2018 Security Report, который содержит сведения, решения и рекомендации для предотвращения кибератак «Пятого поколения».

…2018 Security Report опирается на данные многочисленных исследований среди ИТ-директоров и руководителей бизнеса, а также отчетов Check Point’s

Threat Cloud и Threat Intelligence Report. Исследование охватывает все современные угрозы, направленные на различные отрасли, такие как здравоохранение, промышленность и государственные структуры. Согласно отчету 2018 Security Report, более 300 мобильных приложений, распространяющихся через официальные магазины, содержат вредоносный код» ***(Компании не готовы к кибератакам «Пятого поколения» // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5492373-Kompanii-ne-gotovy-k-kiberatakam.html#ixzz5DDEfLYft). 16.04.2018).***

***

«…Аналитический центр компании InfoWatch подготовил дайджест утечек в сфере футбола…

Важная коммерческая составляющая современного футбола – информация об игровой форме. На футболки наносятся спонсорские логотипы, продажа комплектов формы приносит неплохую прибыль. Зачастую подобного рода информация сливается с подачи самих клубов, чтобы подогреть интерес к продукции, однако бывают и случайные утечки…

Свое влияние на футбольный мир пытаются оказать хакеры. В прошлом году участники группировки Fancy Bears взломали базу Всемирного антидопингового агентства (WADA) и узнали о масштабах употребления запрещенных препаратов игроками. Выяснилось, что только в период 2015-2016 гг. на допинге поймали порядка 350 футболистов.

В результате фишинговой атаки римский «Лацио» лишился 2 млн евро. Эту сумму он должен был перевести голландскому «Фейеноорду» за трансфер защитника Стефана де Врея. Итальянский клуб получил электронное письмо с просьбой сделать финальный платеж за переход футболиста и, ничего не подозревая, перечислил деньги на банковский счет, указанный отправителем. Однако письмо оказалось фальшивкой, поэтому деньги ушли хакерам» ***(Утечки в мире футбола // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5490396-Utechki-v-mire-futbola.html#ixzz5DDIcNmFO). 09.04.2018).***

***

«…Игрофикация становится важным средством повышения эффективности работы службы компьютерной безопасности, говорится в опубликованном на днях докладе фирмы McAfee…

57% участников опроса, проведенного фирмой Vanson Bourne по заказу McAfee, считают, что использование игр повышает осведомленность сотрудников о том, как происходят компьютерные взломы, а 77% руководителей компаний полагают, что игрофикация может помочь повысить безопасность их компании.

…46% опрошенных полагает, что в будущем году им будет труднее справляться с атаками, а возможно, их и вообще не удастся отразить. Осложняет ситуацию и дефицит квалифицированных специалистов. 84% опрошенных говорят о трудностях поиска специалистов, но 31% сообщает, что никаких особых мер для привлечения новых сотрудников они не предпринимают» ***(McAfee: игрофикация поможет в борьбе с кибермошенниками // «Открытые системы»***

(https://www.computerworld.ru/news/McAfee-igrofikatsiya-pomozhet-v-borbe-s-kibermoshennikami). 17.04.2018).

***

«…менее 20% компаний в Азии имеют страхование от кибератаки, по сравнению с 66% в США.

По словам Грейс Райс, вице-президента FM Global и менеджера по страхованию кибер-рисков, страны Азии только начинают осознавать масштабы потенциальных кибер угроз и учатся противодействовать хакерским атакам. Согласно данным группы реагирования на чрезвычайные ситуации в Гонконге (Hong Kong Computer Emergency Response Team), киберриски достигли рекордного показателя в 2017 году и останутся актуальными в 2018 году…» ***(Киберстрахованием в Азии охвачено 20% бизнеса, в США — 66% // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/kiberstrahovaniem-v-azii-ohvacheno-20-biznesa-v-ssha-66). 25.04.2018).***

***

Сполучені Штати Америки

«Комісія з цінних паперів та бірж США розробила та запропонувала компаніям до використання керівництво з боротьби та протистояння кібератакам і віртуальним загрозам.

…Кібератаки завдають серйозної шкоди бізнесу, тому Комісія з цінних паперів та бірж США у своєму керівництві пропонує компаніям розкривати у спеціальних звітах інформацію про кібератаки та кіберзагрози, з якими довелося зіткнутися впродовж визначеного звітного періоду. Це дозволить інвесторам оцінити реальну картину діяльності компанії та прийняти більш виважене рішення щодо капіталовкладень та розвитку бізнесу.

Крім того, керівництво з боротьби та протистояння кібератакам і віртуальним загрозам пропонує алгоритми політик та процедур, які можуть захистити компанії від негативного впливу кібератак, а також запобігти їм» ***(У США розробили керівництво з боротьби із кібератаками // «Юридична газета» (http://yur-gazeta.com/golovna/u-ssha-rozrobili-kerivnictvo-z-borotbi-iz-kiberatakami.html). 10.04.2018).***

***

«Основатель социальной сети Facebook Марк Цукерберг заявил, что понадобится, как минимум, несколько лет, чтобы решить проблемы с безопасностью данных в социальной сети…

По его словам, на данный момент над обеспечением безопасности информации в компании работает около 14 тысяч человек. Цукерберг пояснил, что штат отдела надеются расширить до 20 тысяч человек до конца года.

Ранее газета The New York Times сообщила, что сотрудничавшая с президентом США Дональдом Трампом во время предвыборной кампании британская фирма Cambridge Analytica незаконно получила данные 50 миллионов пользователей Facebook.

Глава Facebook Марк Цукерберг принес извинения, что не оправдал доверия пользователей в ситуации с компанией Cambridge Analytica и признал, что "не должен был доверять" аналитической компании. На фоне новостей о скандале с утечкой данных акции Facebook подешевели на несколько процентов, ряд людей и организаций заявили об удалении своей страницы в социальной сети…» ***(Цукерберг рассказал, когда решатся проблемы безопасности в Facebook // МИА «Россия сегодня» (https://ria.ru/world/20180402/1517777205.html). 02.04.2018).***

***

«Керівництво Державного департаменту США попередило своїх співробітників про спроби проведення кібератак на комп'ютерну мережу зовнішньополітичного відомства…

«Персоналу рекомендується бути в курсі підозрілої діяльності, пов'язаної з поточними кібератаками, націленими на Держдепартамент», - йдеться у внутрішньому електронному листі, розісланому працівникам.

У березні понад 2 тисячі співробітників відомства отримали електронні листи, СМС і текстові повідомлення в соцмережах, в яких містилися посилання на шкідливі програми та на сайти, які вимагали від них введення особистих даних, зокрема пов'язаних з дипломатичною діяльністю, йдеться у матеріалі.

Хакери використовували інформацію про конференції щодо політології, технологій та фондового ринку. В результаті Держдеп тимчасово відключив свою систему обміну незасекреченими електронними листами "для посилення безпеки".

За даними видання, хакерам не вдалося отримати будь-яку персональну інформацію співробітників або секретні дані відомства…» ***(Держдеп попередив співробітників про кібератаки на відомство – ЗМІ // Європейська правда (https://www.eurointegration.com.ua/news/2018/04/13/7080368/). 13.04.2018).***

***

«…Согласно исследованию, проведенному на 5 885 детских Android-приложениях из US Play Store (которые включены в программу Google Designed for Families), более половины из них могут нарушать Закон о защите конфиденциальности детей в Интернете (Coppa)…

У 4,8% приложений зафиксировали "явные нарушения - программа отправляет контактную информацию или данные о местоположении без согласия", 40% отсылали личную информацию без применения мер безопасности, 18% отправляли идентификаторы для запретных целей, например, таргетинга на рекламу, и 39% "игнорируют договорные обязательства, направленные на защиту конфиденциальности детей".

По словам исследователей, 28% приложений получили доступ к конфиденциальным данным, которые защищены Android, а 73% тестируемых программ передавали личную информацию через Интернет…

Исследователи сообщили, что Google помогает обеспечить соблюдение Coppa с помощью программы Designed for Families, которая предоставляет разработчикам приложений для детей информацию о законе и требует сертификации. Однако, по их словам, "похоже, что никто не выполняет правил"…» ***(Ирина Фоменко. Тысячи приложений для Android нарушают закон о защите детей // Internetua (http://internetua.com/tsyacsi-prilojenii-dlya-android-narushauat-zakon-o-zasxite-detei). 17.04.2018).***

***

«Координатор Білого дому з питань кібербезпеки Роб Джойс покине свій пост і повернеться в Агентство національної безпеки США. Про це повідомило агентство Reuters з посиланням на представника Ради національної безпеки при Білому домі…

За словами іншого неназваного високопосадовця, Джойс залишає посаду за власним бажанням…» ***(Самуїл Проскуряков. Reuters: координатор Білого дому з питань кібербезпеки Джойс залишає свій пост // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1725705-reuters-koordinator-bilogo-domu-z-pitan-kiberbezpeki-dzhoys-zalishaye-sviy-post). 17.04.2018).***

***

«Національний комітет Демократичної партії США в п'ятницю подав позов проти виборчої кампанії президента США Дональда Трампа, російського уряду та Wikileaks, звинувативши їх в незаконній змові з метою сприяння перемозі Трампа на виборах у 2016 році…

У багатомільйонному позові, поданому до федерального суду Манхеттена, зазначено, що “у кампанії Трампа Росія знайшла бажаного і активного партнера в своїх зусиллях”, з впровадження “нахабної атаки на американську демократію”, яка включала кібератаку з боку Росії на комп’ютерну мережу партії Демократів.

Кампанія Трампа, згідно з судовим позовом, “радісно вітала російську допомогу”…

Основною метою схеми, на думку Національного комітету Демократичної партії, було “посилити Трампа і принизити кандидатуру від Демократичної партії”, Хілларі Клінтон, форсуючи кандидатуру Трампа, “чия політика була б корисною для Кремля”.

Білий дім і кампанія Трампа не коментували позов.

У списку обвинувачених в судовому позові — син Трампа, Дональд Трамп-молодший, його зять Джаред Кушнер, колишній керівник кампанії Пол Манафорт та офіційний представник кампанії Річард Гейтс, а також союзник Трампа Роджер Стоун.

Також в списку — Російська Федерація, генеральний штаб збройних сил РФ, хакер російської розвідки, відомий як Guccifer 2.0, Wikileaks та її лідер Джуліан Ассандж та ще десяток осіб…» ***(Саша Картер. Партія Демократів США подала позов до Росії, Трампа і WikiLeaks // Інформаційне агентство «Українські***

Національні Новини» (http://www.unn.com.ua/uk/news/1726547-partiya-demokrativ-ssha-podala-pozov-do-rosiyi-trampa-i-wikileaks). 20.03.2018).

***

«Altaba Inc. (бывшая Yahoo! Inc.) выплатит $35 млн для урегулирования претензий Комиссии по ценным бумагам и биржам (SEC), касающихся крупной кибератаки. Об этом говорится на сайте комиссии.

Напомним, в прошлом январе началось расследование утечки личных данных пользователей Yahoo! Несмотря на сотрудничество компании и спецслужб США, механизм кибератаки определить не удалось. В итоге было уволено руководство Yahoo!, а компания была переименована в Altaba. SEC считает, что компания вводила в заблуждение инвесторов, не раскрывая информации о крупной хакерской атаке, жертвой которой она стала…»***(Altaba выплатит $35 млн для урегулирования претензий по делу о кибератаке // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3613479). 25.04.2018).***

***

«Комітет з розвідки палати представників Конгресу США опублікував доповідь про втручання Росії в американські вибори 2016 року. Текст доповіді опублікований на сайті комітету.

"Комітет не знайшов жодних свідчень того, що передвиборний штаб Трампа змовлявся, координувався і вступав у змову з російським урядом, хоча розслідування виявило, що штаби Трампа та Клінтон робили необдумані дії", - йдеться в доповіді.

Так, необдуманими названа зустріч сина Дональда Трампа-молодшого з російським юристом Наталією Весельницькою і зв'язки штабу Трампа з WikiLeaks. При цьому йдеться про те, що екс-кандидат в президенти США Хілларі Клінтон профінансувала дослідження, в результаті якого на базі російських джерел з'явилося досьє, що розповідає про нібито зв'язки нинішнього президента США Дональда Трампа з Росією.

У 2015 році Росія почала організовувати кампанію з таємному впливу, спрямовану на президентські вибори у США, зазначають в комітеті. Втручання російської сторони на виборах в США в 2016 році мало місце у вигляді кібератак і використання соцмереж…» ***(Конгрес США не знайшов свідчень змови між штабом Трампа і Росією// 7dniv.info (http://7dniv.info/politics/101459-kongres-ssha-ne-znayshov-svdchen-zmovi-mzh-shtabom-trampa-rosieiu.html). 27.04.2018).***

***

«…Сенат Конгресса Соединенных Штатов утвердил кандидатуру генерал-лейтенанта Пола Накасоне на должность директора Агентства национальной безопасности (АНБ) и Киберкомандования США…

Накасоне сменил действующего главу АНБ и Киберкомандования США Майкла Роджерса, который занимал эти должности с 2014 года и заявил о намерении уйти в отставку в начале января…» ***(Сенат США утвердил Накасоне директором Агентства нацбезопасности // «РБК-Украина»***

(https://www.rbc.ua/rus/news/senat-utverdil-nakasone-direktorom-agentstva-1524622962.html). 25.04.2018).

***

Країни ЄС

«Рада ЄС на рівні міністрів закордонних справ засудила зловмисну кібердіяльність третіх держав та недержавних суб'єктів, зокрема, кібератаку вірусу NotPetya.

Про це йдеться у заяві, схваленій на засіданні 16 квітня в Люксембурзі…

«Використання інформаційних та комунікаційних технологій для зловмисних цілей є неприйнятним», – наголошують міністри ЄС.

Зазначається, що ЄС продовжить нарощувати свої можливості у боротьбі з кіберзагрозами...» ***(Рада ЄС засудила кібераку вірусу NotPetya // Західна інформаційна корпорація (ttps://zik.ua/news/2018/04/16/rada_yes_zasudyla_kiberaku_virusu_notpetya_1305583). 16.04.2018).***

***

«Евродепутат от Польши Анна Фотыга предложила внести в разрабатываемый проект заявления о кибербезопасности пункт с призывом запретить использование в учреждениях ЕС продуктов «Лаборатории Касперского».

«Поправка ...призывает ЕС провести всестороннюю проверку программного обеспечения, IT и коммуникационного оборудования и инфраструктуры, используемых в учреждениях, чтобы исключить потенциально опасные программы и устройства и запретить те, которые были подтверждены как вредоносные, такие как «Лаборатория Касперского», – передает РИА «Новости» текст проекта документа, обсуждаемого в комитете по иностранным делам ЕП.

В данном документе собраны поправки к проекту резолюции депутата от Эстонии Урмаса Паэта на тему кибербезопасности. В исходной его версии «Лаборатория Касперского» не упоминается, зато упоминаются Россия, Китай и КНДР…

Российская компания «Лаборатория Касперского» сообщила, что обратилась с ходатайством о предварительной судебной приостановке запрета на использование продукции компании властями США…» ***(Дмитрий Зубарев. Евродепутат призвала запретить программы «Касперского» в учреждениях ЕС // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/20/918764.html). 20.04.2018).***

***

«Велика Британія провела масштабну наступальну кіберкампанію проти терористичної групи "Ісламська держава".

Про це заявив директор Центр урядового зв'язку Великої Британії (GCHQ) Джеремі Флемінг, повідомляє ВВС…

Британія вперше систематично придушувала онлайн-зусилля супротивника в рамках військової кампанії…

Флемінг заявив, що більша частина кібероперації - це "надто чутливе питання для обговорення", але вона порушила онлайн-дії групи і навіть знищила обладнання та мережі.

"Ця кампанія показує, наскільки цілеспрямованою та ефективною може бути кібератака", - додав він…» ***(Британія провела масштабну кібератаку проти "Ісламської держави" // Європейська правда (https://www.eurointegration.com.ua/news/2018/04/12/7080325/). 15.04.2018).***

***

«Міністр внутрішніх справ Великої Британії Ембер Радд (Amber Rudd) оголосила війну злочинності в інтернеті…

Уряд Британії вже виділив на боротьбу з даркнетом близько 12,7 мільйонів доларів. З них понад сім мільйонів піде на оснащення поліцейських підрозділів регіонального та місцевого рівнів засобами, які дозволять їм боротися з кіберзлочинністю…

Міністерка внутрішніх справ Великої Британії додала, що власники бізнесу, фахівці з кібербезпеки та приватні особи також можуть суттєво допомогти в боротьбі з кіберзлочинністю…» ***(Уряд Британії виділив понад $12 млн на боротьбу з даркнетом // MediaSapiens (http://ms.detector.media/web/cybersecurity/uryad_britanii_vidiliv_ponad_12_mln_na_borotbu_z_darknetom/). 13.04.2018).***

***

«Британські спецслужби не можуть повністю захистити Сполучене Королівство від передбачуваних кібератак з боку Росії, тому зосереджують свою увагу на їх запобігання шляхом зміцнення систем. Про це в суботу повідомила газета The Sunday Telegraph з посиланням на главу підрозділу кіберзахисту Центру урядового зв’язку (ЦПЗ) Киаран Мартіна…

За його словами, пріоритетом ЦПЗ є забезпечення стійкості систем до кібератаки, таких як енерго- і водопостачання, інтернет, транспорт і охорона здоров’я. “Абсолютний захист не є ні можливим, ні доцільним…”, — сказав Мартін, висловивши впевненість, що масована кібератака проти Великої Британії є питанням часу…» ***(Олексій Супрун. The Telegraph: спецслужби Великої Британії не можуть повністю захистити країну від кібератак РФ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1726697-the-telegraph-spetssluzhbi-velikoyi-britaniyi-ne-mozhut-povnistyu-zakhistiti-krayinu-vid-kiberatak-rf). 22.04.2018).***

***

«…По состоянию на январь 2018 года в британских ВС насчитывается 137 тыс. военнослужащих. Это на 8,2 тыс. (5,7%) меньше установленной цели», –

цитирует ТАСС доклад национального финансово-ревизионного управления (NAO).

Согласно документу, войска испытывают дефицит в 2,4 тыс. инженерах и 800 пилотах авиации. В Королевской армии также существует нехватка специалистов в области цифровых технологий. Ситуация усугубляется и тем, что потребность в таких кадрах возрастает из-за угрозы кибератак…» ***(Алексей Ласнов. В Британии заявили о дефиците военных // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/18/918422.html). 18.04.2018).***

***

«Российские боты помогали лидеру оппозиционной Лейбористской партии Великобритании Джереми Корбину выиграть прошлогодние выборы.

Об этом говорится в совместном расследовании газеты Times и Университета Суонси.

"В рамках исследования удалось обнаружить 6,5 тыс. российских аккаунтов в Twitter, что активно агитировали за Корбина за несколько недель до выборов…", - пишет издание.

В исследовании указано, что 9 из 10 сообщений, которые распространялись этими аккаунтами, поддерживали лидера лейбористов, и наоборот - 9 из 10 твитов, что вспоминали консерваторов, были отрицательными…

Сама Лейбористская партия сообщила, что она не знает ни о каких автоматизированных ботах и не платила за эти услуги.

Британские ученые заявляют, что обнаруженные фейковые аккаунты - лишь вершина айсберга, и призывают Twitter провести более детальное расследование…» ***(Рассказали о вмешательстве российских ботов в британские выборы // Gazeta.ua (https://gazeta.ua/ru/articles/world-life/_rasskazali-o-vmeshatelstve-rossijskih-botov-v-britanskie-vybory/834432). 29.04.2018).***

***

«Газетные издания обвинили почтового оператора Deutsche Post в продаже данных клиентов политическим партиям, которые подтвердили сотрудничество.

…Христианско-демократический союз (ХДС) и Свободная демократическая партия (СвДП) заплатили в 2017 году пятизначную сумму за полученную информацию. Речь может идти о данных покупательской способности, банковских операциях, возрасте и поле, образовании, семейном статусе, жилищных условиях и владении автомобилем. Партии использовали эту информацию якобы для того, чтобы лучше изучить целевую аудиторию в конкретных районах… ХДС и СвДП подтвердили, что сотрудничали с Deutsche Post. В то же время почта отвергла обвинения в продаже данных. Эксперт Левой партии по вопросам кибербезопасности Анке Домшайт-Берг заявила о неприемлемости подобных действий…» ***(Вокруг Deutsche Post разгорается скандал // Телеграф (https://telegraf.com.ua/mir/europa/3988463-vokrug-deutsche-post-razgoraetsya-skandal.html). 01.04.2018).***

***

«…Год назад при бундесвере было создано специальное управление, занимающееся вопросами кибербезопасности. «Здесь будет находиться новое здание с лабораториями для отслеживания и фиксирования следов кибератак, а также помещения для разработчиков программного обеспечения. Всего около 40 000 квадратных метров», - рассказывает профессор Габи Дрео (Gabi Dreo), возглавляющая исследовательский институт кибероборонь CODE при Мюнхенском университете бундесвера.

Здание должно быть построено в 2019 году. Тогда же сюда приедут и новые сотрудники, которые будут в нем работать и учиться на IT-факультете университета. Планируется пригласить сюда 11 профессоров, 2 доцентов и 300 сотрудников. "Мы будем готовить специалистов, которые существенно осложнят доступ хакеров к компьютерным системам", - говорит Габи Дрео.

Уже в этом году, рассказывает Габи Дрео, студенты могут начать обучение и впоследствии получить диплом магистра в области кибербезопасности. "На этот курс мы планируем набрать 120 студентов", - говорит Дрео… Речь идет о людях, которые получат офицерское звание и которые взяли на себя обязательство 12 лет отслужить в бундесвере…» ***(Ольга Тараб. Интернет - как поле для борьбы // Харьковские Известия (http://izvestia.kharkov.ua/on-line/20/1266488.html). 02.04.2018).***

***

«Французское правительство приступило к тестированию собственного защищенного мессенджера, который будет хранить все данные официальных лиц внутри страны. Новый мессенджер призван обеспечить защиту от шпионажа за частными разговорами высокопоставленных чиновников правительства…

В настоящее время в тестировании нового мессенджера принимают участие только 20 чиновников, однако к лету использование сервиса станет обязательным для всех сотрудников правительства. Государственный мессенджер создан на основе открытого кода, доступного в сети, и в будущем его смогут использовать и рядовые гра ждане…» ***(Французские власти разработали свою альтернативу WhatsApp и Telegram // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122546). 17.04.2018).***

***

Російська Федерація та країни ЄАЕС

«Прес-секретар президента Росії Дмитро Пєсков прокоментував заяви західних спецслужб, які звинуватили російських хакерів у зломі мережевого обладнання державних відомств…

"Як правило, такі звинувачення з абсолютною легкістю озвучуються, і ніхто навіть не обтяжує себе пошуком хоч якоїсть аргументації…", - заявив Пєсков.

За його словами, суть і "необґрунтований характер цих звинувачень" ніяк не змінюється…» ***(Анастасія Ткачук. Пєсков відповів на звинувачення Заходу в***

кібератаках // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1725789-pyeskov-vidpoviv-na-zvinuvachennya-zakhodu-v-kiberatakakh). 17.04.2018).

***

«…Массовая атака на официальные аккаунты Государственной думы во «ВКонтакте» и Twitter началась 18 апреля в 19.00. За час количество посещений на страницах ГД выросло на 20 тысяч и продолжает расти…

По словам представителя ГД, на страницах появляется около тысячи спам-комментариев в минуту…» ***(Алексей Ласнов. Аккаунты Госдумы во «ВКонтакте» и Twitter подверглись массовой кибератаке // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/18/918499.html). 18.04.2018).***

***

«…В ніч і вранці 17 квітня були зафіксовані дві DDOS-атаки на офіційні інтернет-ресурси Роскомнагляду. За повідомленням Ростелекому, атаки були успішно відбиті. Інтернет-ресурси Роскомнагляду функціонують в штатному режимі", - йдеться в повідомленні прес-служби.

Однак, незважаючи на заяви Роскомнагляду станом на 15:30 за московським часом сайт продовжує працювати з перебоями…» ***(Анастасія Ткачук. На сайт Роскомнагляду була здійснена масована кібератака // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1725808-na-sayt-roskomnadzora-bula-zdiysnena-masovana-kiberataka). 17.04.2018).***

***

«Росія нікого не боїться і не пробачить ні одного кіберудара, так як давно стала іншою. Про це заявив спецпредставник президента РФ з кібербезпеки, посол з особливих доручень Андрій Крутських під час конференції в Німеччині…

В мережі розмістили відео зі скандальною заявою російського посла, якою він відповів на звинувачення Росії в кібератаках і загрози відповіді з боку США і Великої Британії. Крутських назвав Європу "моською", а Росію — "кіберслоном", який зможе дати жорстку відповідь на кожен випад в свою сторону…» ***(Росія нікого не боїться: у Путіна виступили з новою нахабною заявою // ONLINE.UA (https://novyny.online.ua/797125/rosiya-nikogo-ne-boyitsya-u-putina-vistupili-z-novoyu-nahabnoyu-zayavoyu/). 17.04.2018).***

***

«Самарская область завершила построение контура кибербезопасности к чемпионату мира по футболу…

В настоящее время реализуется комплексный проект регионального правительства по обеспечению информационной безопасности и защиты от компьютерных атак инфраструктуры органов власти, подведомственных учреждений и других объектов регионального значения, задействованных при подготовке и проведении чемпионата мира по футболу…» ***(Андрей Сазонов. В***

Самарской области завершили построение контура кибербезопасности к чемпионату мира по футболу // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3612524?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 23.04.2018).

***

«Дума Ханты-Мансийского автономного округа (ХМАО) приняла закон, согласно которому некоммерческие организации (НКО), занимающиеся борьбой с киберпреступлениями, будут получать господдержку из бюджета округа и финансовые льготы…

Дума ХМАО в среду приняла изменения в закон о поддержке региональных социально-ориентированных НКО. Согласно изменениям, организации, занимающиеся противодействием киберпреступности, войдут в список НКО, которые имеют право на получение господдержки. …ориентированные на кибербезопасность НКО смогут получать финансирование своей деятельности на сумму до 1 млн руб. в течение одного года. Такие НКО могут участвовать в конкурсах на гранты, арендовать помещения и оборудование на льготной или безвозмездной основе, получить льготы на налог на имущество и прибыль, а также консультационную поддержку…» ***(Павел Карпов, Ольга Кураева. Народное ополчение перейдет в интернет. Власти ХМАО помогут борьбе с киберпреступностью субсидиями // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3614088?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 26.04.2018).***

***

«Власти Казахстана рассматривают вопрос о создании в стране специализированного Института развития, который бы занимался актуальными проблемами обеспечения информационной безопасности страны…

В качестве основных задач деятельности головного Института отмечаются такие как, реализация стратегической задачи по поэтапному импортозамещению, участие в реализации государственной политики в сфере обеспечения информационной безопасности, развитие государственно-частного партнерства, поддержка отечественных исследователей и стартапов, актуализация и разработка национальных стандартов в сфере информационной безопасности, подготовка кадров, экспертиза научно-технических проектов и т.д.

Предполагается, что головной Институт будет непосредственным участником государственной системы «Киберщит Казахстана», которой будет оказывать на постоянной основе научно-аналитическое сопровождение ее деятельности» ***(В Казахстане инициировано создание национального Института в сфере информационной безопасности // Digital.Report (https://digital.report/v-kazahstane-initsiirovano-sozdanie-natsionalnogo-instituta-v-sfere-informatsionnoy-bezopasnosti/). 13.04.2018).***

***

«…На офіційний сайт прем'єр-міністра Вірменії primeminister.am здійснені спроби кібератак. Про це повідомили в Управлінні по зв'язках з громадськістю та ЗМІ уряду Вірменії…

Згідно з повідомленням, зі вказаного домену з фальшивих електронних адрес можуть бути відправлені листи з матеріалами, що містять вірус.

«При отриманні повідомлень із зазначеного домену, пропонуємо не відкривати їх або просто видалити…», - йдеться в повідомленні…» ***(У Вірменії повідомили про кібератаки на офіційний сайт прем'єр-міністра // «ДЕТЕКТОР МЕДІА» (http://detector.media/infospace/article/137054/2018-04-28-u-virmenii-povidomili-pro-kiberataki-na-ofitsiinii-sait-premer-ministra/). 28.04.2018).***

***

Інші країни

«…Адреси електронної пошти і паролі для доступу до закритих сайтів чиновників ключових міністерств Японії опублікували в мережі…

«Витік стався з сайтів, які керовані не урядовими структурами. З цих сайтів стався витік адрес електронної пошти і паролів, зареєстрованих в якості акаунтів. Серед цих даних були дані співробітників урядових структур. Ми не думаємо, що урядові інститути зазнали кібератаки, але вважаємо за необхідне вжити заходів до того, щоб ця інформація не була використана зловмисниками…», - розповів генеральний секретар уряду Японії Есіхіде Суга.

Як повідомляють японські ЗМІ, виставленими на продаж в інтернет виявилися дані 2111 чиновників міністерства економіки, торгівлі і промисловості, зовнішньополітичного відомства, міністерства загальнонаціональних справ, міністерства транспорту і інших ключових міністерств…» ***(Хакери виклали у мережу паролі та електронні адреси японських чиновників // "Українські медійні системи" (https://glavcom.ua/world/observe/paroli-ta-elektronni-poshti-yaponskih-chinovnikiv-znayshli-u-merezhi-486808.html). 04.04.2018).***

***

«Міністр закордонних справ Австралії Джулі Бішоп оголосила про відкриття першого pop-up посольства Австралії в Естонії та приєднання країни до Центру передового досвіду НАТО у галузі кібербезпеки у Таллінні…

За її словами, посольство діятиме на тимчасовій основі впродовж 12 місяців. Його завданням буде забезпечення участі Австралії у Центрі передового досвіду НАТО у галузі кібербезпеки.

Очікується, що у рамках діяльності посольства на тримісячний термін буде відряджатися представник австралійських Сил оборони. Цього року Австралія стане спостерігачем на кібернавчаннях Locked Shields 2018…

Бішоп також повідомила, що уряд спільно з Естонською академією електронного урядування та Інститутом стратегічної політики Австралії запустив проект, спрямований на розширення цифрових послуг між урядами Індо-Тихоокеанського регіону.

За словами Джулі Бішоп, ці ініціативи є практичним виконанням зобов'язань Австралії у рамках Міжнародної стратегії в галузі кібервзаємодії, спрямованої на створення відкритого, вільного та безпечного інтернету…» ***(Австралія відкрила посольство в Естонії та приєдналась до центру НАТО з кібербезпеки // Західна інформаційна корпорація (https://zik.ua/news/2018/04/26/avstraliya_vidkryla_posolstvo_v_estonii_ta_pryiednalas_do_tsentru_nato_z_1312749). 26.04.2018).***

***

«…Боаз Долев, гендиректор компании ClearSky сообщил, что в ходе некоторых операций кибермониторинга его специалисты обнаружили, что «ссылка, которая ведет к приложению палестинской партии ФАТХ на Android, доступная через веб-сайт организации, была замещена другой ссылкой, которая устанавливает шпионское ПО на телефоны пользователей».

Шпионская программа давала злоумышленникам доступ ко всей информации на устройствах, включая тестовые сообщения и почту, и позволяла записывать разговоры…

Более глубокий анализ позволил установить, что шпионская программа принадлежит группе хакеров «Arid Viper», связанной с ХАМАСом…» ***(ХАМАС шпионил за ФАТХ через телефоны // ISRAland Online Ltd (http://www.isra.com/news/214251). 23.04.2018).***

***

Протидія зовнішній кібернетичній агресії

«Засновник Facebook Марк Цукерберг на спільних слуханнях юридичного комітету Сенату США і сенатського комітету з торгівлі повідомив, що його компанія веде боротьбу зі спонсорованими Росією групами, які намагаються експлуатувати соцмережа з метою впливу на вибори і громадську думку…

“Ми впровадили новий інструмент ідентифікації фіктивних акаунтів, які використовуються для поширення інформації, і ми змогли видалити десятки тисяч акаунтів перед тим, як вони змогли завдати істотної шкоди. Характер цих атак такий, що є люди в Росії, чия робота полягає в тому, щоб намагатися скористатися нашою системою, іншими інтернет-системами…”, — підкреслю Цукерберг.

За його словами, Facebook найме нових співробітників у відділі по забезпеченню безпеки.

"Ми намагаємося простежити, чим займалося "Агентство інтернет-досліджень“(російська “фабрика тролів”, базується в Санкт-Петербурзі) і що вони робили в 2016 році“, — заявив Цукерберг…» ***(Олексій Супрун. Цукерберг***

прокоментував дії РФ в рамках Facebook // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1724686-tsukerberg-prokomentuvav-diyi-rf-v-ramkazh-facebook). 11.04.2018).

***

«…Британія готова провести кібератаку, якщо російські хакери нападуть на "критичну національну інфраструктуру" Британії.

Центр урядового зв'язку і британське Міноборони зараз вже готові, щоб відповісти "відповідним чином".

Крім кібератак, розвідка також повідомила прем'єр-міністра Терезу Мей, що російська сторона почне публікувати "компромат" на британських офіційних осіб…» ***(Ірина Матюшенко. Британія приготувалася до кібератаки проти Росії у відповідь // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1725424-britaniya-prigotuvalasya-do-kiberataki-proti-rosiyi-u-vidpovid). 15.04.2018).***

***

«Литва ведёт переговоры с США о создании регионального центра кибернетической безопасности в Каунасе…

По словам вице-министра обороны Литвы Эдвинаса Керзы, центр мог бы создавать средства кибербезопасности, проводить научные исследования, обучение. Он сообщил, что в рамках учреждения могли бы работать специалисты по кибербезопасности национальной гвардии Пенсильвании…» ***(Юрий Виноградов. В Каунасе может появиться американский центр кибербезопасности // «Парламентская газета» (https://www.pnp.ru/politics/v-kaunase-mozhet-poyavitsya-amerikanskiy-centr-kiberbezopasnosti.html). 04.04.2018).***

***

«Уряд Росії, дуже ймовірно, стоїть за кібератаками на німецькі урядові мережі.

Про це заявив глава розвідки Німеччини Ханс-Георг Маасен…

Маасен визнав, що при визначенні походження кібератаки важко бути на 100% впевненим.

За його словами, німецька влада уважно стежила за атакою після того, як її було виявлено в грудні минулого року…

Маасен підтвердив, що в атаці було виявлено російське походження, хоча вона не пов'язана з APT28 - російською групою хакерів, які атакували нижню палату німецького парламенту в 2015 році.

Маасен відмовився від коментарів, коли його попросили підтвердити повідомлення від німецьких законодавців і джерел в спецслужбах про те, що нещодавня кібератака була пов'язана з іншою російською хакерською групою, відомою як Turla…» ***(Глава розвідки Німеччини: Москва, дуже ймовірно, стоїть за кібератакою на німецький уряд // Європейська правда (https://www.eurointegration.com.ua/news/2018/04/11/7080217/). 11.04.2018).***

***

«Російські хакери збирають компромат на провідних політиків Великої Британії.

Як повідомляє Sunday Times, посилаючись на доклад британських спецслужб прем'єр-міністру Терезі Мей.

На думку спецслужб, виток цієї інформації стане "помстою" за участь Королівства в ударах по Сирії…» ***(РФ планує виток компромату на британських політиків – ЗМІ // Європейська правда (https://www.eurointegration.com.ua/news/2018/04/15/7080444/). 15.04.2018).***

***

«…НАТО готова в случае потенциальной масштабной кибератаки задействовать пятую статью договора организации, предусматривающую коллективные ответные действия в случае нападения на одну из стран. Об этом в четверг, 5 апреля, в Оттаве заявил генеральный секретарь альянса Йенс Столтенберг…

"НАТО очень серьезно воспринимает киберугрозы, мы наблюдаем все большее количество кибератак", — отметил Столтенберг…

Для противодействия кибератакам в системе НАТО была создана команда из 200 экспертов, готовая "помочь укрепить кибероборону странам альянса", подчеркнул Столтенберг…

В то же время Столтенберг отметил, что НАТО не желает усиления конфронтации с Россией…» ***(НАТО готова ответить на кибератаку коллективной обороной // Українська служба швидких новин (https://sumynews.online/nato-gotova-otvetit-na-kiberataku-kollektivnoj-oboronoj-2/). 05.04.2018).***

***

«Заместитель генерального секретаря НАТО Роуз Гетемюллер подчеркнула, что в Альянсе готовы изучить опыт Украины в противостоянии российским гибридным атакам.

Об этом она заявила на Киевском форуме по безопасности…

"Украина научилась бороться с этими атаками ... В НАТО с нетерпением ждут возможности изучить ваш опыт…", - отметила заместитель генсека…

По ее словам, в нынешних условиях "мы должны быть внимательными, устойчивыми и готовыми ответить на эти гибридные угрозы, возможно, - симметрично".

Гетемюллер также призвала Украину учесть рекомендации Альянса во время принятия закона "О национальной безопасности".» ***(В НАТО готовы изучить опыт Украины в борьбе с гибридными атаками РФ // Европейская правда (https://www.eurointegration.com.ua/rus/news/2018/04/13/7080361/). 13.04.2018).***

***

«…Міністерка оборони Австралії Маріс Пейн (Marise Payne) заявила, що близько 400 австралійських компаній у 2017 році постраждали від кібератак, здійснених російськими хакерами…

Міністр кібербезпеки країни Ангус Тейлор (Angus Taylor) проте зазначив, що їм не вдалося завдати серйозної шкоди. «Ця спроба Росії є чітким нагадуванням про те, що австралійський бізнес та приватні особи є постійною мішенню для незаконної діяльності як звичайних зловмисників, так і хакерів, підтримуваних урядами інших держав, і ми маємо дотримуватися суворих норм кібербезпеки», – додав він.

За словами міністра, отримати доступ до австралійських мереж хакери змогли через комерційно доступні роутери.

«Це демонструє, що будь-який підключений пристрій є вразливим до шкідливої діяльності», – сказав пан Тейлор…» ***(Уряд Австралії звинуватив російських хакерів у низці кібератак // MediaSapiens (http://ms.detector.media/web/cybersecurity/uryad_avstralii_zvinuvativ_rosiyskikh_khakeriv_u_niztsi_kiberatak/). 18.04.2018).***

***

«Національний центр кібербезпеки Великобританії (NCSC), американське ФБР та Міністерство національної безпеки США (DHS) випустили спільне сповіщення про шкідливу інтернет-діяльність, яку провадить уряд Росії.

Заява відомств була опублікована на сайті NCSC. У ній вони попереджають про широкомасштабну кампанію з кібератак та кібершпіонажу, яка керується російським урядом. Головними цілями атак є державні та приватні організації, які водночас мають критично важливе значення для інфраструктури. «Зокрема, ці кібератаки спрямовані на пристрої мережевої інфраструктури по всьому світу, такі як маршрутизатори, комутатори, брандмауери та мережеву систему виявлення вторгнень (NIDS)», - йдеться в заяві.

Відомства вважають, що метою атак було викрадення корисної для розвідки інформації або інтелектуальної власності та намагання надійно закріпитися у вражених мережах.

Жанетт Манфра (Jeanette Manfra) з Міністерства національної безпеки США засудила шкідливу інтернет-активність Росії та закликала всі відповідальні країни «використовувати ресурси, у тому числі дипломатичні, правоохоронні та технічні, аби подолати російську кіберзагрозу». Водночас директор NCSC Кіран Мартін (Ciaran Martin) назвав Росію найсильнішим ворогом у кіберпросторі й визначив боротьбу з нею як головний пріоритет для свого відомства…» ***(США і Великобританія зробили спільну заяву про кібератаки з боку Росії // MediaSapiens (http://ms.detector.media/web/cybersecurity/ssha_i_velikobritaniya_zrobili_spilnu_zayavu_pro_kiberataki_z_boku_rosii/). 17.04.2018).***

***

«Уряд США розгляне усі варіанти дій у відповідь на кібератаки…

«…У ході виступу міністр внутрішньої безпеки США Кіртсен Нільсен на конференції з питань кібербезпеки, яка відбулась у Сан-Франциско відзначила, що США працюють над тим, щоб «дати відсіч» тим, хто атакує Америку у кіберпросторі.

«Маю новини для противників Америки: втручання більше не лишатиметься без наслідків. Ми не будемо терпіти крадіжок нашої інформації, даних, інновацій та ресурсів. І ми не потерпимо втручання, яке націлене у саме серце нашої демократії», – відзначила міністр…

Урядовець також заявила, що її відомство та президент США Дональд Трамп докладають усіх зусиль, щоб недопустити нових втручань у вибори у США з боку Росії, або будь-яких інших країн.

Міністерство внутрішньої безпеки США обрало агресивний підхід, щоб захистити нашу інфраструктуру виборів…» ***(У США готуються дати відсіч всім, хто втручатиметься у кіберпростір країни // Західна інформаційна корпорація (https://zik.ua/news/2018/04/18/u_ssha_gotuyutsya_daty_vidsich_vsim_hto_vtruchatymetsya_u_kiberprostir_krainy_1307031). 18.04.2018).***

***

«Днями в Лондоні відбулася зустріч глав урядів Канади, Великобританії, Австралії та Нової Зеландії. Учасники обговорили стратегію протидії російським кібератакам.

"…Разом з нашими найближчими союзниками, троє з яких перебувають тут зараз, ми цілодобово будемо працювати з усіма доступними нам технологіями, щоб не дозволити агресивним державам і недержавним гравцям взяти верх", - сказала прем'єр-міністр Великобританії Тереза Мей…

Вона звинуватила Росію в "використанні кібернетичного простору як складової більш широких зусиль по підриву міжнародної системи".

Інші присутні прем'єр-міністри також підтвердили свою готовність співпрацювати в відображенні кібератак…» ***(Росія використовує кібератаки, щоб підірвати світовий порядок - Тереза Мей // Gazeta.ua (https://gazeta.ua/articles/world-life/_rosiya-vikoristovuye-kiberataki-schob-pidirvati-svitovij-poryadok-tereza-mej/832658). 19.04.2018).***

***

«Великобританія готується завдати кібернетичного удару по Росії, якщо Москва спробує дистанційно втрутитися у роботу критичної інфраструктури Об'єднаного королівства…

Однак, Великобританія діятиме винятково у межах закону…» ***(Британія готується надати кіберудар по Росії // Gazeta.ua (https://gazeta.ua/articles/politics/_britaniya-gotuyetsya-nadati-kiberudar-po-rosiyi/831918). 15.04.2018).***

***

«Россия непричастна к кибератаке на электронные системы для регистрации избирателей в американском штате Аризона в 2016 году. Об этом сообщает агентство Reuters со ссылкой на источник в администрации США.

По словам собеседника агентства, утверждения о том, что к произошедшему причастна Россия, были основаны на «неполной или устаревшей информации». Он отметил, что за «российское вмешательство» приняли обычное кибермошенничество…» ***(Reuters: США признали, что Россия непричастна ко взлому систем на выборах в Аризоне // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3598355). 09.04.2018).***

***

«Велика Британія звинувачує Росію в кібершпіонажі та ігноруванні норм міжнародного права. Про це …заявив прес-секретар британського уряду, який прокоментував твердження Лондона і Вашингтона про те, що російські хакери атакують мережі державних відомств, підприємств і критичних об'єктів інфраструктури по всьому світу…

…"Виявлення цієї шкідливої діяльності робить чітке послання Росії: ми знаємо, що ви робите, і ви не досягнете успіху", – стверджує представник британського кабміну…» ***(Самуїл Проскуряков. Reuters: уряд Великої Британії звинувачує Росію в кібершпіонажі // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1725690-reuters-uryad-velikoyi-britaniyi-zvinuvachuye-rosiyu-v-kibershpionazhi). 17.04.2018).***

***

«Североатлантический альянс собирается привлечь более 1 тыс. специалистов из почти 30 стран для проведения масштабных международных учений в киберпространстве, сообщила пресс-служба НАТО.

…организаторы базирующегося в Эстонии Центра передового опыта по совместной защите от киберугроз альянса постараются создать условия, приближенные к реальным…

«Специалисты по кибербезопасности проверят и потренируют свои навыки в противодействии кибератакам в рамках крупнейшего международного учения «Закрытые щиты», которое пройдет 23-27 апреля», – сообщили в альянсе.

Согласно легенде учений, вымышленная страна «Берилия» сталкивается с ухудшением ситуации в области безопасности, которая сопровождается серией «враждебных действий» и скоординированными кибератаками против гражданского интернет-провайдера и военной авиабазы. Атаки вызывают серьезные сбои в работе электросети, сетей общественной безопасности, других важных компонентов инфраструктуры…» ***(Антон Никитин. НАТО анонсировало масштабные киберучения // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/21/918964.html). 21.04.2018).***

***

«…Россия нацелилась на компьютеры десятков тысяч семей в Великобритании, чтобы шпионить за ними и устраивать массовые

кибератаки, подчеркивается в совместном заявлении британского Центра правительственной связи (GCHQ) и американской ФБР…

По данным спецслужб, Россия намерена также нанести кибердары по «критической инфраструктуре», включая энергетические сети, службы экстренной помощи и военные объекты.

В том, что Кремль развернул свою кампанию спустя несколько часов после удара по Сирии, уверены и источники Уайтхолла. Угроза со стороны России оценивается на «самом высоком уровне», подтвердили и в Национальном центре кибербезопасности Британии…

Представители США и Великобритании не в первый раз заявляют о том, что Москва угрожает кибератаками по инфраструктуре, в том числе по больницам, банкам, системам управления воздушным движением. Но впервые они выступили с конкретными рекомендациями для гражданских лиц и компаний о том, как защитить себя…» ***(Марина Балтачева. США и Британия призвали Запад приготовиться к кибервойне с Россией // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/17/918132.html). 17.04.2018).***

***

«…посол России в Лондоне Александр Яковенко …отметил, что правительство Соединенного королевства «в официальной переписке не отвергло» возможность кибератаки против России…

Газета Times со ссылкой на источники в правительстве Британии заявила, что Лондон рассматривает возможность совершения кибератаки против России в ответ на отравление в Солсбери экс-полковника ГРУ Сергея Скрипаля и его дочери Юлии. Издание отмечало, что британское минобороны совместно с Центром правительственной связи разрабатывает наступательную киберпрограмму, которая может быть использована для атаки на компьютерную сеть Кремля…

Посольство России в Лондоне официально запросило разъяснений у МИД Британии об угрозах кибератаки. Как заявила официальный представитель МИД России Мария Захарова, распространившиеся в британских СМИ заявления о якобы имеющейся со стороны Москвы «киберугрозе» могут быть подготовкой к массивной кибератаке Лондона на Россию…» ***(Антон Касс. Посол России указал на важный факт в связи с угрозами кибератаки от Британии // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/20/918900.html). 20.04.2018).***

***

«Москва не намерена давать Вашингтону односторонних гарантий невмешательства во внутренние политические процессы, включая выборы. Об этом …заявил спецпредставитель президента РФ по вопросам международного сотрудничества в области информационной безопасности, посол по особым поручениям Андрей Крутских…

Напомним, посол США в РФ Джон Хантсман …сказал, что, если Россия не вмешается в ноябрьские выборы в Конгресс, американская сторона будет готова вернуться к рассмотрению вопроса о проведении двусторонних переговоров по

кибербезопасности, намеченных на конец февраля, но отмененных по инициативе Вашингтона.

По мнению же Андрея Крутских, слова Джона Хантсмана «необязательно воспринимать буквально».

«Я слова американского посла воспринял следующим образом: президенту Трампу нужно в ноябре поправить ситуацию в Конгрессе в свою пользу, и после этого он сможет вступать в переговоры по всем острым вопросам, включая деликатную сферу кибербезопасности»,— сказал высокопоставленный российский дипломат.

По его словам без обвинений в адрес Москвы сегодня не обходится ни одно заявление или выступление западного политика и даже бизнесмена, как мы видели по недавним показаниям основателя Facebook Марка Цукерберга в Конгрессе..» ***(Елена Черненко. МИД РФ: Россия не будет давать США односторонних гарантий по кибербезопасности // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3612180). 22.04.2018).***

***

«Щонайменше в 21 американському штаті було підтверджено хакерське втручання з боку РФ напередодні президентських виборів 2016 року…

Даний факт повідомила керівник відділу кіберзахисту Міністерства внутрішньої безпеки США Джанет Манфра.

"…це підтвердили сенсори в державних системах, а також інформація, надана розвідувальним співтовариством", — підкреслила Манфра під час слухань у Сенатському комітеті із питань внутрішньої безпеки.

Вона висловила думку, що метою російської активності була більшість американських штатів.

"У більшості випадків, проаналізованих міністерством, хакери шукали слабкості систем, а не намагались втрутитись у їх роботу. Лише незначна кількість систем зазнали прямих втручань. …Міністерство агресивно працює над запобіганням втручанню у майбутні вибори. Ми не можемо дозволити повторення цього", — зауважила представник Міністерства внутрішньої безпеки США…» ***(Олексій Супрун. The Hill: щонайменше 21 штат постраждав від хакерських атак РФ перед виборами-2016 // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1727235-the-hill-schonaymenshe-21-shtat-postrazhdav-vid-khakerskikh-atak-rf-pered-viborami-2016). 25.04.2018).***

***

«Конгресс США в рассекреченной части доклада озвучил обвинения в адрес России во вмешательстве в выборы при помощи сетевых атак, активности в соцсетях, действий посредников и государственных СМИ…

«Российская кампания …использовала кибератаки, скрытые платформы, социальные сети, посредников и государственные СМИ», — отмечается в докладе конгрессменов.

Агентство «Россия сегодня», Sputnik, телеканал RT и издание Russia Beyond the Headlines в документе названы «частью российского аппарата медиапропаганды», который, как полагают конгрессмены, использовался для вмешательства в американские выборы в ноябре 2016 года…» ***(Конгресс США обвинил российских хакеров и СМИ во вмешательстве в выборы // «Парламентская газета» (https://www.pnp.ru/politics/kongress-ssha-obvinil-rossiyskikh-khakerov-i-smi-vo-vmeshatelstve-v-vybory.html). 27.04.2018).***

***

«…У проекті заяви Європейської комісії …йдеться про те, що «масштабні кампанії з дезінформації в інтернеті широко використовуються низкою внутрішніх та іноземних гравців, щоб посіяти недовіру і створити соціальну напругу з серйозними потенційними наслідками для нашої безпеки».

«Наприклад, військова доктрина Росії відкрито визнає інформаційну війну як одне зі своїх головних сфер», — сказано в документі Єврокомісії, який мають опублікувати 26 квітня…

У новому документі також йдеться про створення «європейського підходу для боротьби з дезінформацією».

Серед пропозицій — створити незалежну європейську мережу з перевірки фактів, домовитися про спільні методи роботи, обмінюватися найкращими підходами і досягти «якомога кращого покриття по всьому ЄС».

Єврокомісія також планує створити «безпечну європейську онлайн-платформу», яка допоможе боротися з дезінформацією.» ***(Єврокомісія згадає про інформаційну війну Росії в новій заяві // Радіо Свобода (https://www.radiosvoboda.org/a/news/29192212.html). 25.04.2018).***

***

«Парламентська асамблея Ради Європи ухвалила резолюцію про протидію гібридній війні. Про це на своїй сторінці у Facebook повідомив віце-президент ПАРЄ Володимир Ар'єв…

За його словами, Асамблея …закликала протидіяти всім проявам гібридної війни, в тому числі ліквідувати юридичні прогалини та координувати зусилля у протидії цьому новому явищу…

«Асамблея також висловлює глибоку стурбованість з приводу численних випадків масових кампаній з дезінформації, спрямованих на підрив безпеки, громадського порядку та мирних демократичних процесів. Існує надзвичайно важлива потреба у розробці інструментів для захисту демократії від "інформаційної зброї", зберігаючи при цьому свободу слова та свободу засобів масової інформації», - йдеться у резолюції.

За словами Ар'єва, "це вже друга за тиждень резолюція..., спрямована на боротьбу з інформаційними атаками джерел гібридних воєн, головним з яких є Росія. В ній, крім стурбованості, є цілком конкретні звернення…» ***(Тоня Туманова. У ПАРЄ ухвалили резолюцію щодо протидії гібридній війні // Інформаційне агентство «Українські Національні Новини»***

(http://www.unn.com.ua/uk/news/1727614-u-parye-ukhvalili-rezolyutsiyu-schodo-protidiyi-gibridniy-viyni). 26.04.2018).

***

«Службовці Білого Дому оцінили, що за останні два тижні збільшилась кількість повідомлень від автоматичних облікових записів Twitter та акаунтів інших веб-сайтів, пов'язаних з Москвою на 4000%.

Тереза Мей сказала, що Росія використовувала свої кібернетичні можливості, як «спробу підірвати міжнародну систему». Прем'єр-міністр повідомила, що дезінформаційна кампанія була «спрямована не тільки на соціальні медіа та Великобританію – на меті ж підірвати установи та процеси, основаних на правилах Організації по запобіганню хімічної зброї»…

Службовці Білого Дому знайшли ті ж самі анти-західні акаунти, що поширювали фальшиву інформацію про замах на вбивство Сергія та Юлії Скрипалів 4 березня та руйнівну хімічну атаку на Думу в Сирії на початку цього місяця.

Наприклад, акаунт @Partisangirl запостив 2300 повідомлень 7-18 квітня з частотою в 200 постів у день. Це був найпомітніший акаунт, що використовував хештег #falseflag для поширення дезінформації про відповідальних за атаку…» ***(Акаунти кремлеботів поширили 45000 фальшивих новин після газової атаки на Сирію // "iVin" (http://i-vin.info/news/akaunty-kremlebotiv-poshyryly-45000-falshyvykh-novyn-pislya-gazovoyi-ataky-na-syriyu-24882). 22.04.2018).***

***

«З Росією та її президентом Володимиром Путіним потрібно розмовляти лише з позиції сили, єдності та рішучості, адже будь-яка ознака невпевненості сприймається у Кремлі як слабкість, яку можна використовувати.

Таку думку в інтерв'ю The Sydney Morning Herald висловив міністр закордонних справ Естонії Свен Міксер…

Глава МЗС Естонії також розповів про слабкі місця його країни, які виникають через залежність від цифрового простору. Так, естонська влада нещодавно створила так зване "посольство даних" у Люксембурзі – цифрове сховище резервних копій своїх цифрових реєстрів. Саме тому країна може "пережити" технічний збій або навіть кібератаку…

"Потрібно бути обережними, необхідно вибудовувати захист так, щоб можна було зберегти працездатність цих критичних служб навіть під серйозним тиском", – зауважив Міксер.» ***(З позиції сили, єдності та рішучості: глава МЗС Естонії розповів, як боротися з Путіним // Телеканал новин «24» (https://24tv.ua/z_pozitsiyi_sili_yednosti_ta_rishuchosti_glava_mzs_estoniyi_rozpoviv_yak_borotisya_z_putinim_n960466?utm_source=rss). 30.04.2018).***

***

«Вибори у Конгрес відбудуться вже у листопаді цього року, однак США все ще не готові до чергових російських атак на демократичні процеси всередині країни…

За даними Brennan Center for Justice (Університет Нью-Йорка), який аналізує виборчі технології і процедури у всій країні, велика частина штатів використовує електронні машини для підрахунку голосів, яким не менше 10 років і на яких встановлено застаріле програмне забезпечення, що не завжди доступне для регулярного оновлення задля захисту від нових загроз безпеці…

До того ж, у США вразливими для кібератак залишаються такі ресурси, як електронні списки виборців, сервери для підрахунку голосів і сайти про вибори в окремих штатах…» ***(США не готові до нових кібератак із Росії напередодні виборів, – The Washington Post // 7dniv.info (http://7dniv.info/analytics/101350-ssha-ne-gotov-do-novih-kberatak-z-rosii-naperedodn-viborv-the-washington-post.html). 24.04.2018).***

***

Кіберзахист критичної інфраструктури

«Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) NIST.CSWP.04162018.pdf> представил новую редакцию руководства по усилению кибербезопасности критической инфраструктуры Cybersecurity Framework v1.1.

…Новый вариант фреймворка доработан с учетом отзывов специалистов на предыдущие проекты документа. В частности, обновлены рекомендации относительно аутентификации и идентичности, обеспечения кибербезопасности в цепочках поставок, а также раскрытия информации об уязвимостях. В документ добавлен новый раздел, поясняющий, как организации могут использовать фреймворк для оценки рисков кибербезопасности.

Позднее в текущем году NIST намерен выпустить обновленную сопутствующую "дорожную карту" для улучшения кибербезопасности критической инфраструктуры, в которой будут описываться ключевые области разработки, согласования и сотрудничества…» ***(NIST представил новую версию руководства по защите от киберугроз // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122624). 20.04.2018).***

***

Кіберзлочинність та кібертероризм

«Експерти компанії Menlo Security зафіксували хвилю кібератак на фінансові та IT-організації. Напад ведеться новим багатоступеневим методом, що використовує уразливість Microsoft Word…

Шкідливі документи надсилають на електронні адреси співробітникам великих корпорацій у фішингових листах. Як правило, це файли в форматі docx, які містять спеціальні теги HTML із зараженими елементами. Потрапляючи на пристрій, вони активізуються і, в свою чергу, завантажують новий щабель інфікування машини – програмне забезпечення FormBook.

FormBook є шкідливим алгоритмом, який може передати під контроль хакерів більшу частину функціоналу комп'ютера: завантаження файлів, захоплення паролів, запуск різних програм і так далі.

Кібератака націлена на американські компанії та фірми, розташовані в близькосхідному секторі. Фахівці підозрюють, що новий багатоступінчастий механізм – продукт роботи хакерського угруповання Cobalt (також відоме як Carbanak і Anunak)…» ***(Анастасія Ткачук. У Word знайдено новий вірус // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1725053-u-word-znaydeno-noviy-virus). 12.04.2018).***

***

«Канадская компания Hudson's Bay, которая развивает сети магазинов одежды Lord & Taylor и Saks Fifth Avenue, сообщила о похищении данных платежных карт ихклиентов…

…злоумышленники похитили данные владельцев 5 млн карт, которые совершали покупки в магазинахканадской сети начиная со средины 2017 года. При этом 125 тыс карт, принадлежащих преимущественно жителям Нью-Йорка и Нью-Джерси, были выставлены на продажу.

«С заявленным количеством скомпрометированных платежных карт, нынешняя хакерская атака является одной из самых больших и наиболее вредных для сферы ретейла», — утверждают специалисты в области кибербезопасности.

Хакерскую атаку, по версии специалистов, могла организовать группировка JokerStash либо Fin7…» ***(Хакеры похитили данные 5 миллионов покупателей канадского ритейлера // uamarket.info (http://www.uamarket.info/hakery-pohitili-dannye-5-millionov-pokupatelej-kanadskogo-ritejlera/). 02.04.2018).***

***

«Австралийская технологическая компания Nuix провела опрос на тему кибербезопасности среди 112 «белых» хакеров и независимых специалистов из 16 стран…

Согласно новому отчету Nuix, порядка 71% хакеров способны войти в корпоративную сеть максимум за 10 часов, а 18% — даже в течение 60 минут. Более половины (60%) исследователей сообщили, что могут вскрыть практически любую систему, 74% оценили киберзащиту большинства компаний как слабую. Три четверти опрошенных утверждают, что их нападения обнаруживают крайне редко, а 2% ни разу не попадались во время добросовестного взлома.

Чтобы добиться поставленной цели, злоумышленникам может потребоваться от получаса до пяти часов с момента прорыва периметра защиты…

Самой легкой добычей оказались организации в области здравоохранения, а также гостиницы, отели и магазины. Производственный сектор также уязвим к атакам, а лучше всех защищены юридические и авиационные компании наравне с правоохранительными органами и госструктурами.

…Согласно Nuix, специалисты по кибербезопасности укрепляют только внешний периметр сети, безосновательно считая, что тот, кто внутри, априори

имеет на это право. В итоге злоумышленник после взлома быстро обнаруживает конфиденциальные данные.

Среди самых эффективных контрмер опрошенные исследователи назвали «жесткий» хост (34%), системы обнаружения и предотвращения вторжений (18%), обеспечение безопасности конечных точек (14%), а также ханипоты и другие обманные методики (10%). Брандмауэры, контроль доступа пользователей, EMET от Microsoft и прочие меры защиты они охарактеризовали как малоэффективные.

Опрос Nuix показывает, что компании по-разному действуют после обнаружения взлома. Только 7% исправляют все уязвимости — запускают масштабную проверку, устраняют найденные бреши и укрепляют периметры сетей. Примерно половина атакованных компаний ограничивается усилением защиты только критически важных данных, а 18% не принимают каких-либо мер» ***(Egor Nashilov. Хакеры из 16 стран раскрывают свои секреты // Threatpost (https://threatpost.ru/nuix-on-candy-bar-protection-2/25670/). 18.04.2018).***

***

«В феврале-марте 2018 года «Лаборатория Касперского» опросила 500 российских семей с детьми в возрасте от 7 до 18 лет и выяснила, что делает подростков легкой добычей киберпреступников.

Исследование показало, что чаще всего дети погружаются в онлайн-жизнь в возрасте 13-15 лет. При этом лишь 36% взрослых респондентов следят за сетевой активностью младшего поколения. Обычно они устанавливают программы для родительского контроля на свои компьютеры и ноутбуки, а мобильные устройства остаются без защиты. В то же самое время 69% российских подростков, как правило, пользуются именно смартфонами.

Недостаток внимания родителей к безопасности своих детей в Интернете приводит к тому, что те становятся легкой добычей злоумышленников. Несмотря на рост беспокойства, вызванный деятельностью так называемых «групп смерти» в социальных сетях, каждого пятого ребенка не удается оградить от онлайн-общения с незнакомыми взрослыми…

В то же время родители не всегда могут найти верный подход к ребенку, который позволит оградить его от киберугроз и не приведет к ссорам. Эксперт «Лаборатории Касперского» по детской безопасности в Интернете Мария Наместникова объясняет, что речь должна идти не об ограничительных практиках, а о выстраивании в семье доверительных отношений…» ***(Julia Glazova. Наибольшему риску в онлайн-среде подвержены подростки // Threatpost (https://threatpost.ru/teens-are-at-risk-in-the-internet/25663/). 18.04.2018).***

***

«Компания Zscaler, специализирующаяся на безопасности облачных технологий, за последние полгода заблокировала свыше 2,5 млрд попыток добычи криптовалюты...

Активнее всего мошенники пользуются майнером Coinhive, который появился раньше других — в сентябре 2017 года. Эксперты Zscaler засекли более 1,3 млрд попыток добычи криптовалюты с применением этого скрипта…

Помимо Coinhive, постепенно начинает набирать популярность майнер Crypto-Loot (почти 135 млн использований). Специалисты считают, что вскоре его станут применять значительно чаще, поскольку он дешевле в эксплуатации…

Специалисты Zscaler отметили увеличение криптодобычи на 100 тысячах самых посещаемых сайтов по рейтингу Alexa Rank. При этом наиболее популярными среди криптоджекеров оказались порносайты, сервисы потокового видео и корпоративные платформы…

Добычей криптовалюты увлекаются киберпреступники по всему миру, но первое место занимают США — как по количеству криптоджекеров, которых в Штатах насчитывается 37 660 (больше, чем во всей Европе одновременно), так и по количеству задействованных серверов — 55 517 машин.

По вовлеченности граждан в криптодобычу за США следуют Швейцария, Бразилия, Индия и Испания, а по количеству серверов — Германия, Россия, Румыния и Болгария…» ***(Julia Glazova. В корпоративных сетях пресечено 2,5 млрд попыток майнинга // Threatpost (https://threatpost.ru/2-5-mining-attempts-shut-down-by-zscaler/25627/). 17.04.2018).***

***

«В американском штате Мичиган …губернатор Рик Снайдер (Rick Snyder) подписал закон, который устанавливает наказание в три года заключения за хранение ПО «с целью его неавторизованного внедрения в компьютер или компьютерные сети»…

По данным ФБР, в прошлом году в Мичигане зарегистрировано более 1,3 тыс. инцидентов с применением шифрующего данные вымогательского ПО. Суммарный ущерб от этих атак оценивается в 2,6 млн долларов.

Новый закон позволяет лишить свободы подозреваемого в совершении киберпреступления, если сотрудники правоохранительных органов найдут на его компьютере образец шифровальщика и будет доказано, что задержанный намеревался использовать его в злонамеренных целях. Отсутствие случаев заражения при этом значения не имеет — закон позволяет наказывать уже за одно планирование атаки.

…Теперь властям будет проще бороться с создателями шифровальщиков, поставщиками услуг, работающими по модели ransomware-as-a-service, и прочими лицами, которые сегодня вовлечены в этот сегмент теневой экономики…» ***(Maxim Zaitsev. Еще один американский штат поставил шифровальщики вне закона // Threatpost (https://threatpost.ru/michigan-declares-possession-of-ransomware-a-crime/25459/). 04.04.2018).***

***

«…По данным последнего исследования компании Balabit (принадлежит бизнесу One Identity), более трети ИТ-специалистов признают себя наиболее ценной мишенью злоумышленников, целью которых является взлом внутренней ИТ-инфраструктуры...

Глобальный опрос, который проводился в Великобритании, США, Франции и Центральной Европе, рассматривает отношение к инсайдерским угрозам и злоупотреблению привилегированными учетными данными.

По данным исследования, 47% ИТ-специалистов признаются, что время и место авторизации — самая важная информация о пользователе для оперативного обнаружения вредоносных активностей. 41% опрошенных считают, что с точки зрения аналитики информационной безопасности важны данные по использованию корпоративных устройств в личных целях и 31% отметили, что поведенческие характеристики, такие как динамика нажатий на клавиши, также являются важным показателем для идентификации действий злоумышленников. ИТ-специалисты осознают всю важность инструментов, которые могут определить растущие угрозы со стороны инсайдеров и взломанных учетных записей. На вопрос о том, какую технологию безопасности они внедрили бы в следующем году (независимо от бюджета), почти 1/5 респондентов ответили, что планируют использовать инструменты аналитики для отслеживания поведения привилегированных пользователей.

В рамках опроса 42% ИТ-специалистов отметили, системных администраторов как самое уязвимое звено в цепочке привилегированных пользователей в корпоративной сети, за ними следуют руководители высшего звена, это отметили 16% респондентов. Несмотря на то, что у топ-менеджмента, как правило, ограниченные навыки в области ИТ, сведения о таких пользователях также очень важны для хакеров.

Исследование показало, личные данные сотрудников компании тоже являются ценными активами для злоумышленников, поскольку их нетрудно продать — так ответили 56% опрошенных. 50% отметили, что не стоит пренебрегать защитой информации о клиентах, 46% сказали, что хакерам так же интересны финансовые показатели организаций…» ***(ИТ-департаменты представляют собой наибольшую угрозу безопасности компаний // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5491062-ITdepartamenty-predstavlyayut-soboj.html#ixzz5DDFjOU3Q). 11.04.2018).***

***

«Исследователи компании Flashpoint сообщили о массированных атаках на сайты, созданные с помощью системы управления контентом Magento.

Неизвестным киберпреступникам удалось создать несложный скрипт, который в автоматическом режиме осуществляет brute-force атаки, перебирая известные варианты комбинаций логин-пароль, скомпрометированные ранее. Используя эту технику, хакеры взломали уже свыше тысячи административных панелей сайтов на платформе Magento. Статистика весьма тревожная, если учесть, что Magento – самая популярная система управления контентом для интернет-магазинов.

…Эксперты Flashpoint призывают администраторов ресурсов на платформе Magento укрепить безопасность, используя сложные пароли, менее уязвимые для атак brute-force» ***(Хакеры атакуют сайты на платформе Magento // ООО "ИКС-***

МЕДИА" (http://www.iksmedia.ru/news/5489488-Xakery-atakuyut-sajty-na-platforme.html#ixzz5DDKK8iWv). 05.04.2018).

***

«Журналист Брайан Кребс сообщил о закрытии социальной сетью Facebook порядка 120 групп, занимавшихся киберпреступной деятельностью. В общей сложности в группах состояло около 300 тыс. участников.

По словам Кребса, группы предлагали широкий спектр незаконных услуг, включая спам-рассылки, мошенничество, взлом банковских счетов, уклонение от налогов, осуществление DDoS-атак на заказ, а также создание ботнетов. В среднем большинство групп действовали на платформе Facebook порядка двух лет…» ***(Facebook удалила порядка 120 занимавшихся киберпреступной деятельностью групп // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122564). 17.04.2018).***

***

«Центр «Антистихия» назвал наиболее уязвимые цели при хакерских атаках, среди них объекты транспорта, коммунальной инфраструктуры, а также энергетические и коммуникационные сети.

Особую опасность, по мнению специалистов, представляет сращивание хакерских структур с террористами и использование их возможностей для организации массированных кибератак на объекты топливно-энергетического комплекса, узлы связи и системы жизнеобеспечения…

Эксперты предупреждают, что это может привести к чрезвычайным ситуациям и техногенным катастрофам с многочисленными жертвами, а также нанести большой экономический урон…» ***(Ольга Никитина. Названы самые уязвимые цели для кибератак // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/21/918994.html). 21.04.2018).***

***

«…Об угрозе вторжения хакеров в личную жизнь через «умные приборы» сообщает Всероссийский центр мониторинга и прогнозирования чрезвычайных ситуаций «Антистихия». При этом самому большому риску, судя по отчету, подвергаются автомобилисты.

Эксперт по информационной безопасности компании «Монитор безопасности» Тарас Татаринов, сообщил, что происходит с машиной, если в систему управления вторгаются хакеры, и рассказал, как они это делают.

«Я сам видел демонстрацию кибервзлома систем управления автомобилем, вплоть до того, что можно было вмешиваться в торможение и вызвать срабатывание подушек безопасности…»,— пояснил эксперт…

Участники рынка говорят, что кибератаки на уровне интернета вещей — это уже сегодняшний день. Злоумышленники могут использовать бытовые приборы для организации масштабных DDoS-атак, утверждает технический директор компании Check Point Software Technologies Россия-СНГ Никита Дуров. Еще одна актуальная угроза — персональные медицинские приборы, например,

кардиостимуляторы, которые поддерживают жизнеспособность пациентов, подчеркивает эксперт…

По мнению экспертов, заявления МЧС, в первую очередь, сыграют на пользу разработчикам. Некоторые уже объявили, что готовят продукты по кибербезопасности автомобилей и интернета вещей…» ***(Николай Долгополов. Интернет вещей оказался под ударом. Чем вызвана обеспокоенность специалистов МЧС // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3618865?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 30.04.2018).***

***

«Блокчейн-стартап Bezop, который продвигал через свой Твиттер Джон Макафи, допустил утечку персональных данных более чем 25 000 инвесторов. Незащищённую базу данных MongoDB ещё в конце марта обнаружили эксперты по кибербезопасности из Kromtech Security, но информацию о ней опубликовали только 25 апреля. В результате утечки в сеть попали полные имена, адреса, адреса электронной почты, зашифрованные пароли и информация о кошельках. Исследователи также обнаружили общедоступные ссылки на отсканированные паспорта, водительские права и другие идентификационные документы.

Стартап разрабатывал блокчейн-платформу электронной коммерции, которую Джон Макафи в своём Твиттере назвал «распределённой версией Amazon.com»…

Kromtech заключает, что это «не очень хороший старт для компании». ***(Продвигаемый Макафи стартап Bezop допустил утечку данных 25 000 инвесторов // BIGFIN (https://bigfin.net/27/04/2018/%d0%bf%d1%80%d0%be%d0%b4%d0%b2%d0%b8%d0%b3%d0%b0%d0%b5%d0%bc%d1%8b%d0%b9-%d0%bc%d0%b0%d0%ba%d0%b0%d1%84%d0%b8-%d1%81%d1%82%d0%b0%d1%80%d1%82%d0%b0%d0%bf-bezop-%d0%b4%d0%be%d0%bf%d1%83%d1%81%d1%82/). 27.04.2018).***

***

Діяльність хакерів та хакерські угруповування

«…Як убезпечити персональні дані пацієнтів — версія дослідників з PokitDok.

Чому так легко отримати несанкціонований доступ до даних пацієнтів?

…медичні заклади використовують операційні системи, які вже давно не підтримуються їхніми виробниками.

Очевидно, медичні заклади повинні використовувати надійніші протоколи для захисту даних від хакерських атак. Поки в українській системі державної медицини надійним засобом захисту від вірусів та кібератак досі вважається загальний зошит, у США над впровадженням інновацій активно працюють

команди розробників, зокрема PokitDok, яка створила технологію DokChain. Це розподілена мережа процесорів транзакцій, що працюють з фінансовими та медичними даними у сфері охорони здоров'я. Команда PokitDok вважає, що бази даних пацієнтів мають будуватися на технології блокчейн…

Співзасновник компанії Animal Ventures Том Серрез (Tom Serres) вважає, що технологія блокчейн – це ідеальне рішення для зберігання даних пацієнтів. Він говорить, що у порівнянні з системами централізованого доступу, блокчейн забезпечить надійніший рівень безпеки медичних даних. Хакерам буде неймовірно складно отримати доступ до даних пацієнтів, які захищені технологією блокчейн, завдяки шифруванню та створенню численних копій зашифрованих даних.

Блокчейн полегшить життя медичним установам. Пацієнти самі відповідатимуть за власні дані та самостійно вирішуватимуть, кому слід чи не слід надавати доступ до них. Якщо будь-яка державна установа, приватна організація чи навіть хакер вноситиме будь-які зміни у дані пацієнта, що зберігаються на блокчейн, пацієнт це одразу ж побачить…

У деяких країнах вже почали на державному рівні впроваджувати технології на базі блокчейн для зберігання даних пацієнтів. Наприклад, на початку 2017 року уряд Естонії залучив до співпраці місцеву блокчейн-компанію, яка розробила надійну систему зберігання даних пацієнтів на базі технології блокчейн. У цій системі зберігаються медичні дані половини населення Естонії. Щоб запровадити такі зміни в Україні, відповідальні за медичну реформу врешті-решт повинні зосередитися не на риториці, а на конкретних діях, та залучити до справи спеціалістів, які допоможуть подбати про кібербезпеку та конфіденційність даних пацієнтів.» ***(Смарт-медицина: блокчейн на варті персональних даних пацієнтів // Blog Imena.UA (https://www.imena.ua/blog/healthcare-data-blockchain/). 12.04.2018).***

***

«Хакери у США викрали дані про власників п'яти мільйонів банківських карт і виставили інформацію про 125 тисяч карт на продаж…

Цим займалася група хакерів, яка раніше зламувала системи ресторанів і готелів.

Дані хакери отримали через витік інформації в магазинах компаній Saks Fifth Avenue, Saks Off Fifth і Lord&Taylor.

Там визнали недопрацювання у платіжній системі, яким скористалися хакери для викрадення інформації про клієнтів.

Компанії запевнили, що наразі система онлайн-оплати безпечна і наголосили, що вживають заходів для уникнення подібних ситуацій…» ***(У Сполучених Штатах хакери викрали дані 5 мільйонів банківських карт // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/u-spoluchenih-shtatah-hakeri-vikrali-dani-5-milyoniv-bankivskih-kart.html). 02.04.2018).***

***

«Хакери атакували комп'ютерні мережі у низці країн, зокрема в центрах обробки даних в Ірані.

…Під час атаки на екрані пристрою з'являлись зображення прапора США з написом «Не плутайте з нашими виборами».

«Вірус, мабуть, зачепив 200 тисяч маршрутизаторів по всьому світу в результаті широкомасштабної атаки, у тому числі 3 500 комутаторів в Ірані», — повідомили в міністерстві зв'язку та інформаційних технологій Ірану.

Зазначається, що атака стала можливою завдяки уразливості в маршрутизаторах компанії Cisco, яка раніше видала попередження…

Під час атаки по всьому Ірану користувачі скаржились на перебої у доступі до інтернету…» ***(В Ірані повідомили про масштабну кібератаку // громадське телебачення (https://hromadske.ua/posts/v-irani-povidomyly-pro-masshtabnu-kiberataku). 08.04.2018).***

***

«Шестого апреля 2018 г. началась массированная хакерская атака на популярные свитчи компании Cisco, которая привела к отключению целых сегментов интернета

…основной целью атак является рунет. С помощью бота группа хакеров перезаписывает образ Cisco IOS, оставляя в конфигурационном файле сообщение «Do not mess with our elections» («Не вмешивайтесь в наши выборы»).

Одновременно центр мониторинга и реагирования на кибератаки компании Solar JSOC сообщил, что мишенью атак стали значимые объекты критической информационной инфраструктуры России…

Атака стала возможна потому, что в прошивках Cisco IOS и Cisco IOS-XE была найдена уязвимость переполнения стека, которая позволяет атакующему удаленно выполнить на устройстве произвольный код и получить полный контроль над сетевым оборудованием. Уязвимость присутствует в коде Smart Install — функции автоматической настройки параметров для новых устройств, подключенных к сети…

В конце марта 2018 г. Cisco выпустила патч, устраняющий уязвимость. Баг получил название CVE-2018-0171…» ***(По всему миру хакеры выводят из строя устройства Cisco // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5490476-Po-vsemu-miru-xakery-vyvodyat-iz.html#ixzz5DDI3laj8). 09.04.2018).***

***

«**Хакери прибрали з YouTube найпопулярніший кліп «Despacito».** Замість нього на сторінці з’явилася картинка з людьми в масках та зі зброєю в руках.

Як повідомляє BBC, кібератака зачепила й популярні кліпи інших виконавців, серед них - відео репера Drake, поп-співачок Селени Гомез, Тейлор Свіфт, Кеті Перрі. Усі оригінальні кліпи були розміщені на каналі Vevo…

Відповідальність за кібератаку взяли на себе хакери Prosox та Kuroi’sh. Про це вони написали у Twitter.

Хакери «заради розваги» зламали YouTube, але зізнаються, що насправді люблять цю відеоплатформу.

Деякі з кліпів, які зазнали кібератаки, вдалося відновити, але з помилками у назвах або з меншою роздільною здатністю. Компанія Google та платформа

YouTube поки не прокоментували атаку хакерів…» ***(Хакери прибрали з YouTube найпопулярніший кліп «Despacito» // MediaSapiens (http://ms.detector.media/web/cybersecurity/khakeri_pribrali_z_youtube_naypopulyarnishiy_klip_despacito/). 10.04.2018).***

***

«…Неизвестные киберпреступники напали на Boardwalk Pipeline Partners, Eastern Shore Natural Gas, Oneok и Energy Transfer, которые занимаются обслуживанием газопроводов. Атаки были совершены в конце марта.

В компании Oneok, которая управляет газовыми магистралями в пермском нефтегазоносном бассейне в Техасе и Скалистых горах (западная часть Северной Америки), заявили, что в качестве меры предосторожности было принято решение отключить компьютерную систему после того, как подрядчик стал «очевидной целью для кибератаки»…

К 4 апреля 2018 года системы электронного документооборота всех газовых компаний, которые пережили кибернападения, полностью восстановлены…

По мнению эксперта по кибербезопасности промышленных систем Фила Нерая (Phil Neray), хакерская атака на газопроводные компании была проведена с целью финансового обогащения, однако не стоит исключать, что за этим стояли власти каких-либо стран…» ***(Четыре газопроводные компании в США атакованы хакерами // ООО "ИКС-МЕДИА" http://www.iksmedia.ru/news/5489498-Chetyre-gazoprovodnye-kompanii-v.html#ixzz5DDJsU000). 05.04.2018).***

***

«…кіберармія Пхеньяна налічує близько семи тисяч фахівців, частина з яких працюють за кордоном

Кіберармія КНДР, яку раніше країни Заходу не вважали серйозною загрозою, наразі трансформується в одну з найбільш складних і небезпечних хакерських машин світу…

ІТ-фахівці Північної Кореї останнім часом суттєво вдосконалили свої навички, зокрема у проведенні кібератак…

За словами розвідників з Південної Кореї, методи підготовки хакерів у КНДР нагадують роботу зі спортсменами — здібних учнів відбирають та переводять до спеціалізованих шкіл, де їх вчать створювати комп'ютерні віруси вже у 11-річному віці. Юні ІТ-фахівці отримують певні преференції від влади КНДР у виді власних квартир в столиці країни, а також звільнення від обов'язкової військової служби…» ***(КНДР керує семитисячною дитячою кіберармією — Wall Street Journal // «Ракурс» (http://racurs.ua/ua/n103981-kndr-keruie-semytysyachnou-dytyachou-kiberarmiieu-wall-street-journal). 20.04.2018).***

***

«Хакеры атаковали один из крупнейших вьетнамских банков Agribank. Злоумышленникам удалось взломать более 400 счетов его клиентов…

В настоящее время известно лишь, что множество владельцев счетов частично лишились своих средств, однако точная сумма ущерба пока не установлена. Служба безопасности Agribank уже ведет расследование инцидента.

По словам специалистов вьетнамского Центра реагирования на компьютерные угрозы (ЦРКУ), в последние годы уровень киберпреступности в стране значительно вырос. Злоумышленники все чаще похищают через интернет деньги, персональные данные и интеллектуальную собственность.

По данным ЦРКУ, в 2017 году во Вьетнаме было зафиксировано более 40 тыс. кибератак, ущерб от которых превысил $400 млн…» ***(Хакеры взломали более 400 счетов в крупном банке // Goodnews.ua (http://goodnews.ua/technologies/xakery-vzlomali-bolee-400-schetov-v-krupnom-banke/). 28.04.2018).***

***

«Группа, называемая Orangeworm, целью для своих атак выбирает объекты американской системы здравоохранения, хотя среди жертв попадаются и медицинские организации Европы и Азии. Деятельность группы пока не наносит разрушений и классифицируется как корпоративный шпионаж. …взломщики пытаются получить контроль над компьютерами, занимающимися обработкой данных рентгеноскопии и магниторезонансной томографии (МРТ)…

В числе прочего, Orangeworm проявляет интерес к машинам, используемым для оказания помощи пациентам в заполнении форм согласия на медицинское вмешательство…

Наряду с основной целью — отраслью здравоохранения — Orangeworm не обходит вниманием также производство, ИТ, сельское хозяйство и логистику. Часто эти «вторичные цели» имеют связи с медициной. Количество успешных взломов за прошлый и позапрошлый годы исчислялось десятками.

Эксперты не усматривают в деятельности группы признаков поддержки на государственном уровне, по их мнению, за Orangeworm может стоять один человек или несколько одиночек. Нет и никаких фактов, указывающих на национальную принадлежность злоумышленников…» ***(Orangeworm специализируется на медицинском кибершпионаже // «Компьютерное Обозрение» (http://ko.com.ua/orangeworm_specializiruetsya_na_medicinskom_kibershpionazhe_124393). 24.04.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«…Вірусний файл під назвою com.android.boxa виявили в китайському додатку Cloud Module. За даними фахівців з кібербезпеки, троян використовує шкідливий код, який не дозволяє антивірусу провести його ідентифікацію та аналіз. Отримані дані com.android.boxa відправляє на віддалений сервер з автономним програмним забезпеченням.

…В блозі Trustlook також повідомляється, що виявлений вірус збирає інформацію із Telegram, Twitter, Viber, Facebook Messenger, Skype, Line, Weibo та інших популярних додатків» ***(Фахівці виявили вірус, який викрадає дані з популярних месенджерів // Телеканал новин «24» (https://24tv.ua/fahivtsi_viyavili_virus_yakiy_vikradaye_dani_z_populyarnih_mesendzheriv_n948887?utm_source=rss). 06.04.2018).***

***

«…Издание BRG предупреждает пользователей о новом вирусе, который заставляет жертв играть в Playerunknown's Battlegrounds.

Обычно вирусы-вымогатели, такие как WannaCry, блокируют доступ ко всем видам файлов на зараженных машинах. Для обхода блокировки жертве необходимо, как правило, перечислить злоумышленникам деньги.

Но создатели новой вредоносной программы подошли к делу нестандартно. Для обхода их блокировки пользователь вынужден провести за игрой в PUBG не менее одного часа…

Вредоносная программа была впервые обнаружена MalwareHunterTeam и зарегистрирована в BleepingComputer. В отчетах сообщается, что иногда для обхода блокировки достаточно просто запустить файл TSLGame.exe на несколько секунд, чтобы получить код восстановления…» ***(Новый вирус-вымогатель заставляет жертв играть в PUBG // Український телекомунікаційний портал (https://portaltele.com.ua/news/internet/novyj-virus-vymogatel-zastavlyaet-zhertv-igrat-v-pubg.html). 11.04.2018).***

***

«Специалисты ESET обнаружили в Google Play 35 рекламных приложений, замаскированных под антивирусы. Подделки скачали в общей сложности до 7 миллионов пользователей.

Чтобы ввести в заблуждение пользователя, рекламные приложения имитируют настоящие мобильные продукты для безопасности…

Изученные приложения имитируют работу антивируса одним из четырех методов:

Белые и черные списки приложений. В белые списки входят наиболее популярные программы (Facebook, Instagram, LinkedIn, Skype и др.), в черные – всего несколько приложений.

Черные списки разрешений. Все приложения, включая легитимные, помечаются как вредоносные, если для работы им нужны некоторые из перечисленных, потенциально опасных разрешений (например, отправка и получение смс, доступ к данным о местоположении, доступ к камере устройства и др.)

Белые списки ресурсов. Все приложения, кроме загружаемых из Google Play, помечаются как вредоносные (даже если они легитимны и безопасны).

Черные списки активностей. Все приложения, выполняющие операции из заданного списка (например, показ рекламы), помечаются как вредоносные. В черный список входят и легитимные сервисы.

Несколько фальшивых антивирусов имеют характерные особенности. Один из них не является полностью бесплатным – в нем предусмотрен переход на коммерческую «расширенную версию». Еще одно приложение помечает остальные подделки как вредоносное ПО.

Часть приложений предлагает функцию менеджера паролей. Однако функция не способна обеспечить защиту из-за небезопасного хранения данных – для злоумышленника не составит труда получить к ним доступ…» ***(Фальшивые антивирусы в Google Play скачали до 7 миллионов пользователей // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5490867-Falshivye-antivirusy-v-Google-Play.html#ixzz5DDGiP0V7). 10.04.2018).***

***

«Специалисты компании MalwareHunterTeam сообщили об обнаружении нового зловреда-шифровальщика WhiteRose («белая роза»). Инфицируя устройства под управлением ОС Windows, вредоносное ПО зашифровывает большинство файлов, меняя их расширение на .WHITEROSE. По завершении процесса зловред удаляет себя из инфицированной системы.

Способы распространения WhiteRose в настоящий момент точно не установлены, известно, что зловред более активно атакует европейских пользователей, прежде всего, на территории Испании.

Наиболее примечательной чертой вредоносного ПО является требование выкупа, которое выводится на дисплеи инфицированных устройств.

…исследователям уже удалось найти способ расшифровки заблокированных файлов. Инструкции по спасению инфицированных устройств можно найти на портале Bleeping Computer…» ***(Обнаружен новый зловред-шифровальщик // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5490330-Obnaruzhen-novyj-zloverdshifrovalsh.html#ixzz5DDJ012yN). 09.04.2018).***

***

«…Шпионский троян Dimnie, который ранее был угрозой для компаний, приспособили для атак на банки.

По словам руководителя экспертного центра безопасности Positive Technologies Алексея Новикова, данный троян нацелен в первую очередь на клиентов банков, физлиц или организации. «Конечная цель трояна Dimnie, если максимально упростить,— подмена реквизитов получателя в платежных поручениях в 1С, что в конечном счете позволяет перевести деньги на подложный счет злоумышленника»,— пояснил он.

О существовании трояна известно как минимум с ноября 2017 года… Возможности Dimnie широки, указывают эксперты. «Заражение происходит, когда пользователь открывает вредоносное вложение из письма,— говорит эксперт по техническим расследованиям центра мониторинга и реагирования на кибератаки Solar JSOC Виктор Сергеев.— После запуска троян скачивает дополнительные модули и начинает собирать логины и пароли от аккаунтов жертвы в различных интернет-сервисах и установленных программах — от почты и социальных сетей до криптовалютных кошельков». По словам господина Сергеева, Dimnie имеет

встроенный кейлоггер (шпионская программа, перехватывающая все набранные на клавиатуре комбинации клавиш), благодаря которому злоумышленники получают данные учетных записей жертвы в корпоративных системах…» ***(Вероника Горячева. Над банками нависла новая киберугроза // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3607008?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 19.04.2018).***

***

«…Случаи скрытого майнинга растут в геометрической прогрессии. По данным антивирусной компании Symantec, за 2017 год они участились в 340 раз.

…По данным ESET, программы-майнеры распространяются несколькими путями.

Первый — когда пользователь ищет информацию и попадает на скомпрометированный сайт, куда злоумышленники поместили вредоносный код, или на сайт, администраторы которого намеренно добавили в код часть инфицированного кода для дополнительного заработка на посетителях.

При посещении такого сайта срабатывает скрипт, который начинает использовать ресурсы устройства. Этот метод наиболее распространенный и работает почти на всех устройствах и операционных системах.

Второй — социальные сети или файлообменники.

Пользователю могут приходить сообщения от других пользователей или поддельных аккаунтов-ботов о том, что он якобы стал победителем в акции или конкурсе. Для получения приза пользователю предлагается перейти по ссылке, которая выполняет загрузку опасного программного обеспечения…

Первые симптомы присутствия майнера — сбои в работе информационной системы, быстрая разрядка аккумулятора и перегрев устройства, наличие запущенных подозрительных процессов, нетипичное повышение громкости работы видеокарты, повышение уровня используемой электроэнергии…

Еще менее приятной находкой, чем сам майнер, может стать несанкционированное использование данных, например, паролей доступа, в том числе для получения финансовой выгоды…

Специалисты ESET рекомендуют устанавливать и использовать актуальные версии антивирусов, которые блокируют угрозы на этапе загрузки. Если компьютер все же был инфицирован, нужно выполнить его полное сканирование и удалить нежелательные и потенциально опасные программы.

Для сканирования устройства на наличие вредоносного ПО можно использовать бесплатную утилиту Malwarebytes и ее дополнение AdwCleaner.

Первое приложение проверяет жесткий диск и оперативную память на наличие вирусов, второе — на рекламные программы. Регулярное сканирование с большой вероятностью обезопасит гаджеты от скрытого майнинга.

Как одну из мер предосторожности в браузере можно использовать расширения ScriptBlock, NoCoin и MinerBlock, которые блокируют пиратские скрипты и останавливают потенциально опасные алгоритмы» ***(Вас «майнят»: как выявить и обезвредить скрытый майнинг // АНТИКОР — национальный***

антикоррупционный портал (https://antikor.com.ua/articles/233959-vas_majnjat_kak_vyjavitj_i_obezvreditj_skrytyj_majning). 23.04.2018).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В Испании арестован лидер киберпреступного синдиката ответственного за банковские кражи на общую сумму более 1 млрд долларов США…

За последние пять лет хакерская группа «FIN17» нанесла ущерб более чем 100 финансовым учреждениям по всему миру и эффективно воруя миллионы долларов за раз.

«Криминальную прибыль отмывали с помощью криптоконверсий посредством предоплатных карточек, связанных с криптовалютными кошельками, которые использовались для покупки таких товаров, как роскошные автомобили и дома», — говорится в заявлении Европол.

В 2013 году преступная группа выпустила вредоносное программное обеспечение «Anunak», ориентируясь на банкоматы по всему миру, а позднее разработала более совершенное кибер-оружие «Carbanak». Программное обеспечение отправлялось сотрудникам банка посредством фишинговых писем с зараженным вложением, которое после загрузки предоставляло группе удаленный доступ для управления компьютером и входа во внутреннюю банковскую сеть...

Расследование заняло годы из-за сокрытия украденных средств в криптовалюте, и также расширило сотрудничество между Европолом, ФБР, Совместной целевой группой по киберпреступности, Европейской банковской федерацией, испанскими, румынскими, молдавскими, белорусскими и тайваньскими властями, а также частными экспертами по кибербезопасности для отслеживания группы.

Полиция еще не представила подробности о лидере преступной группировки, кроме того, что он имеет украинское происхождение. Также, были арестованы еще трое российских и украинских граждан подозреваемых в связях с синдикатом.» ***(Европол арестовал лидера крупного киберпреступного синдиката — OCCRP // ХВИЛЯ (http://hvylya.net/news/digest/evropol-arestoval-lidera-krupnogo-kiberprestupnogo-sindikata-occrp.html). 05.04.2018).***

***

«…1 апреля пресс-секретарь президента Чехии Йиржи Овчачек заявил, что выдача обвиняемого Россией и США в хакерстве россиянина Евгения Никулина связана со стремлением заинтересованных лиц получить компромат на американского президента Дональда Трампа. Сам Никулин в суде не признал своей вины.

Россия заявила, что возмущена выдачей Чехией США Никулина и разочарована тем, что Прага руководствовалась «союзнической лояльностью».

Евгения Никулина задержали 5 октября 2016 года в Праге чешские правоохранители совместно с представителями ФБР. В Белом доме заявляли, что задержание Никулина в Праге является частью секретного расследования кибератак на серверы Демократической партии. До этого сообщалось, что задержание связано с расследованием кибератаки против американской профессиональной соцсети LinkedIn. Позднее США обвинили Никулина во взломе серверов ЦРУ.» ***(Алина Назарова. Спецборт минюста США прибыл в Прагу до решения суда по делу Никулина // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/4/4/915874.html). 04.04.2018).***

***

«В связи с расследованием деятельности преступной группировки Liberty Reserve федеральные власти Флориды предъявили обвинение 41-летнему программисту из Microsoft Раймонду Уадиале (Raymond Uadiale).

…Программист обвиняется в том, что вместе с гражданином Великобритании занимался распространением вируса Reveton и заражением компьютеров, а также собирал «выкупные» платежи и переправлял их из США через океан в британскую компанию K!NG.

В 2012-2013 годах, когда действовали злоумышленники, криптовалюта еще не имела широкого распространения, и мошенники собирали выкупы ваучерами GreenDot MoneyPak. Код ценной бумаги нужно было ввести в соответствующее окошко на заблокированном вирусом-вымогателем экране. Платежи переводились на принадлежащие Уадиале дебетовые карты, оформленные на фальшивое имя Майка Роланда (Mike Roland).

После поступления средств программист переводил их в цифровую валюту Liberty Reserve и уже в таком виде отправлял своему британскому партнеру в K!NG. Следователи из Флориды полагают, что инженер Microsoft перечислил в Великобританию более 130 000 долларов — не считая его личной доли в 30%.

Если Уадиале признают виновным по всем пунктам, ему грозит тюремный срок до 20 лет, штраф до полумиллиона долларов и контроль поведения до 3 лет после освобождения. В настоящее время Уадиале отпущен под залог 100 000 долларов…» ***(Egor Nashilov. Программист из США задержан за отмывание 130 000 долларов // Threatpost (https://threatpost.ru/microsoft-employee-charged/25637/). 17.04.2018).***

***

«Прокуратура США по Восточному округу штата Висконсин, Федеральное бюро расследований и Налоговая служба США проводят расследование относительно пользователя под псевдонимом «parkerproo». Хакера из Украины подозревают в …незаконном получении через компьютер персональных данных 1 тысячи человек, которые «parkerproo» рекламировал и продавал другим.

…в рамках проводимого американцами расследования 8 февраля 2017 секретный агент ФБР приобрел похищенные федеральные налоговые формы W-2, что подаются в НС США, за 2016 фискальный год, которые рекламировал для продажи в сети «parkerproo», …с персональными данными 7 человек. Позже, 21 и 22 февраля 2017, ФБР приобрело у «parkerproo» похищенные федеральные налоговые формы W-2 за 2016 фискальный год, содержащие персональные данные более 270 человек…

Следственные органы США установили, что формы W-2, полученные от «parkerproo» секретным агентом, являются аутентичными налоговыми формами и содержат персональные данные граждан Соединенных Штатов. Примерно десяток форм W-2, полученных от «parkerproo», были похищены с предприятия, которое находится в Восточном округе штата Висконсин. Данные, полученные американским следствием, свидетельствуют, что с компьютера с IP-адресом 188.163.81.167 был осуществлен противоправный доступ к защищенному аккаунту, которым пользовалось это предприятие для составления налоговых деклараций.

Онлайновые источники свидетельствуют о том, что IP-адрес 188.163.81.167 зарегистрирован на ЧАО «Киевстар», в связи с чем у американцев возникла необходимость следственных действий на территории Украины. Прокурор Киевской местной прокуратуры № 10 г. Киева Адский В.А. подал в суд ходатайство о временном доступе к вещам и документам, находящимися в собственности «Киевстар»…

Суд ходатайство удовлетворил. На данный момент дальнейшая судьба «parkerproo» неизвестна.» ***(Владимир Кондрашов. ФБР ищет в Украине своего «контрагента» // InternetUA (http://internetua.com/fbr-isxet-v-ukraine-svoego-kontragenta-). 23.04.2018).***

***

«…Поліцейська служба Євросоюзу та співробітники Національного кримінального агентства Великої Британії (NCA) заблокували найбільший сайт для здійснення кібератак у світі…

Сайт webstresser.org вважають найбільшим сервісом для здійснення DDoS-атак, який пропонував свої послуги кіберзлочинцям з усіх куточків світу всього лише за 14,99 дол. При цьому, замовити атаку міг навіть технічно неосвічений користувач.

Працівники NCA стверджують, що цей сайт хакери використали для атаки на фінансові установи Великої Британії у 2017 році. Внаслідок нападу банки зазнали втрат у сотні тисяч фунтів стерлінгів.

Наразі затримано шестеро підозрюваних у причетності до створення та існування сайту…» ***(Поліція Британії та ЄС заблокували сайт, який пов'язують із мільйонами кібератак у світі // «Ракурс» (http://racurs.ua/ua/n104279-policiya-brytaniyi-ta-ies-zablokuvaly-sayt-yakyy-pov-yazuut-iz-milyonamy-kiberatak-u-sviti). 26.04.2018).***

***

«Експерт з кібербезпеки, співробітниця компанії SecurityScorecard Келлі Шортрідж помітила, що Google Chrome сканує практично всі файли на комп'ютері на базі Windows, навіть файли в папці "Мої документи"…

Повідомлення Шортрідж викликало резонанс в соціальних мережах, особливо після нещодавнього скандалу навколо витоку даних 50 млн користувачів соціальної мережі Facebook.

"…Всі бояться "великого брата", тим більше, що технологічні гіганти все частіше заходять занадто далеко - браузер переглядає файли, абсолютно не зв'язані з його роботою ", - прокоментував Харун Меєр, засновник консалтингової фірми Thinkst.

При цьому в розділі "Інформація" браузера Chrome йдеться, що сервіс "періодично перевіряє ваш пристрій на предмет виявлення потенційно небажаного програмного забезпечення" з січня 2017 року.

..."Для більшості користувачів ці перевірки є нешкідливими. А для тих, хто стурбований тим, що Google бачить деякі метадані, можу лише порадити не запускати браузер Google", - прокоментував редактор Virus Bulletin і організатор однієї з антивірусних конференцій в світі Мартін Грута…» ***(Google Chrome сканує всі файли на комп'ютері. Чи є привід непокоїтися // Espreso.tv (https://espreso.tv/news/2018/04/04/google_chrome_skanuye_vsi_fayly_na_kompyuteri_chy_ye_pryvid_nepokoyitysya). 04.04.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«…Результати дослідження бездротових мозкових імплантатів були представлені в доповіді «Забезпечення безпеки бездротових нейростимуляторів» на конференції ACM Conference on Data and Application Security and Privacy минулого місяця. За словами дослідників, їм вдалося здійснити реверс-інжиніринг неназваного імплантату і виявити серйозні проблеми з безпекою.

Передача сигналів в пристрої не шифрується і не аутентифікується. Дослідники вважають, що в майбутньому для коригування лікування нейротрансмітери використовуватимуть інформацію, отриману з мозкових хвиль на зразок P-300. Якщо зловмисникам вдасться перехопити і проаналізувати ці сигнали, вони зможуть в буквальному сенсі прочитати думки пацієнта. Однак цього можна уникнути, якщо використовувати інноваційну архітектуру безпеки, вважають дослідники…» ***(Хакери можуть зламати мозкові імплантати і прочитати думки // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/04/20/brain-implants-can-be-hacked.html). 20.04.2018).***

***

«Программист Владимир Серов обнаружил уязвимость, которая позволяла увидеть данные о «цифровом портрете» пользователей интернета в метро Москвы и Петербурга. Оператор Wi-Fi в общественном транспорте – компания «МаксимаТелеком» – признала факт уязвимости…

Уязвимость была обнаружена Серовым 5 марта в публично доступном коде страницы авторизации в сети «МаксимаТелеком» (MT_FREE).

В коде содержались данные о пользователе – номер телефона, примерные возраст, пол, семейное положение, станции, где пользователь предположительно живет и работает, станция, на которой пользователь находится в реальном времени и другая информация, привязанная в системе «МаксимыТелеком» к MAC-адресу устройства, с которого пользователь подключается к сети. Имен и фамилий там не было.

«МаксимаТелеком» составляет и хранит такой цифровой портрет о каждом пользователе для выдачи таргетированной рекламы, на которой зарабатывает. По словам Серова, с помощью программы для сбора MAC-адресов находящихся вокруг устройств можно набрать тысячу таких адресов за пару станций метро и затем, подменяя свой MAC-адрес, выгружать данные об этих пользователях со страницы авторизации.

…В самой компании признали, что уязвимость была и ее устранили шифрованием «с солью». 9 апреля в компании добавили, что сейчас работают над исключением атак с подменой MAC-адреса…» ***(Олег Овечкин. Данные о пользователях Wi-Fi в метро Москвы и Петербурга обнаружили в открытом доступе // Rusbase (https://rb.ru/news/maxima-why/). 09.04.2018).***

***

«В прошлую пятницу, 13 апреля, исследователи из Cisco Talos опубликовали отчет о багах, найденных в системе безопасности роутера Moxa EDR-810…

Обнаруженные Cisco Talos уязвимости можно разделить на несколько категорий:

Часть угроз позволяет произвести командную инъекцию. Отправив запрос HTTP POST на веб-сервер, злоумышленники могут повысить привилегии и получить права суперпользователя.

Отдельные баги вызывают разыменовывание нулевого указателя (null pointer dereference) и приводят к отказу в обслуживании.

Некоторые из обнаруженных брешей в защите можно использовать путем отправки специфических пакетов на TCP-порт 4000 или 4001, что приводит к отказу в обслуживании.

Менее серьезны ошибки, связанные с парольной защитой (передача и хранение таких данных в виде открытого текста), ненадежностью шифрования, раскрытием информации…» ***(Egor Nashilov. Cisco Talos обнаружила новые уязвимости в роутерах Moxa // Threatpost (https://threatpost.ru/cisco-talos-discovered-new-vulnerabilities-in-moxa-routers/25660/). 18.04.2018).***

***

«Американский производитель телекоммуникационного оборудования Juniper Networks выпустил обновление безопасности, затрагивающее целый набор продуктов для провайдеров и крупных корпораций…

Значительная часть заплаток относится к операционной системе JUNOS, на которой работает большинство решений Juniper Networks. Одна из самых серьезных брешей — CVE-2018-0016 — позволяла вызвать критическую ошибку в работе сетевого устройства или выполнить на нем сторонний код.

Уязвимость CVE-2018-0021 открывала возможность для MitM-атаки — злоумышленник мог подобрать секретные пасс-фразы, которыми обмениваются продукты Juniper Networks.

Большой пакет исправлений затронул Juniper Networks Network and Security Manager — унифицированную систему управления сетевой инфраструктурой. Часть устраненных уязвимостей позволяла вызвать сбои в работе решения, а в отдельных случаях — вести MitM-атаки.

К отказу в обслуживании могли также привести бреши под индексами CVE-2018-0019 и CVE-2018-0017. Первая затрагивала SNMP-подсистемы (Simple Network Management Protocol, простой протокол сетевого управления), помогающие администраторам контролировать устройства в IP-сетях, вторая — межсетевые экраны серии SRX. Ошибки в последних подвергали угрозе конфиденциальность пользовательских данных — уязвимость CVE-2018-0018 позволяла обойти установленные администратором правила и получить контроль над устройствами и системами внутри контура сетевой безопасности…»

В комментариях к патчам производитель сообщил, что ему не известно о случаях злоупотребления какими-либо из выявленных уязвимостей.» ***(Egor Nashilov. Сетевые продукты Juniper Networks стали безопаснее // Threatpost (https://threatpost.ru/juniper-networks-patches-everything/25651/). 17.04.2018).***

***

«Совместные усилия Proofpoint, Abuse.ch и канадского исследователя V1rgul3 (@Secu013) увенчались успехом: инфраструктура EITest, которая долгое время использовалась для распространения зловредов через эксплойт и загрузки drive-by, нейтрализована.

Исследователям удалось подменить ключевой сервер в обширной сети скомпрометированных сайтов и эффективно пресечь внедрение редиректоров, перенаправляющих пользователей на вредоносные площадки в объеме до 2 млн событий в сутки.

Известная как EITest мошенническая схема, аналогичная Darkleech и псевдо-Darkleech, активно использовалась с целью привлечения трафика на вредоносные страницы в течение нескольких лет…

Операторы EITest никаких ответных мер пока не приняли. Чтобы они не попытались восстановить контроль над частью взломанных сайтов, собранная информация была передана заинтересованным CERT, и те уже запустили кампанию по очистке.» ***(Maxim Zaitsev. Вредоносные скрипты EITest***

обезврежены // Threatpost (https://threatpost.ru/malicious-eitest-scripts-neutralized/25619/). 17.04.2018).

***

«Группа исследователей израильского Университета Бен-Гуриона представила способ похищения данных с изолированных от интернета и даже внутренних сетей устройств.

Техника, получившая название PowerHammer, позволяет осуществлять атаку непосредственно через электросеть. Израильские ученые разработали вредоносное ПО, которое, инфицируя компьютер, изменяет потребление электроэнергии…» ***(Кабель питания – источник угрозы // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5492283-Kabel-pitaniya-istochnik-ugrozy.html#ixzz5DDFA6ezV). 16.04.2018).***

***

«Дослідники безпеки з компанії Bastille виявили в системах аварійного сповіщення серйозну уразливість, яка дозволяє хакерам дистанційно активувати всі сирени за допомогою радіочастот.

Сирени аварійного попередження використовуються у всьому світі для повідомлення громадян про стихійні лиха, техногенних катастрофах і надзвичайних ситуаціях, таких як небезпечні погодні умови, сильні шторми, торнадо і теракти.

Атака, що отримала назву SirenJack Attack може бути здійснена на сирени виробництва ATI Systems, які використовуються в великих містах, а також в університетах, військових і промислових об'єктах США.

За словами дослідників, оскільки в радіопротоколі, використовуваному для управління вразливими сиренами, відсутнє будь-яке шифрування, зловмисники можуть проексплуатувати дану уразливість для активації сирен.

«Потрібна лише ручна радіостанція вартістю $30 і комп'ютер», - відзначили фахівці…

Дослідники повідомили ATI Systems про проблему 8 січня 2018 року. За словами виробника, в даний час виправлення тестується і незабаром буде доступно для систем, впроваджених в місті Сан-Франциско…» ***(Уразливість в системах аварійного сповіщення дозволяє хакерам запускати помилкові сигнали тривоги // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/04/11/SirenJack.html). 11.04.2018).***

***

«Дослідник безпеки Джек Кейбл (Jack Cable) виявив небезпечну уразливість в соціальній мережі LinkedIn…

Уразливість пов'язана з функцією LinkedIn AutoFill, активує кнопку «Заповнити форму за допомогою LinkedIn». При натисканні вона робить запит на сайт LinkedIn, витягує дані користувача і вставляє їх в форму заявки…

Як з'ясував дослідник, будь-який сайт може зловживати цією функцією для прихованого збору даних користувачів…

Кейбл повідомив команду безпеки LinkedIn про проблему 9 квітня, після чого соціальна мережа тимчасово обмежила використання кнопки, а потім випустила повноцінне виправлення» ***(Уразливість в LinkedIn дозволяла таємно збирати дані користувачів // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/04/20/LinkedIn-flaw.html). 20.04.2018).***

***

«У березні 2018 року компанія «Київстар» відкрила доступ до програми Bug Bounty. У її межах кожен охочий міг повідомити про знайдену вразливість у digital-сервісах і ресурсах компанії, які виносилися на розгляд по даній програмі, та отримати фінансову винагороду

За цей час у програмі від «Київстар» стали учасниками понад 160 спеціалістів з кібербезпеки, …з яких 17 – українці;

…за 2 тижні відкритого доступу до Bug Bounty отримали вшестеро більше повідомлень про потенційні вразливості, ніж за 4 попередні місяці закритого доступу;

з близько 300 отриманих повідомлень 52 були підтверджені як актуальні і вже виправлені.

…Після закінчення відкритої частини програми Bug Bounty найактивніщих кіберспеціалістів запросили продовжити тестувати digital-сервіси і ресурси компанії у межах закритого режиму…» ***(Олександр Мельник. «Київстар» винагородив понад 160 фахівців, котрі попрацювали над кібербезпекою // Na chasi (https://nachasi.com/2018/04/19/kyyivstar-bezpeka/). 19.04.2018).***

***

«…Предприятиям, использующим системы от немецкой компании SAP, рекомендуется изменить настройки своих серверов, поскольку установленные по умолчанию настройки позволяют злоумышленникам получать доступ к корпоративным данным.

Уязвимость связана с заводской конфигурацией программного решения SAP NetWeaver, которую на большинстве предприятий оставляют без изменений. SAP NetWeaver представляет собой связующее программное решение, являющееся основой для других программ…

Проблема затрагивает конфигурацию, отвечающую за передачу данных между различными компонентами инфраструктуры SAP, а именно, между Application Server (бизнес-приложениями), SAP Message Server и SAP Central Instance, где хранятся данные предприятия.

…В SAP Message Server реализована поддержка Access Control List (ACL), однако по умолчанию она отключена и системные администраторы должны сами ее активировать. Дело в том, что все предприятия разные, и будь поддержка ACL включена по умолчанию, у многих из них могли бы возникнуть проблемы с первоначальной настройкой бизнес-приложений.

Проблема с заводской конфигурацией SAP известна еще с 2005 года. В то время производитель выпустил уведомление безопасности и рекомендовал

компаниям не оставлять настройки по умолчанию и как можно скорее настроить ACL, а также разрешить доступ к порту 3900 только с доверенных адресов.

В 2009 и в 2010 годах производитель выпустил еще два уведомления безопасности с дальнейшими инструкциями…

По словам экспертов, злоумышленник со стороны или даже сотрудник предприятия может создать вредоносное приложение, зарегистрировать его в корпоративной SAP-инфраструктуре и с его помощью похищать или изменять корпоративные данные.

Access Control List – список управления доступом, определяющий, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).» ***(13 лет предприятия подвергают себя риску, используя SAP с заводскими настройками // SecurityLabRu (https://www.securitylab.ru/news/492999.php). 28.04.2018).***

***

«…З поширенням «інтернету речей» все більше предметів стають «розумними», але при цьому не дуже захищеними…

За словами голови компанії з кібербезпеки Darktrace Ніколь Іган розповіла, більшість користувачів не знає, які діри існують у придбаних ними гаджетах. «Є багато предметів, що сумісні з інтернетом речей – від термостатів, холодильників і кондиціонерів до людей, які приносять «розумні» колонки в свої офіси…», – говорить вона.

Як з'ясували нещодавно ізраїльські дослідники, численні девайси «інтернету речей» навіть не треба ламати через діри – в них використовуються стандартні паролі.

…Фахівець із кібербезпеки Брюс Шнаєр попереджає, що в близькому майбутньому можливе порушення роботи інтернету. За його словами, хтось протягом останніх років вивчає способи зруйнувати Павутину. Станеться повне відключення: пошта, веб-сайти, онлайнові сервіси. Шнаєр не знає, хто саме це планує, але каже, що зловмисники зараз проводять спрямовані DDoS-атаки, а також атаки, які дозволяють визначити, як добре захищені жертви і якою повинна бути сила удару, щоб паралізувати діяльність мережі.» ***(Євген Корольов. Кмітливі хакери перетворили звичайний акваріум з рибами на діру в корпоративній мережі... // Tech Today (https://techtoday.in.ua/news/kmitlivi-hakeri-peretvorili-zvichayniy-akvarium-z-ribami-na-diru-v-korporativniy-merezhi-kazino-97243.html). 29.04.2018).***

***

«Исследователи кибербезопасности из фирмы Checkmarx нашли способ превратить «умную» колонку Amazon Echo в подслушивающее устройство.

Специалистам не пришлось эксплуатировать какие-либо уязвимости в устройстве Echo или облачном сервисе Alexa, они просто использовали опции, доступные в комплекте разработчика программного обеспечения (SDK) для Alexa.

По словам исследователей, они использовали Alexa SDK для создания приложения калькулятора, которое продолжает прослушивать даже после предоставления пользователю ответа на исходный вопрос…

Исследователи уведомили Amazon о проблеме и компания выпустила соответствующие исправления.» ***(Исследователи превратили Amazon Echo в подслушивающее устройство // Goodnews.ua (http://goodnews.ua/technologies/issledovateli-prevratili-amazon-echo-v-podslushivayushhee-ustrojstvo/). 29.04.2018).***

***

«Специалист по кибербезопасности компании Check Point Ассаф Бахарав (Assaf Baharav) обнаружил уязвимости в стандарте PDF, позволяющие выкрасть учетные данные Windows.

…Незащищенность PDF дает возможность получить хеши NTLM (протокола аутентификации), которые хранят данные для доступа к компьютеру.

Для исследования Бахарав создал PDF-документ, в котором потенциально могут использоваться функции Go To Remote и Go To Embedded (удаленный доступ и внешние вставки).

Алгоритмы устроены таким образом, что при открытии файла документ самостоятельно отправляет запрос на удаленный SMB-сервер.

Все запросы сетевого протокола включают аутентификацию с помощью хешей NTLM: учетные данные пользователя будут сохранены. Хакеру лишь остается прописать путь до вредоносного сервера.

Инициирование запросов SMB из документов, созданных через программы в системе Windows, часто становится способом организации кибератаки…» ***(Данные в опасности: хакеры нашли способ взломать компьютер через PDF-файлы // «Я и Закон» (http://yaizakon.com.ua/dannye-v-opasnosti-hakery-nashli-sposob-vzlomat-kompyuter-cherez-pdf-fajly/). 28.04.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…Стандарт Web Authentication (WebAuthn) предназначен для замены пароля биометрией и устройствами, уже имеющимися у пользователей, например, ключ безопасности, смартфон, сканер отпечатков пальцев или веб-камера.

Вместо того, чтобы запоминать длинные строки символов, пользователи могут пройти аутентификацию биометрией или устройствами через Bluetooth, USB или NFC…

Один из примеров работы WebAuthn: когда пользователь посещает сайт, где требуется аутентификация, он вводит имя пользователя, а затем получает

предупреждение на свой смартфон. Нажав на него, пользователь может войти на веб-сайт без ввода пароля.

WebAuthn обещает защитить пользователей от фишинговых атак и использования украденных учетных данных…

WebAuthn также позволит людям использовать уникальные данные для входа в систему какой-либо службы вместо ввода логина и пароля для каждого сайта.

На данный момент WebAuthn находится на стадии «рекомендации кандидата». Google, Microsoft и Mozilla взяли на себя обязательство поддерживать WebAuthn, а это означает, что все основные веб-браузеры, не принадлежащие Apple Safari, будут внедрять новый стандарт…

Несколько сайтов и сервисов уже используют аналогичные методы для входа в систему, в том числе Google и Facebook - с помощью USB-ключа безопасности…» ***(Ирина Фоменко. RIP пароли: создан новый веб-стандарт для входа в систему // Internetua (http://internetua.com/rip-paroli-sozdan-novi-veb-standart-dlya-vhoda-v-sistemu). 12.04.2018).***

***

«В систему управления ИБ-событиями MaxPatrol SIEM добавлены 26 новых правил обнаружения инцидентов, позволяющих выявлять продвинутые кибератаки на Microsoft Active Directory…

Создание специального пакета правил стало результатом работы экспертного центра безопасности (Expert Security Center) компании Positive Technologies: они проанализировали полный цикл атак на Active Directory и выявили цепочку событий ИБ и запросы в сетевом трафике, которые свидетельствуют о присутствии злоумышленников в инфраструктуре. Далее для автоматического анализа событий на наличие признаков таких атак и для уведомления ИБ-подразделения при помощи MaxPatrol SIEM был разработан пакет с алгоритмами обнаружения аномалий (правила корреляции). Теперь ИБ-специалисты, использующие систему, смогут выявлять атаки на Active Directory на стадии разведки, продвижения внутри сети и удаленного исполнения команд…» ***(MaxPatrol SIEM теперь выявляет продвинутые кибератаки на Microsoft Active Directory в автоматическом режиме // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/292036/). 16.04.2018).***

***

«Google обновила браузер Chrome до версии 66…

Авторы активировали возможность изоляции данных сайта для небольшого количества пользователей браузера…

Изоляция данных сайта препятствует выполнению внешнего кода на открытой в браузере странице. Это обеспечивает дополнительную безопасность данных и является одним из факторов защиты от атак, основанных на уязвимостях Meltdown и Spectre. Google тестирует новую технологию и планирует добавить ее в стандартный функционал браузера в одном из будущих релизов.

Новая версия Chrome стала очередным шагом вендора на пути исключения из числа доверенных SSL-сертификатов Symantec. Начиная с текущего релиза,

браузер будет предупреждать пользователей о переходе на сайты, которые используют такие разрешения, выданные до 1 июня 2016 года. Сертификаты от партнеров Symantec, среди которых популярные сервисы RapidSSL, VeriSign, Equifax, Thawte и GeoTrust, также будут помечены как ненадежные…

Инженеры Google добавили в новый релиз предупреждения о попытках внедрения сторонних скриптов в активные процессы Chrome. Обычно этим грешат антивирусные программы, проверяющие страницы «на лету», и всевозможные утилиты для отладки веб-кода. Теперь пользователя будут предупреждать о том, что одно из приложений мешает корректной работе браузера…

Среди ошибок, исправленных в новой версии Chrome, выделяются две критические уязвимости, связанные с обращением к освобожденной области памяти при реализации кэширования на диск.

Еще несколько серьезных проблем пропатчены в подсистеме обработки PDF-файлов, модуле исполнения байт-кода WebAssembly и графическом движке Skia.

В общей сложности разработчики Google закрыли в новой версии браузера 62 бреши разной степени серьезности…» ***(Egor Nashilov. Новая версия Chrome защищена от атак Meltdown и Spectre // Threatpost (https://threatpost.ru/google-chrome-66-is-here/25692/). 19.02.2018).***

***

«Международная команда исследователей из университетов Израиля и США разработала оригинальный алгоритм, помогающий выявлять фальшивые аккаунты в социальных сетях. Новый метод основан на анализе пользовательских связей и позволяет с высокой точностью определять профили, за которыми не стоят реальные люди.

…Исследователи утверждают, что область применения разработанной ими методики не ограничена лишь Facebook, и технологию можно использовать для поиска ботов в любой социальной сети.

Как заявляют ученые, они протестировали работу алгоритма на данных из десяти разных сервисов. Среди испытанных площадок оказались Facebook, Twitter, LinkedIn, Instagram, «ВКонтакте», «Одноклассники», Google+ и китайский мессенджер Tencent QQ.

Фальшивые аккаунты являются серьезной, но не единственной проблемой социальных сетей. Популярные сервисы регулярно сотрясают скандалы, связанные с утечкой приватных данных…» ***(Egor Nashilov. Ученые научились находить ботов в социальных сетях // Threatpost (https://threatpost.ru/no-more-fakes-algorithm-is-upon-us/25685/). 19.04.2018).***

***

«На днях Альянс FIDO опубликовал два новых стандарта проверки подлинности — Web Authentication (WebAuthn) и Client to Authenticator Protocol (CTAP).

Стандарт WebAuthn — это API, позволяющий создавать гибкие, надежные, защищенные идентификаторы на основе открытого ключа. Независимо от конкретного способа аутентификации пользователя на устройстве (отпечаток

пальца, сетчатка глаза или другое) — Web Authentication примет его учетные данные и сообщит веб-приложению, что клиент распознан и проверен. При этом никакие личные сведения на сервер не передаются, конфиденциальность сохраняется, а вероятность перехвата или взлома пароля сведена к нулю.

Проверка подлинности в стандарте WebAuthn достигается взаимодействием нескольких совместимых аутентификаторов — таких как доверенный апплет, SE (защищенные элементы), TPM (доверенные модули платформы) и другие компоненты, работающие в пользовательской среде. Также возможна идентификация при помощи внешних устройств с USB, Bluetooth или NFC, для них разработан второй стандарт — CTAP. По сути, это протокол прикладного уровня, обслуживающий коммуникацию между аутентификатором и другим клиентом с готовыми транспортными привязками.

Беспарольные стандарты проверки подлинности, созданные FIDO и W3C (World Wide Web), находятся на заключительном этапе утверждения — Candidate Recommendation (CR). Аутентификация по методу WebAuthn и CTAP (так называемый проект FIDO2) уже одобрена Google, Microsoft и Mozilla и внедрена для платформ Windows, Mac, Linux, Android и Chrome OS.

Реализация FIDO2 означает, что в браузеры и web-платформы будут встроены API WebAuthn, а CTAP обеспечит передачу аутентификационных данных через USB, Bluetooth или NFC на подключенное к Интернету устройство (смартфон, ноутбук или ПК)…» ***(Julia Glazova. Пора забыть о паролях: новые стандарты идентификации FIDO2 // Threatpost (https://threatpost.ru/forget-passwords-use-new-authentication-standards-fido2/25597/). 13.04.2018).***

***

«Корпорация Microsoft объявила о новых интеллектуальных инструментах, призванных облегчить защиту данных и корпоративных сетей от наиболее опасных современных угроз, а также помочь в борьбе с новыми видами вредоносного ПО, нацеленного на устройства IoT (Internet of Things). Целью Microsoft является развитие экосистемы кибербезопасности для обеспечения комплексной защиты: от облака до конечного устройства.

…Microsoft использует возможности «умного» облака для противодействия возникающим угрозам, направленным на новый класс подключенных устройств, которые создаются на базе компактного чипа под названием микроконтроллер (microcontroller unit, MCU). Устройства на микроконтроллерах уже занимают крупную нишу на рынке вычислений, и их число каждый год растет на 9 миллиардов. Они могут быть встроены как в игрушки и бытовую технику, так и в индустриальное оборудование – поэтому они становятся новой мишенью для атак злоумышленников. Чтобы обеспечить безопасность нового поколения устройств, Microsoft представляет Azure Sphere – первую в индустрии комплексную платформу для создания решений с высокозащищенными устройствами «умной» периферии на базе микроконтроллеров. Она включает совершенно новый класс микроконтроллеров, которые больше, чем в 5 раз мощнее прежних, специализированную ОС для обеспечения безопасности систем IoT, а также сервис облачной защиты «под ключ» для всех устройств Azure Sphere. Благодаря Azure

Sphere Microsoft расширяет границы «умной» периферии, обеспечивая производительность и безопасность совершенно новой категории устройств…

Сталкиваясь с угрозами безопасности, компании все больше осознают, что инструменты обнаружения и противодействия угрозам, необходимые им, чтобы быть на шаг впереди атакующих, находятся в облаке. Microsoft представила несколько интеллектуальных средств обеспечения безопасности, входящих в облачное решение Microsoft 365…

Secure Score упрощает выбор элементов безопасности, которые необходимо активировать для защиты пользователей, данных и устройств. Этот инструмент помогает быстро оценивать подготовленность системы и предоставляет наглядные контрольные показатели уровня информационной безопасности...

Attack Simulator, входящий в состав Office 365 Threat Intelligence, позволит специалистам по безопасности проводить симуляцию атак, включая внедрение фиктивного вируса-вымогателя и проведение фишинг-рассылки, чтобы на практике проверить, как сотрудники реагируют на угрозы, и, в соответствии с этим, отрегулировать конфигурацию безопасности и параметры защиты систем.

…Последнее обновление Windows 10, доступное на данный момент в предварительной версии, включает решение Windows Defender Advanced Threat Protection (ATP), которое теперь работает с другими элементами Microsoft 365, позволяя интегрировать защиту от угроз и восстановление системы в Office 365, Windows и Azure…

Conditional Access (условный доступ) позволяет проводить оценку рисков в режиме реального времени и обеспечивает контроль доступа к конфиденциальным данным, при этом не снижая продуктивность конечных пользователей. В Microsoft 365 теперь появилась дополнительная возможность оценки степени риска для устройства на основе данных от Windows Defender ATP, который передает информацию напрямую в Conditional Access (доступно в предварительной версии), чтобы предотвратить доступ зараженного устройства к конфиденциальным данным бизнеса.

…Microsoft также объявила о создании новой Ассоциации интеллектуальных средств безопасности Microsoft (Microsoft Intelligent Security Association) для технологических партнеров, работающих в сфере безопасности, чтобы они могли пользоваться преимуществами Intelligent Security Graph и решений информационной безопасности Microsoft, а также вносить вклад в их развитие…» ***(Microsoft представила новые инструменты для защиты облачных решений и устройств от киберугроз // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5493404-Microsoft-predstavila-novye-instrum.html#ixzz5DDDFLkr8). 19.04.2018).***

***

«Эксперты «Лаборатории Касперского» опубликовали на портале GitHub исходный код сканера KLara…

Основная задача KLara — обнаружение родственных образцов вредоносного кода. Это один из ключевых аспектов исследований киберугроз, который помогает экспертам отслеживать развитие вредоносов.

…Это распределённая система, которая может производить быстрый поиск сразу по нескольким базам с применением нескольких правил. Такой подход позволяет быстрее выявлять образцы вредоносного кода, а значит более эффективно защищать пользователей…

Также в открытом доступе можно найти другой инструмент компании – BitScout. Он был разработан ведущим антивирусным экспертом компании Виталием Камлюком в 2017 году. BitScout может удалённо собирать оставленные злоумышленниками цифровые «улики», например, образцы вредоносного ПО». ***(«Лаборатория Касперского» открыла исходный код инструмента для продвинутого поиска киберугроз // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5491049-Laboratoriya-Kasperskogo-otkryla.html#ixzz5DDGEoqYP). 11.04.2018).***

***

«Компания Intel планирует позволить разработчикам антивирусного ПО использовать ресурсы встроенного в процессор графического ядра для сканирования компьютеров на предмет различных киберугроз…

На этой неделе, на конференции RSA 2018, компания Intel анонсировала сразу две новые технологии Threat Detection Technology (TDT) и Security Essentials, которые помогут бороться с различными угрозами с аппаратной точки зрения.

Поддержка Accelerated Memory Scanning будет реализована в Microsoft Windows Defender Advanced Threat Protection уже в конце апреля 2018 года, а после обещают осуществить интеграцию с другими защитными продуктами.

Также инженеры Intel представили Advanced Platform Telemetry, которая сочетает в себе инструмент для отслеживания телеметрии и "облачное" машинное обучение, что позволяет обнаруживать угрозы значительно быстрее, при этом не оказывая влияния на производительность. Уже известно, что эту новинку скоро интегрируют с платформой Cisco Tetration…» ***(Intel разрешит антивирусам использовать встроенную в процессор защиту от угроз // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122596). 19.04.2018).***

***

«Исследователи из американской ИБ-компании Endgame опубликовали, по их словам, первый в мире открытый массив данных для обучения моделей искусственного интеллекта (ИИ) обнаружению вредоносного ПО. Проект получил название EMBER.

EMBER содержит метаданные, описывающие 1,1 млн исполняемых файлов для Windows. 900 тыс. из них представляют собой обучающие образцы, разделенные на три категории – вредоносные, легитимные и неклассифицированные. Еще 200 тыс. файлов – это тестовые образцы, разделенные на вредоносные и легитимные.

…EMBER не содержит Windows-файлы целиком, а только описывающие их метаданные (размер, формат и пр.). Обученный с помощью EMBER ИИ способен отличать вредоносные файлы от легитимных по их свойствам…» ***(Опубликован***

первый в мире массив данных для обучения ИИ обнаружению вредоносного ПО // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122547). 17.04.2018).

***

«…Инженеры Mozilla намерены добавить в Firefox новую функцию безопасности для защиты от межсайтовых подделок запроса (CSRF). Так, в версии браузера Firefox 60, запланированной к выпуску на 9 мая текущего года, будет реализована поддержка атрибута cookie SameSite.

Атрибут SameSite блокирует загрузку сайтом файлов cookie, загруженных с других доменов, которые не совпадают с URL в адресной строке Firefox…

Стоит отметить, реализация функции SameSite ложится не на плечи пользователей или инженеров Mozilla. Атрибут SameSite должны настраивать сами владельцы сайтов в заголовках ответов HTTP точно так же, также как они настраивают в заголовках ответов стандартное поле Set-Cookie…» ***(В Firefox появится защита от CSRF-атак // SecurityLabRu (https://www.securitylab.ru/news/492894.php). 24.04.2018).***

***

«Система BlackBerry PGP считается самой безопасной в современном мире…

BlackBerry PGP для каждого сеанса передачи информации генерирует уникальный 4096-разрядный ключ, подобрать его не представляется возможным. Уникальный ключ применяется при шифровании отправляемых почтовых сообщений по алгоритму AES-256. Этот алгоритм отвечает за создание шифрованного текста. Текст, подвергаемый процедуре шифрования, отображается в виде набора символов, букв и цифр…

Как только завершится процедура шифрования при помощи ключа сеанса, осуществляется шифрование сведений при помощи открытого ключа получателя. BlackBerry PGP обеспечивает объединение зашифрованного текста и зашифрованных ключей в единое сообщение прежде, чем оно пройдет отправку с устройства пользователя. Образуется так называемый «зашифрованный пакет».

…Как только пользователь нажимает кнопку для отправки сообщения, система применяет технологию создания безопасного зашифрованного соединения AES-256 совместно с зашифрованной версией частной сети BlackBerry PGP.

…Доставка информации адресату осуществляется путем перехода зашифрованного сообщения из сети закрытого типа Blackberrypgp.pro в сеть BlackBerry адресата в пределах одного защищенного канала.

..Как только адресату будет доставлен зашифрованный пакет, он сможет инициировать процедуру расшифрования сообщения с применением своего оригинального закрытого ключа и кодовой фразы. Хранение закрытого ключа осуществляется исключительно на пользовательском устройстве. Отправка сообщения возможна при условии наличия на ключевом сервере открытого ключа электронной почты…» ***(Самая безопасная система «BlackBerry PGP» // Український телекомунікаційний портал***

(https://portaltele.com.ua/equipment/mobile-technology/samaya-bezopasnaya-sistema-blackberry-pgp.html). 29.04.2018).

***

«Cisco анонсировала новые сервисы защиты электронной почты для более эффективного предотвращения фишинговых и спуфинговых атак

…Для отражения продвинутых угроз, целью которых являются сотрудники, Cisco предлагает новые сервисы безопасности электронной почты, которые защищают пользователей от мошеннических сообщений, и новые функции защиты пользовательских устройств от программ-вымогателей, вирусного майнинга криптовалют и бесфайловых вредоносных программ.

…Облачное решение защиты оконечных точек Cisco® Advanced Malware Protection (AMP) for Endpoints предотвращает атаки и помогает выявлять необнаруженные угрозы, способные нанести ущерб бизнесу.

- …Новая функция защиты от эксплойтов Cisco AMP for Endpoints борется с бесфайловыми атаками, в том числе с такими, которые располагаются исключительно в памяти устройства, а функция предотвращения вредоносной деятельности останавливает программы-вымогатели, прерывая исполняемые процессы и предотвращая их распространение…

- Cisco Visibility – приложение для исследования угроз. Новое облачное приложение, встроенное в консоль управления оконечными устройствами, упрощает и ускоряет процесс исследования инцидентов безопасности, существенно облегчая работу аналитиков, которые теперь смогут уверенно и быстро расследовать инциденты в требуемом масштабе…» ***(Cisco совершенствует защиту оконечных устройств и электронной почты // <META> (http://pr.meta.ua/read/54814). 25.04.2018).***

***

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

Валіулліна З. В. Економіка та інформаційна безпека зарубіжних країн : навч. посіб. / З. В. Валіулліна. - Рівне, 2017. - 275 с.

Висвітлено актуальні аспекти інформаційної безпеки в країнах світу, включаючи захист від кібератак на сучасному етапі розвитку суспільства, економічний стан інформаційної безпеки у світі, управління інформаційною безпекою корпоративної економіки та ін.

Шифр зберігання НБУВ: ВА818277.

***

Головко О. М. Інформаційно-правова політика України у сфері безпеки людини у медіапросторі : автореф. дис. ... канд. юрид. наук : 12.00.07 / Головко

Ольга Михайлівна ; НДІ інформатики і права Нац. акад. прав. наук України. - Київ, 2018. - 19 с.

Встановлено сутнісне розуміння деожавної інформаційно-правової політики в умовах нових геополітичних виклиеів та соціально-економічної ситуації в Україні. Розкрито політико-правові основи безпеки людини в медіапросторі. Зроблено акцент на сучасному політико-правовому інструментарії, що знаходиться в розпорядженні органів державної влади в Україні. Визначено основні характеристики небезпек та загроз медіа-безпеці людини та політико-правові заходи протидії їм в Україні. Розроблено класифікацію загроз безпеці людини в медіапросторі. Віднайдено та обгрунтовано способи підвищення ефективності практичних засобів вдосконалення політико-правових заходів протидії небезпекам та загрозам безпеці людини у медіапросторі.

Шифр зберігання НБУВ: РА433137.

***

Гриб О. Г. Синтез элементов энергосистемы по критерию надежности в условиях кибербезопасности / О. Г. Гриб, С. В. Швец, А. В. Бортников // Вісник Національного технічного університету "ХПІ". Серія : Інформатика та моделювання. - 2017. - № 50. - С. 97-110.

Серед апаратних рішень кіберзахисту сучасних енергосистем запропоновано в їх інфраструктурі управління вводити резервування ключових елементів для підвищення надійності і тим самим, забезпечення необхідного рівня кібербезпеки.

Отримані співвідношення кратності резервування елементів для випадків наявності і відсутності обмежень на мінімально допустимі значення ймовірностей їх безвідмовної роботи.

Шифр зберігання НБУВ: Ж29210.

***

Дванадцяті юридичні читання. Держава в суспільно-політичних процесах: виклики і загрози : матеріали міжнар. наук. конф., 1-2 черв. 2017 р., м. Київ, Україна. - Київ : Вид-во НПУ ім. М. П. Драгманова, 2017. - 380 с.

Зі змісту:

- Пилипчук В.Г. Права і безпека людини в інформаційній сфері: сучасні проблеми та пріоритети наукових досліджень;
- Брижко В.М. Інформаційна безпека в сфері захисту персональних даних в сучасних європейських правових стандартах;
- Бурлаченко Д.П. Правові аспекти блокування контенту в мережі Інтернет;
- Новіцький А.Б. Інформаційна безпека і проблеми розбудови інформаційного суспільства;
- Цимбалюк В.С. Кібер-право – відгук на загрози безпеці інформаційного суспільства.

Шифр зберігання НБУВ: ВА818224.

***

Діордіца І. В. Кібернетичний простір vs інформаційний у контексті правничої герменевтики / І. В. Діордіца // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2017. - Вип. 28. - С. 56-59.

Продемостровано сутність герменевтичного підходу в дослідженні термінологічних сполучень, висвітлено їх інтеграційні та диференціальні ознаки. Врахування даних, які містяться у статті, дасть змогу у подальшому вдосконалювати юридичну техніку нормотворчості.

Шифр зберігання НБУВ: Ж74042/юр.

***

Дудатьєв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія / А. В. Дудатьєв. - Вінниця : ВНТУ, 2017. - 127 с.

Запропоновано аксіоматику теорії інформаційної взаємодії типу «об'єкт-суб'єкт» та класифікацію інформаційних вірусів, що можуть бути використано для «інфікування» соціальної частини соціо-технічної системи. Представлено модель інформаційного впливу та методи протидії спеціальним кібернетичним операціям.

Шифр зберігання НБУВ: ВА817788.

***

Захаренко К. В. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток : монографія / Костянтин Захаренко. - Київ : Вид-во НПУ ім. М. П. Драгоманова, 2017. - 388 с.

Розглянуто суб'єкт-об'єктні характеристики інформаційної безпеки, місце та роль політичних партій та громадських організацій в стратегії інформаційної безпеки, правовий супровід інформаційної безпеки суспільства, протидію зовнішнім та внутрішнім інформаційно-дестабілізаційним впливам в контексті зміцнення інформаційної безпеки.

Шифр зберігання НБУВ: ВА818201

***

Захарченко С. М. Основи побудови захищених мереж на базі обладнання компанії Cisco : навч. посіб. / С. М. Захарченко, Т. І. Трояновська, О. В. Бойко ; Вінниц. нац. техн. ун-т. - Вінниця : ВНТУ, 2017. - 135 с.

Розглянуто особливості побудови захищених комп'ютерних мереж рзного типу на основі використання обладнання компанії Cisco, зокрема, класифікацію та різновиди атак, методи криптографічного захисту інформації, технології захисту мережевих пристроїв.

Шифр зберігання НБУВ: ВА817730

***

Корченко О. Г. Прикладні системи оцінювання ризиків інформаційної безпеки : монографія / О. Г. Корченко, С. В. Казмірчук, Б. Б. Ахметов. - Київ, 2017. - 435 с.

Розглянуто теоретико-методологічні і практичні аспекти оцінювання ризиків інформаційної безпеки. Значну увагу приділено розробленню методів модифікації порядку лінгвістичної змінної при перевизначенні еталонів параметрів, а також оцінювання ризиків безпеки ресурсів інформаційних систем в реальному часі з використанням CVSS метрик, які містяться у відкритих базах даних уразливостей. Порушено питання практичного оцінювання ризиків без залучення експертів відповідної предметної галузі при нечітких і детермінованих умовах оцінювання з використанням параметрів, які можуть бути представлені як в числовій, так і лінгвістичній формі з урахуванням періоду часу, галузі промисловості, економічної та управлінської специфіки підприємства.

Шифр зберігання НБУВ: ВА817313.

***

Матеріали III Міжнародної науково-практичної конференції «Сучасні тенденції в юридичній науці України» (29-30 червня 2017 р.) : [збірник]. - Київ, 2017. - 111 с.

Зі змісту:

- Шумейко І.В. Проблеми нормативно-правового забезпечення інфомаційної безпеки України.

Шифр зберігання НБУВ: ВА817896.

***

Матеріали IV Всеукраїнської науково-практичної конференції «Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення», 18-20 травня 2017 р., м. Львів : [зб. тез доп.]. - Львів, 2017. - 209 с.

Зі змісту:

- Смолинець М. Безпека інформації в хмарних сервісах: проблеми та перспективи.

Шифр зберігання НБУВ: ВА817767.

***

Матеріали V Міжнародної науково-практичної конференції «Актуальні питання сучасної науки» (7-8 лип. 2017 р.). - Івано-Франківськ, 2017 . - Ч. 2. - 127 с.

Зі змісту:

- Степанов А.С. Обзор крупнейшей в истории Украины кибератаки, ее причин и путей предотвращения.

Шифр зберігання НБУВ: В356976/2.

***

Матеріали XI Міжнародної науково-практичної конференції «Маркетинг інновацій і інновації у маркетингу», 28-30 вересня 2017 року : [збірник]. - Суми , 2017. - 211 с.

Зі змісту:

- Захаркіна Л.С., Задорожня Д.С., Новак К.С. Кібер-страхування як інноваційний механізм забезпечення фінансової безпеки суб'єкта господарювання.

Шифр зберігання НБУВ: ВА817502.

***

Реєстрація, зберігання і обробка даних. Щорічна підсумкова наукова конференція, 17-18 травня 2017 р. : [збірник]. - Київ, 2017. - 131 с.

Зі змісту:

- Горбачик О.С. Проблеми та задачі забезпечення безпеки функціонування об'єктів критичних інфраструктур;
- Кузнєцова М.Г. Системи організаційного управління та безпека об'єктів критичних інфраструктур;
- Сасюк М.М. Визначення та класифікація об'єктів критичних інфраструктур.

Шифр зберігання НБУВ: СО35573.

***

Сазонець О. М. Інформатизація світогосподарського розвитку : підруч. для студентів ВНЗ / О. М. Сазонець, О. І. Качан. - Рівне : Волинські обереги, 2017. - 191 с.

Розглянуто аспекти, пов'язані з інформатизаційними та інноваційними процесами у міжнародному бізнесі. Досліджено стан електронної комерції у світі та Україні. Окремим напрямом дослідження є боротьба із загрозами безпеці в інформаційній сфері. Виявлено її складові. Обгрунтовано необхідність захисту інформаційних систем в економіці.

Шифр зберігання НБУВ: ВА818278.

***

Ткачук Т.Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі / Ткачук Т.Ю. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2017. - Вип. 46(2). - С. 39 – 42.

Визначено основні напрями державної політики у сфері забезпечення інформаційної безпеки. Розглянуто проблеми реалізації державної політики у сфері забезпечення інформаційної безпеки на сучасному етапі.

Шифр зберігання НБУВ: Ж68850.

***

Ткачук Т.Ю. Забезпечення інформаційної безпеки в країнах позаблокового статусу / Т.Ю. Ткачук // Прикарпатський юридичний вісник. - 2017. - Вип. 4. - С. 61-65.

Проаналізовано політику й системи гарантування інформаційної безпеки в країнах позаблокового статусу. Визначено пріоритети та проблеми гарантування інформаційної безпеки в зазначених країнах. Оцінено значущість досвіду країн позаблокового статусу у досліджуваній сфері для України.

Шифр зберігання НБУВ: Ж74200.

***

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.