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

№ 8 (серпень)

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

«…Согласно озвученной спикером УКА [Украинского Киберальянса] информации, на сайте Государственного реестра избирателей ЦИК Украины обнаружена XSS-уязвимость. XSS – тип уязвимости программного обеспечения, который позволяет атакующему внедрить клиентский сценарий в web-страницы, просматриваемые другими пользователями…

Пока может радовать только тот факт, что результаты выборов в Украине считаются вручную, и системы, используемые ЦИК, носят лишь вспомогательный характер.» ***(Владимир Кондрашов. На сайте ЦИК может повториться история с победой Ярош а // InternetUA (http://internetua.com/na-saite-cik-mojet-povtoritsya-istoriya-s-pobedoi-yarosha). 21.08.2018).***

***

«Спустя сутки после того, как в рамках акции #FuckResponsibleDisclosure спикер Украинского киберальянса, известный под ником Шон Таусенд, сообщил об XSS-уязвимости на сайте Государственного реестра избирателей, в Центризбиркоме разразились гневной тирадой о недостоверной информации…

– Никакого несанкционированного проникновения в информационные ресурсы Центральной избирательной комиссии не произошло. Все информационные системы работают в штатном режиме. А очередная попытка приклеить уже ни в кого не вызывающий доверия ярлык «зрада» к работе Комиссии и Государственного реестра избирателей превратилась в тривиальную самодискредитацию некомпетентного автора, – заявили в ЦИК.

Как уточнил в комментариях руководитель Службы распорядителя Государственного реестра избирателей Александр Стельмах, потенциальную уязвимость исправили в течение 10 минут после обнаружения. По его словам, уязвимость позволяла запустить скрипт только на клиенте, и не является чувствительной для сайта…» ***(Владимир Кондрашов. ЦИК «наехала» на хакеров, которые нашли уязвимости на её сайте // Internetua (http://internetua.com/cik-naehala-na-hakerov-kotorye-nashli-uyazvimosti-na-ee-saite). 23.08.2018).***

***

«...кіберзахисники … планують ввести наступні вимоги:

• Державні абоненти повинні використовувати тільки сервери, розташовані на підконтрольній території;

• Державні абоненти повинні працювати тільки з тими постачальниками, які мають захищені вузли доступу до глобальних мереж та атестати відповідності до них;

• Державні органи реєструють свій домен в зоні gov.ua виключно з використанням протоколу HTTPS, а інші абоненти – на нижніх рівнях домену ua.

• Забороняється підключати до глобальних мереж передачі даних інформацію, яка становить державну таємницю.

Всі ці вимоги пояснюються необхідністю забезпечити захист інформаційних ресурсів держави від кіберзагроз…

Але як з'ясовується, з 6 тис. провайдерів, новим вимогам відповідають одиниці. 30 липня Держспецзв'язку затвердила список провайдерів, що мають атестати відповідності системи захисту. До таких відносяться Державний центр кіберзахисту Держспецзв'язку, «Укртелеком», «Датагруп», «Адамант», «Оріон» та ін – всього 15 провайдерів…

Є ще ряд провайдерів, які мають захищені вузли доступу (наприклад, велика трійка мобільників — Київстар, Vodafone, life), але вони в перелік Держспецзв'язку чомусь не включені…» ***(Кібербезпека держпідприємств і владних структур в Україні. Небезпеки і способи їх усунення // Українська служба швидких новин (https://novosti.ternopil.ua/kiberbezpeka-derzhpidpriyemstv-i-vladnix-struktur-v-ukra%d1%97ni-nebezpeki-i-sposobi-%d1%97x-usunennya/). 14.08.2018).***

***

Національна система кібербезпеки

«В Україні буде створено центр управління кібербезпекою у транспортній галузі.

Про це заявив міністр інфраструктури Володимир Омелян на брифінгу…

За його словами, головними завданнями центру буде моніторинг стану кібербезпеки транспорної галузі, своєчасне інформування про кіберзагрози та обмін інформацією про кіберінциденти з національними центрами кібербезпеки, Державною службою спецзв'язку та Службою безпеки України.» ***(Для захисту транспорту від кібератак створять спеціальний центр // Західна інформаційна корпорація (https://zik.ua/news/2018/08/17/dlya_zahystu_transportu_vid_kiberatak_stvoryat_spetsialnyy_tsentr_1388847). 17.08.2018).***

***

Кібервійна проти України

«На Україну постійно чиняться кібератаки з території Російської Федерації…

Начальник Департаменту кіберполіції Національної поліції України Сергій Демедюк розповів, що координує роботу відомств кіберцентр, створений на базі РНБО.

Також, з його слів, виявляти кібернапади Україні допомагають міжнародні партнери: зокрема, Велика Британія, Німеччина, Польща та Австралія. Разом з тим, зауважив він, будь-яка співпраця із Росією наразі відсутня…» ***(Олександр Сивачук. На Україну постійно чиняться кібератаки з території РФ – кіберполіція // Інформаційне агентство «Українські Національні Новини»***

(http://www.unn.com.ua/uk/news/1746348-na-ukrayinu-postiyno-chinyatsya-kiberataki-z-teritoriyi-rf-kiberpolitsiya). 11.08.2018).

***

«Виконавча директорка Інституту масової інформації Оксана Романюк відреагувала на оприлюднення персональних даних українських журналістів на сепаратистських сайтах та заявила, що Україна має залучити найкращих спеціалістів для посилення кібербезпеки та виявлення російських шпигунів у силових структурах…

За словами пані Романюк, дані про журналістів, що працюють на фронті, мають бути запаролені від початку збройного конфлікту на Донбасі. Втім, вона вважає, що навіть зберігання цих даних у захищеній хмарі на Google-диску зробить їх більш убезпеченими, ніж вони є зараз…» ***(Є проблема з кібербезпекою, або хтось свідомо «зливає» списки журналістів – Романюк // «Детектор медіа» (https://detector.media/community/article/140639/2018-08-31-e-problema-z-kiberbezpekoyu-abo-khtos-svidomo-zlivae-spiski-zhurnalistiv-romanyuk/). 31.08.2018).***

***

Боротьба з кіберзлочинністю в Україні

«…Согласно приговору Херсонского городского суда Херсонской области, ранее несудимый курьер ООО «Юридическая компания «Юг Гранд» разместил в даркнете объявление о продаже информации с ограниченным доступом. Парень предлагал к продаже сведения из баз данных Национальной полиции, Государственной фискальной службы, Главного сервисного центра МВД Украины, Интерпола (международной организации уголовной полиции), Государственной миграционной службы Украины, Государственной пограничной службы Украины, «Приватбанка», «Укрпочты», «Новой почты», а также детализированные телефонные соединения мобильных операторов Украины Vodafone, Киевстар, Lifecell…

8 мая между прокурором и обвиняемым было заключено соглашение о признании виновности. Обвиняемый полностью признал свою вину и обязался сотрудничать с правоохранительными органами…

Стороны согласовали наказание за совершенное преступление по ч. 1 ст. 361-2 УК Украины - в виде штрафа в 8500 грн…» ***(Владимир Кондрашов. Курьер зарабатывал на продаже баз данных МВД и мобильных операторов // InternetUA (http://internetua.com/kurer-zarabatyval-na-prodaje-baz-dannyh-mvd-i-mobilnyh-operatorov). 17.08.2018).***

***

«Лейтенант патрульной полиции решил через OLX продавать персональные данные, которые хранятся на базах данных Интегрированной информационно-поисковой системы органов внутренних дел МВД Украины…

Однако долго такой бизнес не просуществовал: одним из первых клиентов предприимчивого полисмена стал оперативник отдела противодействия киберпреступлениям в Ровенской области Полесского Управления киберполиции…

На судебном заседании обвиняемый свою вину в инкриминируемых ему преступлениях признал полностью.

Благодаря тому, что прокуратура и обвиняемый утвердили сделку о признании вины, суд назначил экс-полицейскому (по совокупности преступлений путем поглощения менее строгого наказания более строгим) окончательное наказание в виде лишения свободы на срок три года с лишением права занимать определенные должности или заниматься определенной деятельностью в органах Государственной власти Украины и органах местного самоуправления Украины на три года. Также суд освободил экс-копа от отбывания наказания и установил ему испытательный срок продолжительностью в один год.

Кроме условного срока, бывшему полицейскому придется ещё и оплатить штраф в 17 тысяч гривен и вернуть в доход государства 1300 гривен, заработанных на продаже информации…» ***(Владимир Кондрашов. Ещё одного полицейского поймали на продаже баз МВД // InternetUA (http://internetua.com/esxe-odnogo-policeiskogo-poimali-na-prodaje-baz-mvd). 17.08.2018).***

***

«…Працівники Київського управління Департаменту кіберполіції Національної поліції України задокументували протиправну діяльність 23-річного молодика, який розробив та поширював шкідливе програмне забезпечення.

…розроблена ним програма дозволяла її власнику отримувати несанкціонований доступ до захищених системами логічного захисту Інтернет-ресурсів. Відтак, її володілець отримував доступи до ігрових та криптобіржових акаунтів, після чого спустошував рахунки учасників криптовалютних бірж…

За даним фактом триває досудове розслідування за ч.2 ст.361 (незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж) КК України…» ***(Кіберполіція викрила хакера у створенні програми для викрадення коштів учасників криптовалютних бірж // Кіберполіція (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-stvorenni-programy-dlya-vykradennya-koshtiv-uchasnykiv-kryptovalyutnyx-birzh-839/). 16.08.2018).***

***

«Следственный отдел СУ ГУНП в Днепропетровской области подозревает пока неустановленных сотрудников территориальных подразделений Нацполиции в области в том, что они …злоупотребляя своим служебным положением, с целью получения неправомерной выгоды для себя и других физических лиц, с использованием Всемирной сети Интернет образовали сетевую активность вредоносного программного обеспечения, предназначенного для похищения паролей доступа пользователей и получения удаленного доступа к компьютерной технике граждан с дальнейшей добычей

криптовалюты на территории Днепропетровской области. Такими действиями полицейские нанесли значительный вред общественным интересам.

Следствием установлено, что для совершения уголовного преступления используется вредоносное программное обеспечение «stealer AZORult3» для похищения паролей доступа пользователей и получения удаленного доступа к компьютерной технике граждан с дальнейшей добычей на ней криптовалюты…

Проведенными мероприятиями установлено, что в результате распространения неустановленными лицами клиентской части указанного вредоносного ПО пораженные ПЭВМ граждан передавали собранную информацию в серверную часть с IP адресом 5.8.88.26, что фиксировалось в лог-файлах…» ***(Владимир Кондрашов. Полицейских опять подозревают в майнинге криптовалют // Internetua (http://internetua.com/policeiskih-opyat-podozrevauat-v-maininge-kriptovaluat). 29.08.2018).***

***

«30 серпня 2018 року Нікопольським міськрайонним судом Дніпропетровської області було розглянуто кримінальну справу про масштабні кібератаки вірусу PETYA (NOT PETYA)…

У судовому засіданні обвинувачений Н. визнав себе винним повністю. Вироком суду була затверджена угода про визнання винуватості, укладена між прокурором відділу процесуального керівництва Генеральної прокуратури України та обвинуваченим, у присутності захисника.

Громадянина визнано винуватим у скоєнні кримінального правопорушення передбаченого ч.1 ст.361-1 КК України і призначено узгоджене сторонами покарання у вигляді одного року позбавлення волі.

На підставі ст.75 КК України громадянина Н. звільнено від відбування призначеного покарання з випробуванням, з іспитовим строком один рік…» ***(Суд виніс вирок у справі вірусу «Petya» // «Українське право» (http://ukrainepravo.com/news/ukraine/sud-vynis-vyrok-u-spravi-virusu-petya-/). 31.08.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«…Росія запропонувала Сполученим Штатам спільну …роботу відповідальних російських і американських державних органів на ухвалення …заходів щодо недопущення дестабілізуючих дій на критичну інфраструктуру" Росії і США.

…таку пропозицію включили в проект заяви президентів РФ і США Володимира Путіна та Дональда Трампа на саміті в Гельсінкі.

…Москва запропонувала Вашингтону внести в документ пункт про неприпустимість "дестабілізуючих дій щодо внутрішніх політичних процесів, включаючи вибори". Вашингтон, однак, від цих ініціатив відмовився…» ***(США***

відмовили Росії в спільній боротьбі з кібератаками - Ъ // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/ssha-vidmovili-rosiyi-v-spilniy-borotbi-z-kiberatakami-285149_.html). 09.08.2018).

***

«Ассоциация государств Юго-Восточной Азии (АСЕАН) намерена заключить с Россией соглашение по кибербезопасности…

Планируется, что заявление будет опубликовано …4 августа, в последний день работы саммита стран АСЕАН, проходящего в Сингапуре…

В АСЕАН входят Бруней, Вьетнам, Индонезия, Камбоджа, Лаос, Малайзия, Мьянма, Сингапур, Таиланд и Филиппины.» ***(Страны АСЕАН собираются заключить с Россией соглашение по кибербезопасности // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3702553). 02.08.2018).***

***

«Сбербанк и Всемирный экономический форум объявили о подписании партнерского соглашения в рамках Центра кибербезопасности Всемирного экономического форума (С4С)…

Основными направлениями сотрудничества в рамках центра станут: автоматизированный обмен данными о современных киберугрозах на основе специальных платформенных решений; построение глобальной сети для взаимодействия оперативных центров реагирования на киберинциденты; формирование стратегии и выработка ключевых направлений развития индустрии кибербезопасности; создание глобального аналитического центра для сбора данных о текущей ситуации в киберпространстве и распространении данной информации в мировом сообществе…» ***(Сбербанк стал первым партнером-основателем Центра кибербезопасности ВЭФ // «Открытые системы» (https://www.computerworld.ru/news/Sberbank-stal-pervym-partnerom-osnovatelem-Tsentra-kiberbezopasnosti-VEF). 23.08.2018).***

***

Світові тенденції в галузі кібербезпеки

«…Компания Finn Partners Research опубликовала результаты исследования Cybersecurity at Work (Кибербезопасность на работе), в котором изучался уровень риска, создаваемый сотрудниками для своих организаций.

В ходе исследования были опрошены 500 штатных сотрудников компаний из США. Как следует из доклада, двое из пяти работников хотя бы раз нажимали на ссылку или открывали вложение от незнакомого отправителя.

Согласно исследованию, более половины сотрудников (55%) используют свои персональные устройства для работы, напрямую повышая риск кибератак, заражения вредоносными программами и утечек данных. Кроме того, только 26% сотрудников меняют свои учетные данные для личных и рабочих приложений не реже одного раза в месяц…

Помимо этого, только 25% сотрудников сообщили о ежемесячном прохождении инструктажей по кибербезопасности и своевременном обновлении программного обеспечения. Несмотря на подобное поведение, 93% респондентов считают, что их компания принимает все нужные меры по кибербезопасности для защиты личных и корпоративных данных. Более того, По словам 94% сотрудников, они делают все возможное, чтобы обеспечить безопасность данных своей компании.» ***(Эксперты назвали обучение кибербезопасности нечастым и непоследовательным // SecurityLabRu (https://www.securitylab.ru/news/494958.php). 08.08.2018).***

***

«Совет страховых агентов и брокеров (Council of Insurance Agents & Brokers, CIAB) опубликовал результаты опроса и аналитические выкладки о перестраховании в секторе кибербезопасности.

…результаты свидетельствуют об устойчивом росте этого вида перестрахования при стабильно низкой процентной ставке 32%.

89% респондентов считают, что величина премий остается неизменной, а емкость рынка отличается многочисленностью из-за притока страховщиков, которые осваивают новые направления страхования/перестрахования…

Согласно результатам опроса, брокеры отмечают проблемы в отсутствии ясности условий киберстрахования. Примерно 83% респондентов отмечают недостаточное понимание клиентами, что именно покрывается страховкой.» ***(Перестрахование киберрисков отличается устойчивым ростом и стабильными ставками // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/perestrahovanie-kiberriskov-otlichaetsya-ustoychivyim-rostom-i-stabilnyimi-stavkami). 06.08.2018).***

***

«Специалист по компьютерной безопасности Роджер Граймз решил выяснить, …машина какой мощности необходима для взлома современных асимметричных ключей. Опрошенные им специалисты сходятся в том, что для этого потребуется компьютер на примерно 4000 «совершенных» кубитов. То есть таких, в цепи которых не возникает ошибок…

Если же речь идет не о системе «совершенных» кубитов, а о высококачественном компьютере с редкими ошибками и системой их коррекции, речь может идти о «миллионе физических кубитов», прогнозирует профессор из Техасского университета в Остине Скотт Ааронсон.

Вопрос о том, как скоро будет создан такой квантовый компьютер, пока открыт…» ***(Спецслужбы всего мира архивируют шифровки в ожидании квантовых компьютеров // Goodnews.ua (http://goodnews.ua/technologies/specsluzhby-vsego-mira-arxiviruyut-shifrovki-v-ozhidanii-kvantovyx-kompyuterov/). 07.08.2018).***

***

«Безопасность наших онлайн-жизней становится все более важной. Будь то вмешательство в выборы, нападения враждебных сил или онлайн-мошенничество, безопасность Интернета кажется хрупкой. Нам нужно решить, куда двигаться дальше…

В одном направлении – балканизация, фрагментация и изоляция индустрии. Балканизация — естественный ответ на страх и недоверие, но для кибербезопасности она означает растущее политическое вмешательство и срыв международных проектов и сотрудничества. Так, каждая страна будет противостоять глобальным киберугрозам самостоятельно. Для потребителей это чревато высокими издержками, поскольку предприятия стремятся компенсировать расходы на кибербезопасность, а также снижением уровня защиты, так как конкуренция и выбор ограничены.

В другом направлении — сотрудничество и совместная разведка, партнерство между национальными полицейскими силами и компаниями кибербезопасности: объединенное сообщество против киберугроз. Такая стратегия будет стимулировать конкурентоспособную индустрию кибербезопасности, которая ведет к лучшим технологиям и более эффективной защите…

Интернет-угрозы становятся более изощренными и серьезными…

Государства, естественно, хотят защитить своих граждан, предприятия, инфраструктуру и отрасли от этих угроз. И самый простой, однако наименее эффективный способ сделать это – "закрыть дверь".

Тенденция "закрытия дверей" реальна: отрасль делят геополитическими и нормативными барьерами. …За последние несколько лет в Европейском союзе, Великобритании, США, России, Германии, Сингапуре и Китае были введены новые строгие требования. Такое регулирование может привести к протекционизму и войне в киберпространстве. Более 30 стран уже объявили о военных кибердивизиях, а фактическая цифра, вероятно, даже выше. Киберпространство милитаризируется с ужасающей скоростью.

Что это значит для нас? Помимо обычных недостатков милитаризации, таких как более высокие налоги и неопределенность, есть еще один: рано или поздно кибероружие попадет в руки злоумышленников…

Способ борьбы — это партнерство, а не изоляция...» ***(Если мы будем бороться только с кибератаками, мы обречены на провал // Goodnews.ua (http://goodnews.ua/technologies/esli-my-budem-borotsya-tolko-s-kiberatakami-my-obrecheny-na-proval/). 01.08.2018).***

***

«Самым сложным месяцем с точки зрения кибербезопасности является август, следует из данных DeviceLock DLP. На этот месяц приходится почти 20% всех инцидентов, связанных с неправомерным доступом и копированием конфиденциальных данных сотрудниками компаний. Это связано с повышенным количеством отпусков и увольнений, готовясь к которым, сотрудники копируют внутренние документы, считают эксперты.

…чуть более половины утечек корпоративных данных происходит по вине инсайдеров, а не хакеров, и доля таких утечек растет. При этом большинство

сотрудников не считают такие случаи нарушениями. Чаще всего похищаются персональные данные клиентов (около 50%), которые затем попадают к конкурентам или на рынки спам-рассылок. На втором месте — объекты авторских прав: тексты, программный код, изображения и видео (около 35%), на третьем — финансовые и иные документы (около 15%). Наименее защищена сфера обслуживания, в первую очередь — салоны красоты, автомобильные и компьютерные сервисы, частные медицинские клиники, event-агентства…» **(Кристина Жукова. Кадры выносят всё // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3708218?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). 09.08.2018).**

***

«Центральные банкиры Европы предупреждают, что постепенный отказ от бумажных денег, который происходит во многих странах, - это серьезная угроза для финансовой системы.

…регуляторы настаивают, что технологические ошибки и систематические атаки доказывают необходимость сохранения в обращении наличности. Кроме того, они подчеркивают, что в безналичном мире наиболее уязвимые группы населения, которые больше других нуждаются в наличности, станут отчужденными от всех других.

Исследование Европейского Центрального Банка показало, что почти 80% всех платежей в еврозоне осуществляются с помощью наличных. Однако, некоторые страны, такие как Эстония, Нидерланды и Финляндия, полагаются на электронные платежные системы в 50% от всех транзакций. В Швеции в магазинах наличными рассчитываются только в 13% случаев. А больше половины отделений банков в стране даже не держат бумажных денег…

Перебои в работе платежной системы Visa в июне, которые произошли из-за технических проблем, дали небольшой, но реальный шанс проверить все риски, - настаивает профессор кибербезопасности ирландского Университета Ульстер Кевин Курран…

Движение в направлении отказа от наличных денег происходит частично из коммерческих соображений. Поскольку бизнесы переходят только на электронные расчеты ради эффективности и в ответ на требования клиентов. Некоторые правительства поощряют переход на электронные услуги, потому что они видят в этом решение проблем с отмыванием денег и налоговым мошенничеством. Кроме того, это позволяет повысить конкуренцию в финансовом секторе. Другие утверждают, что электронные платежи защищают людей от ограблений. Также электронные деньги нельзя потерять…» ***(Банкиры Европы прогнозируют хаос после отмены бумажных денег // Телеграф (https://telegraf.com.ua/mir/europa/4374731-bankiryi-evropyi-prognoziruyut-haos-posle-otmenyi-bumazhnyih-deneg.html). 16.08.2018).***

***

«…Исследователи Ponemon Institute опросили 650 специалистов в области IT и ИБ с целью выявить проблемы, с которыми сталкиваются компании при реализации защиты конечных пользователей от угроз, связанных с электронной почтой. Одной из таких угроз являются вредоносные электронные письма, имитирующие легитимные письма от доверенных отправителей.

По словам 79% опрошенных, за последние 12 месяцев их организации столкнулись с серьезными кибератаками или утечками данных, но только 29% предприняли существенные меры по предотвращению фишинговых атак с использованием поддельных электронных писем.

65% опрошенных намерены реализовать для защиты от спама и фишинга технологию DMARC.

Только 27% респондентов сообщили, что их компании хорошо знают всех поставщиков и все сервисы, отправляющие корреспонденцию, используя доменное имя организации в поле «От:», где указывается отправитель.

Почтовая инфраструктура компаний, как правило, весьма сложная. …В почтовую инфраструктуру этих компаний в среднем входят шесть серверов и 15 облачных сервисов. Однако только в 41% организаций действует инфраструктура по обеспечению безопасности, в том числе электронных сервисов.

Несмотря на низкую эффективность спам-фильтров, они являются главным средством защиты от поддельных писем, используемым на предприятиях (спам-фильтры используются на 69% предприятий)…» ***(Компании переоценивают свои силы по защите от атак с использованием поддельных писем // Goodnews.ua (http://goodnews.ua/technologies/kompanii-pereocenivayut-svoi-sily-po-zashhite-ot-atak-s-ispolzovaniem-poddelnyx-pisem/). 14.08.2018).***

***

Сполучені Штати Америки

«**Американские вооруженные силы запрещают своим сотрудникам использовать функции геолокации на смартфонах, фитнес-трекерах и других устройствах, поскольку они могут создавать угрозы безопасности, раскрывая местоположение.**

…На прошлой неделе Пентагон обнародовал меморандум, согласно которому геолокация представляет собой "значительный риск".

"Геолокация может раскрывать персональную информацию, местоположения, распорядок и количество сотрудников Департамента, создавать непреднамеренные последствия для безопасности и увеличивать риск", - сообщается в меморандуме…» ***(Ирина Фоменко. Пентагон запретил военным использовать геолокацию // Internetua (http://internetua.com/pentagon-zapretil-voennym-ispolzovat-geolokaciua). 08.08.2018).***

***

«Адміністрація президента США Дональда Трампа запросила 15 млрд доларів на наступний рік для забезпечення безпеки у кіберпросторі. Про це заявив віце-президент США Майкл Пенс у вівторок на форумі з питань кібербезпеки…

В якості одного з супротивників США в кіберпросторі віце-президент назвав Росію. "Наші кіберпротивники прагнуть потрапити в ті елементи інфраструктури, що мають найважливіше значення, включаючи енергосистему і електростанції, щоб в разі можливих конфліктів в майбутньому вони могли паралізувати нервовий вузол американської енергетики", — заявив Пенс…

США потрібно нове федеральне відомство, що займається питаннями забезпечення безпеки у кіберпросторі, зокрема, для забезпечення безпеки виборчого процесу, додав Пенс.» ***(Олексій Супрун. Трамп просить надати 15 млрд доларів у рік на кібербезпеку // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1744407-tramp-prosit-nadati-15-mlrd-dolariv-u-rik-na-kiberbezpeku). 01.08.2018).***

***

«Табіта Існер, яка балотується в Конгрес у штаті Алабама, заявила, що в середині липня хакери здійснили 1,4 тис. спроб зламати сайт її виборчої кампанії. За словами політика, перевірка показала, що не менш ніж 1100 атак було скоєно з російських IP-адрес, а також серверів в Україні та в Казахстані…

Жодна зі спроб злому не опинилася успішною. Як повідомила Існер, її виборчий штаб зв'язався з ФБР, яке почало розслідування інциденту.

…Про хакерські атаки заявляли і нинішні депутати від Демократичної партії — Клер Маккаскілл і Джина Шахін. Обидві вважають кібератаки реакцією на їх жорстку позицію по відношенню до Кремля.» ***(Самуїл Проскуряков. Кандидат у Конгрес США звинуватила російських хакерів у спробі злому сайту її штабу // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1745479-kandidat-u-kongres-ssha-zvinuvatila-rosiyskikh-khakeriv-u-sprobi-zlomu-saytu-yiyi-shtabu). 07.08.2018).***

***

«Федеральне бюро розслідувань США займається з'ясуванням обставин кібератаки на виборчу кампанію кандидата від Демократичної партії Девіда Міна, який балотується др Конгресу США від Каліфорнії…

Джерела пояснили, що невстановлені хакери зламали комп'ютер передвиборного штабу Девіда Міна, що призвело до поразки кандидата на червневих попередніх виборах.

…прес-секретар ФБР заявила, що не може ні підтвердити, ні спростувати цю інформацію…

Експерти національної безпеки США висловили стурбованість тим, що політичні кампанії виявилися "не захищені напередодні виборів у Конгрес", які пройдуть в листопаді 2018 року. При цьому у короткий час захистити кандидатів від атак не вийде - за словами дослідника кібербезпеки і колишнього аналітика Агентства національної безпеки Блейка Дарча, для створення ефективної програми

безпеки потрібні роки…» ***(ФБР розслідує ще одну кібератаку на кандидата до Конгресу // "Дзеркало тижня. Україна" (https://dt.ua/WORLD/fbr-rozsliduye-sche-odnu-kiberataku-na-kandidata-do-kongresu-285970_.html). 18.08.2018).***

***

«Сейчас, когда до промежуточных выборов в США остается менее 100 дней, появляется все больше доказательств того, что электоральная система Америки остается желанной мишенью для хакеров, а, самое примечательное, для агентов российского правительства», - пишет The New York…

"…Несмотря на многократные предостережения об уязвимых местах страны, исходящие от разведслужб США, у Белого дома все еще нет никакого целеустремленного, слаженного плана для решения этой ключевой проблемы безопасности. А у президента Трампа, похоже, вызывает дискомфорт идея критиковать и уж тем паче привлекать к ответственности самого злокозненного из злокозненных акторов, идентифицированных американскими разведслужбами, - Путина"…

"На данный момент практически весь Вашингтон, за исключением Трампа (и кучки его подхалимов из Конгресса), признает угрозу, исходящую от России", - пишет издание…» ***(Россия атакует электоральную систему Америки. Трамп пожимает плечами // Украинское рейтинговое агентство "УРА" (http://ura-inform.com/ru/interesno/2018/08/03/rossija-atakuet-elektoralnuju-sistemu-ameriki-tramp-pozhimaet-plechami). 03.08.2018).***

***

«Министерство внутренней безопасности США было вынуждено временно отключить от интернета …с 26 июля …две программы, проводимые командой Национальным центром кибербезопасности и интеграции коммуникаций (National Cybersecurity and Communications Integration Center, NCCIC) National Cybersecurity Assessments and Technical Services (NCATS) – Cyber Hygiene и Phishing Campaign Assessment. Cyber Hygiene предназначена для удаленного обнаружения известных уязвимостей в подключенных к интернету сервисах. Программа Phishing Campaign Assessment является частью сервиса по тестированию на проникновение. Обе программы используются сотнями клиентов по всей территории США. По данным Министерства внутренней безопасности, результаты сканирования с помощью Cyber Hygiene получают 34 штата.

Из-за сильных ливней здание NCCIC сильно пострадало. Днем 26 июля часть фасада и потолок на первом этаже обвалились, а электрическая сеть была полностью выведена из строя. Из-за сбоя в электроснабжении в серверных комнатах перестали работать системы охлаждения, и как только температура достигла определенного уровня, сработала противопожарная система, залившая серверы водой. В результате серверы, используемые Cyber Hygiene и Phishing Campaign Assessment, также вышли из строя.» ***(Сканер уязвимостей Министерства внутренней безопасности США был залит водой // Goodnews.ua (http://goodnews.ua/technologies/skaner-uyazvimostej-ministerstva-vnutrennej-bezopasnosti-ssha-byl-zalit-vodoj/). 02.08.2018).***

***

«По данным Комиссии обеспечения выборов США… две трети суммы, которую Конгресс США выделил на обеспечение безопасности процедуры выборов, власти американских штатов планируют потратить на закупку нового оборудования и новые программы кибербезопасности. Из $380 млн, выделенных Конгрессом, на закупку оборудования пойдет $102,6 млн, а на обновление программ — $134,2 млн.

…за получением средств по этой статье к правительству обратились все штаты и территории США, и на данный момент 96% всей суммы уже перечислены им. При этом не все штаты успеют закупить оборудование и обновить программы до ноябрьских выборов в Конгресс, большинство рассчитывают реализовать планы усиления кибербезопасности в течение двух-трех ближайших лет.» ***(Алена Миклашевская. США выделяют на кибербезопасность выборов $380 млн // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3719795). 21.08.2018).***

***

«…Представитель офиса директора национальной разведки США Ланая Джонс (LaNaia Jones) заявила о нехватке квалифицированных специалистов в сфере кибербезопасности…

Помимо этого, по словам представителя ФБР Джона Адамса (John Adams), данную проблему нельзя решить простым увеличением количества специалистов. У экспертов недостаточно времени и ресурсов на обработку невероятно большого объема поступающих данных. В качестве возможного решения он назвал разработку системы искусственного интеллекта.

Как сообщил Адамс, в настоящее время ФБР работает над созданием самообучающихся машин, способных отслеживать подозрительную активность в киберпространстве.» ***(США не хватает специалистов для борьбы с киберугрозами // SecurityLabRu (https://www.securitylab.ru/news/495253.php). 23.08.2018).***

***

«Сегодня утром президент США Дональд Трамп в Twitter …процитировал статью издания The Daily Caller о том, что китайские хакеры взломали электронную почту его соперницы по президентским выборам, члена Демократической партии Хиллари Клинтон. Господин Трамп возмутился кражей большого объема секретной информации…

Через несколько часов господин Трамп написал еще одно сообщение в Twitter, в котором сам факт взлома почты китайскими хакерами уже не подвергался сомнению: «E-mail Хиллари Клинтон с большим количеством секретной информации взломан Китаем. Следующий шаг должны были бы сделать ФБР и Минюст, или после всех остальных провалов (Коми, Маккейб, Сток, Пейдж, Ор, FISA, "грязное досье" и прочее) доверие к ним уйдет навсегда»…

Представитель госпожи Клинтон Ник Мерилл отрицает любые заявления о взломе почты своего шефа…» ***(Кирилл Кривошеев. Дональд Трамп обвинил***

Китай во взломе почты Хиллари Клинтон. Президент США возмущен кражей «большого объема секретной информации» // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3726281?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). 29.08.2018).

***

«Після того, як президент США Дональд Трамп звинуватив Китай у зломі електронної пошти колишнього держсекретаря Хілларі Клінтон, Федеральне бюро розслідувань заявило, що не має доказів цієї заяви…

Представник ФБР відмовився прокоментувати заклик Трампа зробити "наступний крок"…» ***(Самуїл Проскуряков. ФБР спростовує заяву Трампа про злом сервера Клінтон компанією з Китаю // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1749378-fbr-sprostovuye-zayavu-trampa-pro-zlom-servera-klinton-kompaniyeyu-z-kitayu). 30.08.2018).***

***

«По мнению высокопоставленных членов комитета Сената по делам вооруженных сил США, Пентагон не предпринимает достаточно усилий для того, чтобы уберечь сугубо технические, но не засекреченные данные от попадания в руки хакеров.

В письме, направленном министру обороны Джиму Мэттису, утверждается, что «министерство обороны попросту не предпринимает достаточных мер, чтобы защитить незасекреченную информацию»…

Поводом для письма стал июньский сюжет в газете Washington Post. В нем сообщалось, что ранее китайские хакеры получили доступ к данным небольшой фирмы-подрядчика, работавшей с Центром подводной войны в Ньюпорте штата Род-Айленд.

Законодатели полагают, что «необходимо предпринять немедленные действия, чтобы привести практику в соответствие с существующими нормами и имеющимся опытом, а также повысить стандарты кибербезопасности для оборонных подрядчиков».

Как пишет аналитик в области информационной безопасности Марк Риддл, новые директивы безопасности, принятые в 2015 году Пентагоном, столкнулись с некоторым сопротивлением со стороны промышленников и других негосударственных структур. Это произошло в связи с тем, что новые требования сочли слишком строгими…» ***(Анастасия Норина. Важные данные Пентагона «оказались под угрозой» из-за проблем в кибербезопасности // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/23/938597.html). 23.08.2018).***

***

«Национальный центр кибербезопасности Литвы изучил «угрозы», которые якобы могут исходить от сервиса «Яндекс.Такси», выяснив, что у программы есть активная связь с 11 адресами в России…

В связи с этим центр кибербезопасности рекомендует не устанавливать этот сервис, в особенности это касается госслужащих и должностных лиц министерства обороны Литвы…» ***(Сергей Гурьянов. Литва разъяснила суть претензий к «Яндекс.Такси» // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/3/935528.html). 03.08.2018).***

***

«Яндекс.Такси» в ответ на претензии Литвы относительно связи сервиса с серверами в России заявляет, что это не имеет никакого отношения к хранению данных пользователей ЕС…

В компании пояснили, что данные пользователей «хранятся и используются полностью в соответствии с законодательством ЕС и, в частности, GDPR (Общий регламент по защите данных ЕС)». Также отмечается, что строго соблюдаются требования владельцев смартфонов с платформами Andoid и iOS по работе с пользовательской информацией…» ***(Сергей Гурьянов. В «Яндекс.Такси» ответили на претензии Литвы // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/3/935562.html). 03.08.2018).***

***

«В понедельник, 13 августа правительство Литвы утвердило Национальную стратегию кибербезопасности. Документ подготовлен министерством обороны…

Документ гласит, что в последние годы в Литве увеличилось число кибератак против общественного и энергетического секторов, аэропортов, средств массовой информации и на инфраструктуры важных для национальной безопасности объектов…» ***(Юрий Виноградов. Литва решила защититься от «российских хакеров» // «Парламентская газета» (https://www.pnp.ru/in-world/litva-reshila-zashhititsya-ot-rossiyskikh-khakerov.html). 13.08.2018).***

***

«Міністерство оборони Литви, підпорядкований йому Національний центр кібернетичної безпеки і литовські ЗМІ у вівторок підписали угоду про співпрацю в сфері кібербезпеки

…угода підписана у зв'язку з тим, що в останні роки майже всі найбільші ЗМІ Литви пережили кібернетичні атаки.

…Міністерство оборони Литви і Національний центр кібернетичної безпеки планують запрошувати фахівців з інформаційних технологій засобів масової інформації для участі в навчаннях, а також спілкуватися і обмінюватися інформацією, надавати допомогу на випадок кібератак.

Угода передбачає можливість участі представників ЗМІ в засіданнях Ради з кібернетичної безпеки і спільного тестування імунітету до атак хакерів…» ***(ЗМІ Литви співпрацюватимуть з урядом для протидії хакерам // Espreso.tv (https://espreso.tv/news/2018/08/29/zmi_lytvy_spivpracyuvatymut_z_uryadom_dlya_protydiyi_khakeram). 29.08.2018).***

***

«Федеральний уряд Німеччини 29 серпня ухвалив рішення створити дві спеціалізовані агенції: з інновацій і з кібербезпеки…

Агенція з інновацій у кібербезпеці розпочне роботу 2019 року. У міністерстві оборони ФРН заявили, що протягом наступних п'яти років вона отримає для свого розвитку 200 мільйонів євро. 80% фінансування перерахують на дослідження розробок. Планується, що в новій агенції працюватиме близько 100 співробітників…» ***(Німецький уряд створить агенції з інновацій і кібербезпеки // MediaSapiens(http://ms.detector.media/web/cybersecurity/nimetskiy_uryad_stvorit_agentsii_z_innovatsiy_i_kiberbezpeki/). 30.08.2018).***

***

«В рамках полицейской операции по защите Великобритании от атак киберпреступников 14-летний парень оттачивает свои навыки, чтобы помешать хакерам… Бен Абрамасон был в группе, собравшейся на военной базе в Уилтшире в пятницу, чтобы противостоять вымышленным, но сложным кибератакам…

Он сдал онлайн-тесты, чтобы провести день с экспертами из Национального агентства по борьбе с преступностью. Полиция заявляет, что для них важно привлечь талантливых хакеров…

Была еще одна причина для пятничного события: нехватка навыков угрожает быстро растущему сектору кибербезопасности. Роберт Ханниган, бывший глава GCHQ, агентства разведки и безопасности, предсказал "огромный дефицит навыков" к 2025 году.

Глава отдела подготовки профессиональной квалификации в области кибербезопасности в Национальном агентстве по борьбе с преступностью Крейг Джонс предупредил, что, если Великобритания не сможет нанять экспертов высшего уровня, она не сможет препятствовать злоумышленникам…» ***(Ирина Фоменко. Великобритания привлекает молодых хакеров для защиты киберпространства // InternetUA (http://internetua.com/velikobritaniya-privlekaet-molodyh-hakerov-dlya-zasxity-kiberprostranstva). 20.08.2018).***

***

Китай

«…За два последних дня крупнейшие китайские соцсети Momo, Weibo и YY потеряли от 11% до 17% стоимости… Вместе с ними опустились котировки Baidu и Tencent. Причина в том, что Администрация киберпространства Китая

начала официальное расследование, не нарушают ли платформы социальных медиа новый закон по кибербезопасности.

Предварительные результаты данного расследования китайских властей показали, что пользователи платформ распространяли слухи, порнографию и информацию террористического характера, что угрожает общественной безопасности. Нарушения закона будут наказываться, но пока не известно каким образом.

Еще одним рычагом давления на интернет бизнес стала заморозка одобрения китайскими властями лицензий на онлайн-игры…

Усиление контроля над онлайн-играми и потоковым видео затронет весь китайский интернет-сектор. Практически все соцсети в КНР предоставляют широкий спектр онлайн-трансляций развлекательного контента, в том числе игрового…»***(Усиление цензуры в Китае ударило по интернет-бизнесу // РосКомСвобода (https://roskomsvoboda.org/40965/). 16.08.2018).***

***

«Правительство КНР использует 300 так называемых «национальных стандартов кибербезопасности», чтобы не дать иностранным технологическим компаниям попасть на китайских рынок. Такие выводы содержатся в отчете американского Центра стратегических и международных исследований (The Center for Strategic and International Studies, CSIS).

Вышеупомянутые стандарты представляют собой …рекомендации по проектированию и функционалу целого ряда продуктов с точки зрения кибербезопасности. Рекомендации касаются таких продуктов, как маршрутизаторы, межсетевые экраны и даже программное обеспечение.

Некоторые стандарты описывают методы предоставления правительству доступа к конфиденциальным данным китайских граждан, обрабатываемым определенными сервисами или устройствами. Одни стандарты касаются допустимых алгоритмов шифрования, тогда как другие описывают требования к технологиям передачи данных за пределами страны.

По уверению китайских властей, в настоящее время стандарты носят лишь рекомендательный характер. Тем не менее, согласно отчету CSIS, многие из них являются обязательными для выполнения китайскими компаниями…» ***(Китайские «стандарты кибербезопасности» направлены на борьбу с конкурентами // Goodnews.ua (http://goodnews.ua/technologies/kitajskie-standarty-kiberbezopasnosti-napravleny-na-borbu-s-konkurentami/). 21.08.2018).***

***

Російська Федерація та країни ЄАЕС

«…В начале июля ряд файлов пользователей облачного сервиса Google Docs оказались доступны в поисковой выдаче «Яндекса». Доступными оказались те файлы, владельцы которых сами разрешили к ним доступ по гиперссылке.

Роскомнадзор направил запрос в «Яндекс» по утечке данных. В ответ в интернет-компании заявили, что поисковый сервис «индексирует содержание интернет-ресурсов, которое не закрыто настройками защиты от соответствующего индексирования».

После утечки Google сообщил в официальном блоге, что поисковые системы могут индексировать только публичные документы...» ***(Роскомнадзор направил запрос в Google по утечке данных Google Docs // «Открытые системы» (https://www.computerworld.ru/news/Roskomnadzor-napravil-zapros-v-Google-po-utechke-dannyh-Google-Docs). 19.08.2018).***

***

«В АНО «Цифровая экономика» разработали законопроект, согласно которому, …получив данные человека с его согласия, компания дальше сможет самостоятельно ими распоряжаться и передавать на обработку подрядчику без уведомления владельца. Подрядчик, в свою очередь, также сможет передавать информацию, но только уведомив компанию-заказчика. Отвечать за сохранность персональных данных будет компания, которая первоначально получила согласие человека на их обработку…

При правильном регулировании новый порядок обращения с персональными данными поможет бизнесу оптимизировать их обработку, а для граждан сделает оборот данных более прозрачным и подконтрольным, предполагает представитель «Ростелекома».

Есть и не согласные с идеей, зафиксированной в поправках. Человек потеряет четкий контроль за передачей его персональных данных и станет бесправным в этом процессе, комментирует документ директор по правовым инициативам Фонда развития интернет-инициатив (ФРИИ) Александра Орехович: он разрешает нынешним и будущим – любым партнерам компании распоряжаться данными без ведома человека. Такой подход, по мнению Орехович, нарушает права пользователя. Данные могут принадлежать только субъекту и только он может ими распоряжаться, присваивать его данные себе не может никто, непреклонна она…» ***(«Цифровая экономика»: персональные данные можно сливать // РосКомСвобода (https://roskomsvoboda.org/40990/). 17.08.2018).***

***

Інші країни

«Лидер партии «Йеш Атид» Яир Лапид (Yair Lapid) в понедельник поднял вопрос о кибербезопасности, чтобы гарантировать, что на следующих всеобщих выборах в Израиле стороны и кандидаты не будут распространять «фальшивые новости» об их политических противниках.

Эта инициатива включала обращение в центральную избирательную комиссию ходатайство, которое будет отправлено всем сторонам. В ходе этого стороны пообещают играть честно перед выборами 2019 года…

«В ближайшие месяцы в Израиле пройдут выборы, которые, как всегда, будут агрессивными, вредными и интенсивными, - написал Лапид на своей странице в Facebook. - Но теперь всё может быть по-другому. Ведь велики шансы, что на этих выборах будут использоваться кибер-технологии, которые могут повлиять на результаты и, возможно, даже подделать их». ***(Яир Лапид просит избирательную комиссию не допустить "фальшивые новости" // ISRAland (http://www.isra.com/news/219113). 20.08.2018).***

***

«Израильское агентство по инновациям, Министерство экономики и промышленности и Национальное управление по кибербезопасности объявили о новой трехлетней программе стоимостью 24 млн. долларов США, направленной на развитие кибер-индустрии Израиля.

…Программа трехсторонняя: она будет инвестировать в технологии, которые будут восприниматься как «изменяющие игру»; она будет поддерживать более крупные компании, которые переходят с этапа разработки, финансируя пилотные испытания своих технологий с потенциальными клиентами; и увеличит ресурсы для CyberSpark, израильской кибер-инновационной арены в Беэр-Шеве, чтобы еще больше укрепить свои позиции в качестве глобального центра кибербезопасности.» ***(Израиль выделил 24 миллиона долларов на новую программу по активизации стартапов в сфере кибербезопасности // ISRAland (http://www.isra.com/news/218857). 14.08.2018).***

***

«Администрация аэропортов Израиля открыла центр киберзащиты из-за увеличения количества кибератак на системы авиаузлов. Базой для нового центра стала воздушная гавань им. Давида бен-Гуриона (Тель-Авив)…

Благодаря новой IT-технологии при фиксировании кибератаки, которая может нанести угрозу деятельности аэропорта, компьютер, на котором она обнаружена, немедленно изолируется от аэропортовых систем.

Центр работает в полном сотрудничестве с Национальным кибернадзором Израиля (INCD), который занимается киберзащитой на национальном уровне…» ***(В аэропорту Тель-Авива открыли центр защиты от кибератак // ЦТС (https://cfts.org.ua/news/2018/08/14/v_aeroportu_tel_aviva_otkryli_tsentr_zaschity_ot_kiberatak_48869/). 14.08.2018).***

***

«Правительство Австралии запретило китайским компаниям Huawei и ZTE поставлять в страну телекоммуникационное оборудование для сетей связи 5G.

В правительстве, как говорится в заявлении, проделали большую работу по анализу угроз для национальной безопасности, связанных с сетями 5G. Технологии 5G значительно отличаются от технологий предыдущих поколений, и эти отличия увеличивают потенциальные угрозы для телекоммуникационных сетей. …В правительстве считают, что участие в строительстве сетей компаний, которые

могут быть обязаны подчиняться внесудебным указаниям зарубежных государственных органов, противоречащим австралийскому законодательству, поставит под угрозу способность операторов связи защитить сеть от несанкционированного доступа.

В компании Huawei заявляют, что решение австралийских властей чрезвычайно досадно для потребителей. Huawei, говорится в заявлении компании, является мировым лидером в области 5G и поставляет надежное и безопасное беспроводное оборудование в Австралию уже почти 15 лет.» ***(Власти Австралии наложили запрет на поставки продукции Huawei и ZTE для сетей 5G // «Открытые системы» (https://www.computerworld.ru/news/Vlasti-Avstralii-nalozhili-zapret-na-postavki-produktsii-Huawei-i-ZTE-dlya-setey-5G). 27.07.2018).***

***

Протидія зовнішній кібернетичній агресії

«У США готуються до ймовірних кібератак, які Іран може завдати у відповідь на повторне введення санкцій цього тижня президентом США Дональдом Трампом…

"Хоча поки що ми не маємо жодних конкретних загроз, ми спостерігаємо збільшення чуток, пов'язаних з іранською загрозою, протягом останніх декількох тижнів", - заявила директор з розробки стратегічних загроз у компанії Recorded Future Прісцилла Моріучі.

Компанія, що базується в штаті Массачусетс, ще в травні передбачала, що виведення США з ядерної угоди спровокує кібер-відповідь уряду Ірану протягом двох-чотирьох місяців…

Компанія Accenture Security, глобальна компанія з консалтингу, управління та технологій, також попередила у вівторок, що нові санкції, "ймовірно, спонукатимуть цю країну активізувати діяльність, що фінансується державою", в тому числі, якщо Іран не зможе зберегти своїх європейських колег відданими ядерному пакту…» ***(Саша Картер. США очікує помсти від Ірану у кіберпросторі – ЗМІ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1745804-ssha-ochikuye-pomsti-vid-iranu-u-kiberprostori-zmi). 08.08.2018).***

***

«В Белом доме подготовили перечень мер по борьбе с кибератаками на американскую инфраструктуру, которые якобы поддерживаются Россией.

В администрации президента США разработали план по противодействию хакерским атакам и привлечению хакеров к ответственности…

Отмечается, что о разработке подобных мер в правительстве США задумались после взлома американских энергетических компаний российскими хакерами.

Предполагается, что ответные меры будут нацелены на самих хакеров, а не на инфраструктуру страны, откуда совершена атака.

Также, согласно новым мерам, хакеров будут объявлять в розыск, в том числе через Интерпол…» ***(В США решили ужесточить борьбу с хакерами // Телеграф (https://telegraf.com.ua/mir/usa/4337943-v-ssha-reshili-uzhestochit-borbu-s-hakerami.html). 07.08.2018).***

***

«Держави-члени ЄС повинні вжити заходів проти можливих кібератак під час виборів до Європарламенту, які заплановані на травень 2019 року. Про це заявив єврокомісар з питань безпеки Джуліан Кінг…

"Хакери атакують виборчу кампанію з допомогою неправдивої інформації або фейкових новин, які здатні впливати на громадську думку", - заявив єврокомісар…

Єврокомісар закликав соціальні мережі, зокрема, Facebook і Youtube, до більш змістовної боротьби з дезінформацією. На його думку, повинні існувати чіткі правила, які будуть заважати роботам видавати себе за користувачів інтернету…

Єврокомісія вважає одним з невідкладних заходів розробку інтернет-платформами кодексу поведінки…» ***(Юлія Шрамко. У ЄС попередили про загрозу кібератак на виборах до Європарламенту // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1744477-u-yes-poperedili-pro-zagrozu-kiberatak-na-viborakh-do-yevroparlamentu). 01.08.2018).***

***

«В США предложили свести в единую систему все санкции против России. Для этого в американском правительстве хотят создать «санкционный координационный офис», который будет вести переговоры со странами Европейского союза о поддержке санкций**.**

«Законопроект предполагает объединение всех вводившихся отдельными актами антироссийских санкций, от «украинских» до «кибертеррористических», в единый механизм», — говорится в «Акте по защите американской безопасности от агрессии Кремля 2018»…

Республиканцы предлагают предъявлять федеральные обвинения лицам, причастным к кибератакам на системы, связанные с выборами…

Документ был внесен в Сенат членами Республиканской партии 2 августа, однако его полный текст до сих пор не опубликован на сайте Конгресса…» ***(В США предложили свести в единую систему, от «украинских» до «кибертеррористических», все санкции против России // Черноморские новости (https://www.blackseanews.net/read/143482). 08.08.2018).***

***

«Самая масштабная в истории Сингапура кибератака была осуществлена по заказу правительства иностранного государства, …в результате которого произошла утечка данных 1,5 млн человек, включая премьер-министра…

Власти Сингапура сообщили об утечке 20 июля текущего года, хотя сам инцидент имел место в конце июня. В ходе атаки злоумышленники похитили персональные данные и записи о лекарственных препаратах, выписанных амбулаторным пациентам сингапурских больниц за последние три года.

Министр связи отказался называть источник кибератаки из соображений безопасности. Тем не менее, С. Исваран отметил, что она была осуществлена «группой Advanced Persistent Threat» (APT-группой), а подобные группы, как правило, связаны с правительством. По словам министра, спецслужбам Сингапура известно, кто стоит за атакой, однако собранных доказательств недостаточно для предъявления официального обвинения…» ***(За самой масштабной кибератакой на Сингапур стоит иностранное правительство // Goodnews.ua (http://goodnews.ua/technologies/za-samoj-masshtabnoj-kiberatakoj-na-singapur-stoit-inostrannoe-pravitelstvo/). 08.08.2018).***

***

«В Италии разгорается конфликт вокруг информации о вмешательстве российских "троллей" в знаковые события итальянской политики…

В понедельник после обеда специальный парламентский комитет по вопросам безопасности, осуществляющий надзор за деятельностью секретных служб Италии (COPASIR), должен заслушать доклад главы Департамента по информации и вопросам безопасности (DIS, одна из трех разведывательных служб Италии).

COPASIR ранее уже обращал внимание разведки на попытки внешнего воздействия через интернет на итальянские выборы, но тогда не хватило доказательств.

… На днях будет открыто производство по факту возможных онлайн-атак против главы Итальянской Республики в мае этого года…

Конечно, подтверждение интернет-атаки на Италию в мае само по себе мало что изменит, но может дать толчок к дальнейшим законотворческим действиям…» ***(Виктория Вдовиченко. Ольгино против президента Италии: что известно об атаке с почерком российской "фабрики троллей" // Европейская правда (https://www.eurointegration.com.ua/rus/articles/2018/08/6/7085261/). 06.08.2018).***

***

«…В Гудзоновском институте с получасовым сообщением выступил директор Национальной разведки Дэн Коутс… координатор разведывательных служб США (их в стране семнадцать)…

Начал Коутс свое выступление, заявив, что …кибератаки разной степени интенсивности на объекты в США регулярно проводят четыре государства: Китай, Россия, Иран и Северная Корея. Самые большие технологические ресурсы для подобной деятельности имеются у Китая. Вторая в этом ряду – Россия. Но характер криминального поведения Китая и России, по словам Коутса, принципиально различен.. . Да, китайцы стремятся украсть уникальные высокие технологии, чтобы успешнее конкурировать с теми же США. А русские занимаются в киберсфере совершенно иным: ничего воровать они не собираются, а ориентированы (так же

как в свое время организаторы теракта 9/11) прежде всего на нанесение максимального ущерба Соединенным Штатам…

По словам Коутса, Кремль демонстрирует возможности нанести кибердары по самым критическим объектам инфраструктуры США: линии электропередачи, банковские сети, ядерный комплекс, системы управления полетами и т. д… Со стороны Москвы это естественное и логичное продолжение гибридной войны, которую она ведет против Запада…» ***(Андрій Піонтковський. Співпрацюйте з нами, інакше на вас очікують теракти. Як Кремль хоче домовитися з США // "Українські медійні системи" (https://glavcom.ua/columns/andriypiontkovskiy/spivpracyuyte-z-nami-inakshe-na-vas-ochikuyut-terakti-yak-kremlya-hoche-domovitisya-z-ssha-517125.html). 01.08.2018).***

***

«Советник президента США по национальной безопасности Джон Болтон заявил, что Вашингтону нужно отвечать кибератаками на попытки вмешательства в американские выборы…

«Необходимо установить средства сдерживания, чтобы наши противники, которые осуществляли операции в киберпространстве против нас или которые рассматривают это, понимали, что они заплатят высокую цену»,— уверен господин Болтон.

При этом Джон Болтон подчеркнул, что США хотят мира в киберпространстве…» ***(Советник Трампа выступил за проведение США кибератак в ответ на вмешательство в выборы // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3718790). 20.08.2018).***

***

«Высокопоставленный представитель аппарата нацразведки США Майкл Мосс утверждает, что Россия якобы …предпринимает попытки взлома компьютерных систем, чтобы «украсть информацию у кандидатов и госчиновников».

Мосс заявил, что подобной деятельностью против США могут заниматься и другие страны, которые «заинтересованы в попытках повлиять на американскую внутреннюю политическую обстановку».

«Наибольшие киберугрозы» для США представляют, по мнению разведки, Россия, Китай, Иран и КНДР, но главной угрозой остается Россия, сказал Мосс.

По его мнению, в следующем году «российские» кибератаки станут «более смелыми и более разрушительными», а «новые возможности» будут использованы против Украины…» ***(Антон Антонов. Разведка США предсказала «более разрушительные» кибератаки со стороны России // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/21/938203.html). 21.08.2018).***

***

«Компанія Microsoft нещодавно зірвала спробу афільованих із російським урядом хакерів викрасти дані користувачів з консервативних груп, які агітують за розвиток демократії та кібербезпеки у світі…

Минулого тижня відділ із боротьби з дигітальними злочинами компанії, за рішенням суду, взяв під контроль шість інтернет-доменів, створених групою Strontium, більш відомою як Fancy Bear або APT28, які пов'язані з російським урядом.

За даними компанії, зловмисники створили три фейкові веб-сторінки в інтернеті, які схожі на сайти Сенату США, Міжнародного республіканського інституту, який агітує за демократичні принципи в світі, та Інституту Хадсона, в якому вже відбулися кілька дискусій щодо кібербезпеки та який критикував російський уряд. Російські хакери надсилали з цих веб-сторінок електронні листи з вимогою ввести свої логіни й паролі для входу на зазначені сайти, щоб таким чином викрасти дані.» ***(Microsoft перешкодила кремлівським хакерам вкрасти важливі дані // Західна інформаційна корпорація (https://zik.ua/news/2018/08/21/microsoft_pereshkodyla_kremlivskym_hakeram_vkrasty_vazhlyvi_dani_1390755). 21.08.2018).***

***

«Заявления компании Microsoft о российских хакерах, якобы попытавшихся вмешаться в американские выборы, рассчитаны на максимальный политический и публичный «вау-эффект», заявили в МИДе…

В МИД так же, как и пресс-секретарь российского президента Дмитрий Песков, не знают, «о чем говорит компания Microsoft, о каких попытках вмешательства идет речь, что за «русские хакеры», тем более «ассоциированные с Кремлем»…

«Видимо, американские коллеги не хотят предъявлять какие-либо доказательства «российского электронного вмешательства», которые якобы имеются у них в наличии, чтобы не опозориться. Их просто нет и быть не может», – предположили в МИДе…». ***(Анна Инсарова. Россия сделает «необходимые выводы» относительно Microsoft // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/21/938178.html). 21.08.2018).***

***

«Президент США Дональд Трамп підписав наказ, що передбачає оновлену директиву щодо заходів забезпечення кібербезпеки.

Директива 20, підписана раніше екс-главою Білого Дому Бараком Обамою, являє собою план щодо забезпечення кібербезпеки. У ній містяться стандарти, що визначають діяльність американських органів у боротьбі з загрозами у кіберпросторі…

Згідно з наказом, знімаються обмеження на умови, за яких Трамп може піти на "застосування кіберзброї проти своїх противників".

Одне з джерел WSJ описало наказ як "наступальний крок вперед", який може сприяти проведенню військових операцій, запобігати кражам інтелектуальної власності США, а також сприятиме запобіганню іноземного втручання в американські вибори…» ***(Трамп дозволив собі застосовувати кіберзброю проти інших країн – WSJ // "Дзеркало тижня. Україна" (https://dt.ua/WORLD/tramp-***

dozvoliv-sobi-zastosovuvati-kiberzbroyu-proti-inshih-krayin-wsj-285744_.html). 16.08.2018).

***

«…Національний центр кібероперацій (NCKO) розробив стратегію кіберзахисту Чеської Республіки на період 2018-2022, який встановлює політичні умови для національної оборони в кіберпросторі…

Стратегія кібернетичної оборони Чехії відповідає на ключові проблеми в цій області, які включають, в першу чергу, «нові тенденції роботи впливу», збільшення ризику з боку недержавних суб'єктів, кібертероризм, все більша кількість пристроїв, що працюють у мережі Інтернет, низький рівень комп'ютерної грамотності, відсутність обізнаності користувачів про принципи безпеки в кіберпросторі і зростаючу залежність підрозділів державної оборони від інформаційно-комунікаційних технологій.

Розроблений документ відповідає Плану дій з національної стратегії кібербезпеки на період 2015-2020 років…» ***(Чехія розробила стратегію кібербезпеки до 2022 року // Західна інформаційна корпорація (https://zik.ua/news/2018/08/16/chehiya_rozrobyla_strategiyu_kiberbezpeky_do_2022_roku_1387465). 16.08.2018).***

***

«Американская компания FireEye, занимающаяся проблемами кибербезопасности, выпустила доклад, в котором утверждается, что Китай использует проект «Один пояс — один путь» для шпионажа за компаниями и правительствами других стран.

…среди целей китайских хакеров уже оказались Белоруссия, Мальдивы, Камбоджа, а также европейские министры иностранных дел и некоммерческие организации…

При этом авторы доклада утверждают, что серьезно вырос риск кибератак на Малайзию, чей премьер-министр Махатхир Мохамад недавно критически отозвался об инфраструктурном мегапроекте Китая. По данным FireEye, китайская группировка хакеров Temp.Toucan уже пыталась пробить защиту государственных и частных компаний Малайзии. А хакерская группировка Roaming Tiger атаковала объекты в Белоруссии, где Китай совместно с белорусскими властями создает крупнейший в Европе индустриальный парк «Великий камень» ***(Кирилл Сарханянц. Китай обвинили в использовании проекта «Один пояс — один путь» в целях шпионажа // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3714116). 15.08.2018).***

***

«Президент Эстонии Керсти Кальюлайд заявила, что Таллин не боится кибератак благодаря серьезным мерам защиты.

«Мы беспокоимся меньше, чем другие страны, потому что у нас высокий уровень компьютеризации, и мы начали защищаться от кибератак еще тогда, когда цифровые технологии были «молоды», – цитирует CNBC Кальюлайд…

Президент отметила, что эстонцы «имеют высокий уровень кибергигиены». По словам Кальюлайд, Эстония создала ряд баз данных вместо единой правительственной базы, разместив их в других странах. Одним из партнеров стал Люксембург, на территории которого есть «цифровое посольство» Эстонии с базами данных…» ***(Алексей Ласнов. Эстония объяснила, почему не боится кибератак России // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/15/937253.html). 15.08.2018).***

***

«Американское руководство провело трехдневные общенациональные учения по кибербезопасности на выборах, сообщается на сайте министерства внутренней безопасности США.

…Отмечается, что в учениях принимали участи жители 44 штатов и столичного округа Колумбия, а также сотрудники Пентагона, минюста, руководство национальной разведки, агентство национальной безопасности, киберкомандование ВС США и ряд прочих ведомств и организаций.» ***(В США прошли общенациональные учения по кибербезопасности на выборах // Goodnews.ua (http://goodnews.ua/technologies/v-ssha-proshli-obshhenacionalnye-ucheniya-po-kiberbezopasnosti-na-vyborax/). 17.08.2018).***

***

«Госдепартамент США в 2016 году отправил послам в Европе информацию о кибератаках, якобы совершенных Россией…

Письмо в первую очередь было посвящено вмешательству России в президентские выборы в США 2016 года, однако там также упоминается, что Москва «сосредоточила значительные ресурсы» на Швеции и Финляндии.

По данным Госдепа, российские хакеры пытались распространять порочащую НАТО информацию в шведских СМИ и соцсетях, а также в аналитических центрах. В документе отмечается, что Россия участвует в «широкомасштабной кампании по дестабилизации Альянса». ***(США заподозрили российских хакеров в попытках поссорить Швецию и НАТО // Goodnews.ua (http://goodnews.ua/technologies/ssha-zapodozrili-rossijskix-xakerov-v-popytkax-possorit-shveciyu-i-nato/). 12.08.2018).***

***

«Агентство національної безпеки (АНБ) США створило робочу групу з протидії російським загрозам в кіберпросторі.

Про це заявив директор АНБ генерал Пол Накасоне на щорічному форумі з безпеки в Аспені…

Створення групи щодо Росії відбувається на тлі заяви президента США Дональда Трампа про те, що він довіряє висновку американських розвідслужб про втручання Росії в хід виборчої кампанії в США і вважає президента РФ Владіміра Путіна особисто відповідальним за це…» ***(У США створили робочу групу з протидії російським загрозам в кіберпросторі // Західна інформаційна корпорація***

(https://zik.ua/news/2018/07/23/u_ssha_stvoryly_robochu_grupu_z_protydii_rosiyskym_zagrozam_v_kiberprostori_1371519). 23.08.2018).

***

«Министерство внутренней безопасности США и Федеральное бюро расследований обсудили с Facebook и Microsoft угрозу иностранного вмешательства и предпринимаемые компаниями меры для борьбы с ней. Участники совещания подчеркнули, что ни одна организация, министерство или частное лицо не способны решить эту проблему в одиночку…

Исполняющий обязанности помощника директора ФБР по национальной безопасности Майкл Маккарти уверен, что подобное сотрудничество может быть плодотворным и способствовать предотвращению угроз в будущем…» ***(ФБР и МВБ обсудили с Facebook и Microsoft вопросы кибербезопасности // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3724561). 25.08.2018).***

***

«Корпорация Google заявила, что она обнаружила и удалила 39 каналов на YouTube, шесть блогов на платформе Blogger и 13 аккаунтов Google+…

Речь идет об аккаунтах, связанных с иранской государственной пропагандой, а именно с иранской государственной телерадиокомпанией «Голос Исламской Республики Иран», которая находится под американскими санкциями с 2013 года…

Google обратилась к услугам компании FireEye, специализирующейся на кибербезопасности. В FireEye заявили, что подозревают «операцию по оказанию влияния», которая предположительно исходит от Ирана и нацелена на США, Латинскую Америку, Великобританию и Ближний Восток…» ***(Яна Рождественская. Google заблокировал несколько десятков связанных с Ираном аккаунтов // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3722322). 24.08.2018).***

***

«Міністерство фінансів США розширило пов’язані з кібербезпекою санкції проти Росії…

У міністерстві зазначили, що результатом нових заходів є блокування власності й інтересів осіб, які потрапили під санкції, в американській юрисдикції. Крім того, громадянам США заборонено мати спільні операції з цими особами.

Згідно з повідомленням, санкції запроваджені проти компанії Vela-Marine Ltd. і громадян Марини Царьової та Антона Нагибіна. На думку американської влади, вони були пов’язані з компанією Divetechnoservices, яка раніше потрапила під санкції. Крім того, США запровадили обмеження проти словацької Lacno S.R.O…» ***(США розширили пов’язані з кібербезпекою санкції проти Росії // Радіо Свобода (https://www.radiosvoboda.org/a/news-us-russia-sanctions/29445754.html). 31.08.2018).***

***

«…У серпні в естонській армії з'явилися кібервійська, що відповідають за забезпечення кібербезпеки країни. Нова структура налічує 300 осіб…

Основна ідея створення кібервійськ і формування їх командування полягає в тому, щоб об'єднати різні частини нашої оборонної системи, які ми використовуємо для роботи в кіберпросторі, для більш ефективного використання ресурсів. Об'єднаний центр кібервійськ допоможе вдосконалити захист від потенційних комп'ютерних загроз…

Незалежно від розвинених наступальних можливостей кібервійськ, основним завданням нового підрозділу є підтримка командування оборонних сил Естонії, а саме надання інформації та її захист.

Наступальні кіберможливості, які ми розвиваємо, будуть використовуватися для перевірки безпеки власних інформаційно-комунікаційних систем і створення реалістичної середовища для навчань оборонних підрозділів. Наприклад, під час недавніх навчань ми відправили фішингові листи, щоб перевірити, чи можуть учасники впоратися з підозрілою розсилкою.

У разі війни або збройного конфлікту ми будемо підтримувати військові операції сил оборони в кіберпросторі. Але знову ж таки, тільки при необхідності, і якщо для цього буде правова основа…» ***(Командувач кибервойсками Естонії: Щоб захиститися, треба вміти атакувати // Українська служба швидких новин (https://sumynews.online/komanduvach-kibervojskami-estoni%d1%97-shhob-zaxistitisya-treba-vmiti-atakuvati/). 18.08.2018).***

***

«Федеральний уряд Німеччини з ініціативи міністерства оборони та міністерства внутрішніх справ країни розробляє плани зі створення держагентства з розвитку кіберзброї…

Уряд планує схвалити створення "агентства з інновацій у сфері кібербезпеки" на своєму засіданні …15 серпня.

Нове відомство має забезпечити Бундесвер та спецслужби країни необхідними засобами для захисту від кібератак. Очікується, що завдяки агентству урядові структури володітимуть продуктом для аналізу загроз та можливого віртуального удару у відповідь та не будуть змушені чекати його появи на ринку і купувати…

У створенні відомства Німеччина орієнтується на відповідні державні агенції США та Ізраїлю. Міністерство оборони планує у 2019 та 2020 роках виділяти щорічно близько 50 мільйонів євро на дослідження та технологічні розробки в кіберсекторі» ***(У Німеччині можуть створити держагентство з розвитку кіберзброї // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/u-nimechchini-mozhut-stvoriti-derzhagentstvo-z-rozvitku-kiberzbroyi.html). 11.08.2018).***

***

«Министерство обороны Грузии объявило прием специалистов по кибербезопасности в резерв.

Согласно заявлению ведомства, лица, зачисленные в резерв специалистов, пройдут программу специальной подготовки, длительность которой составляет 45 календарных дней в год.

Срок контракта определяется периодом от 1 до 5 лет…

Лицо, зачисленное в резерв специалистов, не будет подлежать призыву в территориальный резерв. В то же время специалисты будут получат зарплату соответственно военному званию.

Кандидат должен соответствовать квалификационным требованиям, определенным приказом министра обороны Грузии от 18 мая 2018 года за №47, "О порядке отбора лиц для приема в активный резерв военной резервной службы, и утверждении квалификационных требований"» ***(Минобороны Грузии начинает прием в резерв специалистов по кибербезопасности // Черноморские новости (https://www.blackseanews.net/read/143652). 15.08.2018).***

***

Кіберзахист критичної інфраструктури

«…впервые за всю историю Министерство энергетики США проверит устойчивость американских электростанций к хакерским атакам. Минэнерго проведет эксперимент под названием «Затмение свободы» («Liberty Eclipse») с целью проверить способность предприятий электроэнергетического сектора восстанавливать работу электросети после кибератаки.

Эксперимент будет проходить на острове Плам неподалеку от Нью-Йорка в течение одной недели. Начало тестирования запланировано на 1 ноября текущего года. В ходе эксперимента будут созданы условия, имитирующие реальную ситуацию, когда операторам критической инфраструктуры придется восстанавливать работу электросети, одновременно отражая кибератаки.

Главной целью учений является подготовка к устранению последствий хакерских атак на объекты критической инфраструктуры, которые в недалеком будущем могут стать обычным делом» ***(Минэнерго США проверит электростанции на устойчивость к кибератакам // Goodnews.ua (http://goodnews.ua/technologies/minenergo-ssha-proverit-elektrostancii-na-ustojchivost-k-kiberatakam/). 09.08.2018).***

***

«Исследователи из Университета Бен-Гуриона (Израиль) предупредили об опасности кибератак на городские системы водоснабжения с использованием ирригационных смарт-систем.

Исследователи обнаружили уязвимости в наиболее популярных коммерческих системах орошения GreenIQ, BlueSpray и RainMachine, позволяющие злоумышленникам удаленно их включать и выключать. Если проэксплуатировать эти уязвимости одновременно, ботнет из 1355 поливальных систем за час сможет истощить весь запас воды в городской водонапорной башне, а ботнет из 23866 «поливалок» за ночь опустошит все водохранилище.

Системы водоснабжения относятся к национальной критической инфраструктуре и, как правило, защищены от попыток злоумышленников подмешать что-то в воду…

Описанный экспертами Университета Бен-Гуриона способ не предполагает атак вредоносного ПО на сами городские системы водоснабжения. Вместо этого злоумышленники могут поступить намного проще и причинить вред городской системе водоснабжения с помощью ботнета из умных «поливалок». ***(Ботнет из умных «поливалок» может осушить водохранилище // Goodnews.ua (http://goodnews.ua/technologies/botnet-iz-umnyx-polivalok-mozhet-osushit-vodoxranilishhe/). 13.08.2018).***

***

Захист персональних даних

«Один из крупнейших в мире сайтов имиджборд Reddit на своём сайте сообщил о кибератаке и утечке данных пользователей.

Как поясняет администрация ресурса, взлом заметили 19 июня. В ходе проверки выяснилось, что неизвестный хакер получил доступ к некоторой информации юзеров, включая адреса электронной почты, пароли и сообщения в период с 2005 по 2007 годы…

В Reddit заверили, что заблокировали все данные и поменяли ключи шифрования. Пароли пострадавших пользователей сбросили и сгенерировали новые.» ***(Очередная хакерская атака: получены личные данные пользователей // «Я и Закон» (https://yaizakon.com.ua/ocherednaya-hakerskaya-ataka-polucheny-lichnye-dannye-polzovatelej/). 02.08.2018).***

***

«Количество зарегистрированных в мире утечек персональных данных, в том числе номеров социального страхования, реквизитов платежных карт, специфических медицинских записей о состоянии здоровья, историй болезни пациентов, сократилось за год на 7,7% до 370 случаев, объем скомпрометированных в результате утечек записей данных снизился по сравнению с предыдущим годом в два раза — с 26,8 млн записей до 14,2 млн… Такие результаты показало глобальное исследование утечек конфиденциальной информации из медицинских учреждений в 2017 году, которое подготовил Аналитический центр InfoWatch.

Авторы исследования связывают снижение числа инцидентов и объема утекших записей в мире с повышением уровня защиты медицинских данных в самой большой системе здравоохранения мира — США. По оценкам экспертов, в 2017 году более 80% организаций сферы здравоохранения США увеличили расходы на информационную безопасность. В то же время в исследовании отмечается, что развитие технологий, в том числе телемедицины, а также способов использования медицинских данных в электронном виде, увеличивает ценность

медицинской информации. Поэтому в ближайшей перспективе число утечек такой информации и объем скомпрометированных данных в мире неизбежно будут расти.

Если в глобальной картине «медицинских» утечек около 30% инцидентов были связаны с внешними атаками злоумышленников, то в России все зафиксированные случаи носили исключительно внутренний характер. Классический для России пример внутренней утечки из медицинских учреждений — это «слив» сотрудниками больниц и клиник данных о тяжелобольных и умерших пациентах ритуальным агентам.

Авторы исследования также отмечают, что доля умышленных утечек информации, совершенных сотрудниками медучреждений, в России существенно выше, чем в мире — 39% против 30% соответственно.

В России и в мире примерно четверть «медицинских» утечек была сопряжена с квалифицированными действиями злоумышленников – мошенничеством или превышением прав доступа к информационным системам…

Как отмечается в исследовании, организации сферы здравоохранения занимают одно из первых мест среди всех отраслей мирового хозяйства по такому показателю, как воздействие на информационные активы со стороны внутренних злоумышленников. Именно по вине сотрудников, топ-менеджеров и системных администраторов медучреждений происходит подавляющее большинство инцидентов, утекает основной объем записей в данной сфере…» ***(InfoWatch: в России резко выросло число утечек конфиденциальных медицинских данных // «Открытые системы» (https://www.computerworld.ru/news/InfoWatch-v-Rossii-otmechen-rezkiy-skachok-utechek-konfidentsialnyh-meditsinskih-dannyh). 24.08.2018).***

***

Кіберзлочинність та кібертероризм

«По мере того, как США готовится наложить новые санкции на Иран, хакеры этой страны работают над вирусом, перехватывающим транзакции биткоина. Так считают эксперты по кибербезопасности компании Accenture PLC.

Эксперты изучали пять разных иранских вирусов в течение двух лет. Эти вирусы были направлены либо на выведение денег с кошельков пользователей, либо на скрытый майнинг…

CrowdStrike Inc., одна из компаний, работающая в сфере кибербезопасности, недавно изучила один из подобных вирусов — The Tyrant. Иранские власти использовали его, чтобы граждане этой страны перестали пытаться избавиться от государственной слежки за их устройствами…

Эксперты из Accenture считают, что в недавнем поражении нефтегазовой индустрии на ближнем востоке скрытыми майнерами виноват Иран — на это указывают улики. Эти майнеры доставили немало проблем нефтяным и газовым компаниям, направив значительное число вычислительных циклов на майнинг. Ущерб от этого вируса оценивается в миллионы долларов…

Власти Ирана заявляют, что они не причастны к кибератакам, более того, они утверждают, что сами являются жертвами хакеров.

Тем не менее следы, найденные в коде программы, говорят о непосредственной причастности Ирана: там содержатся сообщения на Фарси, государственном языке данной страны…» ***(Иран обвиняют в разработке скрытых майнеров и воровстве криптовалют // BIGFIN (https://bigfin.net/08/08/2018/iran-obvinjajut-v-razrabotke-skrytyh-majnerov-i-vorovstve-kriptovaljut/). 08.08.2018).***

***

«Исследователи кибербезопасности из фирмы Sucuri обнаружили новую тактику распространения вредоносных майнеров криптовалюты, в ходе которой злоумышленники используют неофициальный сервис, связанный с GitHub.

Речь идет о RawGit – сети доставки контента, которая кэширует файлы GitHub даже после того, как исходные данные были удалены с сервиса или пользователь GitHub удалил свою учетную запись.

По словам экспертов, в ходе недавней кампании по распространению майнера криптовалют Crypto-Loot, злоумышленники загрузили вредонос в учетную запись GitHub с именем jdobt, кэшировали вредоносный скрипт с помощью RawGit, а затем удалили исходную учетную запись на GitHub.

Далее злоумышленники встроили скрипт, используя адреса RawGit — домена, который обычно не считается подозрительным и не подвержен дополнительным проверкам с помощью решений безопасности.

Однако, как отметили исследователи, данная вредоносная кампания оказалась провальной по ряду причин. Во-первых, мошенники не смогли правильно загрузить скрипт Crypto-Loot на взломанные сайты, а следовательно не получили никакой прибыли.

Во-вторых, команда RawGit оперативно отреагировала на уведомление о незаконной деятельности и удалила вредоносный скрипт в течение нескольких часов.» ***(Хакеры распространяли майнер криптовалют с помощью удаленного аккаунта GitHub // Goodnews.ua (http://goodnews.ua/technologies/xakery-rasprostranyali-majner-kriptovalyut-s-pomoshhyu-udalennogo-akkaunta-github/). 03.08.2018).***

***

«В прошлом месяце более 170 000 устройств в Бразилии пострадали от криптоджекинга, пишет Coindesk.

Компания Trustwave в своём блоге сообщила, что маршрутизаторы MicroTik подверглись широкомасштабной кибератаке, в результате которой на более чем 170 000 устройств был установлен «скандально известный» майнер Coinhive.

Специалист по безопасности в Trustwave Саймон Кенин утверждает, что все устройства используют один ключ. Это указывает на то, что с их помощью майнил только один хакер (или группа хакеров)…

Сервис Coinhive стал популярным в 2017 году. Его создатели предоставляют решение для монетизации веб-сайтов без использования каких-либо рекламных объявлений…

Trustwave выпустила инструменты, которые блокируют вредоносное ПО…». ***(Майнер Coinhive «заразил» 170 000 устройств в Бразилии и продолжает распространяться // BIGFIN (https://bigfin.net/10/08/2018/majner-coinhive-zarazil-170-000-ustrojstv-v-brazilii-i-prodolzhaet-rasprostranjatsja/). 10.08.2018).***

***

«Специалисты по безопасности из компании Oracle сообщили о кибератаках на DNS-серверы трех крупных фирм, занимающихся обработкой платежей в США…

Как следует из доклада, злоумышленники использовали технику BGP-перехвата для атаки на серверы компаний WorldPay, Datawire и Vantiv…

Как полагают специалисты, данные атаки был лишь частью вредоносной кампании…» ***(В США сервисы по обработке платежей стали жертвами кибератак из Луганска // ООО "Cxid Media Холдинг" (http://cxid.info/v-ssha-servisy-po-obrabotke-platejey-stali-jertvami-kiberatak-iz-luganska-n141808). 07.08.2018).***

***

«Генпрокуратура России сообщила о семикратном росте количества мошенничеств с использованием электронных средств платежа (ст. 159.3 УК РФ) в январе–июне 2018 года. «Наибольшее число указанных преступлений совершено в Ставропольском крае (66), Мурманской области (52), Республике Татарстан (37), городе Москве (34), Саратовской области (31)»,— говорится в сообщении Генпрокуратуры.

В 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось на 37% (с 65 949 до 90 587). Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4%. Самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)…» ***(Количество кибермошенничеств в России за полгода выросло в семь раз // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3713619). 14.08.2018).***

***

«…В конфиденциальном уведомлении в пятницу Федеральное бюро расследований США …предупредило о схеме мошенничества "jackpotting": злоумышленники взламывают банк или процессинговые центры и используют копии карт в банкоматах по всему миру для вывода миллионов всего за несколько минут.

Британские банки, такие как HSBC и Barclays, были осведомлены об этой угрозе…

Обычно этот метод включает физический доступ к банкомату с использованием специализированной электроники и вредоносного ПО, чтобы взломать систему и заставить ее выдавать наличные до тех пор, пока они не закончатся…

Как утверждают в консалтинговой фирме по кибербезопасности NCC Group, небольшие частные банки наиболее уязвимы для таких атак…

Киберпреступники обычно крадут данные кредитной карты для создания мошеннических копий с магнитной полосой. В назначенное время преступники снимают все наличные с банкоматов.

ФБР призвало банки пересмотреть способы защиты внутри страны, в том числе внедрение надежных паролей и двухфакторной аутентификации с использованием физического и цифрового токенов…» ***(Ирина Фоменко. Хакеры могут украсть все наличные из банкоматов // InternetUA (http://internetua.com/hakery-mogut-ukrast-vse-nalicsnye-iz-bankomatov). 14.08.2018).***

***

«Масштабна кібератака, яка, ймовірно, надійшла з Росії, заблокувала сотні акаунтів користувачів соціальної мережі Instagram…

Хакери змінюють назви облікових записів Instagram, паролі до них та фотографії профілей, а також — адреси електронної пошти користувачів на адреси російських провайдерів. У деяких акаунтів, що зазнали атаки, зловмисники змінили фотографії профілів на кадри з популярних фільмів, таких як “Пірати Карибського моря” або “Нікчемний я-3”.

У Instagram повідомили, що обізнані з приводу ситуації…» ***(Саша Картер. Хакери з Росії атакували сотні акаунтів в Instagram – ЗМІ // InternetUA (http://www.unn.com.ua/uk/news/1747053-khakeri-z-rosiyi-atakuvali-sotni-akauntiv-v-instagram-zmi). 15.08.2018).***

***

«…Согласно статистическим данным, в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587…

Самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ). Если в 2017 году зарегистрировано 1 883 таких преступления (+7,7%), то за первое полугодие 2018 г. – 1 233 (+3,4%)…

Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ). Их количество в первом полугодии 2018 г. возросло в 7 раз…» ***(Генпрокуратура: число преступлений в IT-сфере возросло // РосКомСвобода (https://roskomsvoboda.org/40924/). 14.08.2018).***

***

«**Эксперты по кибербезопасности зафиксировали рост фишинговой активности в мессенджерах и соцсетях.** Для распространения "вирусного" контента мошенники все чаще начали использовать WhatsApp.

Как уточняет "Лаборатория Касперского", в сообщениях киберпреступников речь, как правило, шла о несуществующих розыгрышах, либо выгодных предложениях…

В другом варианте жертве предлагали установить расширение для браузера. Вредоносное ПО затем перехватывало вводимые личные данные.

Еще один способ мошенничества эксперты обнаружили в Twitter. В соцсети создавались поддельные аккаунты известных лиц (например, Илона Маска, Павла Дурова, Виталика Бутеритна) и различных компаний. От их имени пользователям сообщали о "бесплатной раздаче криптомонет"…» ***(Пользователей атаковали мошенники в WhatsApp // Goodnews.ua (http://goodnews.ua/technologies/polzovatelej-atakovali-moshenniki-v-whatsapp/). 18.08.2018).***

***

«Преступная сеть инфицированных компьютеров (ботнет) Necurs в прошлом году была уличена в нелегальном сборе данных и получении снимков экрана ПК. В прошлую среду стартовала новая фишинговая кампания Necurs, в этот раз она нацелена на банки.

…к настоящему времени мишенями для атак Necurs стали 2700 банковских доменов и персонал, работающий в этих банках.

Рассылаемые ботнетом электронные письма содержат файлы Microsoft Publisher (.PUB). При попытке их открыть запускается макрос, который загружает троянца с удалённого хостинга. Эта троянская программа, в свою очередь, обеспечивает полный дистанционный контроль взломанной машины. Помимо извлечения из него файлов и идентификационных данных, захваченный компьютер используется как плацдарм для дальнейшего расширения ботнета внутри сети организации…» ***(Прошлогодний ботнет используется в масштабной фишинговой атаке на банки // «Компьютерное Обозрение» (https://ko.com.ua/proshlogodnij_botnet_ispolzuetsya_v_masshtabnoj_fishingovoj_atake_na_banki_125733). 20.08.2018).***

***

«…У мережі поширився новий вид шахрайства: хакери надсилають жертві листа з одним з її паролів, витік якого, скоріш за все, стався набагато раніше, після чого заявляють, що нібито зламали веб-камеру і зняли, як людина дивиться порно і що при цьому робить. Далі вони вимагають перерахувати певну суму на біткоін-гаманець…

Компанія Banbreach переглянула загалом близько 770 електронних гаманців. Більшість із них, близько 540, не отримували жодних коштів. Але в інших 230 було понад 1000 транзакцій, які отримали загалом близько 70,8 біткоінів.

Ця цифра, ймовірно, далека від справжньої, оскільки компанія не могла відстежити всі повідомлення, що надійшли від хакерів, і дані їхніх біткоін-

гаманців. Фахівці Banbreach вважають, що деякі з паролів, які використовуються для шантажу, було взято з LinkedIn і бази даних Anti-Public Combo, що являє собою велику кеш-колекцію з кількох джерел. Однак точні джерела витоку паролів визначити не вдалося.» ***(Хакери заробили півмільйона доларів, прикидаючись, що дивляться, як ви дивитеся порно // Ракурс (http://racurs.ua/ua/n109907-hakery-zarobyly-pivmilyona-dolariv-prykydauchys-scho-dyvlyatsya-yak-vy-dyvytesya-porno). 23.08.2018).***

***

Діяльність хакерів та хакерські угруповування

«…Исследователь безопасности IBM X-Force Red Дэниэл Кроули обнаружил 17 различных типов уязвимостей в датчиках, используемых в городах по всей Великобритании, Европе и США, заявив, что "простота ошибок вызывает беспокойство".

Террористы могут захватить инфраструктуру интеллектуального города для манипулирования реагированием правоохранительных органов на атаки. Они могут поднять ложные сигналы тревоги, чтобы вызвать массовую панику - или подавить законные - и остановить работу промышленных систем управления, используемых в телекоммуникациях и электростанциях…

Кроули и его команда обнаружили уязвимости в датчиках систем управления трафиком: они позволяют хакеру перехватывать и изменять данные, что создает пробки. Преступники могут использовать их вместе с физической атакой, что затруднит прибытие полицейских и служб экстренной помощи.

Хакеры могут имитировать стихийные бедствия или скрывать их от обнаружения, используя уязвимости в системах сигнализации, включая датчики излучения в Испании, расположенные рядом с ядерной установкой. По словам Кроули, хакеры могут вызвать панику, искажая данные…» ***(Ирина Фоменко. "Умные города" уязвимы перед кибератаками // Internetua (http://internetua.com/umnye-goroda-uyazvimy-pered-kiberatakami). 10.08.2018).***

***

«…Скрытый майнинг и воровство криптовалют в последнее время становятся очень популярными практиками у местных хакеров, отмечает Нидерландское Агентство по Безопасности и Контртерорризму в своём ежегодном докладе по кибербезопасности.

…За последние 12 месяцев они стали значительно популярнее среди мошенников, в то время как традиционные виды онлайн-мошенничества наоборот стали менее распространёнными.

…главной причиной активного роста популярности этих преступлений стала высокая цена биткоина и других криптовалют. Эксперты также обратили внимание на распространённый скрытый майнер Monero (XMR) — Coinhive, который не так давно поразил несколько десятков компаний в стране и при этом продолжает распространяться.» ***(Нидерландские мошенники переключаются на***

криптовалюты // BIGFIN (https://bigfin.net/10/08/2018/niderlandskie-moshenniki-perekljuchajutsja-na-kriptovaljuty/). 10.08.2018).

***

«Хакеры подсоединили парковочный IoT-терминал к порносайту, что, как предполагается, было атакой без злого умысла со стороны "серой шляпы"…

Компания по кибербезопасности Darktrace опубликовала отчет "2018 Threat Report" во вторник, в котором подчеркивается, что терминал для парковки подключен к веб-сайтам с содержанием для взрослых, но он фактически не показывал этот контент…

В другом инциденте компания обнаружила попытку взлома через устройства IoT на линии производства пищевых продуктов. Все устройства, включая блендеры, слайсеры и упаковочные машины, были скомпрометированы…

Многие устройства IoT остаются незащищенными и могут представлять угрозу для более широкой сети…» ***(Хакеры подсоединили парковочный терминал к порносайту // Goodnews.ua (http://goodnews.ua/technologies/xakery-podsoedinili-parkovochnyj-terminal-k-pornosajtu/). 02.08.2018).***

***

«Российские хакеры имеют доступ к сотням тысяч маршрутизаторов, принадлежащих американцам и другим людям по всему миру, рассказал сотрудник Агентства национальной безопасности (АНБ) США Роб Джойс…

Джойс сообщил, что в данных маршрутизаторах установлены вредоносные российские программы. Впервые вредоносное ПО было обнаружено в мае, говорится в материале. Такая ситуация опасна тем, что ПО может позволить украсть данные физических лиц или привлечь их устройства к массивной хакерской атаке, которая нанесет вред глобальной экономической деятельности и организациям, полагает источник издания…

Джойс считает необходимым, чтобы американское правительство, компании и специалисты по кибербезопасности нашли способ открыто рассказать людям, как обнаружить присутствие вредоносного ПО на своих маршрутизаторах, а затем восстановить устройство до его надежного состояния. Однако чиновник отмечает, что правительство вряд ли сможет сделать такое, потому что это частные устройства пользователей.» ***(Вредоносные программы хакеров из России расположены в устройствах американцев // Goodnews.ua (http://goodnews.ua/technologies/vredonosnye-programmy-xakerov-iz-rossii-raspolozheny-v-ustrojstvax-amerikancev/). 16.08.2018).***

***

«…3 августа вышел на свободу из московского СИЗО "Лефортово" лидер хакерской группировки "Шалтай-Болтай" Владимир Аникеев… "Шалтаи-болтаи" работали из стран Юго-Восточной Азии и объективно сделали немало полезного (при этом явно сотрудничая с разными группировками в

российских спецслужбах) для разоблачения преступлений путинского режима, но промышляли откровенным шантажом, на чем, возможно, и погорели…

А пока что Владимир Аникеев готовится к новой работе. Официально …ему предложили место в адвокатском бюро "Коблев и партнеры", и тот предварительно согласился… Коблев - непростой юрист, поскольку в …течение четырех лет работал в военной прокуратуре во Владикавказе. Так что от дела "Шалтай-Болтая" и карьеры Аникеева "попахивает" Главным разведывательным управлением Генштаба (ГРУ)…» ***(Максим МИХАЙЛЕНКО . Шалтай-не-болтай. Зачем хакера, взломавшего друзей Путина, выпустили из тюрьмы // DsNews (http://www.dsnews.ua/world/shaltay-ne-boltay-zachem-iz-lefortovo-vypustili-hakera-anikeeva-13082018220000). 14.08.2018).***

***

«Провластная российская хакерская группировка Fancy Bear …пыталась получить доступ к электронной почте ключевых помощников главы Константинопольской церкви патриарха 78-летнего Варфоломея I…

У самого главы православной церкви нет электронной почты. Хакеры пытались взломать электронные ящики трех митрополитов - Варфоломея (в миру Михаил Самарас), Эммануила (Адамакис) и Элпидофора (Ламбриниадис).

Злоумышленники случайно опубликовали сведения о своей операции. Их заметила компания по кибер-безопасности Secureworks и сообщила об этом журналистам.

Российская церковь отказалась комментировать попытку взлома…». ***(Российские хакеры атаковали Вселенский патриархат // Gazeta.ua (https://gazeta.ua/ru/articles/world-life/_rossijskie-hakery-atakovali-vselenskij-patriarhat/855686). 27.08.2018).***

***

«Корпорация Google предупредила представителей американского сенатора-республиканца Патрика Туми о том, что хакеры пытались получить доступ к информации его предвыборного штаба… В Google считают, что хакеры, поддерживаемые неустановленным государством, пытались взломать аккаунты электронной почты сотрудников штаба.

Пресс-секретарь Патрика Туми Стив Келли заявил, что возникшая ситуация «подчеркивает наличие киберугроз по отношению к нашему правительству, предвыборным кампаниям и избирательному процессу». Он также призвал Конгресс США предпринять меры с тем, чтобы все, кто пытается подорвать американские институты власти, не смогли уйти от ответственности…» ***(Google сообщила американскому сенатору о кибератаке на сотрудников его штаба // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3724590). 25.08.2018).***

***

«Нет свидетельств того, что атаки якобы российских хакеров оказались успешными, заявил президент Microsoft Брэд Смит.

«Мы сумели перехватить контроль над доменами прежде, чем их смогли использовать», – приводит его слова ТАСС со ссылкой на MSNBC.

Как заявил Смит, угроза кибератак существует как для представителей Демкоратической партии США, так и для республиканцев – «российские» хакеры действуют против и тех и других. Активность киберпреступников он связал с грядущими выборами в американский Конгресс…» ***(Антон Антонов. Президент Microsoft счел атаки «российских хакеров» неудачными // Деловая газета «Взгляд» (https://vz.ru/news/2018/8/22/938206.html). 22.08.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«… WannaCry продолжает свою деятельность. К примеру, недавно под удар попал один из заводов по производству деталей для смартфонов компании Apple.

Заражению подверглись предприятия компании Taiwan Semiconductor Manufacturing Co. (TSMC), которая производит чипсеты для существующих и будущих айфонов. Как стало известно из недавно опубликованного пресс-релиза, заражение техники фирмы произошло 3 августа и тогда пришлось остановить производство на несколько часов…

Представители компании отмечают, что инфицирование WannaCry произошло не из-за плохой системы кибербезопасности, а из-за операционной ошибки во время установки программного обеспечения нового производственного инструмента…» ***(Вирус WannaCry заразил завод по производству iPhone // IGate (http://igate.com.ua/lenta/22416-virus-wannacry-zarazil-zavod-po-proizvodstvu-iphone). 07.08.2018).***

***

«Trend Micro Incorporated (TYO: 4704; TSE: 4704) каждый месяц публикует новый отчет по ландшафту киберугроз, которые удалось обнаружить исследователям по всему миру…

Угрозы, распространяющиеся по электронной почте, по-прежнему являются наиболее популярным инструментом злоумышленников (84% от числа всех заблокированных угроз). В топ-5 стран по обнаружению почтовых угроз входят: США, Китай, Япония, Франция, Германия. Россия, Украина и Казахстан находятся на 12, 30 и 52 местах соответственно…

Распространенным спам-вложением в отчетном периоде стали файлы типа .XLS - более 2,5 млн обнаружений. В тоже время рассылка файлов с расширением .EXE и .DOCX упала на 41% и 39% соответственно.Список топ вредоносных программ возглавляет COINMINER. Среди мобильных вредоносов список возглавляет FLOCKER.

WCRY по-прежнему остается лидером среди обнаруженных программ-вымогателей…» ***(Дмитрий Сизов. Киберугрозы во втором квартале 2018 // Internetua (http://internetua.com/kiberugrozy-vo-vtorom-kvartale-2018). 05.08.2018).***

***

«8 августа в Лас-Вегасе, штат Невада, прошла конференция Black Hat, на которой 17 тысяч ученых и экспертов по кибербезопасности обсуждали соответствующие вопросы.

…По словам экспертов, самыми распространёнными киберпреступлениями, связанными с криптовалютами, являются:

Крипто-фишинг — Преступники создают сайт, идентичный сайту криптокомпании (биржи, ICO и т.д.), и/или рассылают электронные письма, чтобы получить приватный ключ пользователя либо для того, чтобы жертва сама перечислила деньги на кошелек мошенника.

Скрытый майнинг — На компьютер жертвы тайно устанавливается скрытый майнер, который перенаправляет мощности компьютера на майнинг криптовалют.

Также эксперты упомянули старый, но все еще рабочий способ, а именно так называемый “Вирус ФБР”, когда компьютер жертвы блокируется до тех пор, пока мошеннику не будут переведено некоторое количество криптовалюты.

…Экспертами было отмечено, что мошенники любят прибегать к использованию Google Ads для распространения рекламы фишинговых сайтов, которые мимикрируют под сайты блокчейн-проектов, ICO или даже бирж…» ***(Эксперты Cisco рассказали о криптовалютных преступлениях на конференции Black Hat // BIGFIN (https://bigfin.net/09/08/2018/jeksperty-cisco-rasskazali-o-kriptovaljutnyh-prestuplenijah-na-konferencii-black-hat/). 09.08.2018).***

***

«…Администрации района Матануска-Суситна столицы Аляски Анкориджа пришлось заново перестраивать всю свою цифровую инфраструктуру в результате атаки шифровальщика-вымогателя…

Работникам администрации и частным подрядчикам предстоит восстановить 650 рабочих станций и серверов, пострадавших от шифровальщика.

Сама атака произошла 24 июля 2018 г. К 30 июля удалось вернуть к работе 110 рабочих станций.

Эрик Уайятт (Eric Wyatt), директор по ИТ Матануски-Суситна, заявил, что сеть была атакована комплексным вредоносом, включавшим функции «троянца, криптолокера», «бомбы замедленного действия» и «аварийной кнопки». Вредоносная программма, которую Уайятт назвал «вирусом», также пыталась добраться до резервных копий, но этого ей сделать не удалось.

…Впоследствии он опубликовал технический отчёт, в котором дал название этого вируса — BitPaymer.

Этот шифровальщик, также известный как FriedEx...

В отчёте Уайятт указал, что вредоносная программа попала в инфраструктуру Матануски-Суситны ещё в начале мая и до 24 июля пребывала в неактивном режиме…

Эксперты, занимающиеся расследованием атаки, заявили, что администрация Матануски-Суситны стала 210 жертвой шифровальщика…» ***(Из-за кибератаки чиновники на Аляске перешли на пишущие машинки // Goodnews.ua***

(http://goodnews.ua/technologies/iz-za-kiberataki-chinovniki-na-alyaske-pereshli-na-pishushhie-mashinki/). 02.08.2018).

***

«Преступники используют DLink DSL роутеры в Бразилии для изменения настроек DNS на подконтрольный хакерам DNS-сервер. Это позволяет им перенаправить пользователей, пытающихся подключиться к интернет-банкам, на фейковые банковские веб-сайты, которые крадут информацию пользователя...

Согласно исследованию Radware, эксплойт, используемый злоумышленниками, дает им возможность выполнять удаленные неаутентифицированные изменения параметров DNS на некоторых DLink DSL модемах/маршрутизаторах. Так они легко могут сканировать и писать скрипты изменения большого количества уязвимых маршрутизаторов, чтобы их настройки DNS перенаправляли на DNS-сервер преступников…

Фейковые веб-сайты выглядят почти так же, как оригинальный банковский сайт. На поддельном ресурсе им предлагается указать номер банковского агентства, номер счета, восьмизначный код, номер мобильного телефона, PIN-код карты и номер CABB. Именно эту информацию и получают злоумышленники…

Узнав о новой кампании, Radware уведомил банки, и все вредоносные сайты были заблокированы…» ***(Ирина Фоменко. Хакеры могут получить ваши банковские данные через Wi-Fi-роутер // InternetUA (http://internetua.com/hakery-mogut-polucsit-vashi-bankovskie-dannye-cserez-wi-fi-router). 13.08.2018).***

***

«В Японии обезвредили Момо – смертельно опасную игру, рассылающую пользователям WhatsApp угрозы и задания, склоняющие людей к суициду. Оказалось, что Момо – бот, созданный японским хакером.

«Из-за высокой скорости обучения и знания нескольких десятков языков, опасный бот признали агентом искусственного интеллекта, — рассказала эксперт по психологической кибербезопасности Наталия Бугаева. — По сообщениям СМИ, настоящая Момо не появляется в сети с 11 июля 2018 года, а при попытках дозвониться по номеру, никто не отвечает, хотя гудки идут…».

При этом эксперт просит не забывать, что у настоящей Момо появилась очень много клонов, которые звонят адресатам с других номеров…» ***(Юлия Мороз. Момо обезврежена: раскрыта тайна опасной игры // Woman.ua (http://woman.ua/106044-momo-obezvrezhena-raskryta-tajna-opasnoj-igry/). 13.08.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Трех украинцев арестовали по обвинению в хакерстве, включая кражу номеров платежных карт. Злоумышленники атаковали более чем 100 американских компаний, что обойдется предприятиям в десятки миллионов долларов…

Прокуроры США утверждают, что три украинца, арестованные в Европе в период с января по июнь, являются членами FIN7, известной организации киберпреступности.

Как заявили в Министерстве юстиции США, среди жертв - Chipotle Mexican Grill, Emerald Queen Hotel, казино в штате Вашингтон, Jason's Deli, Red Robin Gourmet Burgers, Sonic Drive-in и Taco John's. The Emerald Queen удалось предотвратить атаку, и данные клиентов не украли…

Члены FIN7 отправляли фишинговые электронные письма компаниям, призывая сотрудников открывать вложения.

Как заявил глава отдела разведки BAE Systems Адриан Ниш, FIN7, также известная как Carbanak, включает десятки людей, которые занимаются узкоспециализированными задачами: взломом сетей, кражей номеров платежных карт и продажей украденных данных на подпольных криминальных форумах…» ***(Ирина Фоменко. США обвиняют трех украинцев во взломе платежных карт // Internetua (http://internetua.com/ssha-obvinyauat-treh-ukraincev-vo-vzlome-platejnyh-kart). 03.08.2018).***

***

«На прошедшей неделе открылись слушания касательно юного 16-летнего австралийского хакера из Мельбурна, который за 2018 год несколько раз проник на сервера Apple и загрузил с них приблизительно 90 ГБ данных…

Адвокат обвиняемого сообщил, что парень преследовал исключительно благие намерения – юный хакер мечтал работать в Apple и подобным способом хотел обратить на себя внимание руководства компании. В таком случае остаётся непонятно с какой целью он скачал и хранил у себя 90 ГБ «защищенных файлов», в число которых входят аккаунты пользователей Apple.

Представитель Apple сообщил изданию Reuters, что пользователи не имеют обоснованных причин для волнения, так как за все прошедшее время после взлома их личные данные ни разу не подвергались риску…

Взлом серверов был обнаружен после того, как сотрудники Apple засекли неавторизованный доступ к системе компании и обратились в ФБР для передачи дела федеральной полиции Австралии. В результате этого хакер был найден, во время обыска следователи изъяли два MacBook, телефон и переносной HDD…

Подсудимый хакер уже признался во взломе, однако окончательный приговор будет вынесен судом лишь 20 сентября…» ***(Богдан Лаевский. 16-летний хакер скачал 90 ГБ пользовательских данных с серверов Apple, но компания не видит в этом проблем // MobiDevices.ru (https://mobidevices.ru/16-age-hack-apple). 18.08.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Исследователи из кибербезопасности Check Point рассказали об обнаруженной недавно уязвимости в WhatsApp. Она позволяет изменять и перехватывать сообщения как в групповых, так и в приватных чатах…

Брешь была найдена в инструментах для синхронизации данных в мобильной и веб-версии сервиса. Благодаря этому хакеры могут использовать сразу несколько способов манипуляции с перепиской пользователей…

Так, они могут менять имя настоящего отправителя на любое другое, используя функцию "Цитата". Это возможно даже в том случае, если этот человек не состоит в группе.

Также злоумышленники могут редактировать в ответном сообщении текст собеседника.

Разработчики WhatsApp уже признали наличие проблемы и работают над ее устранением…» ***(Хакеры могут менять в WhatsApp чужие сообщения // NewsOboz (http://newsoboz.org/it_tehnologii/hakery-mogut-menyat-v-whatsapp-chuzhie-soobshcheniya-09082018101500). 10.08.2018).***

***

«Гаджеты и приложения, используемые маленькими магазинами и трейдерами для превращения смартфонов и планшетов в карманные платежные терминалы, уязвимы к кибератакам. Об этом сообщили исследователи безопасности Ли-Энн Галлоуэй (Leigh-Anne Galloway) и Тим Юнусов (Tim Yunusov) из компании Positive Technologies…

Подобные мобильные терминалы часто используются в кафе, спортзалах и других небольших заведениях для осуществления безналичных платежей. Исследователи протестировали устройства от PayPal, SumUp, iZettle и два гаджета от Square.

По словам специалистов, злоумышленник может перехватить зашифрованное Bluetooth-соединение между устройством и его мобильным терминалом и изменить данные, заставив клиента заплатить больше.

Помимо этого, исследователи обнаружили в двух устройствах критические уязвимости, позволяющие злоумышленнику исследовать файловую систему устройства, считывать PIN-коды и выполнять произвольный код.

Если продукт стоит менее $100, у него не будет должных механизмов безопасности. Некоторые продавцы выполняют только минимальные…» ***(Хакеры нашли способ атаковать мобильные платежные устройства // PaySpaceMagazine «доступно о платежах» (https://psm7.com/pos-terminal/xakery-nashli-sposob-atakovat-mobilnye-platezhnye-ustrojstva.html). 10.08.2018).***

***

«…авторы отчета Appthority, проанализировав тысячу популярных приложений для Android и iOS, …обнаружили, что хотя многие приложения не содержат следов вредоносного программного обеспечения и вопиющих уязвимостей, они обмениваются и хранят данные на ненадежных бэкэнд-серверах, предоставляя доступ к пользовательским данным всем желающим.

…В своем новом отчете эксперты Appthority проанализировали уже более 2,7 млн мобильных приложений под Android и iOS. Исследователи обнаружили, что из 27 227 приложений для Android и 1275 приложений для iOS, использующих для организации бэкэнда системы базы данных Firebase, 3046 приложений были уязвимы, а 2271 и вовсе хранили данные в незащищенных базах данных, доступ к которым мог получить буквально любой желающий…

Всего в уязвимых приложениях (более 100 млн записей в 113 гигабайт данных), по оценкам исследователей, скомпрометировано 2,6 млн идентификаторов пользователей и паролей в текстовом формате, 25 млн хранимых записей местоположения GPS, 50 000 записей о финансовых транзакциях и данные более 4,5 млн аккаунтов в социальных сетях и корпоративных базах данных. Легкой добычей злоумышленников среди прочего могут стать 4 млн записей PHI (Protect Health Information, защищенные данные о здоровье), содержащих личные чаты и записи рецептов. Затронутые в отчете Android-приложения были загружены более чем 620 млн раз из магазина Google Play, что делает разработчиков приложений наиболее успешными распространителями уязвимого программного обеспечения…

Вдогонку Appthority обнародовали рейтинг риска для информационной безопасности корпораций тех или иных популярных у пользователей приложений, в котором тройка лидеров и вовсе поражает — WhatsApp, Facebook Messenger, Telegram для Android и WhatsApp Messenger, Facebook Messenger и Waze для iOS признаны самыми опасными мобильными приложениями по состоянию на конец апреля 2018 года…

Помимо рейтинга самых опасных приложений Appthority также представили черный список мобильных приложений по версии служб безопасности компаний…

Самые «популярные» категории приложений из черного списка составляют сервисы для обмена сообщениями, социальные сети и приложения для знакомств. Для Android это: Facebook Messenger, Wickr Me и WhatsApp Messenger; для iOS: Facebook Messenger, WhatsApp Messenger и Tinder…» ***(Находка для шпиона: как Telegram и Facebook попали в список опасных мобильных приложений // Goodnews.ua (http://goodnews.ua/technologies/naxodka-dlya-shpiona-kak-telegram-i-facebook-popali-v-spisok-opasnyx-mobilnyx-prilozhenij/). 04.08.2018).***

***

«…Исследование компании Check Point показало, что хакеры могут навредить организациям через факсимильные аппараты с помощью уязвимостей в протоколах связи.

Злоумышленнику нужен только номер факса компании, который обычно находится в свободном доступе на корпоративном сайте. Ошибки в протоколах позволяют кодировать вредоносный код в изображения, которые факсимильный

аппарат загружает в свою память. Далее этот код распространяется по сетям, к которым подключено устройство.

Многие компании даже не знают, что к ним подключен факсимильный аппарат или возможности факса встроены во многие многофункциональные офисные и домашние принтеры, рассказали в Check Point Software Technologies. Исследование продемонстрировало, что хакеры могут атаковать устройства, безопасность которых зачастую упускается из виду…» ***(Злоумышленники атакуют компании через факсы // «Открытые системы» (https://www.computerworld.ru/news/Zloumyshlenniki-mogut-atakovat-kompanii-cherez-faxy). 14.08.2018).***

***

«В рамках ежегодного мероприятия DefCon в Лас-Вегасе (США) — крупнейшей в мире конференции для хакеров — эксперты по кибербезопасности представили новый способ взлома «умных» колонок, популярность которых стремительно растет в последние годы.

…специалисты одного из подразделений китайского технологического гиганта Tencent By Хуэйю и Цянь Вэнь Сян представили способ, благодаря которому им удалось взломать динамик Amazon Echo. Чтобы осуществить задуманное, им потребовалось разобрать колонку, изъять чип флеш-памяти из материнской платы, перепрошить встроенное программное обеспечение и вставить чип обратно. Таким образом, «модифицированный» динамик стал идеальным устройством для совершения атак на другие колонки Echo через подключение его к той же сети Wi-Fi. Используя уязвимости интерфейса Amazon Alexa (встроенный в колонки голосовой помощник) на сайте Amazon.com, китайские специалисты задействовали перенаправление URL-адресов, межсайтовый скриптинг и понижение уровня веб-шифрования. После получения контроля над другими динамиками удалось прослушать и записать разговоры в комнате, а также дать команду о воспроизведении музыки.

Как отметили представители Tencent, этот способ практически невыполним, так как как минимум необходимы физический доступ к колонке Echo и знания о том, как разобрать устройство…» ***(Евгения Чернышева. Говорите громче! // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3713531?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). 14.08.2018).***

***

«Американская компания IOActive, специализирующаяся на кибербезопасности, опубликовала во вторник доклад, в котором рассказала о существенных проблемах с безопасностью и уязвимостях многих трейдинговых приложений.

Аналитики IOActive в течение года — с середины 2017 года по июнь 2018 — рассматривали деятельность популярных трейдинговых платформ, в том числе 34 мобильных приложений, 16 приложений для ПК и 30 сайтов. Среди них были такие платформы, как Ally Financial, TradeStation, Yahoo! Finance, AvaTrade, IQOption.

Аналитики пришли к выводу, что трейдинговые приложения в среднем защищены хуже, чем приложения розничного банкинга. Трейдинговые приложения довольно легко взломать хакеру — во многих из них пароли пользователей хранятся в незашифрованном виде, также часто пользователь не может воспользоваться двухфакторной аутентификацией, например, с помощью кода в сообщении.

В докладе IOActive содержится информация о том, какие из приложений более надежны, а каким нужно поработать над уровнем безопасности.» ***(Яна Рождественская. Специалисты по кибербезопасности рассказали об уязвимостях трейдинговых приложений // АО «Коммерсантъ» https://www.kommersant.ru/doc/3708226). 08.08.2018).***

***

«Количество банковских троянов для мобильных телефонов, с помощью которых могут быть похищены средства граждан, выросло втрое, отмечают эксперты…

Во втором квартале 2018 года число банковских троянов для мобильных устройств выросло в 3,2 раза по сравнению с первым кварталом, следует из исследования «Лаборатории Касперского». В результате на конец первого полугодия общее число выявленных вирусов этого типа составило 61 тыс. штук. Трояны используют фишинговые окна для кражи сведений о банковской карте и аутентификационных данных онлайн-банкинга. Кроме того, они воруют деньги посредством СМС-сервисов, в том числе сервисов мобильного банкинга. Наиболее уязвимы для троянов мобильные устройства с операционной системой Android…

Принцип действия выявленных троянов следующий: вредонос скачивается на телефон, затем подменяет собой легальное приложение и получает логин и пароль, дающий доступ к мобильному банку…». ***(Вероника Горячева. Трояны множатся в мобильном банке // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3707072?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 07.08.2018).***

***

«Некорректная настройка страниц на Trello, популярном web-сайте для управления проектами, правительствами Великобритании и Канады привело к раскрытию уязвимостей в программном обеспечении и планов по обеспечению безопасности, а также паролей для серверов, официальных интернет-доменов и пр…

По словам обнаружившего утечку исследователя Кушгары Патака (Kushagra Pathak), он выявил 25 общедоступных досок Trello, принадлежащих разным правительственным ведомствам Великобритании. Они включали учетные данные для входа в учетную запись у регистратора домена, электронные письма, ссылку на фрагмент кода межсетевого экрана правительственного сайта и отчеты об ошибках.

Также были обнаружены доски с информацией о конференц-вызовах и кодах доступа и информация для входа в инструмент администрирования сервера, известный как CPanel. Патак сообщил об этом через Национальный центр

кибербезопасности Великобритании, который удалил большинство досок в течение нескольких дней.

Вскоре после этого эксперт нашел 25 канадских правительственных досок, содержавших еще более чувствительную информацию, такую как удаленный доступ к файлам или FTP и учетные данные для входа в платформу планирования событий Eventbrite. Другие доски включали ссылки на файлы Excel об управлении web-приложениями, обсуждение дополнительных мер по обеспечению безопасности и другие важные документы…» ***(Британские и канадские правительства случайно раскрыли планы безопасности всему интернету // Goodnews.ua (http://goodnews.ua/technologies/britanskie-i-kanadskie-pravitelstva-sluchajno-raskryli-plany-bezopasnosti-vsemu-internetu/). 18.08.2018).***

***

«Эксперты по кибербезопасности из компании Okta REX обнаружили способ обхода двухфакторной аутентификации в ОС Windows с помощью уязвимости в службе ADSF (Active Directory Federated Services).

…система аутентификации ADFS не проверяет соответствие данных при получении запроса на доступ. Таким образом, хакер может использовать перехваченный ранее ключ авторизации…

Данная атака работает и на других устройствах, использующих решения на базе ADFS, например, Authlogics, Duo Security, Gemalto, Okta, RSA и SecureAuth. В настоящее время Microsoft выпустила исправления, устраняющие проблему.» ***(Обнаружен способ обхода двухфакторной аутентификации Microsoft // Goodnews.ua (http://goodnews.ua/technologies/obnaruzhen-sposob-obxoda-dvuxfaktornoj-autentifikacii-microsoft/). 20.08.2018).***

***

«Эксперты по кибербезопасности Раймонд Хилл (Raymond Hill) и Майк Кукец (Mike Kuketz) признали опасным популярное расширение для браузера Mozilla Firefox под названием Web Security…

Специалисты заметили, что надстройка отправляет загруженные юзерами URL-адреса на немецкий сервер. Благодаря этому из-за установленного расширения информация о посещенных сайтах становится доступна третьим лицам. Более того, каждый пользователь получал уникальный идентификатор, поэтому хакеры имели возможность шпионить за поведением определенного человека в интернете.

Создатели расширения пообещали расследовать ситуацию с незаконным сбором данных.

Вскоре после сообщения экспертов по кибербезопасности программа Web Security пропала из списка рекомендуемых приложений, однако ее до сих пор можно загрузить в официальном магазине Firefox. За все время существования ее скачали более 220 тысяч раз…» ***(Популярное расширение для браузера уличили в шпионаже // Goodnews.ua (http://goodnews.ua/technologies/populyarnoe-rasshirenie-dlya-brauzera-ulichili-v-shpionazhe/). 17.08.2018).***

***

«Производитель программного обеспечения для кибербезопасности Check Point Software Technologies сообщил об уязвимости в операционной системе Android. Ее злоумышленники могут использовать для атаки устройств, автоматической загрузки вредоносных приложений и т. п…

Уязвимость позволяет проводить атаки типа "отказ в обслуживании" для легитимных приложений и вызвать сбои в их работе, а также атаки типа "внедрение кода", которые затем могут запускаться в привилегированном контексте атакуемого приложения.

В Check Point отмечают, что внешнее хранилище устройства Android является общедоступной областью, которая может быть обнаружена или изменена сторонним (вредоносным) приложением. Android не предоставляет встроенных средств защиты для данных, хранящихся на внешнем накопителе.

Многие предустановленные и популярные приложения хранят конфиденциальные данные в незащищенном внешнем хранилище. Это может привести к атаке "Man-in-the-Disk" и манипулированию и злоупотреблению незащищенными конфиденциальными данными, предупреждают эксперты.» **(В Android нашли уязвимость, позволяющую атаковать устройства // Goodnews.ua (http://goodnews.ua/technologies/v-android-nashli-uyazvimost-pozvolyayushhuyu-atakovat-ustrojstva/). 15.08.2018).**

***

«Хакеры научились взламывать нагрудные камеры полицейских и удалять оттуда записи. Об этом рассказал консультант по кибербезопасности компании Nuix Джош Митчелл на ежегодной хакерской конференции DefCon.

Уязвимость продемонстрировали на пяти различных камерах, которые были разработаны специально для сотрудников правоохранительных органов. Среди взломанных устройств были камеры Vievu, Patrol Eyes, Fire Cam, Digital Ally и CeeSc.

Эксперт также показал, что хакеры могут манипулировать девайсом по своему усмотрению. Например, они имеют возможность удалять все кадры и связанные с ними метаданные, такие как местоположение, время и дата записи…»***(Хакеры научились взламывать нагрудные камеры полицейских // Я и Закон (https://yaizakon.com.ua/hakery-nauchilis-vzlamyvat-nagrudnye-kamery-politsejskih/). 15.08.2018).***

***

«К нашумевшим уязвимостям Meltdown и Spectre присоединилась еще одна, которую назвали Foreshadow. В Intel о ней узнали еще в начале года от двух групп исследователей, а публично раскрыли сведения только недавно.

Атака Foreshadow позволяет получить данные, хранимые в «анклавах» SGX (Security Guard Extensions, система, защищающая участки памяти от доступа привилегированных процессов), с использованием механизма упреждающего выполнения. При попытке внешнего считывания анклава механизм упреждающего выполнения может изменить кэш в зависимости от считанных данных, однако в

этом случае процессор отключает возможность считывания кэша. Но исследователи выяснили, что если конфидециальные данные находятся в кэше первого уровня, механизм упреждающего выполнения может использовать их еще до того, как процессор определит, что это запрещено.

Эксперты выражают опасение, что уязвимость, в частности, позволяет разрушать защитные барьеры между виртуальными машинами, работающими в одной инфраструктуре.

Брешь присутствует в чипах Core 7-го поколения и более новых, а также в Xeon соответствующих поколений. Ошибка, которую в самой Intel называют L1TF, будет устранена на аппаратном уровне в Xeon Cascade Lake, а также во всех процессорах Intel, которые выйдут в этом году. В корпорации подчеркивают, что случаи реальных атак с использованием Foreshadow на сегодня неизвестны. В AMD в свою очередь заявляют, что, по данным компании, ее процессоры бреши не подвержены.» ***(В процессорах Intel обнаружена еще одна серьезная брешь // «Открытые системы» (https://www.computerworld.ru/news/V-protsessorah-Intel-obnaruzhena-esche-odna-sereznaya-bresh). 21.08.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Исследователи предложили «засевать» ПО поддельными безвредными уязвимостями и тем самым заставить хакеров тратить свое время впустую.

Как ни парадоксально это звучит, но чем больше уязвимостей в системе, тем надежнее она защищена. Если при разработке умышленно добавить в продукт поддельные, неэксплуатируемые уязвимости, хакерам придется потратить много времени и ресурсов в попытках осуществить атаку с их помощью. В итоге, так и не добившись успеха, злоумышленники оставят попытки еще до того, как найдут настоящую уязвимость.

Идея защиты ПО с помощью поддельных уязвимостей изложена в исследовании специалистов Политехнического института Нью-Йоркского университета (США)…

Как бы то ни было, но из-за ряда ограничений техника «засевания» ПО фальшивыми багами может так никогда и не стать широко используемой. Во-первых, она не подходит для ПО с открытым исходным кодом. Во-вторых, разработчики должны быть на сто процентов уверенными в том, что добавленная ими уязвимость по-настоящему безвредна и никак не связана с настоящими. В третьих, техника работает только в том случае, если допустимо аварийное завершение работы ПО в результате ввода вредоносных данных.» ***(Защитить ПО от хакеров помогут уязвимости // SecurityLabRu (https://www.securitylab.ru/news/494952.php). 08.08.2018).***

***

«На конференции Black Hat, посвящённой вопросам кибербезопасности, компания BlackBerry представила новое ПО, которое, как она заявляет, поможет организациям ускорить восстановление работоспособности после атак ransomware…

Новое ПО анонсировано как часть платформы совместной работы BlackBerry Workspaces. Его задача: помочь изолировать и ограничить ущерб от вымогательских атак путём замораживания учётных записей пострадавших пользователей.

Используя данный инструмент, администратор может проверять журналы активности пользователей, чтобы в точности установить какие рабочие пространства, папки и файлы подверглись атаке, и избирательно вернуть их ненарушенные версии. При этом глубина «отката» не ограничивается.

В отличие от часто практикуемого восстановления из бэкапа всей системы, возможность удалять только инфицированные файлы позволит организациям нормализовать ситуацию с минимальным ущербом для продуктивности их рабочих процессов.

Новая функция восстановления после атак ransomware будет доступна в версиях BlackBerry Workspaces Collaborate и Secure Plus без какой-либо дополнительной оплаты. Фирма продемонстрирует эту технологию на саммитах BlackBerrySecurity 2018 в Лондоне 12 сентября и в Нью-Йорке 4 октября.» ***(BlackBerry представила ПО для быстрого восстановления после кибератак // «Компьютерное Обозрение» (https://ko.com.ua/blackberry_predstavila_po_dlya_bystrogo_vosstanovleniya_posle_kiberatak_125599). 08.08.2018).***

***

«Check Point объявила о новых возможностях своего мобильного корпоративного решения для защиты от угроз, SandBlast Mobile. Версия SandblastMobile 3.0 представляет новую парадигму мобильной безопасности с предотвращением сетевых угроз на уровне устройства.

Среди новых возможностей SandBlast Mobile в компании отмечают:

Предотвращение фишинговых атак для всех приложений.

Блокировка просмотра вредоносных сайтов, на которых устройства могут заразиться.

Блокировка зараженных устройств от отправки конфиденциальных данных в бот-сети.

Защита корпоративных приложений и данных от доступа из зараженных устройств.

Автономное устранение угроз, без зависимости от пользовательских действий или мобильных платформ управления…» ***(Check Point SandblastMobile 3.0 предотвращает сетевые угрозы на уровне устройств // «Компьютерное Обозрение» (https://ko.com.ua/check_point_sandblastmobile_3_0_predotvrashhaet_setevye_ugrozy_na_urovne_ustrojstv_125538). 02.08.2018).***

***

«Компания ESET представила новую линейку продуктов для усиления защиты малых и средних предприятий, а также обеспечения более высокого уровня безопасности корпораций…

Одной из главных новинок продуктовой линейки стало решение ESET Dynamic Threat Defense — встроенная облачная песочница, которая осуществляет анализ «0-дневных» угроз и программ-вымогателей, предупреждая их проникновение в корпоративную сеть.

…в обновленную линейку решений для корпоративных пользователей вошло решение ESET Security Management Center, которое является новой версией известной онлайн-консоли ESET Remote Administrator. Обновленный продукт для удаленного управления обеспечивает не только полный обзор сети и управление безопасностью с одной консоли, но и возможность полной настройки отчетности и устранения угроз в один клик...

Еще одним важным решением для повышения кибербезопасности предприятий является инструмент для выявления и отслеживания событий на рабочих станциях — ESET Enterprise Inspector. Решение сообщает специалисту по ИТ-безопасности о подозрительной активности, помогает исследовать инцидент безопасности и мгновенно отреагировать на него…

Кроме новых решений, в рамках новой продуктовой линейки была также представлена версия 7 продуктов для обеспечения безопасности рабочих станций и серверов…

Новая версия продуктов для защиты рабочих станций и серверов уже доступна для загрузки на страницах украинского официального сайта.» ***(ESET выпустила новую продуктовую линейку для корпоративных пользователей // «Компьютерное Обозрение» (https://ko.com.ua/eset_vypustila_novuyu_produktovuyu_linejku_dlya_korporativnyh_polzovatelej_125722). 17.08.2018).***

***

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

Біленчук П.Д. Криміналістична характеристика транснаціональних комп'ютерних злочинів / П.Д. Біленчук, Л.В. Борисова, В.П. Колонюк // Криміналістика і судова експертиза. – 2018. – Вип. 63.- Ч. 1.- С. 163-174.

На основі аналізу нормативних документів встановлено, що сьогодні не існує чітко визначеного поняття «комп'ютерний злочин». Запропоновано уточнюючі поняття основних елементів криміналістичної характеристики транснаціональних комп'ютерних злочинів.

Шифр зберігання НБУВ: Ж29323.

***

Васильковський І.І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення / І.І.Васильковський // Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). – 2018. – Вип. 1-2. – С. 276-282.

Визначено основні поняття кіберзлочинності, кіберзлочинів і їх співвідношення. Охарактеризовано ризики, які виникають у результаті здійснення такого виду діяльності.

Шифр зберігання НБУВ: Ж74495.

***

Глобальні виміри захисту економічної конкуренції. ІІ Міжнародна науково-практична конференція, 28 лютого 2018 року. – Київ, 2018. – 133 с.

Зі змісту:

Волков О.О. Заходи кібербезпеки підприємницької діяльності.

Шифр зберігання НБУВ: ВА820910.

***

Гуйван О.П. Превентивний правовий захист інформаційних ресурсів /О.П. Гуйван // Прикарпатський юридичний вісник. – 2017. – Вип. 6. – Том 1.- С. 74-78.

Проаналізовано теоретичні та практичні засади організації захисних правових дій, спрямованих на перешкоджання протиправним посяганням в інформаційному середовищі.

Шифр зберігання НБУВ: Ж74200.

***

Діордіца І. В. Основні поняття та ідеї кібернетики як засади виділення кібернетичної функції держави / І. В. Діордіца // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. – 2017. – Вип. 30(1). – С. 86-88.

Проаналізовано основні поняття та ідеї кібернетики як засад виділення кібернетичної функції держави. Сформульовано уніфіковане визначення поняття кібернетичної функції держави на національному та універсальному рівнях. Подано авторське розуміння поняття засадничих положень кібернетики та її застосування в сучасних реаліях державотворення.

Шифр зберігання НБУВ: Ж74042.

***

Діордіца І.В. Функціїї кібернетичної деонтології / І.В. Діордіца // Прикарпатський юридичний вісник. – 2017. – Вип. 6. – Том 2.- С. 26-31.

Охарактеризовано визначення понять «деонтологія», «кібернетична деонтологія». Виокремлено основні аспекти кібернетичної деонтології. Проаналізовано функції кібернетичної деонтології.

Шифр зберігання НБУВ: Ж74200.

***

Матеріали всеукраїнської науково-практичної конференції «Сучасна наукова дискусія: питання юриспруденції», 20-21 жовтня 2017 р., м. Запоріжжя. – Запоріжжя, 2017. – 103 с.

Зі змісту:

Гріщенко А.О. Правові засади створення ефективного сектору інформаційної та кібернетичної безпеки в Україні.

Шифр зберігання НБУВ: ВА820665.

***

Матеріали Всеукраїнської науково-практичної конференції «Одеські юридичні читання», 10-11 листопада 2017 року. – Одеса, 2017. – 307 с.

Зі змісту:

Забара І.М. Сучасні пріоритети правового регулювання кібербезпеки Європейського Союзу.

Шифр зберігання НБУВ: ВА821338.

***

Матеріали Міжнародної науково-практичної конференції «Теорія і практика актуальних наукових досліджень» (27-28 жовтня 2017 року). – Львів, 2017.- Ч. 1. – 179 с.

Зі змісту:

Рябуха А.І., Пацановська Л.О. Кіберзлочинність – як основний виклик сучасному світу.

Шифр зберігання НБУВ: В357110/1.

***

Матеріали Міжнародної науково-практичної конференції «Теорія і практика актуальних наукових досліджень» (27-28 жовтня 2017 року). – Львів, 2017.- Ч. 2. – 179 с.

Зі змісту:

Кисельов Д.О., Власенко С.М. Законодавство в сфері захисту інформації та забезпечення кібербезпеки;

Кільдішев В.Й., Стайкуца С.В., Овчаров В.О. Аналіз уразливостей персональних мобільних пристроїв.

Шифр зберігання НБУВ: В357110/2.

***

Міжнародне право: de lege praeterita, instante, futura : матеріали VII Міжнар. Наук.-практ. конф., 8 груд. 2017 р. – Одеса, 2017. – 199 с.

Зі змісту:

Забара І.М. Ретроспектива і сучасність правового регулювання забезпечення кібернетичної безпеки Європейського Союзу.

Шифр зберігання НБУВ: ВА821337.

***

Піцик Ю. М. Класифікація кіберзлочинів проти власності /Ю. М. Піцик // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. – 2017. – Вип. 30(2). – С. 65-68.

Розглянуто заходи, вжиті в законодавчій, інституційній сфері в Україні, напрями науково-криміналістичного забезпечення, спрямовані на боротьбу з кіберзлочинністю. Надано авторську класифікацію кіберзлочинів проти власності.

Шифр зберігання НБУВ: Ж74042.

***

Самойленко О.А. Природа кіберпростору як об'єкта криміналістичного дослідження / О.А.Самойленко // Криміналістика і судова експертиза. – 2018. – Вип. 63.- Ч. 1.- С. 174-182.

Визначено особливості кіберпростору, які злочинець використовує з метою досягнення злочинного результату.

Шифр зберігання НБУВ: Ж29323.

***

Становлення і розвиток правових основ та ситеми захисту персональних даних в Україні : монографія / Прилипчук В. Г., Брижко В.М., Баранов О.А., Мельник К.С. – Київ, 2017. – 225 с.

На основі історичного та системного аналізу розглянуто проблеми формування і розвитку правових основ та системи захисту персональних даних в контексті євроінтеграції України. Висвітлено відповідний досвід країн-членів Ради Європи та Європейського Союзу. Охарактеризовано організаційно-правові проблеми захисту персональних даних.

Шифр зберігання НБУВ: ВА820523.

***

Сьома міжнародна науково-практична конференція «Інфокомунікації – сучасність і майбутнє», 26-27 жовтня 2017 року : зб. Тез. – Одеса : ОНАЗ, 2017. – Ч. 1. – 147 с.

Зі змісту:

Замега М.О. Аналіз методів забезпечення безпеки інформації в комп'ютерних мережах;

Пономарьов А.К. Забезпечення захисту інформації в технології WIMAX;

Цвілій О.О., Майстренко А.В. Застосування в Україні критеріїв оцінки безпеки в комп'ютерній системі;

Цикалевич О.М. Мережі передачі даних та засоби захисту інформації;

Шматько Ю.М. Процесний підхід до побудови системи захисту інформаційної системи організації від несанкціонованого доступу.

Шифр зберігання НБУВ: В357103/1.

***

Юдін О.К. Державні інформаційні ресурси. Методологія побудови та захисту українського сегмента дерева ідентифікаторів / О. К. Юдін, С. С. Бучик. – Київ, 2018. – 318 с.

Проведено аналіз існуючого забезпечення захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах та українського сегмента дерева ідентифікаторів. Визначено правові аспекти формування системи державних інформаційних ресурсів.

Шифр зберігання НБУВ: ВА821336.

Виготовлено в друкарні
ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, ул.. 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.