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

№ 2 (лютий)

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

«Чотири роки поспіль президент Петро Порошенко бере участь у найпрестижнішому міжнародному форумі з питань світової безпеки… Переговори з міністром оборони США, прем'єрами Британії та Польщі, з керівниками НАТО та Єврокомісії – достатній привід для поїздки на Мюнхенську безпекову конференцію (далі – MSC, Munich Security Conference)…

…Сюди приїхали 25 президентів та голів урядів, перші особи ООН, НАТО, ЄС...

Темою, яку згадували найчастіше, стала загроза ядерної війни. Нині, вперше від часів холодної війни, про неї говорять як про реальну небезпеку…

На одному з чільних місць – проблема кібербезпеки…

Як приклад кіберзагроз нового типу найчастіше наводили дії Росії…

Питання про те, що робити з кібервійною, залишилося відкритим. Ідея генсека ООН про розробку міжнародного договору про правила кібервійни (на кшталт Конвенції про закони і звичаї війни, яка діє ще від початку минулого сторіччя) не знайшла підтримки – жоден зі світових лідерів не став її розвивати…

Світові безпекові зустрічі, на кшталт Мюнхена, традиційно є гарною нагодою, щоби позбавитися ілюзій щодо "україноцентричності" світової політики – достатньо просто перерахувати всі гарячі точки і проблеми, щоб зрозуміти, що світ не обертається навколо нас…

Найяскравішою ілюстрацією став виступ президента України.

…Так, президент знову говорив про наш конфлікт, але тепер – у глобальному контексті.

Росія напала не лише на Україну, а на цивілізований світ. Злам світової системи вдарить по всіх. Кібератаки проти нас вже зараз б'ють далеко не лише по Україні, а й по інших державах…

Йдеться про світову гібридну війну, наголосив український президент.

І до всього цього додається готовність РФ використати війська та відновлення російської ядерної загрози.

Отже, учасники конференції в Мюнхені могли почути промову представника України, яка звучить в унісон зі світовим порядком денним (нехай навіть є питання щодо щирості окремих заяв Порошенка).

Ми пишемо "могли почути" – бо президента не почув майже ніхто.

Фото з порожнім залом під час його виступу – правдиві. Причому люди не йшли під час його виступу, і це не було "бойкотом". Просто українське питання здалося нецікавим більшості учасників. Зал почав порожніти ще на попередній панелі…

Через навалу інших проблем у різних куточках світу – світ продовжує втрачати інтерес до подій в Україні. Ідея про миротворців – у глухому куті… А нинішньої "стабілізації" на лінії зіткнення на Донбасі, яка є в останні роки, цілком достатньо, щоби відкласти українське питання у довгу шухляду.

Чи не єдиною українською темою, яка й досі викликає зацікавленість партнерів, лишаються реформи в нашій державі…

..варто підкреслити ще один висновок за підсумками Мюнхенської конференції.

…світ зіткнувся з безпрецедентною кількістю викликів, і навіть якщо говорити про глобальне протистояння Росії та Заходу, то воно є лише однією з низки сучасних проблем. Так, світ нині не бачить шляху, який дозволив би здолати російську загрозу…» ***(Сергій Сидоренко. Україна в довгій шухляді: в Мюнхені визначили нові пріоритети світової безпеки // Європейська правда (http://www.eurointegration.com.ua/articles/2018/02/19/7077699/). 19.02.2018).***

***

«Українські волонтери близько двох років використовували вразливість на сайті Міністерства оборони РФ для збору закритої інформації про зарплатні відомості російських військових, які воюють в Україні та Сирії.

Про це, посилаючись на речника Українського кіберальянсу…

Зокрема, в одній з публікацій міжнародної розвідувальної спільноти InformNapalm розміщено скріншоти зарплатних відомостей матроса 99-ї тактичної групи Північного флоту РФ (в/ч №74777) Юрія Попова…

Через вразливість на сайті Міністерства оборони РФ також було доведено, що матрос, перебуваючи на Донбасі в складі бандформувань «ДНР» продовжував отримувати зарплатню від Міноборони Російської Федерації.

…Міністерство оборони РФ офіційно підтвердило, що витік інформації з їхнього сайту є достовірною інформацією, і всі зарплатні відомості військовослужбовців, помічених на Донбасі, вказують на пряме фінансування агресії» ***(Українські волонтери збирали закриту інформацію на сайті Міноборони РФ – Informnapalm // Західна інформаційна корпорація (https://zik.ua/news/2018/02/06/ukrainski_volontery_zbyraly_zakrytu_informatsiyu_na_sayti_minoborony_rf__1259951). 06.02.2018).***

***

«В Україні на підприємствах часто недооцінюють загрози інформаційної безпеки, які пов'язані з масовою втратою даних через комп'ютерні віруси. Про це …розповів IT-директор компанії Eastern Beverage Trading Дмитро Фомін…

«Питання своєчасних оновлень, наявності актуальних резервних копій, виконання регламентів доступу до інформаційних систем не менш важливі, ніж контроль і обмеження доступу до даних або надія на встановлений антивірус», — наголосив Д.Фомін.

Експерт підкреслив, що “саме контроль над базовими процесами інформаційної безпеки є найкращою профілактикою від вірусів подібних WannaCry і Petya”…» ***(Петро Івасюк. Загрози інформаційної безпеки часто недооцінюють – Фомін // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1714119-zagrozi-informatsiynoyi-bezpeki-chasto-nedootsinyuyut-fomin).08.02.2018).***

***

«Державне підприємство Укренерго планує витратити $20 млн на нову систему кіберзахисту для компанії, яка за останні два роки кілька разів страждала від кібератак…

Система повноцінно запрацює в 2020 році. Вона буде містити нове програмне забезпечення і "адміністративні заходи"…

Крім цього, в компанії створили Центр реагування на кіберінциденти й реорганізували відділ IT-безпеки…» ***(На систему кіберзахисту "Укренерго" планують витратити $20 млн, - Reuters // «iPress»(http://ipress.ua/news/na_systemu_kiberzahystu_ukrenergo_planuyut_vytratyty_20_mln__reuters_243906.html). 06.02.2018).***

***

Національна система кібербезпеки

«Секретар Ради національної безпеки і оборони України Олександр Турчинов 2 лютого відкрив Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC)…

За словами Турчинова, Центр виявлятиме кіберзагрози на ранніх стадіях їх виникнення.

«Центр, який побудований в Україні, буде співпрацювати з аналогічними центрами країн НАТО. Взаємодіючи з ними, значно покращиться якість реагування на кіберінциденти, за рахунок обміну інформації, підтягування потужних обчислювальних машин і ресурсів. Все це дає можливість і інформувати наших колег і використовувати від них інформацію в онлайн-режимі», – заявив Турчинов…» ***(У Києві з'явився Центр реагування на кіберзагрози // Західна інформаційна корпорація (https://zik.ua/news/2018/02/02/u_kyievi_zyavyvsya_tsentr_reaguvannya_na_kiberzagrozy_1257219). 02.02.2018).***

***

«Военные и представители других ведомств, занимающиеся киберзащитой и кибербезопасностью, будут получать надбавку к зарплате — до 100% должностного оклада. Такое решение принял Кабинет министров Украины.

…постановление правительства распространяется на лиц, занимающихся кибербезопасностью и киберзащитой в таких структурах, как Вооруженные Силы, СБУ, Служба внешней разведки и другие разведывательные органы, а также Государственная служба спецсвязи и защиты информации.

Вознаграждение составит до 100% должностного оклада с учетом надбавок за воинское звание и выслугу лет…» ***(Военнослужащие-киберзащитники будут получать двойную зарплату // Факты и комментарии® (http://fakty.ua/259330-voennosluzhacshie-kiberzacshitniki-budut-poluchat-dvojnuyu-zarplatu). 27.02.2018).***

***

«На днях Государственный центр киберзащиты и противодействия киберугрозам Госспецсвязи провел небольшой научно-технический семинар-лекцию на тему своей деятельности в сфере киберзащиты и безопасности государственных информационных ресурсов.

…Вектор дискуссии во вступительном слове обрисовал начальник ГЦК Госспецсвязи Роман Боярчук…

Он также упомянул о необходимости прислушиваться к общественности и популяризировать кибергигиену…

…Александр Палий, сотрудник Правительственной команды реагирования CERT-UA рассказал об основных задачах его команды в сфере обеспечения кибербезопасности…

На CERT-UA лежит функция анализа систем на счет уязвимостей, которые могут использоваться злоумышленниками для компрометации сайтов, взломов госресурсов и т.д. Также в обязанности правительственной команды входит сбор информации об угрозах в ИТС ОГВ и объектов критической информационной инфраструктуры в рамках Центра реагирования на киберугрозы…

Отдельным направлением работы Команды является оценка защищенности сайтов, состоящая из 5 элементов: поиск уязвимостей веб-сайтов с помощью сканера уязвимостей веб-приложений; поиск панелей администратора; эксплуатация найденных уязвимостей; получение прав администратора; загрузка веб-шэла.

После запуска Центра реагирования на киберинциденты… он происходит этап тестирования. На этом этапе (несколько месяцев) будет внедрен регламент взаимодействия участников системы, чтобы понять, как Центры реагирования должны сотрудничать с теми, кто к ним обращается, и какие функции на себя в будущем возьмет тот или иной Центр…

Практически 2/3 доклада Первого заместителя начальника Госцентра киберзащиты Николая Худинцева были посвящены теоретическим основаниям работы ГЦК. В частности, Худинцев разработал систему «семи шагов», объясняющую принципы будущей успешной работы Центра и основ информационной безопасности Украины…

Первый замначальника ГЦК особо подчеркнул важность научной работы, которая должна стать основой для взаимодействия и органов государственной власти и частно-государственного партнерства в сфере киберзащиты…

Коснулся Николай Худинцев и вопроса уже реализуемых инфраструктурных проектов…

Первым делом Николай Николаевич рассказал о создании Национальной телекоммуникационной сети. Это транспортная сеть, сеть доступа между органами государственной власти в Украине. На сегодня завершен этап проектирования и начинается этап строительства этой системы…

Упомянул Худинцев и о системе защищенного доступа органов государственной власти к сети интернет…

Следующая задача, которой занимается Госспецсвязи и Центр – построение основного и резервного защищенных дата-центров сохранения информации и сведений государственных электронных информационных ресурсов…

Из «интересных» инфраструктурных проектов отметил Худинцев также систему защищенной межведомственной мобильной и телефонной связи, а также систему киберзащиты государственных информационных ресурсов и объектов критической информационной инфраструктуры…» ***(Владимир Кондрашов. Госцентр киберзащиты поделился планами и секретами // InternetUA (http://internetua.com/goscentr-kiberzasxit-podelilsya-planami-i-sekretami). 28.02.2018).***

***

«На Правительственном портале опубликована одобренная в январе 2018 года Концепция развития цифровой экономики и общества Украины на 2018-2020 годы и план мероприятий по ее реализации…

В Плане на 2018 преобладают «подготовительные работы»…

…Согласно тексту Концепции, её целью является реализация ускоренного сценария цифрового развития, ...который предусматривает устранение бюрократических препятствий, мешающих развитию цифровой экономики (на этом, согласно, Плану, сконцентрируются в 2018-м году); поощрения для бизнеса, стремящегося к цифровизации; внедрение государством масштабных проектов цифровых преобразований на базе современных моделей государственно-частного партнерства; создание и развитие цифровых инфраструктур; развитие и углубление цифровых компетенций граждан; развитие цифрового предпринимательства.

Концепция ставит достаточно амбициозные цели к 2020-му году:

– 30 место в рейтинге Networked Readiness Index (WEF) (в 2016 году - 64 место);

– 40 место в рейтинге Global Innovation Index (INSEAD, WIPO) (в 2016 году - 56 место);

– 50 место в рейтинге ICT Development Index (ITU) (в 2016 году - 79 место);

– 60 место в рейтинге Global Competitiveness Index (WEF) (в 2016 году - 85 место)…

…Документ одним из ключевых направлений определяет преодоление цифрового разрыва в обществе путем развития цифровых инфраструктур…

В частности, речь идет о широкополосной фиксированной телекоммуникационной инфраструктуре и мобильной (подвижной) телекоммуникационное инфраструктуре, инфраструктуры цифрового телевидения, радио и технологической инфраструктуры для проектов Интернета вещей, инфраструктуры вычислений, виртуализации и хранения данных (облачных и туманных), инфраструктуры кибербезопасности, специализированных инфраструктур…

Кроме того, документ говорит о развитии цифровых компетенций и внедрении концепции цифровых рабочих мест. Цифровое рабочее место определяется как виртуальный эквивалент физического рабочего места, а сама Концепция, помимо прочего, предусматривает преобразования рабочих мест чиновников в цифровые рабочие места…

…Среди главных приоритетов документа – цифровизация реального сектора экономики. Для этого предлагается создавать индустриальные парки, обеспечить

доступ к капиталу для инновационных проектов и подготовить соответствующих специалистов…

– Другими важными задачами являются официальное признание международных стандартов, составляющих общепризнанную основу индустрии 4.0 (около 100 стандартов), государственная поддержка деятельности технических комитетов, которые принимают участие в работе над стандартами, касающиеся индустрии 4.0, создание механизма поощрения подачи заявок на изобретения в Украине; создание механизма государственной поддержки патентования отечественных объектов интеллектуальной собственности; возможность защиты патентных прав через обращение к специализированных судов; создание механизмов трансфера технологий, – гласит текст Концепции…

…Концепция предусматривает внедрение цифрового земледелия – «принципиально новой стратегии менеджмента, основанной на применении цифровых технологий»…

Среди других громких заявлений – цифровизация образования, медицины, общественной безопасности, туризма, охраны окружающей среды, жизнедеятельности городов, государственного управления, обеспечение безналичных расчетов и развитие электронной демократии. В последнем пункте особенно интересно выглядит пункт об электронном голосовании…» ***(Владимир Кондрашов. Появился текст Концепции развития цифровой экономики Украины // InternetUA (http://internetua.com/poyavilsya-tekst-koncepcii-razvitiya-cifrovoi-ekonomiki-ukrainy). 23.02.2018).***

***

«…Результаты исследования EY «Cybersecurity regained: preparing to face cyber attacks», в котором приняли участие около 1200 руководителей крупнейших международных (в том числе и украинских) компаний, показывают, что 56% опрошенных планируют или уже реализуют изменения в стратегии кибербезопасности…

– …Более 90% респондентов заявили, что ожидают выделения больших бюджетов на защиту в этом году. Борьба с киберугрозами потребует более жесткой реакции, поэтому 87% отметили, что будут требовать увеличить бюджет на кибербезопасность крайней мере на 50%. Однако только 12% ожидают повышения финансирования, по крайней мере, на 25%, – утверждают в EY. – В Украине 75% руководителей департаментов информационной безопасности, учитывая текущую ситуацию, будут вносить предложения для менеджмента об увеличении бюджета на ИТ на 50% или более.

Многие респонденты утверждают, что недостаточное финансирование может повысить киберриски. 56% респондентов заявили о том, что рассматривают или уже внесли изменения в свои стратегии и планы борьбы с рисками. Однако 20% признают, что не имеют надлежащей оценки состояния информационной безопасности и потенциальных уязвимостей...

…50% от числа всех респондентов утверждают, что в их компаниях отчеты по кибербезопасности регулярно подаются руководству. В то же время, только 24% респондентов утверждают, что лицо, ответственное за кибербезопасность их

организации, является членом правления, и только 17% заявили, что высшее руководство имеет достаточные знания в области информационной безопасности для эффективного управления киберрисками.

В Украине несколько лучшие показатели: руководство опрошенных компаний регулярно получает информацию и отчеты о состоянии кибербезопасности в своих предприятиях, 22% респондентов также отметили, что в компаниях ответственное за кибербезопасность лицо является членом правления. 44% респондентов уверены в достаточной осведомленности высшего руководства в области информационной безопасности предприятия…» ***(Владимир Кондрашов. Пока гром не грянет: украинские компании готовы увеличивать бюджеты на кибербезопасность // InternetUA (http://internetua.com/krupneishie-ukrainskie-kompanii-gotov-uvelicsivat-buadjet-na-kiberbezopasnost). 23.02.2018).***

***

«В рамках акции мониторинга уязвимостей украинских государственных ресурсов хактивисты обнаружили несколько проблем с кибербезопасностью у украинских телевизионщиков и их регулятора…

В ночь с субботы на воскресенье консультант по кибербезопасности Егор Папышев опубликовал на своей странице в Facebook информацию, что телеканал UA:Перший оставил открытым без пароля ftp-сервер для обмена материалом с партнерами…

…В подтверждение своих слов он выставил скриншоты документов телеканала, среди которых – инструкция по вещанию в формате 16:9, данные о телепрограммах с шифрами и скриншоты папок с видеоматериалом…

В воскресенье, несмотря на выходной, уязвимость была закрыта.

…В это же воскресенье, 18 февраля, на сайте Национального совета по вопросам телевидения и радиовещания появилось уведомление «На этом месте могла бы быть какая-нибудь непристойная гужва»…

Авторы «предостережения» – Украинский кибералььянс, организация «белых хакеров», одним из направлений деятельности которой является мониторинг уязвимостей украинских государственных ресурсов #FuckResponsibleDisclosure (FRD).

…на сайте Нацсовета по вопросам ТВ и радио обнаружен так называемый «пассивный XSS» – тип уязвимости интерактивных информационных систем, который возникает, когда на страницы, сгенерированные сервером, по какой-то причине попадают пользовательские скрипты...

…В Нацсовете уже отреагировали на обнаруженную проблему и поблагодарили УКА за «находку»...» ***(Владимир Кондрашов. У телевизионщиков нашли проблемы с кибербезопасностью // InternetUA (http://internetua.com/u-televizionsxikov-nashli-problem-s-kiberbezopasnostua). 19.02.2018).***

***

«…Національний банк має намір почати будівництво нового основного центру обробки даних регулятора в поточному році…

…введення центру в експлуатацію заплановано на 2020 рік. Новий центр буде відповідати найсучаснішим технологічним вимогам, стандарту TIER IV і дасть можливість широко застосовувати переваги хмарних технологій в роботі інформаційних систем регулятора…» ***(Максим Овчаренко. Національний банк цього року розпочне будівництво нового центру обробки даних // Національний промисловий портал (http://uprom.info/news/other/natsionalniy-bank-tsogo-roku-rozpochne-budivnitstvo-novogo-tsentru-obrobki-danih/). 24.02.2018).***

***

Правове забезпечення кібербезпеки в Україні

«На засіданні Кабінету міністрів було схвалене внесення змін до законопроекту щодо санкцій проти Росії «Про застосування персональних спеціальних економічних та інших обмежувальних заходів»…

Йдеться про заборону або обмеження на використання програмного забезпечення на об'єктах критичної інфраструктури, виробником якого є країна, проти якої ввели санкції (Росія).

Таким чином, якщо Рада прийме відповідний закон, а їй Кабмін вже передав схвалений документ, то це дозволить в правовому полі відмовитися від російського ПО…» ***(Кабмін схвалив зміни до законопроекту про санкції проти Росії // kherson-news.info (http://kherson-news.info/politics/kabmin-shvaliv-zmini-do-zakonoproekty-pro-sankciyi-proti-rosiyi/). 13.02.2018).***

***

«На заседании 27 февраля, Национальная комиссия, осуществляющая госрегулирование в сфере связи и информатизации, согласовала с замечаниями присланный Нацполицией проект Закона Украины «О внесении изменений в некоторые законодательные акты Украины относительно имплементации положений Конвенции о киберпреступности»…

Законопроект разработан Национальной полицией Украины для реализации Плана по организации выполнения Указа Президента от 13 февраля 2017 года о Решении СНБО от 29 декабря 2016 года «Об угрозе кибербезопасности государства и неотложных мерах их нейтрализации»…

…целями и задачами законопроекта является имплементация отдельных норм Конвенции о киберпреступности в отечественное законодательство с целью усовершенствования противодействия криминальным правонарушениям, которые совершаются с использованием компьютерных систем, путем определения полномочий, необходимых для достижения этой цели.

– Законопроектом предусматривается внесение изменений в КПУ, КУоАП и Закон Украины о телекоммуникациях. Вместе с тем, положения законопроекта не в полной мере соответствуют обозначенным целям, а именно - отдельные его положения не соответствуют требованиям указанной Конвенции и не согласовываются с Законом Украины «О телекоммуникациях». В частности, реализация предложенных разработчиком изменений невозможна в связи с

отсутствием обязательной регистрации абонентов у оператора, провайдера телекоммуникаций, – отметили в НКРСИ…

…Представители профильных организаций обратились к членам НКРСИ с просьбой не поддерживать данный законопроект. Дело в том, что после мая прошлого года общественность и Нацполиция несколько месяцев совместно работали над подготовкой изменений касательно имплементации Конвенции. В частности, телекоммуникационная палата Украины и Ассоциация «Телас» в ходе ряда рабочих встреч выработали предложения, которые и направили в Нацполицию. Суть предложений заключалась в том, что операторы и провайдеры сотрудничают с правоохранителями и помогают им в ограничительных мерах только в случае наличия технической возможности, а блокирование ресурсов осуществляется теми, кто размещает эту информацию, то есть компаниями, предоставляющими услуги хостинга. Аналог этих норм уже есть в Законе «О защите авторских и смежных прав».

Эти предложения в тексте не были учтены.

Представители профильных организаций также просили Нацкомиссию подчеркнуть в своих предложениях, что этот документ подлежит общественному обсуждению и является регуляторным актом…

В НКРСИ согласились с тем, что данный законопроект – регуляторный акт, …однако парировали тем, что не могут определять, являются ли те или иные проекты регуляторными актами – это полномочия Государственной регуляторной службы.

Представители общественности также обратили внимание регулятора на тот факт, что в Конвенции о кибрепреступности нет норм о блокировке. В европейском документе, на котором якобы основан украинский законопроект, говорится исключительно о временном хранении информации и сохранении информации в телекоммуникационных системах, а также о сотрудничестве между операторами, провайдерами телекоммуникаций и контролирующими органами. О блокировках или каких-либо других нормах речи в документе нет.

В НКРСИ согласились также и с тем, что в европейской Конвенции, на которую опирается законопроект, действительно нет упоминаний о блокировках, однако подчеркнули, что законопроект предлагает предоставить право блокировать не сайты, а только запрещенную информацию…

После возмущений представителей общественности и телеком-рынка, глава НКРСИ Александр Животовский спокойным голосом поставил проект на голосование с теми замечаниями, которые предлагались изначально самим регулятором. Решение согласовать было принято единогласно» ***(Владимир Кондрашов. Нацполиция пытается "продавить" блокировку сайтов под видом европейской конвенции // InternetUA (http://internetua.com/nacpoliciya-ptaetsya-prodavit-blokirovki-saitov-pod-vidom-evropeiskoi-konvencii). 28.02.2018).***

***

«Британське МЗС офіційно поклало на російську владу відповідальність за спрямовану проти України масовану кібератаку з використанням вірусу-здирника NotPetya, що заразив у червні минулого року сотні тисяч комп'ютерів по всьому світу…

Як стверджують в міністерстві, …справжньою метою вірусу було не отримання викупу, а порушення роботи українських держустанов, фінансового і енергетичного секторів економіки. У результаті вірус поширився далі, заразивши підприємства і організації по всій Європі, в тому числі і в Росії…

Припущення про те, що за вірусом NotPetya стоять російські спецслужби, висловлювалися і раніше. Зокрема, такі заяви робили в Службі безпеки України і в американській компанії FireEye, що займається забезпеченням кібербезпеки…» ***(Британське МЗС офіційно звинуватило РФ в атаці вірусу NotPetya // Західна інформаційна корпорація (https://zik.ua/news/2018/02/15/brytanske_mzs_ofitsiyno_zvynuvatylo_rf_v_atatsi_virusu_notpetya_1266207). 15.02.2018).***

***

«Білий дім виступив в четвер з твердженням про те, що російські військові в червні 2017 року організували кібератаку з використанням вірусу NotPetya, яка торкнулася Європу, Азію, Західну півкулю і привела до втрати мільярдів доларів…

…Представники американської адміністрації вважають, що "це було частиною триваючих спроб Кремля дестабілізувати Україну", сама атака також "ще більш ясно демонструє причетність Росії до триваючого конфлікту".

"Це також була позбавлена розуму і невибіркова кібератака, яка спричинить за собою міжнародні наслідки", — резюмували в Білому домі…» ***(Білий дім звинуватив Росію в організації кібератаки з використанням вірусу Petya // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1715470-biliy-dim-zvinuvativ-rosiyu-v-organizatsiyi-kiberataki-z-vikoristannyam-virusu-petya). 16.02.2018).***

***

«Австралія, слідом за Великою Британією та США, звинуватила Росію в організації глобальної кібератаки з використанням вірусу Petya у червні 2017 року…

«На підставі висновків австралійських розвідувальних агентств і за результатами консультацій з США і Великою Британією урядом Австралії визнало, що відповідальність за цей інцидент лежить на діячах, які користувалися російською держпідтримкою», — заявив міністр у справах правоохоронних органів і кібербезпеки Енгуса Тейлора…» ***(Самуїл Проскуряков. Австралія звинуватила Росію в організації кібератаки з використанням вірусу Petya // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1715484-avstraliya-zvinuvatila-rosiyu-v-organizatsiyi-kiberataki-z-vikoristannyam-virusu-petya). 16.02.2018).***

***

«Данія висловила солідарність з Великобританією щодо відповідальності РФ за масштабні кібератаки з використанням вірусу Petya. Саме Росія, на думку датського міністра оборони Клауса Йорта Фредеріксена, стояла за великою кібер-атакою, яка влітку вразила датську компанію-гіганта Maersk та завдала їй мільярдні збитки…

Фредеріксен стверджує, що Данія погоджується з британською оцінкою…

За словами міністра, російські кібератаки не мають нічого спільного з шпигунством, метою якого є отримання інформації…

На думку Фредеріксена, зараз весь світ стурбований тим, що росіяни будуть продовжувати рух вже знайомим шляхом, як під час втручання у вибори в США.

“Це стратегія, спрямована на підрив західних демократій. Звичайно, ми повинні захистити себе від цього”, — сказав він…» ***(Саша Картер. Міноборони Данії: Росія стояла за кібератакою на Maersk // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1715422-minoboroni-daniyi-rosiya-stoyala-za-kiberatakoyu-na-maersk). 15.02.2018).***

***

«Обвинения России в причастности к кибератакам с помощью вируса NotPetya являются абсолютно беспочвенными и бездоказательными, заявил председатель Комитета Госдумы по международным делам Леонид Слуцкий (ЛДПР).

«Обвинения Белого Дома США, МИД Великобритании и ряда других западноевропейских государств в адрес России в организации кибератак вновь выдвигаются без каких-либо весомых доказательств. Они абсолютно пусты, беспочвенно и вряд ли могут иметь под собой серьёзные основания», — цитирует парламентария его пресс-служба…

Слуцкий, в свою очередь, отметил, что «в отношении России на Западе априори действует презумпция виновности», в результате чего Москва становится объектом шельмования и против неё выдвигаются всё более абсурдные претензии» ***(Слуцкий назвал беспочвенными обвинения России в создании вируса NotPetya // «Парламентская газета» (https://www.pnp.ru/politics/sluckiy-nazval-bespochvennymi-obvineniya-rossii-v-sozdanii-virusa-notpetya.html). 16.02.2018).***

***

«В Кремле категорически отвергают обвинения в причастности России к хакерским атакам, считают их бездоказательными, заявил пресс-секретарь президента Дмитрий Песков.

«Мы категорически отвергаем подобные обвинения, мы считаем их бездоказательными, беспочвенными. Это не что иное, как продолжение не основывающейся на каких-либо доказательствах русофобской кампании», – передает РИА «Новости» ответ Пескова на просьбу прокомментировать обвинения России в проведении массовой хакерской атаки вирусом NotPetya…» (***Дмитрий***

Зубарев. Кремль отреагировал на обвинение в хакерских атаках // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/2/15/908462.html). 15.02.2018).

***

«На сьогодні розглядається питання про створення кібервійськ у складі Збройних сил України. Про це розповів секретар РНБО Олександр Турчинов під час відкриття Центру реагування на кіберзагрози…

О.Турчинов наголосив, що у випадку агресії Україна має використовувати засоби адекватного реагування» ***(Олександр Сивачук. Турчинов заявив, що розглядається питання створення кібервійськ у лавах ЗСУ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1713031-turchinov-zayaviv-scho-rozglyadayetsya-pitannya-stvorennya-kiberviysk-u-lavakh-zsu). 02.02.2018).***

***

«В течение следующего года Россия будет проводить более мощные кибератаки и, очевидно, применит их против Украины.

Об этом сообщил директор Национальной разведки США Дэниел Коатс в своем докладе, представленном на слушаниях в комитете по разведке Сената США…

Также в США прогнозируют, что российские спецслужбы продолжат испытывать на прочность не только инфраструктуру США и стран-союзников, а также укреплять недоразумения между Соединенными Штатами, НАТО и другими партнерами страны» ***(Украина предупредили о кибератаках российских хакеров // Gazeta.ua (https://gazeta.ua/ru/articles/world-life/_ukraina-predupredili-o-kiberatakah-rossijskih-hakerov/820516). 14.02.2018).***

***

«У 2018 році в Міністерстві оборони України почнуть роботу два радника зі Сполучених Штатів Америки. Про це повідомив представник США в українському оборонному відомстві Стівен Сильверштейн…

З його слів, йдеться про радників з кібербезпеки і стратегічних комунікацій…» ***(Америка вирішила зміцнити Міноборони України // ONLINE.UA (https://novyny.online.ua/795484/amerika-virishila-zmitsniti-minoboroni-ukrayini/). 13.02.2018).***

***

Боротьба з кіберзлочинністю в Україні

«В «темном Интернете» выставили на продажу две базы данных с самой свежей информацией о клиентах "Новой почты" - на 500 тыс. человек и на 18 млн записей.

«…первая содержит информацию около полумиллиона человек, с персональными данными в разбивке ФИО / телефон / город / серия и номер паспорта / e-mail. Вторая - 18 миллионов записей, но с меньшей детализацией

(только ФИО и телефон)», - сообщил консультант по кибербезопасности Егор Папишев на своей странице в Facebook.

Папишев утверждает, что связался с продавцом, который озвучил цену в гривнах и позволил проверить «качество» базы…

Продавец вышел на связь с российской почтового сервера и указал цену в 1500 грн. за детальную базу (полмиллиона клиентов)…

«Как используются эти данные злоумышленниками? Прежде всего, навязчивая реклама, спам SMS и по электронной почте, холодный звонки. Далее следуют варианты использования этих данных в качестве компонента атак социальной инженерии с различными, далеко идущими последствиями», - объясняет консультант» **(В сети нашли полную базу данных клиентов "Новой почты" // Gazeta.ua (https://gazeta.ua/ru/articles/science/_v-seti-nashli-polnuyu-bazu-dannyh-klientov-novoj-pochty/819108). 06.02.2018).**

***

«Прокурори області затвердили обвинувальний акт відносно членів організованої злочинної групи, які здійснили несанкціоноване втручання в роботу електронних мереж електрозв'язку…

Ще у 2015 році хмельничанин, закупивши необхідну комп'ютерну техніку та підключивши її у себе вдома до мережі Інтернет, з метою отримання незаконного заробітку, порушував порядок маршрутизації електронного зв'язку. В результаті таких дій міжнародний телефонний трафік проходив поза межами міжнародних центрів комутації, а зловмисник отримував можливість одержувати прибуток.

Зрозумівши, що такі дії приносять заробіток та, намагаючись збільшити його розмір, чоловік закупив та розмістив у домівках двох своїх знайомих додаткове обладнання, яке віддалено, з власної квартири, також використовував для функціонування каналу з перенаправлення вхідного міжнародного телефонного трафіку…

Розмір матеріальної шкоди, завданої злочином складає близько 140 тис. грн.

За результатами досудового розслідування, проведеного за процесуального керівництва галузевого відділу прокуратури області слідчим управлінням ГУ НП в області, зібрано достатню кількість доказів для оголошення трьом членам організованої групи про підозру у вчиненні кримінальних правопорушень, передбачених ч 2 ст.361 - несанкціоноване втручання в роботу мережі електрозв'язку, що заподіяло значної шкоди ККУ.

Обвинувальний акт направили для розгляду до Хмельницького міськрайонного суду…» ***(До шести років ув'язнення загрожує ділкам, які на Хмельниччині "привласнили" телефонний трафік // Internetua (http://internetua.com/do-shesti-rokiv-uv-yaznennya-zagrojuye-dilkam-yaki-na-hmelnicscsini-privlasnili-telefonnii-trafik). 15.02.2018).***

***

«У Києві затримали організатора міжнародної злочинної платформи «Avalanche», яка щодня інфікувала по всьому світу до півмільйона комп'ютерів…

…Поліцейські виявили у нього паспорт громадянина України на ім’я іншої особи, за якими зловмисник прибув до столиці…

…в орендованій зловмисником квартирі поліцейські вилучили під час обшуку ноутбук, гроші та флеш-накопичувачі.

Затриманому інкримінують причетність до вчинення кількох кримінальних правопорушень: ч. 3 ст. 209, за ч. 1 ст. 361, ч. 2 ст. 342 та ч. 4 ст. 190 Кримінального кодексу України. Водночас прокуратура Вердена і поліція Люнебурга (ФРН) розслідують кримінальну справу щодо міжнародної платформи злочинної інфраструктури, відомої як «Avalanche», яка використовувалась як майданчик для запуску та управління масовими глобальними шкідливими атаками і відмиванням грошей. У Німеччині, за оцінками експертів, це спричинило збитків на понад 6 мільйонів євро. Крім того, грошові втрати пов’язані з кібератаками, проведеним по мережі «Avalanche», за попередніми підрахунками, становлять сотні мільйонів євро по всьому світу…» ***(У столиці правоохоронці затримали організатора кібермережі Avalanche // Західна інформаційна корпорація (https://zik.ua/news/2018/02/26/u_stolytsi_pravoohorontsi_zatrymaly_organizatora_kibermerezhi_avalanche_1273761). 26.02.2018)***.

***

«Команда реагирования на компьютерные чрезвычайные события Украины (CERT-UA) Госспецсвязи обнаружила факт распространения вредоносного программного обеспечения Smokeloader, которое скачивало на компьютеры жертв программу для майнинга криптовалюты Monero.

…распространение Smokeloader происходит через рассылку почтовых сообщений со злокачественным Javascript-ом…

В самом Javascript вредоносный код зашифрован в виде Base64. Он скачивает с сайта hXXp: //enterwords.ru/uadoc/crsse.exe файл crsse.exe и сохраняет его в директории C: \ tmp \ 1964.exe...

Далее Smokeloader запускает поток, проверяющий на наличие запущенных программ, которые используются для анализа вредоносного кода. Если они присутствуют, он закрывает их…

После этого запускается и инфицируется, вредоносным кодом, процесс explorer.exe…

Дабы уберечься от опасного вируса, в CERT-UA рекомендуют:

– Обеспечить недопустимость открытия вложений в подозрительных сообщениях (в письмах от адресантов, по которым возникают сомнения…

– Системным администраторам и администраторам безопасности обратить внимание на фильтрование входящих / исходящих информационных потоков, в частности почтового веб-трафика.

– Проверить наличие полученных сообщений клиентов почтового сервера, для определения потенциально пораженных пользователей.

– Проверить наличие переходов по ссылкам, которые содержали вредоносные файлы, для определения потенциально пораженных пользователей.

– Провести мероприятия по выявлению и удалению ВПО.

– Обновить антивирусную базу и просканировать потенциально зараженные системы» ***(Владимир Кондрашов. Украинцы массово получают опасные письма с вирусом для майнинга криптовалюты // InternetUA (http://internetua.com/ukraincy-massovo-polucsauat-opasne-pisma-s-virusom-dlya-maininga-kriptovaluat). 26.02.2018).***

***

«За 13 суток на Google Play вредоносное мобильное приложение «Универсальный мобильный банкинг», … похитило около 5500 паролей от систем «мобильного банкинга», было заражено не менее 6000 смартфонов, скомпрометировано более 2000 банковских карт. За вредоносным приложением стояла группа украино- и русскоговорящих лиц…

…расчет злоумышленников был сделан на то, что в этом приложении объединен функционал «мобильного банкинга» сразу нескольких финучреждений (ПриватБанк, Ощадбанк, ОТП Банк, Альфа-Банк, Райффайзен Банк Аваль)…

Около 22:00 19.02.2018 вредоносное приложение было удалено из Google Play. Специалисты по кибербезопасности считают, что получилось это благодаря тому, что Google Play получил множество запросов из разных источников.

…В результате исследования угрозы украинской компанией была получена информация о жертвах, чьи данные в полном составе были переданы на сервер злоумышленникам и могли бы быть использованы для последующего (не считая уже осуществленного) мошенничества, итогом которого было бы хищение денежных средств и нанесения материального и морального ущерба клиентам банков…» ***(Владимир Кондрашов. Злоумышленники выудили через Google Play пароли от "мобильного банкинга" украинцев // InternetUA (http://internetua.com/zloumshlenniki-vudili-cserez-google-play-paroli-ot-mobilnogo-bankinga-ukraincev-). 20.03.2018).***

***

«Співробітники Служби безпеки України спільно із Нацполіцією викрили у Дніпрі хакерське угруповання, яке здійснювало кібератаки на центри обробки даних та автоматизовані системи управління технологічними процесами, у тому числі й об'єктів критичної інфраструктури.

… Хакери отримали незаконний доступ до адміністративної панелі серверів, заблокували роботу автоматизованої системи управління технологічними процесами та викрали її програмні коди. Для приховування слідів кібератаки зловмисники видалили системні файли серверів, що призвело до припинення роботи «зламаного» телекомунікаційного обладнання.

Перевіряється також інформація щодо організації кібератаки «на замовлення» спецслужб країни-агресора…

Наразі тривають слідчі дії у рамках кримінального провадження, відкритого за ч. 2. ст. 361 Кримінального кодексу України» ***(У Дніпрі СБУ викрила хакерське угруповання на здійсненні кібератак державних автоматизованих систем // Народна Рада (http://narodnarada.info/news/dnipri-sbu-vikrila-hakerske-ugrupovannya-news-91449.html). 23.03.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Палата представителей Конгресса США 404 голосами «за» поддержала законопроект Бойла-Фицпатрика H.R.1997 - Ukraine Cybersecurity Cooperation Act of 2017. О документе, усиливающем сотрудничество между Украиной и США в сфере кибербезопасности, уже говорят как о победе, хотя его должен ещё поддержать Сенат и потом подписать Дональд Трамп…

…согласно данным Управления Конгресса США по бюджету, внедрение законопроекта обойдется Соединенным Штатам в сумму около 500 000 долларов в период с 2018-2022 годов…

…Принятый Палатой представителей Билль утверждает поддержку Украины Соединенными штатами в трех ключевых направлениях:

– усовершенствование системы безопасности правительственных систем, особенно таких, которые защищают критическую инфраструктуру Украины.

– снижение зависимости от российских информационно-коммуникационных технологий.

– наращивание потенциала, расширение обмена информацией по кибербезопасности и сотрудничества в киберпространстве.

В случае утверждения документа Сенатом и подписания его президентом США, за 180 дней будет подготовлен доклад о состоянии сотрудничества США и Украины в сфере кибербезопасности.

Отчет, как того требует документ, должен содержать сведения:

– об усилиях Соединенных Штатов по укреплению способности Украины предотвращать, смягчать и реагировать на киберинциденты, в том числе посредством обучения, образования, технической помощи, наращивания потенциала и стратегий управления рисками кибербезопасности.

– о новых областях сотрудничества и взаимопомощи между Соединенными Штатами и Украиной в решении общих проблем кибербезопасности, включая киберпреступность, защиту критической инфраструктуры и устойчивость к ботнетам и другим киберугрозам.

– об усилиях НАТО по оказанию помощи Украине в разработке технических возможностей для противодействия киберугрозам…

…принятый документ «визуализирует агрессора» – в нем говорится о «поддерживаемых Россией дезинформационных и пропагандистских усилиях в киберпространстве», «пророссийской пропаганде и наступательных кибероперациях»…

..в утвержденном законопроекте… «неудачная попытка уничтожить ПО компьютеров избирательной комиссии посредством кибератаки» стала «атакой хакеров на избирательную инфраструктуру страны», а «опыт внеплановых отключений электроэнергии из-за кибератак» – «злонамеренным

кибервмешательством в работу украинских предприятий электроэнергетики» и пр…

Документ в Украине профильным сообществом – практиками и экспертами в сфере кибербезопасности – был воспринят достаточно позитивно. Впрочем, с одной существенной поправкой – на украинские реалии.

– Это, прежде всего, серьезный политический шаг: США признает Украину как союзника в киберпространстве, – говорит специалист по информационной безопасности Владимир Стыран. – …Акт также свидетельствует о том, что теперь Украина сможет получить помощь напрямую, что значительно ускорит рост отрасли и, возможно, за 2-3 года мы выйдем на уровень Польши и Эстонии.

…Принятый документ может иметь, мягко говоря, малоприятные последствия для украинских властей – отчет, который должны будут составить американцы, может стать «точкой невозврата» для украинских государственных деятелей от кибербезопасности, считает спикер Украинского киберальянса, известный под ником Sean Brian Townsend…

По разным оценкам, американским парламентариям может понадобиться около года, дабы Акт прошел все необходимые процедуры и был подписан Трампом…» ***(Ирина Фоменко, Владимир Кондрашов. Что сулит Украине Акт о сотрудничестве с США в сфере кибербезопасности // Інформаційне агентство «Українські Національні Новини» (http://internetua.com/csto-sulit-ukraine-akt-o-sotrudnicsestve-s-ssha-v-sfere-kiberbezopasnosti). 12.02.2018).***

***

«Міністр закордонних справ України Павло Клімкін вдячний палаті представників Конгресу США за підтримку проекту закону про співпрацю з Україною з питань кібербезпеки й переконаний, що ця ініціатива дасть свої результати в боротьбі з російською гібридною агресією…

П.Клімкін також висловив упевненість у тому, що "у віртуальному просторі ми теж переможемо"…» ***(Клімкін про законопроект США щодо кібербезпеки: Це нове спільне поле битви з гібридною агресією РФ // Інтерфакс-Україна (http://ua.interfax.com.ua/news/political/483635.html). 08.02.2018).***

***

«Україна посилює співпрацю з США у сфері кібербезпеки на фоні заяви Білого дому з приводу причетності Росії до кібератаки NotPetya проти України, а також прогнозів американської розвідки про очікуване посилення російських кібероперацій проти нашої держави. Про це УНН повідомляє з посиланням на заяву посольства України у Вашингтоні…

«Реагуючи на ці виклики, ми посилюємо практичну співпрацю зі Сполученими Штатами у сфері кібербезпеки: у вересні минулого року з державним департаментом започатковано кібердіалог; ведеться активна робота з конгресом США; розвивається взаємодія з американськими академічними та бізнес-експертами кіберсфери - з Університетом Дж.Вашингтона започатковано партнерство з кібербезпеки», - додали у посольстві.

Як зазначається, підтриманий минулого тижня палатою представників законопроект про зміцнення співпраці України та США в галузі кібербезпеки «дозволить системно вибудовати відносини у цій критично важливій для обох країн сфері та разом протистояти російській агресії у кіберпросторі».

«Посольство України в США продовжуватиме приділяти пріоритетну увагу розвитку співпраці зі Сполученими Штатами у сфері кібербезпеки…», - вказали у посольстві…» ***(Юлія Шрамко. Україна посилює співпрацю з США у кібербезпеці на фоні викривальних заяв щодо РФ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1715533-ukrayina-zayavila-pro-posilennya-spivpratsi-z-ssha-u-kiberbezpetsi-pislya-vikrivalnikh-zayav-schodo-rf). 16.02.2018).***

***

«…В рамках официального визита министра иностранных дел Украины Павла Климкина в Нидерланды он встретился с министром внутренних дел страны Кайсой Оллонгрен, договорившись о налаживании сотрудничества в сфере кибербезопасности между государствами и о противодействии российской пропаганде. Об этом сообщила пресс-служба МИД Украины…

«Украина и Нидерланды сталкиваются с общими проблемами безопасности, создаваемыми гибридными действиями России», – сообщает МИД…» ***(Украина и Нидерланды будут вместе противостоять гибридной агрессии России – Климкин. //* Agrimpasa.com *(http://agrimpasa.com/ukraina-i-niderlandy-budut-vmeste-protivostoyat-gibridnoj-agressii-rossii-klimkin.html). 02.02.2018).***

***

«…В Сенат США внесен законопроект об усилении сотрудничества между Украиной и США в сфере кибербезопасности…

…документ направлен на оказание помощи Украине в совершенствовании собственной стратегии кибербезопасности, в частности, что касается усиления защиты компьютерных сетей органов государственной власти, уменьшения зависимости Украины от российских информационных и коммуникационных технологий; содействия расширению участия Украины в программах обмена информацией и международных усилиях по противодействию угрозам во всемирной Интернет-сети. Кроме того, в законопроекте подтверждается приверженность США Хартии о стратегическом партнерстве между Украиной и США, Будапештскому меморандуму о гарантиях безопасности, поддержке сотрудничества нашего государства с НАТО.

Для вступления в силу документ должен быть поддержан Сенатом и подписан Президентом США» ***(В Сенат США внесли законопроект о киберпомощи Украине // InternetUA (http://internetua.com/v-senat-ssha-vnesli-zakonoproekt-o-kiberpomosxi-ukraine). 27.02.2018).***

***

«У четвер відбулась зустріч Секретаря Ради національної безпеки і оборони України Олександра Турчинова з Надзвичайним і повноважним Послом Великої Британії в Україні Джудіт Гоф…

…Під час зустрічі співрозмовники обговорили посилення співпраці між Україною та Великою Британією в секторі безпеки і оборони, а також ситуацію, яка сталась на сході України та в Криму внаслідок російської агресії…

Сторони приділили увагу обговоренню інтенсифікації співпраці держав в питаннях кібербезпеки…

Окрему увагу співрозмовники приділили обговоренню питань реформування сектору безпеки і оборони України відповідно до стандартів НАТО. Британський посол наголосила, що Великобританія, "як і багато країн НАТО, схвально ставиться до підтриманого РНБО проекту Закону „Про національну безпеку України", відповідно до якого в Україні буде запроваджено європейську модель сектору безпеки і оборони".

Водночас Гоф зазначила, що Великобританія стурбована тим, як розгортається ініційована Росією гібридна війна, та занепокоєна тим, яку загрозу представляє Росія для України та загалом для Європи. В цьому контексті сторони констатували необхідність продовження санкцій проти Росії…» ***(Саша Картер. Турчинов зустрівся з послом Британії: говорили про співпрацю, кіберзахист та санкції // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1716753-turchinov-zustrivsya-z-poslom-britaniyi-govorili-pro-spivpratsyu-kiberzakhist-ta-sanktsiyi). 22.02.2018).***

***

Світові тенденції в галузі кібербезпеки

«…Кибератаки являются наибольшей угрозой безопасности и стабильности во всем мире, заявила министр обороны ФРГ Урсула фон дер Ляйен (Ursula von der Leyen) журналистам телеканала CNBC в рамках Мюнхенской конференции по безопасности.

По словам министра, в текущем десятилетии усовершенствованию кибербезопасности будет уделено особое внимание...

Обеспокоенность вопросами защиты от киберугроз фон дер Ляйен объяснила увеличением количества кибератак в современном мире…» ***(Министр обороны ФРГ назвала кибератаки главной мировой угрозой // SecurityLabRu (https://www.securitylab.ru/news/491607.php). 18.02.2018).***

***

«В Израиле проходит Международная конференция мэров, где единственным представителем Украины является глава Днепра Борис Филатов. Очередной день съезда посвятили обмену опытом в сфере развития стартап-платформ и киберзащиты для «умных городов»…

Среди лекторов - известный израильский предприниматель Йосси Варди, который основал и помог создать около сотни высокотехнологичных компаний, в частности, в области программного обеспечения, энергетики и Интернета.

Также присутствовали представители мировых компаний по разработке программного обеспечения для «умных городов» R-Mor и WeWork…

Всего в израильской отрасли hi-tech задействованы 8% от всех трудоустроенных граждан.

Кроме этого, обсуждали влияние социальных сетей. Интернет-пространство уже давно используют не только для досуга, покупок и знакомств…

Часть лекции также посвятили кибербезопасности и предотвращению хакерским атакам…» ***(Борис Филатов в Израиле: развитие стартапов и кибербезопасность // Паноптикон. (http://www.panoptikon.org/articles/102077-boris-filatov-v-izraile-razvitie-startapov-i-kiberbezopasnost.html). 16.02.2018).***

***

«…В четвертом квартале ушедшего года специалисты компании Positive Technologies, специализирующейся на производстве программного обеспечения в сфере кибербезопасности, зафиксировали больше уникальных инцидентов, чем в предыдущие периоды. В начале ноября и конце декабря наблюдался рост количества атак на частных лиц. Это можно связать с периодами распродаж («черная пятница», предновогодние акции), когда люди склонны совершать спонтанные покупки, в том числе на подозрительных сайтах.

Пугающая тенденция — снижение возраста злоумышленников. «Если прежде атаки выполняли опытные программисты, то сегодня мы все чаще видим несовершеннолетних, участвующих в киберпреступлениях», — комментирует аналитик Positive Technologies Ольга Зиненко…

Продолжило расти число желающих заработать на криптовалюте за счет чужих ресурсов — с помощью нового ВПО (например, майнера Coinhive) или путем подмены криптокошельков…

Повышение информационной грамотности пользователей заставляет злоумышленников придумывать новые способы распространения ВПО. Так, например, они используют взломанные веб-ресурсы. Интересно, что для поднятия позиций фишинговых сайтов в поисковой выдаче киберпреступники используют методы SEO, размещая на них ключевые слова, а также увеличивая рейтинг с помощью специальных SEO-ботнетов» ***(Positive Technologies: хакеры используют вредоносное ПО для сокрытия следов и истинных мотивов преступления // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/290304/). 09.02.2018).***

***

«…6 февраля 2018 года в Москве, на площадке Digital October состоялся форум по кибербезопасности - Cyber Security Forum 2018, организованный РАЭК и РОЦИТ.

В рамках CSF 2018 эксперты презентовали тренды в области кибербезопасности по итогам 2017 года…

– Появление новых вирусов и расширение арсенала киберпреступников за счет использования новых технологий.
– Атаки класса APT (advanced persistent threat — «развитая устойчивая угроза»; также целевая кибератака) — злоумышленник обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения (например, информационных, физических и обманных)…
– Увеличится количество атак на разработчиков легитимного ПО…
– Шифровальщики. Атаки WannaCry, ExPetr и Bad Rabbit показали, что технологические сети могут быть даже более уязвимыми, чем корпоративные…
– Атаки на персональные данные. Персональные данные, оцениваются как «новая нефть»(в контексте монетизации данных в самом широком смысле). При этом Большие данные будут использоваться и в самих атаках — для более адресного обращения к пользователю.
– Рост сложности обнаружения и удаления вредоносных программ (использование DNS, шифрование, бестелесность и др.)

Инфраструктурные киберугрозы

– Атаки на программный интерфейс UEFI (Unified Extensible Firmware Interface), пришедший на смену BIOS.
– Массовые взломы роутеров и модемов.
– Взлом банкоматов, PoS-терминалов…
– Рост рынка облачных структур и перенос хранения данных в облака повлечет за собой увеличение кибератак на облачные сервисы.

Атаки на криптовалюты

– Использование ботнет-сетей для майнинга криптовалют.
– Кража криптовалют (у пользователей и атаки на биржи) как одна из основных целей хакеров.

Изменения в законодательстве

– Вступает в силу законодательство по безопасности Критической информационной инфраструктуры (187-ФЗ и др)...
– ЦБ становится регулятором в области информационной безопасности для финансовых организаций.
– Импортозамещение, усиление требований к средствам ИБ, ужесточение требований к лицензиатам по защите информации.
– Вступление в силу (или перенос) “Закона Яровой”.
– С 25 мая 2018 г. начнет применяться Европейский регламент GDPR (Общие положения о защите данных), что неизбежно приведет к увеличению расходов российских компаний, деятельность которых связана со странами-членами ЕС…» ***(Развитие цифровой экономики привлекает мошенников // (http://www.iksmedia.ru/news/5473372-Razvitie-cifrovoj-ekonomiki-privlek.html#ixzz57v5tYMeV). 07.02.2018).***

***

«…Эксперты M1Cloud (Stack Group) рассказали о возможных киберугрозах и трендах по защите информации при размещении информационных систем в облаках в 2018 году…

По оценке экспертов M1Cloud (Stack Group), около 80% компаний размещают свои защищенные ИТ-системы в colocation-среде, а 20% - доверяют облачным сервисам на базе виртуализированных сред. Рынок средств и услуг защиты информации растет высокими темпами, сопоставимыми с темпами роста рынка виртуализированной инфраструктуры, который составляет порядка 40% ежегодно…

Бизнес, размещая информационные системы в облаке, всё чаще стремиться получить комплексные услуги по защите информации, например, размещение систем внутри межсетевых экранов, построение защищенного канала, защищенного соединения с использованием западных и российских криптоалгоритмов, обеспечение безопасности данных на уровне информационных систем путем установки соответствующих средств защиты от несанкционированного доступа, средств антивирусной защиты, защиты в рамках внедрения контура обнаружения и предотвращения вторжений и другие…

Основной объем запросов на ИТ-инфраструктуру в России связан с безопасностью персональных данных, так как в соответствии с Федеральным законом №152 «О персональных данных» все компании являются операторами персональных данных и обязаны организовать защиту в соответствии с требованиями нормативных документов ФСТЭК и ФСБ, в части защиты информации, передаваемой по каналам связи и шифровальных средств…

В России доминирующее положение занимают технологические решения российских вендоров, построенные на отечественных программных продуктах и оборудовании, прошедших сертификацию в соответствии с установленными требованиями ФСБ по использованию средств шифрования данных и криптографической защиты, а также ФСТЭК в отношении различного функционала средств безопасности по защите конфиденциальной информации» ***(Тренды информационной безопасности в облаках // ООО "ИКС-МЕДИА" (IKSMEDIA.RU: http://www.iksmedia.ru/news/5476630-Trendy-informacionnoj-bezopasnosti.html#ixzz57vMSTxW2). 22.02.2018).***

***

«В настоящее время с точки зрения инвесторов кибератаки являются самой серьезной угрозой для бизнеса, свидетельствуют данные глобального опроса инвесторов, проведенного PwC.

Так, 41% инвесторов и аналитиков серьезно обеспокоены кибератаками, которые воспринимаются как самая серьезная угроза для бизнеса. Если в 2017 году киберугрозы находились на пятом месте в перечне угроз для бизнеса, в этом году они поднялись на первое место. Аналогичное количество руководителей компаний (40%) включили киберугрозы в тройку самых серьезных рисков…

По мнению инвесторов, для повышения уровня доверия клиентов к бизнесу компании должны сосредоточиться на вопросах кибербезопасности (64% инвесторов, 47% руководителей)…» ***(Инвесторы считают проблему***

кибербезопасности самой серьезной угрозой бизнесу – PwC // Интерфакс-Украина (http://interfax.com.ua/news/telecom/488536.html). 28.02.2018.

***

Сполучені Штати Америки

«Мэр Нью-Йорка Билл Де Блазио планирует направить $500 тыс. на защиту городской избирательной системы от действий хакеров во время промежуточных выборов в ноябре 2018 года…

Мэр хочет предложить укрепить кибербезопасность в городской комиссии за наблюдением ходов выборов. Он собирается объявить об этом предложении во время выступления в Бруклине…» ***(WSJ: мэр Нью-Йорка хочет потратить $500 тыс. на кибербезопасность во время виборов // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3547609?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). 13.02.20180).***

***

«Руководители спецслужб США призвали граждан отказаться от китайских смартфонов. Американские силовики посоветовали не пользоваться устройствами Huawei и ZTE, так как они могут быть использованы для слежки. Заявления об угрозе шпионажа прозвучали на заседании комитета Сената по разведке…

Глава Агентства кибербезопасности Евгений Лифшиц считает, что подозрения американцев вполне обоснованны…

Специалисты по информационной безопасности отмечают, что произведенные в Китае телефоны могут оказаться под влиянием вредоносных программ…

Призывы отказаться от китайских гаджетов со стороны США могут быть вызваны и политическими причинами, считает руководитель проектов по информационной безопасности компании КРОК Павел Луцик… ***(Американцы косо смотрят на китайские смартфоны. Могут ли устройства представлять опасность // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3549202?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 15.02.2018).***

***

«Спецслужбы США заплатили $100 тыс. гражданину России, который пообещал вернуть им похищенное при кибератаке на Агентство национальной безопасности (АНБ) секретное кибероружие… Имя россиянина не приводится.

…россиянин связан с хакерами из стран Восточной Европы и представителями спецслужб в Москве…

…за свои услуги россиянин попросил $1 млн. Первую часть этой суммы спецслужбы США передали ему в сентябре прошлого года в одном из отелей Берлина… «Вместо украденного программного обеспечения он передал АНБ непроверенную и, возможно, сфабрикованную информацию о Дональде Трампе и других лицах, включая данные банковских счетов, электронную переписку и предполагаемые данные российской разведки»,— рассказали они.

От дальнейшего общения с российским гражданином американские спецслужбы отказались, опасаясь огласки. Они также полагали, что россиянин мог работать на спецслужбы своей страны, которые и организовали эту операцию, чтобы спровоцировать новый внутриполитический конфликт в США…» ***(Разведслужбы США заплатили $100 тыс. россиянину, пообещавшему вернуть АНБ коды // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3546555?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 10.02.2018).***

***

«…По словам заместителя председателя Объединенного комитета начальников штабов ВВС Пола Селвы (Paul Selva), США сильно уступают России и Китаю в области кибербезопасности в космическом пространстве…

Как заявили представители Минобороны, РФ и КНР разрабатывают генераторы помех и перехватчики сигналов, позволяющие нарушить работу американских спутников. Сельва добавил, что и у России, и у Китая есть «утонченные радарные системы и утонченные системы космического обнаружения», которых более чем достаточно для обнаружения спутников» ***(Американские военные спутники могут взломать даже хакеры-любители // SecurityLabRu (https://www.securitylab.ru/news/491233.php). 02.02.2018).***

***

«Діючий президент США Дональд Трамп представив генерал-лейтенанта Пола Накасоне, який нині керує кібер-командуванням Сухопутних сил країни, як кандидата на пост глави Агентства національної безпеки (АНБ) Сполучених Штатів…

…спеціальний помічник американського лідера і координатора Білого дому з питань кібербезпеки Роб Джойс назвав генерала Накасоне «винятковим лідером для двох виняткових організацій», який має великий досвід у сфері кібербезпеки.

…президент США Дональд Трамп підписав 19 січня закон про продовження на шість років терміну дії програми по здійсненню прослуховування телефонних розмов і перехоплення електронної переписки жителів інших держав, підозрюваних в тероризмі.

…Агентству дозволяється переглядати електронну пошту, прослуховувати голосові і відеочати, дивитися фотографії, відео, відстежувати файли, дізнаватися інші подробиці з соціальних мереж…

Представники спецслужб запевняють, що не стежать за американцями свідомо і що дані громадян США виявляються в базах даних випадково. Спецслужби також стверджують, що за допомогою даних програм вдалося

запобігти чимало терактів в США, але відмовляються говорити, про які саме нереалізовані атаки йдеться» ***(Самуїл Проскуряков. Трамп висунув кандидатуру на посаду глави АНБ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1715054-tramp-visunuv-kandidaturu-na-posadu-glavi-anb). 14.02.2018).***

***

«…Во вторник, 20 февраля, Генеральный прокурор США Джефф Сэшнс (Jeff Sessions) объявил о создании рабочей группы по вопросам глобальных киберугроз. В частности эксперты займутся проблемами вмешательства в выборы и кибератак на критическую інфраструктуру…

В рабочую группу войдут представители различных ведомств Министерства юстиции США, в том числе ФБР. Эксперты займутся изучением того, как интернет используется для распространения идеологий, пропагандирующих жестокость и насилие, и вербовки последователей. Рабочая группа исследует используемые хакерами методы взлома корпоративных и правительственных информационных систем, а также изучит проблемы, с которыми сталкиваются правоохранительные органы в связи с шифрованием данных…

…Согласно подписанному Сэшнсом меморандуму, Минюст должен представить результаты своих исследований к концу июня текущего года» ***(Минюст США создаст рабочую группу по вопросам глобальных киберугроз // SecurityLabRu (https://www.securitylab.ru/news/491666.php). 21.02.2018).***

***

«…В связи с ядерной угрозой, представляемой Северной Кореей, в течение последних шести месяцев правительство США ведет секретную подготовку к возможному кибердудару по ней из Южной Кореи и Японии. Подготовка предполагает установку на территории этих стран оптоволоконных кабелей и мостов, настройку удаленных баз и станций для перехвата коммуникаций, с помощью которых хакеры смогут получить доступ к изолированному от остального мира северокорейскому интернету…

Правительство вкладывает миллиарды долларов в создание технической инфраструктуры и подготовку специалистов для кибератак на Северную Корею…

…Подготовка к кибердудару по КНДР также предполагает возвращение на службу из запаса аналитиков военной разведки. За последние несколько месяцев американское правительство также открыло вакансии на должность аналитиков со знанием корейского языка…» ***(США уже полгода активно готовятся к возможному кибердудару по КНДР // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121512). 19.02.2018).***

***

«Администрация Дональда Трампа, президента США, рассматривает новые санкции против России в ответ на вмешательство в выборы и кибератаки прошлого года.

Об этом в среду… на брифинге для группы журналистов трое должностных лиц, принимающих участие в работе над санкциями, рассказали, что процесс продолжается медленно по юридическим причинам и не может быть ускорен в ответ на критику. Однако не предоставили подробную информацию о том, когда администрация президента США примет решение о санкциях или ограничительные меры будут рассмотрены…» ***(США готовят санкции против РФ за вмешательство в выборы и кибератаки // Gazeta.ua (https://gazeta.ua/ru/articles/world-life/_ssa-gotovyat-sankcii-protiv-rf-za-vmeshatelstvo-v-vybory-i-kiberataki/822159). 22.02.2018).***

***

«Адміністрація Дональда Трампа не давала Агентству національної безпеки США додаткових повноважень для перешкоджання російському кібервтручанню у вибори

Про це директор АНБ адмірал Майк Роджерс заявив Сенатському комітету з питань збройних сил…

Роджерс відзначив, що сам не звертався з проханням надати йому додаткові повноваження для перешкоджання кібератакам Росії у зародку, але відзначив, що саме до повноважень президента Трампа належить ухвалення такого рішення…

При цьому директор АНБ заявив, що доручив своїм підлеглим "розпочати конкретну роботу", але не навів деталей можливих дій його агентства для попередження кібервтручання у вибори у США.

Роджерс також відзначив, що дії Росії не змінились значним чином внаслідок санкцій США…» ***(Трамп ще не дав АНБ завдань боротися з російськими кібератаками // Espreso.tv (https://espreso.tv/news/2018/02/27/tramp_sche_ne_dav_anb_zavdan_borotysya_z_rosiyskymy_kiberatakamy). 27.02.2018).***

***

«Влада Каліфорнії схвалила зміни в правила дорожнього руху в штаті…

Дозволи можуть почати видавати вже 2 квітня… Досі при русі безпілотних автомобілів в Каліфорнії вимагалася в салоні присутність людини, яка могла взяти на себе управління у разі надзвичайної ситуації.

Виробникам автомобілів треба буде довести, що їхні технології безпечні і стійкі до кібератак. Крім того, компанії повинні будуть представити план взаємодії з правоохоронними органами. П'ятдесят компаній вже тестують безпілотні автомобілі. Серед них – Uber, Apple, Ford і Toyota…

Прихильники нових правил кажуть, що комп'ютери водять краще людей, яких можна відволікти. Противники стверджують, що тепер водіння буде схоже на відеогру…» ***(У Каліфорнії дозволили використовувати безпілотні автомобілі // Є! «ЄДНІСТЬ-ІНФОРМ» (https://www.ednist.info/news/80264). 27.02.2018).***

***

«Євросоюз хоче створити у країнах-членах мережу центрів із кібербезпеки. Ціна питання – 50 мільйонів євро.

Рішення про запровадження пілотного проекту з кібербезпеки ухвалила у четвер Єврокомісія…

У Єврокомісії також очікують на пропозиції щодо зміцнення кібербезпеки в інтересах єдиного цифрового ринку від університетів, дослідницьких центрів та інших організацій у цій сфері.

Метою проекту є набуття Європою можливостей для відбиття кібератак та розбудови міцної системи кібербезпеки в ЄС» ***(Євросоюз виділить 50 мільйонів на мережу центрів із кібербезпеки // Західна інформаційна корпорація (https://zik.ua/news/2018/02/01/yevrosoyuz_vydilyt_50_milyoniv_na_merezhu_tsentriv_iz_kiberbezpeky_1256687). 01.02.2018).***

***

«Госоператор «Ростелеком» ведет переговоры о приобретении 100% российской компании Solar Security, которая работает в сфере кибербезопасности…

…уже достигнута предварительная договоренность о покупке. Сумма сделки пока не известна, однако ожидается, что она может быть закрыта во втором квартале этого года…» ***(РБК: «Ростелеком» намерен купить занимающуюся кибербезопасностью Solar Security // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3541384?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). 07.02.2018).***

***

«Рынок корпоративных услуг в области кибербезопасности в России вырастет до $103 млн. в 2021 году по сравнению с $82 млн в 2016-м, следует из прогноза Orange Business Services и IDC. Быстрее других сегментов будет расти консалтинг в этой сфере, объем рынка которого приблизится к $38 млн…

…Компании изучили сегменты управляемых услуг безопасности… К 2022 году среднегодовой темп роста этих сегментов рынка составит 3,9%. Спрос на услуги корпоративной кибербезопасности наиболее высок в финансах, промышленности и энергетике. На рынок при этом выходят новые игроки, ранее известные в других IT-сферах, например телеком-операторы…

В ближайшие пять лет наибольшие темпы роста ожидаются на рынке консалтинга по кибербезопасности, указано в исследовании. В 2017 году его объем в России составил почти $30,9 млн, а в 2021 году достигнет $37,8 млн. В частности, наиболее высокие темпы роста будут у тестирования на проникновение и уязвимости (4,7% в год) и планирования стратегии безопасности (5,9%)…

Драйвер роста сектора — дефицит специалистов на рынке труда. В организациях в девяти случаях из десяти не хватает квалифицированного персонала в области информбезопасности…

Ключевым трендом для России будет обеспечение безопасности критической информационной инфраструктуры, закон о которой был подписан в июле 2017 года…» ***(Кристина Жукова. Хакеры атаковали рынок труда. Спрос на специалистов по кибербезопасности превышает предложение // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3546784?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). 12.02.2018).***

***

«Одна из крупнейших российских ИТ-компаний Softline приобрела контроль в группе компаний «Инфосекьюрити»… После сделки «Инфосекьюрити» планирует выйти с решениями в сфере кибербезопасности на международный рынок.

…Сумму сделки стороны не раскрывают. «Инфосекьюрити» планируется интегрировать в структуру группы Softline….

Это первая для Softline покупка компании со специализацией в сфере кибербезопасности…

Международную экспансию компания начнет со стран Латинской Америки и Юго-Восточной Азии. Цель покупки — усиление позиций Softline на рынке кибербезопасности и расширение спектра услуг за счет сервисов центра управления информационной безопасностью (SOC) и компьютерной криминалистики. В Softline планируют и другие сделки в этой сфере...» ***(Кристина Жукова. Softline занялась безопасностью. Компания приобрела группу «Инфосекьюрити» // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3547329?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). 12.02.2018).***

***

«…InfoWatch и Национальный исследовательский университет «Высшая школа экономики» запускают магистерскую программу «Интернет вещей и киберфизические системы» на базе Московского института электроники и математики им. А.Н. Тихонова. Курс направлен на комплексную подготовку специалистов в области Интернета вещей, рассчитан на два года по очной форме обучения и включает 19 дисциплин. В него входят теоретические и практические занятия по инженерии устройств Интернета вещей и киберфизических систем, разработке программного обеспечения, анализу больших данных, а также кибербезопасности корпоративной и промышленной инфраструктуры в рамках концепции интернета вещей…» ***(В России появятся специалисты по обеспечению безопасности Интернета вещей // «Открытые системы» (https://www.computerworld.ru/news/V-Rossii-poyavyatsya-spetsialisty-po-obespecheniyu-bezopasnosti-Interneta-veschey). 05.02.2018).***

***

«…Российский Центробанк работает над созданием департамента информационной безопасности. …департамент получит статус центра компетенции по обеспечению киберустойчивости организаций кредитно-финансовой сферы.

Помимо прочего, в обязанности новой структуры войдет координирование обмена данными о хакерских атаках между представителями финансового сектора и Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Участие российского Центробанка в предоставлении информации ГосСОПКА обусловлено законом о критической инфраструктуре, вступившем в силу в прошлом году. В частности, документ обязывает Банк России обеспечить обмен данными о кибератаках между Национальным координационным центром по компьютерным инцидентам и субъектами критической информационной инфраструктуры…» ***(ЦБ РФ создаст центр по кибербезопасности финорганизаций // SecurityLabRu (https://www.securitylab.ru/news/491473.php). 13.02.2018).***

«Алмаз-Антей» сообщил о разрабатываемом для российских военных компьютере, который будет полностью защищен от вторжений киберпреступников. …компоненты компьютера будут исключительно российского производства… На данном этапе работы по созданию такого компьютера находятся в стадии завершения…

Планируется, что такой подход заинтересует Минобороны и МЧС России» ***(Олег Иванов. Неуязвимый компьютер создадут для российских военных // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-02-01-1447/25412). 01.02.2018).***

***

«…Каждая пятая компания в России подвергалась хакерским атакам в прошлом году — это данные «Лаборатории Касперского». Причем все чаще киберпреступники не просто крадут информацию и требуют выкуп, а пытаются нарушить работу предприятий. Также с помощью компьютерных вирусов стали похищать продукцию…

Суммы, которые тратятся на обеспечение безопасности, бизнесмены не раскрывают. По данным компании Positive Technologies, бюджеты составляют от 5 млн до 100 млн руб. в год в зависимости от размера и значимости предприятия. Но такие траты оправданы, ведь ущерб от действий хакеров может быть в разы больше…

Обезопасить компании в России можно только технически. За рубежом, например, можно застраховать предприятие от кибератак, и в случае ущерба от действий хакеров получить компенсацию. Наш рынок к этому не готов, считает замгендиректора компании «РЕСО-Гарантия» Игорь Иванов…

В целом российский бизнес по-прежнему не способен успешно противостоять кибератакам. Как выяснила PwC, у 40% компаний нет стратегии информационной безопасности, а больше половины вообще не реагируют на подобные инциденты…» ***(Хакеры пошли на заводы. Как компании борются с киберпреступниками // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3535571?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 01.02.2018).***

***

«Специалисты ФСБ России выступили с инициативой разработать требования к средствам для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на подобные сетевые инциденты…

Проект к соответствующему приказу ФСБ размещён в четверг на официальном портале проектов нормативных актов...

Предполагается, что руководство предприятий критической важности в течение 45 календарных дней согласовывает с Национальным координационным центром по компьютерным инцидентам установку спецсредств и предоставляет в центр следующие сведения: наименование, предназначение, производитель устанавливаемого средства, перечисляет лиц, ответственных за эксплуатацию техники, а также сообщает, на каких именно объектах критически важной инфраструктуры предполагается установить спецсредства защиты.

Установка, настройка, проверка работоспособности и подключение средств к информационным системам проводятся лицензированной организацией в области защиты информации…

При аварийном отключении электропитания предприятие критически важной инфраструктуры должно обеспечивать продолжение работы средств в текущем режиме или корректное автоматическое завершение их работы с оповещением оператора средств защиты.

Восстановление работоспособности средств после сбоя или отказа должно осуществляться в максимально короткие сроки…» ***(Александр Андреев. В ФСБ предложили новый механизм кибербезопасности критической инфраструктуры // «Парламентская газета» (https://www.pnp.ru/social/v-fsb-predlozhili-novyy-mekhanizm-kiberbezopasnosti-kriticheski-vazhnoy-infrastruktury.html). 08.02.2018).***

***

«Правительство установило порядок и сроки категорирования объектов критической инфраструктуры в России. Соответствующее постановление кабмина, подписанное его председателем Дмитрием Медведевым, опубликовано во вторник на официальном портале нормативных и правовых актов.

Как следует из документа, категорирование критической инфраструктуры проводится её субъектами в рамках исполняемых ими функций.

Непосредственно процесс включает определение процессов субъектами критической инфраструктуры по видам деятельности, формирование релевантного

перечня важных объектов, оценку масштаба возможных негативных последствий при попытке совершения кибератак на критическую инфраструктуру и присвоение каждой из её объектов критериев значимости от 1 до 3, где 1 является наивысшей…» ***(Александр Андреев. В России установлено категорирование критической инфраструктуры для обеспечения кибербезопасности // «Парламентская газета» (https://www.pnp.ru/economics/v-rossii-ustanovleny-pravila-kategorirovaniya-kriticheskoy-infrastruktury-dlya-obespecheniya-kiberbezopasnosti.html). 13.02.2018).***

***

«Странам Евразийского экономического союза (ЕАЭС) необходимо задуматься об общей системе кибербезопасности, считает премьер-министр Киргизии Сапар Исаков…

Премьер-министр отметил, что в Киргизии начата "цифровая" реформа, которая направлена на повышение качества работы государственных органов.

"Разработана и принята серия важных законов по защите данных. В процессе разработки находятся еще несколько десятков законов и подзаконных актов… ", - сказал он…» ***(Киргизский премьер предлагает ввести в ЕАЭС общую систему кибербезопасности // (Киргизский премьер предлагает ввести в ЕАЭС общую систему кибербезопасности // Interfax-Azerbaijan (http://interfax.az/view/724858). 02.02.2018).***

***

«**Премьер-министр Российской Федерации Дмитрий Медведев дал Министерству финансов, а также Министерству связи и массовых коммуникаций, поручение к 15 марта 2018 года внести в правительство проект, который обяжет госорганы централизовано закупать отечественные офисные и бухгалтерские программы, а также программное обеспечение в сфере защиты информации…**

В документе, разработкой которого сейчас занимаются министерства, должно быть предусмотрено внедрение механизма приобретения госорганами отечественного офисного программного обеспечения, которое интегрировано с системами электронного документооборота. Также в документе необходимо установить порядок консолидации и анализа предложений госорганов, касающихся доработки и внедрения новых функций в российское офисное ПО, а также реализовать механизм доработки отечественного офисного ПО на основе результатов, полученных в процессе анализа...» ***(Централизованная закупка отечественного ПО может стать обязательной для госорганов РФ // SecureNews (https://securenews.ru/russian_software_2/). 22.02.2018).***

***

«Почта России завершила установку современного программного обеспечения для защиты компьютеров, предоставленного «Лабораторией Касперского», на более 130 тыс. машин.

В среднем, защита Почты России обнаруживает и отражает около 5 тыс. попыток вирусных атак в неделю. Этот показатель увеличивается в период вирусных эпидемий…

«Обеспечение антивирусной защиты является важной частью глобальной программы Предприятия по обеспечению информационной безопасности, которая уже приносит свои результаты. Кроме этого, в 2017 году мы запустили пилотный проект по созданию централизованной системы сбора и анализа событий информационной безопасности», - сообщил заместитель генерального директора Почты России по информационным технологиям, развитию новых продуктов Сергей Емельченков…

Для повышения знаний работников предприятия в области информационной безопасности, в том числе в вопросах защиты от вирусов, в 2017 году был разработан и внедрен обучающий курс…» ***(Почта России защитила более 130 тыс. компьютеров от виру сов // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5476174-Pochta-Rossii-zashhitila-bolee-130.html#ixzz57vHTn3pD). 20.02.2018).***

***

«АльфаСтрахование» выпускает полис АльфаCyber, защищающий от киберрисков…

Договор страхования АльфаCyber может быть заключен как от всех, так и от некоторых видов киберопасности…

Базовый пакет полиса покрывает риски утраты и искажения данных, программ, разглашения персональных данных и включает расследование и диагностику кибератаки. Тремя вариантами предлагаемых пакетов будут «Базовый», «Базовый+» и «Расширенный»…

Стоимость страхования определяется индивидуально в зависимости от набора рисков, страховой суммы и франшизы, а также рода деятельности страхователя и результатов оценки рискозащищенности. Страховая сумма начинается от 5 млн руб. и может превышать 150 млн руб., а цена полиса – от 25 тыс. до 750 тыс. руб. в год и более…» ***(«АльфаСтрахование» застрахует от кибератак // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5476559-AlfaStraxovaniezastraxuet-ot-kibera.html#ixzz57vLSOXV5). 22.02.2018).***

***

«Президент России Владимир Путин расширил полномочия Федеральной службы охраны (ФСО). Теперь ведомство сможет участвовать в мероприятиях по борьбе с кибератаками «в рамках своей компетенции». Соответствующий указ опубликован на официальном интернет-портале правовой информации.

Согласно документу, ФСО также поручено защищать персональные данные объектов государственной охраны и членов их семей. Кроме того, служба получила право давать согласие на обработку персональных данных охраняемых лиц и их родственников и определять перечень вещей или грузов, запрещенных к проносу и провозу на охраняемые объекты…» ***(Владимир Путин поручил ФСО защищать***

госресурсы от хакерских атак // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3559614?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 27.02.2018).

***

«Глава Минкомсвязи Николай Никифоров заявил, что «российского следа» в атаке вируса NotPetya нет, зато есть украинский…, потому что он распространился через украинскую систему M.E.Doc…

Министр с уверенностью заявил, что оснований для обвинений в адрес России нет.

«Этот вирус мог сделать кто угодно, потому его собрали, по сути, из двух компонентов, которые западные СМИ, по сути, называют компонентами кибероружия, разработанного АНБ, которое утекло в открытые источники до того, как был этот вирус собран, то есть лежали (компоненты – прим. ВЗГЛЯД) в открытом доступе», – подчеркнул Никифоров.

По его словам, из этих компонентов и собрали вирус NotPetya…» ***(Алексей Ласнов. Глава Минкомсвязи заявил об украинском следе в атаке NotPetya // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/2/27/910201.html). 27.02.2018).***

***

«Секретарь Совета безопасности России Николай Патрушев сообщил об активизации деятельности иностранных разведок, которые разрабатывают сложные сценарии кибератак против России. По его словам, перед выборами росийского президента спецслужбы ожидают хакерские атаки на систему «Выборы» и другие политические, экономические и информационные акции.

На выездном совещании в Ростове-на-Дону господин Патрушев также рассказал, что в результате трех массовых атак вируса-шифровальщика в 2017 году в России было выведено из строя более 500 тыс. компьютеров, в том числе, атакам подверглись информационные системы МВД России, компаний «Роснефть», «Евраз»…» ***(Николай Патрушев предупредил о готовящихся кибератаках перед выборами // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3554910?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 20.02.2018).***

***

Інші країни

«Израильские системы безопасности …не готовы к противостоянию кибератакам… Об этом рассказал бывший директор "Моссада" Тамир Пардо.

"Много чего было сделано", - сказал экс-глава израильской разведки на конференции по кибербезопасности в Тель-Авиве вчера. – "Но я считаю, что этого недостаточно, этого даже близко недостаточно. В этом и проблема"…

Пардо отметил, что никто не хочет инвестировать в достойное обеспечение систем кибербезопасности, пока угроза кажется далекой» ***(Израиль вообще не***

готов к кибератакам // ISRAland Online (http://www.isra.com/news/211472). 14.02.2018).

***

«…Австралійська поліція організує курси з кібербезпеки для чотирирічних дітей…

За словами міністра з питань кібербезпеки Ангуса Тейлора, правоохоронні органи помічають шокуючі випадки, коли чотирирічні діти знімають матеріал сексуального характеру і завантажують його в соціальні мережі. Таким чином, на його думку, діти стають об'єктом зацікавлення сексуальних інтернет-злочинців.

Депутат від ліберальної партії Анна Рустон зазначила, що безпека в інтернеті є ключовим фактором, оскільки зростає доступ до цифрових технологій

..з кінця березня федеральний уряд Австралії розширює чинну програму освіти у відповідь на інциденти, що спричиняють появу малолітніх жертв» ***(В Австралії кібербезпеку вивчатимуть з чотирьох років // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/v-avstraliyi-kiberbezpeku-vivchatimut-z-chotiroh-rokiv-268416_.html). 06.02.2018).***

***

Протидія зовнішній кібернетичній агресії

«**Наибольшую угрозу США в киберпространстве в 2018 году составят Россия, Китай, Иран и Северная Корея.** На это указывает письменный доклад директора национальной разведки США Дэна Коутса «Оценка глобальных угроз разведывательными службами США», который он предоставил Сенатскому комитету по вопросам разведки…

…Американская разведка, как указывается в докладе, считает, что от России следует ждать новой опасности в сферах, где она уже осуществляет кибермеры против Украины. Среди них, в частности, срыв работы украинской энергосистемы, похищение и дальнейшее распространение конфиденциальной информации, DDOS атаки и мероприятия под прикрытием (false flag operations) в киберпространстве.

«Российская разведка и службы безопасности и в дальнейшем будут атаковать критическую инфраструктуру США и их союзников и пытаться получить закрытую информацию о политике США из компьютерных сетей США и НАТО», — отмечается в докладе…» ***(В США предупреждают, что в кибератаках против Украины РФ использует новые инструменты // «Факты и комментарии®» (http://fakty.ua/258429-v-ssha-preduprezhdayut-chto-v-kiberatakah-protiv-ukrainy-rf-ispolzuet-novye-instrumenty). 13.02.2018).***

***

«Спецслужби Великої Британії в минулому році відбили 54 млн кібератак і сприяли видаленню 120 тис. помилкових інтернет-сайтів…

У доповіді Національного центру кібербезпеки (National Cyber Security Centre, NCSC), який входить до складу спецслужби Центр урядового зв'язку (Government Communications Headquarters, GCHQ)… стверджується, що видалення

сайтів і відбиття кібератак велося за допомогою захисної системи Great British Firewall, яка передбачає впровадження в комп'ютерну мережу програмного елемента, що здійснює фільтрацію мережевого трафіку. Розроблена NCSC програма активного захисту дозволила в порівнянні з даними на липень 2016 роки скоротити на 2% кількість глобальних фішингових і вірусних атак, що вживаються в Сполученому Королівстві.

У доповіді також вказується, що переважна більшість подібних злочинів відбувається не "ворожими державними суб'єктами", а угрупованнями, які мають намір отримати вигоду з продажу викрадених персональних даних або отримання незаконного доступу до банківських рахунків. За наведеними у документі словами технічного директора NCSC Іена Леві, сьогодні вже "нереалістично думати, що можна перемогти кіберзлочинність". Однак створити їй максимально можливі проблеми NCSC буде всіляко прагнути…» ***(Самуїл Проскуряков. Британські спецслужби у 2017 році відбили 54 млн кібератак // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1713384-britanski-spetssluzhbi-u-2017-rotsi-vidbili-54-mln-kiberatak). 04.02.2018).***

***

«…8 лютого, міністр оборони Франції Флоранс Парлі представила законопроект щодо збільшення фінансування на оборонні потреби, зокрема, з 2019 до 2025 року загалом має бути виділено 295 мільярдів євро…

Передбачається, що до 2022 року року щорічні видатки на потреби оборони зростатимуть з нинішніх 34,2 мільярда євро на 1,7 мільярда євро в рік, коли спливає президентський термін Макрона… Уряд Франції планує досягнути фінансування військової сфери на рівні 2% від ВВП, у порівнянні з 1,7% минулого року…

За даними уряду, до 2025 року буде створено близько 6 тисяч робочих місць, зокрема, половина з них у сфері кібербезпеки та розвідувальних службах.

Голосування за проект закону має відбутися влітку цього року…» ***(Франція вперше за десятиріччя збільшить видатки на армію // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/franciya-vpershe-za-desyatirichchya-zbilshit-vidatki-na-armiyu-268767_.html). 09.02.2018).***

***

«…Північноатлантичний альянс в рамках зусиль щодо стримування агресії Росії може створити на території США і Німеччини командний центр, що відповідає за планування і стратегію в інтересах захисту судноплавних маршрутів від ворожих підводних човнів, а також логістичний центр НАТО, який відповідатиме за прискорення переміщення військ по Європі в разі виникнення конфліктів…

Дипломати повідомляють, що Вашингтон пропонує розмістити центр в Норфолку, штат Вірджинія, де вже є інші об'єкти НАТО. Німеччина пропонує Ульм або Кельн, де також діють об'єкти НАТО. У цих центрах працюватимуть до 1500 співробітників. …такі центри відповідатимуть за протиповітряну оборону і кібербезпеку, а також за підготовку і передислокацію військ другого ешелону.

…Наступного тижня міністр оборони США Джеймс Меттіс зустрінеться з колегами з інших країн НАТО, щоб обговорити плани щодо створення нових командних центрів…

За словами представника НАТО, питання про місця розміщення нових командних центрів розглянуть у найближчі місяці…» ***(Стримування РФ: США та Німеччина хочуть створити нові масштабні командні центри НАТО // «Ракурс» (http://racurs.ua/ua/n100816-strymuvannya-rf-ssha-ta-nimechchyna-hochut-stvoryty-novi-masshtabni-komandni-centry-nato). 08.02.20180.***

***

«Генеральний секретар ООН Антоніо Гуттеріш вважає, що світ стикнувся з необхідністю встановити дозволені рамки міждержавних кібернетичних атак.

Про це він заявив у виступі на Мюнхенській безпековій конференції…

Він нагадав, що взаємні удари у кіберпросторі вже стали реальністю.

«Настав час говорити про міжнародні правові рамки ведення кібернетичної війни», - наголосив генсек ООН. Він запропонував розпочати дискусію з цього приводу на майданчику Генасамблеї ООН…

Водночас у кібернетичній сфері, за словами посадовця, немає єдності навіть щодо того, що вважати нападом…

Гуттеріш став першим посадовцем такого високого рівня, який ініціював узгодження правил ведення кібервійни…» ***(Генсек ООН: настав час запровадити правила ведення кібервійни // Європейська правда (http://www.eurointegration.com.ua/news/2018/02/16/7077641/). 16.02.2018).***

***

«Запад планирует обвинить Россию в хакерских атаках на информационные ресурсы, связанные с проведением Олимпийских игр в Пхенчхане, сообщается на сайте Министерства иностранных дел РФ…

МИД не исключает, что к антироссийской кампании могут быть привлечены не только «ангажированные» издания вроде Washington Post и Buzzfeed, но и компании Threatconnect, Trend Micro и Eset, тесно связанные с американскими спецслужбами…» ***(Запад готовится обвинить Россию в кибератаках на Олимпиаду // «Парламентская газета» (https://www.pnp.ru/social/zapad-gotovitsya-obvinit-rossiyu-v-kiberatakakh-na-olimpiadu.html). 07.02.2018).***

***

«Россия передала США предложения по договоренности о предотвращении кибератак, Вашингтон рассматривает их, заявил спецпредставитель президента России по международному сотрудничеству в области информационной безопасности, посол по особым поручениям МИД Андрей Крутских.

«Есть соглашение (между РФ и США) о мерах доверия в киберпространстве (с 2013 года). Пресса в свое время назвала этот документ первым соглашением по предотвращению кибервойны. И это действительно так, потому что оно охватывает

практически весь спектр подобных угроз. Если вдруг что-то произойдёт, мы должны друг друга об этом уведомлять», – сказал Крутских.

…«… Мы официально передали администрации (президента США Дональда) Трампа предложение обсудить и эту тему, адаптировав принцип Соглашения о предотвращении конфликтов. Они его рассматривают», – сказал Крутских…» ***(Алина Назарова. США рассмотрят предложения России о предотвращении кибератак // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/2/2/906434.html).02.02.2018).***

«…Глава ЦРУ Майк Помпео, директор национальной разведки США Дэн Коутс и директор Агентства национальной безопасности США Майкл Роджерс заявили, что располагают данными, указывающими, что Россия попытается вмешаться в промежуточные выборы в стране в 2018 году…

"Да, мы засекли действия со стороны России (указывающие на - ИФ) ее намерения повлиять на следующий цикл выборов (промежуточные выборы в США - ИФ)", - заявил Помпео во вторник на слушаниях в комитете по разведке Сената США.

Коутс и Роджерс также положительно ответили на вопрос члена комитета о том, располагают ли они информацией в подтверждение этого...

«Не должно быть никаких сомнений в том, что Россия считает свои прошлые попытки успешными и видит в (промежуточных) выборах в 2018 году потенциальную цель для своих операций», - добавил Коутс.

На ноябрь 2018 года в США назначены выборов губернаторов и конгрессменов…» ***(Американские спецслужбы заподозрили РФ в намерении повлиять на выборы в США в 2018 году // INTERFAX.RU (http://www.interfax.ru/world/599832). 13.02.2018)***

***

Кіберзахист критичної інфраструктури

«…Федеральная служба безопасности РФ подготовила ряд документов, касающихся защиты объектов критической информационной инфраструктуры. Первый — проект приказа «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации», второй — «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

Согласно пояснительной записке, первый документ направлен на совершенствование правового регулирования в сфере координации деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, а также на реализацию пункта 10 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»…

В пояснительной записке второго документа ФСБ сказано, что он также «направлен на совершенствование правового регулирования в сфере координации деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, а также на реализацию 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»».

Приказ должен «утвердить прилагаемые Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

«Настоящие Требования определяют требования к устанавливаемым и используемым на всей территории Российской Федерации техническим, программным, программно-аппаратным и иным средствам для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ, предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографическим средствам защиты такой информации», — говорится в приложении к приказу…» ***(ФСБ разработала порядок отражения компьютерных атак // РосКомСвобода (https://roskomsvoboda.org/36144/). 09.02.2018).***

***

Кіберзлочинність та кібертероризм

«Российский программист Петр Левашов, задержанный в Испании по запросу США, передан американской Службе федеральных маршалов. Об этом сообщает Национальная полиция Испании.

…Ему инкриминируется создание и управление Kelihos — глобальной сетью зараженных компьютеров, занимавшихся рассылкой спама, распространением вредоносных программ и сбором персональных данных пользователей…» ***(Испания передала США обвиняемого в кибератаках россиянина Левашова // АО«Коммерсантъ»(https://www.kommersant.ru/doc/3539483?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 02.02.2018).***

***

«Российский программист Петр Левашов, которого власти США обвиняют в кибермошенничестве, заявил в суде о своей невиновности. Об этом сообщил адвокат Игорь Литвак.

«Сегодня вечером у нас было первое слушание в суде в Коннектикуте. Петя Левашов сказал, что он невиновен по 8 пунктам, по которым его обвиняют в обвинительном заключении»,— сказал господин Литвак. Он подчеркнул, что сторона защиты не получила «никаких документов от прокуратуры, никаких улик». По словам юриста, Петра Левашова минимум до понедельника будут содержать в тюрьме в городе Бриджпорт в Коннектикуте…» ***(Обвиняемый в США в кибератаках россиянин заявил в суде о своей невиновности // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3539830?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B00. 03.02.2018).***

***

«…Евгений Касперский рассказал о новой мошеннической схеме для майнинга… Так, киберпреступники встраивают скрипты для майнинга в рекламные объявления в видеороликах на YouTube. По мнению Касперского, пользователи доверяют видеохостингу, поэтому, если видео начинает тормозить, с большой вероятностью спишут проблему на интернет-соединение, а не на проблемы с безопасностью. Признаками атаки через YouTube является замедление работы компьютеров и рост энергопотребления…» ***(Евгений Касперский: кибермошенники вставляют скрипты для майнинга в рекламу на YouTube // «Открытые системы» (https://www.computerworld.ru/news/Kibermoshenniki-vstavlyayut-skripty-dlya-mayninga-v-reklamu-na-YouTube). 06.02.2018).***

***

«Федеральный суд в Нью-Джерси признал виновными россиян Владимира Дринкмана и Дмитрия Смилянца в хакерских атаках и приговорил их к 12 и 4 годам и 4 месяцам соответственно.

Дринкмана и Смилянца экстрадировали в США из Нидерландов в 2013 году. В американском суде оба признали себя виновными в создании компьютерной мошеннической схемы, с помощью которой были украдены 160 млн номеров кредитных и дебетовых карт. По версии обвинения россияне Владимир Дринкман, Александр Калинин, Роман Котов, Дмитрий Смилянец и украинец Михаил Рытиков на протяжении семи лет крали информацию из сети крупных американских и международных компаний…» ***(В США россиян признали виновными в хакерстве // Internetua (http://internetua.com/v-ssha-rossiyan-priznali-vinovnmi-v-hakerstve). 15.02.2018).***

***

«Вслед за сайтами с большой посещаемостью и видеохостингом YouTube атакам «чёрных майнеров» подверглись сайты государственных органов США и Великобритании. Эксперт по кибербезопасности Скотт Хельме сообщает,

что на данный момент в скрытую добычу криптовалюты вовлечены тысячи сайтов государственных органов.

О проблеме Хельме рассказал у себя в твиттере, опубликовав несколько постов, посвящённых сайтам, на которых удалось выявить скрипты, установленные злоумышленниками…

Практически на всех сайтах, уличённых в скрытом майнинге криптовалют, установлено программное обеспечение CoinHive, которое хакеры смогли внедрить через уязвимость расширения BrowseAloud, которое позволяет пользоваться сайтами людям с плохим зрением…» ***(Вячеслав Ларионов. Хакеры заразили майнером государственные сайты США и Великобритании // Hi-News.ru (https://hi-news.ru/technology/xakery-zarazili-majnerom-gosudarstvennye-sajty-ssha-i-velikobritanii.html). 12.02.2018).***

***

«…стало відомо про найбільший витік інформації за всю історію Apple. В мережу потрапив вихідний код операційної системи iOS. Компанія вже підтвердила, що …код завантажувача iBoot дійсно з'явився у вільному доступі.

«Старий вихідний код трирічної давності дійсно втік», – відзначили в Apple…

Попри те, що в компанії запевнили про неактуальність цього коду, адвокати, що діють від імені яблучної корпорації, все одно вимагають видалити його з GitHub. Адже опублікована інформація, у будь-якому випадку, належить компанії. А отже, на неї поширюється закон про захист авторських прав.

За словами спеціалістів, неважливо наскільки актуальний код, це не завадить вивчати вихідні коди для пошуку вразливостей. Цілком ймовірно, що цей витік також дозволить емулювати iOS на інші пристрої…» ***(Грицина Вікторія. Apple підтвердила найбільший витік в історії компанії // Pingvin.Pro (https://pingvin.pro/gadgets/news-gadgets/apple-pidtverdyla-vytik.html).09.02.2018).***

***

«Співробітники правоохоронних органів США викрили мережу кіберзлочинців Infraud, яку в 2010 році заснував українець Святослав Бондаренко…

У Міністерстві юстиції США зазначають, що група кіберзлочинців діяла під гаслом "In Fraud We Trust", тобто "Ми віримо в шахрайство".

Зловмисники створили розгалужену й добре організовану мережу, що протизаконним шляхом отримувала особисті дані інтернет-користувачів…

На думку слідчих, члени угруповання намагалися отримати дані про 4,3 мільйона кредитних карток та банківських рахунків.

В американському відомстві наголошують, що за час існування угруповання злочинці завдали своїми діями збитків на понад $530 млн.

Наразі слідчі вважають причетними до злочинного угруповання загалом 36 осіб. 13 членів кібербанди вже заарештували…» ***(У США викрили засновану українцем міжнародну мережу кіберзлочинців. Ті хотіли вкрасти дані 4,3 млн кредитних карток // Espreso.tv***

(https://espreso.tv/news/2018/02/08/u_ssha_vykryly_zasnovanu_ukrayincem_mizhnarodnu_merezhu_kiberzlochynciv_ti_khotily_vkrasty_dani_4_3_mln_kredytnykh_kartok). 08.02.2018).

***

«…Поліція Таїланду за запитом американських правоохоронних органів затримала росіянина Сергія Медведєва, якого підозрюють в причетності до міжнародної хакерської мережі, що займалася шахрайством…

Його взяли під варту в Бангкоку на запит ФБР 6 лютого, в місті він проживав близько 6 років.

Медведєва підозрюють у тому, що він є одним з творців інтернет-майданчика з девізом "в шахрайство ми віримо" (In Fraud We Trust), який раніше заблокувало ФБР. Він, імовірно, використовувався для торгівлі зброєю і наркотиками з використанням біткоїнів, а також який займався продажем вкрадених даних про номери кредитних карток та банківські рахунки.

На рахунках росіянина виявлені кошти в криптовалюті еквівалентні сумі три мільйони доларів…» ***(У Таїланді за наводкою ФБР затримали російського хакера // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/u-tayilandi-za-navodkoyu-fbr-zatrimali-rosiyskogo-hakera-268802_.html). 09.02.2018).***

***

«**Експерти з кібербезпеки компанії Trustwave Spiderlabs повідомили, що хакери знайшли спосіб зламувати комп'ютери за допомогою файлу Word**…

Кіберзлочинці розробили метод для виманювання і розкрадання паролів доступу до персональних комп'ютерів. Підчепити вірус можна, отримавши документи в форматі DOCX, RTF, HTA, VBScript і PowerShell.

Користувачеві надсилають спам-лист, до якого прикріплений файл в таких форматах. Він завантажує прикріплений файл і це призводить до установки на його комп'ютері шкідливого програмного забезпечення. Потім програма отримує доступ до логін-паролів і пересилає хакерам…» ***(Хакери винайшли новий спосіб злому комп'ютерів // "Багнет" (http://www.bagnet.org/news/tech/357433/hakeri-vinayshli-noviy-sposib-zlomu-kompyuteriv). 16.02.2018).***

***

«…С подачи США и Южной Кореи Северная Корея получила статус главного поставщика кибероружия, а северокорейских хакеров нередко называют лучшими в мире…

Агентству Bloomberg удалось поговорить с северокорейцем, который служил в КНДР хакером, но бежал на Юг, и узнать, как устроены кибервойска Пхеньяна….

Северокорейский хакер Чен Хек (имя было изменено)… выглядит как обычный программист. Он говорит, что не имеет отношения к известным на весь мир атакам, но на тот момент как раз стал «пехотинцем» в хакерской армии Северной Кореи.

Главная цель таких хакеров не посеять хаос, а заработать деньги для страны, поскольку из-за международных санкций Северная Корея испытывает экономические трудности…

Чонг, которому сейчас около 40 лет, жил в Китае в трехэтажноме доме с такими же северокорейскими хакерами, как и он сам.

Каждый из них зарабатывал около 100 тысяч долларов в год, из которых разрешалось оставить себе не более десяти процентов…

Кибервойска в КНДР начали создавать еще при Ким Чен Ире. На протяжении десятилетий правительство Северной Кореи стремилось использовать современные технологии…

Кибервойска Ким Чен Ира точечно атаковали правительственные сайты и банковские сети. Но когда Ким умер в 2011 году, его сын расширил программу. Вскоре начались более интенсивные атаки на более важные цели, такие как атомные станции, оборонные сети и финансовые учреждения.

Чен рассказывает, что попал в кибервойска, созданные еще при Ким Чен Ире. В школе он увлекался биологией и хотел стать врачем, но по распределению попал на факультет компьютерных наук.

В конце 1990-х его отправили на учебу в Китай.. Вернувшись домой, он устроился программистом, однако вскоре его отправили в Китай «на заработки».

Ему говорили, что он должен провести исследование программного обеспечения, которое должно было «принести светлое будущее» информационным технологиям Северной Кореи…

Интересно, что Чену компьютер не выдали — он должен был заработать на него сам… Сперва он продавал ворованное программное обеспечение, затем занимался взломом программ по заказу…

…он был на хорошем счету, принося около 100 тысяч долларов в год…

Каждое подразделение контролировалось «главным делегатом», который организовывал транзакции и собирал платежи. Отдельный наблюдатель от государственной полиции Северной Кореи находился там для решения вопросов безопасности.

Чен вспоминает, что для создания функциональной копии одной программы требовалось 20 программистов. Хакеры часто работали без передыха, чтобы найти уязвимости в части программного обеспечения…

Проработав в Китае несколько лет Чен решил бежать после инцидента с госслужащим, о котором он не стал рассказывать. Два года он ездил по Китаю, останавливался в гостиницах и зарабатывал себе на жизнь хакерством, а потом купил поддельный китайский паспорт за 1,6 тысячи долларов, улетел в Бангкок и обратился в посольство Южной Кореи.

Он месяц проходил проверку безопасности, прежде чем отправиться в Сеул, где ему помогли начать новую жизнь… Недавно он получил повышение в компании по обеспечению безопасности программного обеспечения…» ***(Как работают кибервойска КНДР. История беженца Сюжет // AllSvit (http://allsvit.net/allnews/kak_rabotayut_kibervoyska_kndr_istoriya_bezhencasyuzhet/) 12.02.2018).***

***

«Киберпреступная группировка Coinhoarder, связанная с Украиной, заработала около $50 млн в биткоинах. Интересно, что результата они достигли с помощью Google AdWords для заманивания пользователей на фишинговые сайты…

В феврале текущего года украинская киберполиция смогла приостановить деятельность группировки, но, несмотря на то, что правоохранители отключили серверы, на которых размещались некоторые фишинговые сайты, арестовать злоумышленников пока не удалось…

Особенностью преступной кампании стало то, как мошенники привлекают трафик на свои сайты. Вместо рассылки фишинговых писем…, злоумышленники вполне законно купили рекламу через платформу Google AdWords и разместили ссылки на фишинговые сайты в результатах поиска Google, связанных с Bitcoin.

…По данным Cisco Talos, одно из объявлений смогло привлечь более 200 тыс. пользователей, а общее количество посетителей вредоносных сайтов исчисляется десятками миллионов...

Еще одним продуманным шагом стало то, что для своих объявлений мошенники использовали гео-фильтры, ориентируясь главным образом на владельцев биткоинов в Африке…

Фишинговые сайты были размещены на серверах украинского провайдера Highload Systems. По данным Cisco, Coinhoarder стала одной из крупнейших фишинговых кампаний, направленных на пользователей Blockchain.info…» ***(Иван Николенко. Как украинские фишеры заработали $50 млн на Google Adwords // ChannelForIT (http://channel4it.com/publications/Kak-ukrainskie-fishery-zarabotali-50-mln-na-Google-Adwords-29447.html#). 15.02.2018).***

***

«Один из IT-партнеров Western Union подвергся кибератаке, в результате которой злоумышленникам удалось похитить конфиденциальную информацию клиентов компании…

…31 января текущего года Western Union разослала своим клиентам уведомление об утечке. Согласно уведомлению, подрядчик, услугами которого компания пользовалась для безопасного хранения данных, был скомпрометирован, и данные клиентов Western Union могли оказаться в руках у хакеров. По всей вероятности, злоумышленникам удалось взломать системы вендора, чьими облачными или внешними хранилищами резервных копий пользовалась компания…

В настоящее время компания прекратила любое использование системы скомпрометированного вендора, а сама система была отключена от интернета. Взломанный архив содержал контактные данные клиентов Western Union, названия банков, внутренние идентификационные номера сотрудников компании, суммы денежных переводов, а также время осуществления и идентификационные номера транзакций.

Данные банковских карт не пострадали. Внутренние платежные и финансовые системы Western Union не были затронуты атакой…» ***(Компания***

Western Union предупредила клиентов об утечке // "Багнет" (http://www.bagnet.org/news/society/357330/kompaniya-western-union-predupredila-klientov-ob-utechke). 15.02.2018).

***

«…Проблема кіберзлочинності в тій чи іншій мірі зачепила не менше 41 відсотка користувачів інтернету в Німеччині. На це вказують підсумки оприлюдненого 5 лютого опитування, проведеного на замовлення німецьких спецслужб, зокрема Федерального відомства з безпеки інформаційної техніки (BSI)…

Результати опитування свідчать, що кожен п'ятий німецький користувач інтернету постраждав від наслідків поширення шкідливих програм, приміром, вірусів та так званих "троянів". Ще вісім відсотків опитаних стали жертвами кібершахраїв під час онлайн-шопінгу. Шість відсотків потрапили в пастку так званого "фішингу", коли зловмисникам вдалося отримати шляхом обману особисті дані користувачів. Від наслідків крадіжки особистих даних постраждали п'ять відсотків учасників опитування.

Також з'ясувалося, що для німецьких інтернет-користувачів особливе значення має безпека фінансових даних...

Водночас більше половини опитаних визнали, що їм вдалося самотужки впоратися зі завданими кіберзлочинцями наслідками. 24 відсотки зверталися по допомогу до членів родини чи друзів. І лише 19 відсотків жертв кіберзлочинів зверталися з відповідними заявами до поліції.

Опитування проводилося з 28 вересня по 9 жовтня 2017 року соціологами Ipsos Public Affairs. У ньому взяло участь 2010 респондентів віком від 14 до 66 років» ***(Валерій Сааков. Жертвами кіберзлочинців стали понад 40 відсотків інтернет-користувачів у ФРН // Deutsche Welle (http://www.dw.com/uk/%D0%B6%D0%B5%D1%80%D1%82%D0%B2%D0%B0%D0%BC%D0%B8-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D1%86%D1%96%D0%B2-%D1%81%D1%82%D0%B0%D0%BB%D0%B8-%D0%BF%D0%BE%D0%BD%D0%B0%D0%B4-40-%D0%B2%D1%96%D0%B4%D1%81%D0%BE%D1%82%D0%BA%D1%96%D0%B2-%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D1%96%D0%B2-%D1%83-%D1%84%D1%80%D0%BD/a-42461141). 05.02.2018).***

***

«Майнеры теперь могут добывать криптовалюту с помощью нового функционала в Microsoft Word, который позволяет добавлять в текстовые документы видеоролики из интернета, не встраивая саму видеозапись в файл.

Пользователь может скопировать код iframe в поле во всплывающем окне. Когда файл будет открыт снова, в документе отобразится видео. При нажатии на

кнопку воспроизведения начнется загрузка и проигрывание ролика. Специалисты израильской компании Votiro обнаружили, что хакеры могут воспользоваться этим механизмом, чтобы загружать JS-скрипты для добычи криптовалюты Monero. Проведение такой атаки возможно благодаря тому, что Word не осуществляет проверку источника, откуда был загружен код iframe, а также из-за того, что видеоролик воспроизводится в браузере Internet Explorer…» ***(Добыча криптовалюты может осуществляться майнерами через документы Microsoft Word // SecureNews (https://securenews.ru/word_2/). 21.02.2018)***.

***

«**Неизвестные злоумышленники скомпрометировали сервер Linux-дистрибутива Mageia и украли базу данных пользователей, а затем разместили ее в открытом доступе.**

…взломщики получили доступ к серверу Mageia, на котором хранились имена пользователей, хэши паролей и адреса электронной почты…

Сразу после того, как утечка была выявлена, разработчики сбросили все пароли и предложили пользователям восстановить их через соответствующий интерфейс…

Сейчас администрация проекта расследует данный инцидент…» ***(Хакеры взломали сервер проекта Mageia // SecureNews (https://securenews.ru/mageia/). 21.02.2018).***

***

«Неизвестные злоумышленники заполучили доступ к системам индийского банка City Union Bank и перевели на свои счета 1800000 долларов.

По словам сотрудников City Union Bank, хакеры вывели средства через банковскую систему SWIFT. Как утверждают представители банка, он был атакован со стороны международной кибергруппировки. Кроме того, в City Union Bank опровергли возможную причастность своих сотрудников к атаке.

В заявлении представителей банка говорится о том, что транзакции мошенников были выявлены 7 февраля...» ***(Хакеры украли у одного из индийских банков около 2000000 долларов // SecureNews (https://securenews.ru/city_union_bank/). 19.02.2018).***

***

«Эксперты из NewSky Security выявили новую ботсеть DoubleDoor, состоящую из устройств «Интернета вещей» (IoT)…

DoubleDoor сначала задействует эксплоит для уязвимости в Juniper Networks ScreenOS, на базе которой функционируют межсетевые экраны Netscreen. Используя первый эксплоит, вредоносная программа обходит межсетевой экран, а затем активирует второй эксплоит для уязвимости в модемах ZyXEL PK5001Z.

…В большинстве случаев атаки на IoT-устройства проводятся с IP-адресов, зарегистрированных в Южной Корее…» ***(Ботсеть DoubleDoor может обходить межсетевые экраны // SecureNews (https://securenews.ru/doubledoor/). 15.02.2018).***

***

«…Английский язык пополнился словом «криптоджекинг» (cryptojacking). Это гибрид терминов cryptocurrency (криптовалюта) и hijacking (похищение), обозначающий тайный майнинг криптовалют, т.е. использование вычислительных мощностей пользовательских устройств для добычи криптовалюты в кошельки хакеров…

Хакеры, принявшие на вооружение криптоджекинг, естественно, охотятся на ресурсы, наиболее востребованные пользователями интернета. Очередным таким ресурсом стал форум Deepfakes…» ***(Тайный майнинг обрел имя // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5474792-Tajnyj-majning-obrel-imya.html#ixzz57vCQfnkv). 14.02.2018).***

***

«Ущерб российских банков и платежных систем от действий киберпреступников в 2017 году составил 1,35 млрд. рублей, следует из данных обзора несанкционированных передов денежных средств за 2017 год, подготовленного Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России.

…Один из банков сообщил в ЦБ об успешной атаке на рабочее место оператора SWIFT. В результате из банка было выведено 339,5 млн. руб. Часть этих средств удалось вернуть.

Еще два банка сообщили в ЦБ о несанкционированных операциях, которые злоумышленники совершали с их корреспондентских счетов в Банке России, на сумму 54 млн. рублей…

Шесть банков зафиксировали случаи, когда кассиры переводили денежные средства на банковские счета злоумышленников в результате воздействия так называемой социальной инженерии - побуждения человека к совершению необходимого злоумышленникам действия путем обмана или злоупотребления доверием. Объем несанкционированных операций составил 7 млн руб.

При этом зафиксировано снижение объема краж средств с банковских счетов россиян. Наряду с этим в прошедшем году наблюдался незначительный рост количества несанкционированных операций по счетам физических лиц, говорится в обзоре…

Больше всего от действий хакеров в 2017 году пострадали жители и компании Московского региона…» ***(Ущерб банковской сферы РФ от киберпреступников в 2017 году превысил 1,3 млрд. рублей // ООО "ИКС-МЕДИА" // (http://www.iksmedia.ru/news/5475384-Ushherb-bankovskoj-sfery-RF-ot-kibe.html#ixzz57vDP4KAK). 16.02.2018).***

***

«Программы-вымогатели продолжают атаковать организации по всему миру наряду с всплеском скрытого майнинга криптовалют. Тенденции продолжат развиваться в 2018 году, а вымогательство, вероятно, будет нацелено на организации, пытающиеся соответствовать новым законам конфиденциальности «Общего регламента по защите данных» (GDPR, General Data Protection Regulation).

К таким выводам пришли аналитики Trend Micro Incorporated в ходе подготовки отчета «Парадокс киберугроз» (The Paradox of Cyberthreats). По данным экспертов, преступники все чаще отказываются от использования эксплойтов и беспорядочных нападений в пользу стратегических атак, направленных, в первую очередь, на финансовую выгоду...

Количество программ-вымогателей увеличилось на 32% за период с 2016 по 2017 год. Число BEC-атак во второй половине 2017 года вдвое превысило показатели первой половины. По прогнозам экспертов Trend Micro, потери от таких атак превысят 9 млрд долларов в 2018 году.

Темпы разработки вредоносных программ для майнинга криптовалют постоянно растут – в октябре было обнаружено 100 тыс. программ. Устройства Интернета вещей (IoT) также подвержены риску. Решения Trend Micro обнаружили 45,6 млн случаев скрытого майнинга, которые составляют большую часть от всех обнаруженных инцидентов, связанных с Интернетом вещей…» ***(Киберпреступники могут использовать GDPR в своих целях // ООО "ИКС-МЕДИА"(http://www.iksmedia.ru/news/5476161-Kiberprestupniki-mogut-ispolzovat.html#ixzz57vGyuezq). 20.02.2018).***

***

«…Общая сумма убытков от хакерских нападений в прошлом году составила $600 млрд, говорится в исследовании Центра стратегических и международных исследований (CSIS) и компании McAfee, которая разрабатывает системы защиты и анализа вредоносного и нежелательного ПО…

Наибольший ущерб нанесли хакерские нападения, связанные с военной промышленностью. Наиболее распространенными преступлениями стали кража личных данных, банковских реквизитов и других конфиденциальных данных.

Лидером по уровню киберпреступности является Россия. На втором месте - КНДР. Много хакерских атак было осуществлено из Индии, Вьетнама и Бразилии. ***(Мировой рейтинг киберпреступников возглавила Россия // Gazeta.ua (https://gazeta.ua/ru/articles/world-life/_mirovoj-rejting-kiberprestupnikov-vozglavila-rossiya/822585). 23.02.2018).***

***

Діяльність хакерів та хакерські угруповування

«Американские хакеры с 2013 по 2016 годы похитили у различных компаний в общей сложности $5,2 млрд. …хакеры смогли украсть такую сумму, рассылая электронные письма с вредоносным содержимым под видом известных получателям адресатов.

Схема рассылки вредоносных писем заключается в том, что сначала хакеры получают информацию о сотрудниках фирмы с помощью фишинга. Затем рассылаются письма, которые на первый взгляд не выглядят подозрительно, так как их авторами являются клиенты компании. Используя такую схему, кибермошенники украли данные о 15,4 млн человек…» ***(Хакеры в США через***

рассылку писем похитили более $5 млрд // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3539608?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). 03.02.2018).

**

«…В США группировку Fancy Bear, которую считают связанной с российскими спецслужбами, обвинили в краже информации у крупнейших американских компаний в сфере авиации…

Специалистам американской компании Secureworks, которая работает в области кибербезопасности, стало известно о массивной атаке хакеров на компьютеры сотрудников оборонного сектора США и крупных компаний, связанных с авиаразработками, — Boeing, Airbus, Lockheed Martin, а также General Atomics, которая является производителем беспилотников, в том числе ударного дрона Reaper.

Злоумышленники почти 20 тыс. раз пытались получить доступ к электронной почте сотрудников этих компаний, и у нескольких десятков человек данные все-таки удалось украсть…

…на официальном сайте группировки информации о взломе нет, хотя там обычно публикуются сообщения о деятельности киберпреступников…

Руководитель Агентства кибербезопасности Евгений Лифшиц подчеркивает, что хотя ситуация и похожа на современную версию промышленного шпионажа, на практике же русских хакеров в историю могли добавить журналисты…

Кроме разработок в сфере беспилотных аппаратов, в руки хакерам также могла попасть информация, касающаяся разработки орбитального самолета и «облачных» сервисов хранения данных…» ***(Информация «улетела» к хакерам. Какие данные об авиаразработках в США стали доступны // АО «Коммерсантъ»(https://www.kommersant.ru/doc/3541830?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). 07.02.2018).***

***

«Сотрудники Агентства финансовых услуг Японии сегодня проведут проверку в офисе криптовалютной биржи Coincheck в Токио после произошедшей на прошлой неделе крупной хакерской атаки на биржу…

…сотрудники агентства хотят проверить финансовую отчетность биржи и выяснить, хватит ли у Coincheck средств на выплату $420 млн компенсации пострадавшими от кибератаки клиентам. Помимо этого власти проверят системы безопасности биржи.

…Японское Управление по контролю за финансовыми рынками (FSA), тем временем, планирует проверить все криптовалютные биржи страны…» ***(В офисе биржи криптовалют Coincheck в Японии пройдет проверка после кибератаки // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3536132?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 02.02.2018).***

***

«Глава Group-IB Илья Сачков сообщил о росте количества хакерских группировок, которые специализируются на хищениях криптовалют…

По его словам, хакерские группы, ранее «специализировавшиеся» на атаках банковских систем, переключились на криптовалюты. «Они наносят значительный ущерб крипто-проектам… Возможность конвертации в привычные деньги — это одна из мотиваций. При этом законодательно пользователь криптовалюты ничем не защищен»,— пояснил Сачков…» ***(Выросло число хакерских группировок, специализирующихся на крипто валютах // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3541211?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 07.02.2018).***

***

«Хакеры, похитившие данные 57 млн клиентов и водителей сервиса такси Uber в 2016 году, действовали из штата Флорида в США и из Канады, заявил в Конгрессе глава службы информационной безопасности Uber Джон Флинн…

Господин Флинн заявил, что компания «совершила ошибку», не сообщив об утечке данных клиентам и правоохранительным органам, и этому «нет оправдания». Он подтвердил, что компания заплатила $100 тыс. одному из хакеров за удаление похищенных данных, платеж был проведен в рамках компании по выплате премий за обнаружение уязвимости программного обеспечения.

Bloomberg сообщает, что по этой же программе Uber заплатил около $1,3 млн сотням независимых хакеров с целью поиска уязвимых мест в системе безопасности…

В том, что Uber заплатила хакерам $100 тыс., чтобы скрыть серьезную кражу данных в конце 2016 года, компания официально призналась в ноябре 2017 года. Глава Uber Дара Хосровшахи заявил, что ему стало известно о случившемся лишь недавно, поскольку руководитель службы безопасности компании Джо Салливан всеми силами старался скрыть утечку» ***(Uber обвинил в кибератаке в 2016 году хакеров из США и Канады // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3541392?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 07.02.2018).***

***

«Экспертный центр безопасности Positive Technologies зафиксировал серию кибератак, направленных на организации оборонно-промышленного комплекса (ОПК) России…

Как выяснили эксперты, неизвестная хакерская группировка запустила вредоносную кампанию под названием SonXY в апреле 2017 года. По предварительной информации, жертвами атак стали не менее 17 компаний из России, США, Японии, Белоруссии, Казахстана, Украины и других стран.

Как считает Positive Technologies, ключевой целью кампании был шпионаж… Аналитики выяснили, что вредоносное ПО попадало в компьютеры при помощи

целевой фишинговой рассылки, распространявшейся как для организаций, так и для физических лиц…

Антивирусный эксперт «Лаборатории Касперского» Денис Легезо заявил, что атака на предприятия ОПК могла вестись из Китая…» ***(Эксперты сообщили о кибератаках на предприятия российского ОПК // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3542716?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 09.02.2018).***

***

«**Эксперты в области безопасности считают кибератаку на серверы Олимпийских игр 2018 года, которая стала причиной приостановки работы официального сайта, местью российских хакеров на решение МОК о недопуске спортсменов**…

Речь идет о кибератаке за 45 минут до начала церемонии открытия Олимпиады. Серверы пришлось отключить на 15 часов для предотвращения дальнейшего ущерба. В итоге сайт Олимпиады некоторое время не работал, а зрители не смогли распечатать билеты на мероприятие, купленные онлайн…

Россия отрицает причастность к любым кибератакам…» ***(Сергей Гурьянов. СМИ назвали атаку на серверы Олимпиады «местью российских хакеров» // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/2/11/907750.html). 11.02.2018).***

***

«**Хакеры в 2017 году провели 11 «успешных» атак на российские банки с помощью вируса Cobalt Strike**, сумма хищений составила 1 млрд 156 млн рублей, сообщил зампред ЦБ Дмитрий Скобелкин.

Всего же за 2017 год были зафиксированы более 20 попыток атак с помощью Cobalt Strike. Были атакованы порядка 240 кредитных организаций…

«При этом восемь из 11 пострадавших организаций являются участниками информационного обмена с ФинЦЕРТом», – заметил Скобелкин.

По его словам, ФинЦЕРТ направил индивидуальные предупреждения более чем 400 организациям с указанием конкретных электронным почтовых адресов, с которых поступали письма группы Cobalt.

Основной задачей Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ, FinCERT) является координация действий финансовых организаций и своевременное их информирование со стороны ЦБ об инцидентах и происшествиях…» ***(Наталья Ануфриева. ЦБ подсчитал, сколько хакеры похитили у банков за год // ООО Деловая газета «Взгляд» (https://vz.ru/news/2018/2/13/908037.html). 13.02.2018).***

***

«**С помощью популярного мессенджера Telegram хакеры почти год имели возможность получить доступ к компьютерам пользователей, заражая ПК вредоносным программным обеспечением, способным скрыто добывать криптовалюту**. О проблеме сообщила «Лаборатория Касперского», специалисты

которой и обнаружили уязвимость в Telegram для Windows, позволяющую отправлять пользователям вредоносные приложения под видом различных вложений, например картинок…

Захваченные компьютеры использовались мошенниками для майнинга криптовалюты и других малоприятных вещей. Например, хакеры выкачивали у жертв весь локальный кеш Telegram. По данным «Лаборатории Касперского», за всё время пострадало более тысячи компьютеров, которые скрыто майнили Monero, Zcash и Fantomcoin.

…Команда разработчиков сообщила, что проблема уже устранена… , а глава Telegram отметил, что отчеты антивирусных компаний должны приниматься с долей скептицизма, поскольку они склонны преувеличивать серьезность своих выводов для получения огласки в массмедиа. В официальном заявлении Telegram также сказано, что никто не сможет удалённо управлять компьютером, если сам пользователь не запустил предварительно вредоносную программу…» ***(Вячеслав Ларионов. В Telegram обнаружили уязвимость, позволяющую хакерам майнить криптовалюту // Hi-News.ru (https://hi-news.ru/technology/v-telegram-obnaruzhili-uyazvimost-pozvolyayushhuyu-xakeram-majnit-kriptovalyutu.html). 14.02.2018).***

***

«…Экономика США только в 2016 году потеряла до $109 млрд из-за кибератак организованных хакерских групп, которые поддерживаются, в частности, правительствами РФ, Китая, КНДР и Ирана. Об этом сообщает Белый дом со ссылкой на отчет Совета экономических консультантов (СЕА)…

Отмечается, что кибератаки, направленные против частных и государственных организаций, происходили в виде атак с отказом в обслуживании, уничтожения данных и имущества, срыва бизнес-сделок (иногда с целью потребовать выкуп) и хищения запатентованных данных, интеллектуальной собственности и конфиденциальной финансовой и стратегической информации…

Эксперты уточняют, что действия хакеров, как правило, мотивированы политическими, экономическими, техническими или военными программами, они имеют конкретно определенные цели, которые могут изменяться в разное время…» ***(США оценили ущерб от кибератак за 2016 год в $100 млрд – отчет // Информационное агентство ЛІГАБізнесІнформ (http://news.liga.net/news/world/14900613-ssha_otsenili_ushcherb_ot_kiberatak_za_2016_god_v_100_mlrd_otchet.htm). 17.02.2018).***

***

«…Колишній директор ЦРУ Джеймс Клаппер наголошував, що понад 30 країн зараз використовує агресивні кіберможливості. Деякі з них покладаються на хакерів, які не працюють на уряд…

Про це на сторінках Washington Post пише співдиректор ініціативи з кібер-політики в Carnegie Endowment for International Peace Тім Мауер.

Він пригадує, як в листопаді 22-річний канадський хакер був засуджений за співпрацю з двома офіцерами ФСБ Росії. За рік до того Німеччина передала США

члена "Сирійської електронної армії"… Ці та інші випадки дають нову інформацію про відносини між хакерами і державами.

Політики і вчені намагаються відстежувати, як кібербезпека змінюється на місцях. Тривожні дебати про початок кібервійни охопили багатьох важливих політиків, а громадськість зацікавилася своєю кібербезпекою. Але в цьому процесі увага зосереджена лише на віртуальних атаках з боку інших країн. Роль окремих хакерів, які не мають очевидних прямих зв'язків з урядами, не враховуються…

…Одна з найбільших проблем у кібербезпеці - це можливість виявити того, хто атакує. Це називають "проблемою компетенції". Втім, в останні роки визначити, хто веде певну активість онлайн, стало легше. …уряд США тепер краще розуміє, як йому виявити винуватців…

Звісно, частково виявляти кіберзлочинців стало легше тому, що вони допускають помилки. Більше того, вони можуть собі це дозволити до тих пір, поки американські спецслужби далеко і не можуть їх арештувати.

Арешт хакерів-посередників допомагає краще зрозуміти мислення держав-замовників стосовно кіберзагроз і способів проектувати владу через мережу… Масштабні інциденти останніх п'яти років доводять цей світогляд…» ***(Ворожі держави ховаються за "незалежними" хакерами - Washington Post // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/vorozhi-derzhavi-hovayutsya-za-nezalezhnimi-hakerami-washington-post-268045_.html). 02.02.2018).***

***

«О взломе "неприступной" защиты Windows 10 UWP заявила группа киберпреступников CODEX…

Известно, что до настоящего момента универсальная платформа Windows UWP являлась наиболее защищенной из всех продуктов корпорации.

Тем не менее, хакерам удалось проникнуть в реализуемую на базе UWP игру Zoo Tycoon Ultimate Animal Collection. В итоге они смогли обойти все пять алгоритмов защиты (DRM или digital restrictions management).

Если верить киберпреступникам, то также подверглись взлому такие структуры, как Arxan, MSStore, UWP, XBLive и EAppX.

По мнению специалистов кибербезопасности, Microsoft должна в скором времени обновить защиту платформы…» ***(Хакеры взломали все пять уровней защиты Windows 10 // ГолосUA (https://golos.ua/i/596845). 17.02.2018).***

***

«Как сообщает FireEye Inc., северокорейская кибер-шпионская организация Reaper становится глобальной угрозой…

Организация, известная также как APT37, в 2017 году проводила кибератаки в Японии, Вьетнаме и на Ближнем Востоке… Хакерская группировка, отслеженная по IP-адресу в Северной Корее, теперь атакует целый ряд отраслей, от электроники и аэрокосмической промышленности до автомобильной и медицинской сферы.

Reaper вошла в список хакерских организаций, связанных с режимом Ким Чен Ына…

Reaper работает с 2012 года, отправляя жертвам электронные письма с вредоносным ПО, чтобы украсть конфиденциальную информацию. Среди главных целей группировки - ближневосточная телекоммуникационная компания, ведущая бизнес в Северной Корее; японская организация, связанная с ООН; и генеральный директор вьетнамской торговой компании…» ***(Ирина Фоменко. Северокорейская хакерская организация Reaper становится глобальной угрозой // InternetUA (http://internetua.com/severokoreiskaya-hakerskaya-organizaciya-reaper-stanovitsya-globalnoi-ugrozoi). 21.02.2018).***

***

«Хакерська група APT28, яку зазвичай пов'язують з Росією, атакувала сервери МЗС і Міноборони Німеччини…

Хакерська група APT28 змогла встановити на урядових комп'ютерах шкідливе програмне забезпечення і викрасти дані.

Німецькі спеціалісти з комп'ютерної безпеки виявили слід атаки у грудні, а сама вона могла тривати цілий рік.

…шкідливе програмне забезпечення вразило також мережу, якою користуються відомство федерального канцлера, міністерства, Федеральний суд аудиту та служби безпеки у Берліні, Бонні та інших містах…» ***(Пов'язані з РФ хакери атакували сервери МЗС і Міноборони Німеччини – ЗМІ // Європейська правда (http://www.eurointegration.com.ua/news/2018/02/28/7078203/). 28.02.2018).***

***

«…Розвідка США підозрює Росію в кібератаках на електронні системи, які обслуговували Олімпійські ігри в Пхьончхані…

…російські хакери намагалися діяти так, щоб склалося враження, ніби кібератаку влаштувала Північна Корея. …російська військова розвідка до початку лютого через зламані маршрутизатори мала доступ до трьох сотень комп'ютерів, пов'язаних з Іграми.

Крім того, спецслужби США припускають, що російські хакери намагалися зірвати церемонію закриття Олімпійських ігор у Пхьончхані.

…9 лютого, на церемонії відкриття Ігор глядачі і журналісти зіткнулися із серйозними перебоями у роботі Інтернету та зв'язку на стадіоні…

За словами організаторів Олімпіади, відбувалася серйозна кібератака на теле- та інтернет-ресурси змагань. Але вдалося швидко усунути наслідки цієї кібератаки. У МОК відмовилися розкривати інформацію про те, хто організував цю кібератаку» ***(Російські хакери здійснили кібератаку на Олімпіаду, прикинувшись КНДР — The Washington Post // Ракурс (http://racurs.ua/ua/n101520-rosiyski-hakery-zdiysnyly-kiberataku-na-olimpiadu-prykynuvshys-kndr-the-washington-post). 25.02.2018).***

***

«…хакер осуществил взлом серверов компании Retina-X Studios, занимающейся разработкой шпионских программ, и удалил оттуда все данные. По словам взломщика, он действовал из идеологических соображений.

Американская компания Retina-X Studios разрабатывает и продает шпионские программы родителям и работодателям, но часто эти инструменты применяются для того, чтобы следить за людьми без их согласия…

…хакер заявил, что он удалил с серверов Retina-X около 1 терабайта информации.

Сам взломщик сказал, что его беспокоит то, что шпионские программы нарушают конфиденциальность пользователей, прежде всего, молодежи.

Как утверждают представители компании, они знают об инциденте и сейчас сотрудники пытаются усилить безопасность Retina-X» ***(Разработчик шпионских программ потерял всю информацию на своих серверах // SecureNews (https://securenews.ru/retina-x/). 21.02.2018).***

***

«Китайская кибергруппировка получила 3400000 долларов посредством взлома серверов Jenkins и установки на них майнера JenkinsMiner, добывающего криптовалюту Monero.

Серверы автоматизации Jenkins имеют открытый исходный код и поддерживаются американской компанией CloudBees и сообществом Jenkins. Всего в мире сейчас существует около 133000 активных установок Jenkins и свыше миллиона пользователей.

По словам экспертов из Check Point, хакеры в ходе атак пользуются уязвимостью, которая связана с реализацией Java-десериализации в серверах Jenkins. Причиной возникновения проблемы является недостаточная проверка сериализованного объекта, что дает киберпреступникам возможность для загрузки и установки майнера JenkinsMiner на сервер Jenkins.

…В большинстве своем загрузки JenkinsMiner производились с китайских IP-адресов, которые принадлежат правительственному информационному центру в городском округе Хуайань. Неизвестно, были ли серверы взломаны или же они применяются хакерами, работающими на правительство КНР» ***(С помощью майнера для серверов Jenkins хакеры получили 3400000 долларов // SecureNews (https://securenews.ru/jenkins/). 19.02.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«Експерти з кібербезпеки виявили новий шкідливий ботнет, який… атакує пристрої на базі операційної системи Android…

Ботнет є комп'ютерною мережею, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням.

Нова шкідлива програма націлена на пошук відкритих портів налагодження, в тому числі на порт 5555, який використовується важливим компонентом системи Android і надає доступ до ключових функцій. Проникаючи в пристрій, ботнет змушує його добувати криптовалюту Monero.

Дослідники безпеки з підрозділу організації QiHo 360 Network Security Research Lab (Netlab), що виявили ботнет, назвали його ADB.miner. За їх словами, небезпека від шкідливої програми загрожує всім пристроям Android, таким як смартфони, смарт-телевізори і телевізійні приставки.

..наразі ботнет заразив орієнтовно 7 400 девайсів. Більшість з них знаходяться в Китаї і Південній Кореї – близько 40% і 30% відповідно» ***(Саша Картер. Пристрої на Android атакує новий ботнет, який майнить крипто валюту // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1713635-pristroyi-na-android-atakuye-noviy-botnet-yakiy-maynit-kriptovalyutu). 06.02.2018).***

***

«Самообучающиеся кластеры, собранные из скомпрометированных устройств, могут стать одной из ключевых проблем в сфере компьютерной безопасности уже в ближайшем будущем.

Роевые системы — искусственные нейросети, элементы которых взаимодействуют по принципу «равный — равному», не только применяются для анализа больших объемов данных, но и могут быть приняты на вооружение киберпреступниками.

…ботнеты разовьются в роевые системы, которые смогут находить уязвимости без участия человека. Сеть скомпрометированных устройств самостоятельно определит наиболее перспективные направления атаки так, чтобы использовать вычислительные мощности новых жертв для экспоненциального роста популяции «улья».

Подобные нейросети получили название Hivenet. Они не требуют внешнего управляющего воздействия и способны самообучаться в процессе деятельности. Со временем кластер пораженных устройств сможет не только находить известные уязвимости, но и применять свои ресурсы для поиска новых.

Борьба с атаками ботнетов, которые используют роевой интеллект, потребует значительных ресурсов, поскольку даже небольшое количество скомпрометированных устройств способно со временем вырасти в глобальную киберугрозу…» ***(Julia Glazova. Ботнеты нового поколения смогут сами находить уязвимости // Threatpost (https://threatpost.ru/hivenet-can-become-skynet/24713/). 20.02.2018).***

**

«Бельгийской полиции удалось захватить командный сервер Cryakl и с помощью «Лаборатории Касперского» получить ключи для расшифровки файлов, полоненных этим вымогательским ПО…

По свидетельству «Лаборатории», шифровальщик Cryakl активно используется с 2014 года; большинство его жертв проживают в России. Данный зловред распространяется через спам-рассылки и примечателен тем, что шифрует не только документы «офисных» форматов, но также архивы, образы дисков и файлы популярных программ резервного копирования…

Проект No More Ransom был запущен в июле 2016 года; за время своего существования он помог около 1,6 млн жертв заражения из 180 стран. В этом проекте принимают участие более 120 организаций: агентства Евросоюза, IT- и ИБ-компании, правоохранительные органы разных стран — в том числе недавно присоединившаяся федеральная полиция Бельгии. Сайт nomoreransom.org ныне доступен на 29 языках и предлагает в свободное пользование 52 утилиты для восстановления файлов, зашифрованных представителями 84 вредоносных семейств» ***(Maxim Zaitsev. Cryakl обезоружен // Threatpost (https://threatpost.ru/cryakl-ransomware-disarmed/24578/). 13.02.2018).***

***

«…с 23 по 27 февраля 2018 года по всей Европе прокатилась волна высокоскоростных DDoS-атак, с использованием техники амплификации на основе memcache (программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе хеш-таблицы). Особенностью данной техники является отправка множества поддельных UDP-пакетов в единицу времени от широкого диапазона IP-адресов.

По словам исследователей безопасности из компании Qrator Labs, уязвимости в memcache существуют по меньшей мере с 2014 года…

«…Все чаще мы фиксируем появление новых «брешей» в инфраструктуре интернета, которыми с успехом пользуются злоумышленники для реализации нападений. Атаки с использованием memcache, скорость которых достигала нескольких сотен Гб/с, стали тому подтверждением. Уязвимых memcache ресурсов в интернете огромное количество, и мы настоятельно рекомендуем техническим специалистам производить корректную настройку memcache, не забывая об установках по умолчанию. Это поможет избежать прослушивания всего UDP-трафика, отправляемого на сервер, и снизить вероятность проведения DDoS-атак», - отметил генеральный директор Qrator Labs Александр Лямин» ***(Крупнейшие web-ресурсы России и Европы подверглись высокоскоростным DDoS-атакам // SecurityLabRu (https://www.securitylab.ru/news/491762.php). 27.02.2018).***

***

«Програмне забезпечення шифрує файли на комп'ютерах жертв, вимагаючи викуп у вигляді криптовалюти…

Новий вірус-вимагач масового ураження має назву Data Keeper. Експерти відзначають, що вірус не змінює розширення в документах, тому користувачі не знають, які саме з них заражені.

Крім того, Data Keeper може обчислити і зашифрувати всі загальні мережі, до яких отримав доступ через комп'ютер жертви.

З початку 2018 року ця вже третя масова кібератака…» ***(У мережі виявили новий вірус-вимагач // Ваш магазин (https://news.vash.ua/news/nauka-ta-it/u-merezhi-vyyavyly-novyy-virusvymagach-56331). 27.02.2018).***

***

«Европол обнародовал данные об успешной операции по борьбе с шпионским трояном Luminosity Link, прошедшей в сентябре 2017 года. Расследование провело Юго-Западное региональное управление по борьбе с организованной преступностью под руководством Национального агентства по борьбе с преступностью Великобритании.

Правоохранительным организациям удалось остановить распространение RAT-трояна…

Зловред Luminous Link распространялся через веб-сайт, и купить его мог любой желающий всего за 40 €. Помимо доступной цены троян отличался еще и простотой в использовании…

После установки троян обеспечивал злоумышленнику доступ ко всем файлам жертвы, позволял отслеживать ввод данных с клавиатуры и незаметно активировать веб-камеру. По данным полиции, от зловреда пострадали тысячи пользователей, у которых похитили конфиденциальные данные, пароли, фотографии, видеозаписи и прочую информацию. Всего, по оценкам сотрудников правоохранительных органов, Luminosity Link успели приобрести более 8600 человек из 78 стран мира…» ***(Egor Nashilov. Европол остановил распространение трояна Luminosity Link // Threatpost (https://threatpost.ru/europol-against-rat-trojan-luminosity-link/24464/). 06.02.2018).***

***

«Российский хакер Константин Козловский, которого обвиняют во взломе систем российских банков, заявил, что разработал программу LDCS, которая повлияла на выдачу результатов в день голосования на президентских выборах в США. Об этом сообщает корреспондент Дождя из зала Мосгорсуда, где проходит заседание по продлению меры пресечения Козловскому…

…Он уточнил, что «выполнял разные задания под руководством сотрудников ФСБ», в том числе взлом серверов Демпартии, переписки кандидата в президенты США Хиллари Клинтон, а также атаки на другие «очень серьезные военные предприятия США и прочие организации». Поручение взлома серверы партии, по его словам, он получил от сотрудника ФСБ по имени Илья. Позднее хакер заявил, что Илья — это майор ФСБ Дмитрий Докучаев.

Сам бывший сотрудник ЦИБ ФСБ Докучаев, обвиняемый в госизмене, заявил, что не знаком с Козловским…

Козловский также рассказывал, что создание вирусов WannaCry и Lurk курировали сотрудники ФСБ…» ***(Хакер Козловский рассказал о влиянии на выдачу результатов выборов в США // До///дь (https://tvrain.ru/news/haker_kozlovskij-457484/?utm_term=457484&utm_source=facebook&utm_medium=social&utm_campaign=instant&utm_content=tvrain-main#0_5__12419_982_0). 13.02.2018)***

***

«Работники Центрального следственного бюро Польши, которые отвечают за борьбу с киберпреступностью, при сотрудничестве с ФБР задержали 44-летнего гражданина Украины. Его подозревают в распространении вредоносных программ…

«Мужчину подозревают в участии в организованной преступной группе, которая занимается распространением вредоносных программ и хакерскими атаками. Злонамеренные программы отслеживали, а затем фильтровали данные кредитных карт. Ущерб, нанесенный деятельностью преступной группы, достигают нескольких сотен миллионов долларов», - сообщили в Центральном следственном бюро Польши.

Теперь хакеру грозит до 30 лет лишения свободы.

Сейчас он находится под арестом в ожидании решения об экстрадиции в Соединенные Штаты Америки» ***(Задержали украинского хакера, которому грозит 30 лет тюрьмы в США // Gazeta.ua (https://gazeta.ua/ru/articles/world-life/_zaderzhali-ukrainskogo-hakera-kotoromu-grozit-30-let-tyurmy-v-ssa/822638). 24.02.2018).***

***

Технічні аспекти кібербезпеки

«Инженерный совет Интернета (Internet Engineering Task Force, IETF) предлагает ввести стандарт всеобщего шифрования электронных писем, который позволит отказаться от использования простого текстового формата (cleartext)…

Созданный в 1986 году совет объединяет интернет-проектировщиков, сетевых операторов и провайдеров, которые работают над развитием протоколов и архитектуры Сети. Рабочий вариант нового стандарта подготовили специалисты компаний Windrock и Oracle Кит Мур (Keith Moore) и Крис Ньюман (Chris Newman).

В документе они пояснили, что хотя IMAP, POP и SMTP уже поддерживают защищенный TLS-протокол, в некоторых ситуациях безопасность конечного пользователя остается под угрозой…

Эксперты утверждают, что все коммуникации нужно вести через TLS с использованием выделенного порта. Документ определяет этот подход как «повсеместный TLS» (implicit TLS).

Авторы документа призывают провайдеров электронной почты «как можно скорее» отказаться от небезопасных протоколов, а разработчиков Outlook, Mac Mail, Thunderbird и прочих клиентов — внести соответствующие изменения в свои продукты…» ***(Egor Nashilov. Эксперты IETF призвали устранить бреши электронной почты // Threatpost (https://threatpost.ru/ietf-calls-for-secure-emailing/24412/_). 02.02.2018).***

***

«По заявлению Panasonic и Trend Micro, компании планируют совместно разработать систему защиты автопилотов и подключаемых к интернету автомобилей от кибератак…

Новое совместное решение объединит компоненты, устанавливаемые в автомобиле, и облачные системы. Разработанная компанией Panasonic технология Control Area Network (CAN) будет использоваться для обнаружения и предотвращения несанкционированного доступа… В то же время, решения Trend Micro для безопасности IoT будут использоваться в IVI устройствах, в т.ч., навигационных системах, для обнаружения атак из Интернета. Непрерывный мониторинг автомобильных систем будет вестись из облака. Данные о любых попытках взлома будут поступать в облачную платформу для анализа и последующей выработки мер по защите транспортных средств.

Сообщается, что Panasonic и Trend Micro планируют доработать и коммерциализировать продукт после 2020 года» ***(Panasonic и Trend Micro защитят автопилоты и подключаемые автомобили от кібератак // «Компьютерное Обозрение» (http://ko.com.ua/panasonic_i_trend_micro_zashhityat_avtopiloty_i_podklyuchaemye_avtomobili_ot_kiberatak_123573). 20.02.2018).***

***

«ИБ-эксперты из Kromtech Security Center сообщили, что отсканированные копии паспортов, водительских удостоверений и других документов, принадлежащие 119000 клиентов службы доставки FedEx, попали в открытый доступ из-за неправильно настроенного сервера Amazon S3.

Отсканированные копии документов принадлежали клиентам из Австралии, Канады, Китая, Мексики, Саудовской Аравии, США и Японии, а также ряда стран Европы…

Как сообщают исследователи, владельцем сервера является компания Bongo International LLC, которая предоставляла услуги в области логистики и расчетов при обмене валют. В 2014 году Bongo была куплена FedEx, а затем переименована в FedEx Cross-Border International. Сервис прекратил работу в апреле прошлого года.

Представители FedEx заявили, что архивные данные аккаунтов Bongo International, хранящиеся на сервере стороннего облачного провайдера, находятся в безопасности. Они подчеркнули, что ничто не указывает на кражу информации злоумышленниками…» ***(В открытом доступе обнаружена информация 119000 клиентов FedEx // SecureNews (https://securenews.ru/fedex/). 16.02.2018).***

***

«…Национальный институт стандартов и технологий США (NIST) опубликовал проект документа под названием «Статус международной стандартизации кибербезопасности Интернета вещей» («The Status of International Cybersecurity Standardization for IoT»)...

NIST предлагает разделить IoT на пять функциональных областей: подключенные устройства; IoT потребительского класса; медицинское оборудование и устройства, используемые в сфере здравоохранения; «умные» здания; «умное» производство (в том числе, АСУ ТП). Для каждой области должны быть разработаны свои стандарты с учетом их особенностей.

Между стандартами кибербезопасности для каждой из вышеперечисленных областей и общепринятыми в настоящее время стандартами есть свои различия. Если традиционно приоритетами в обеспечении кибербезопасности считаются конфиденциальность, целостность и доступность (в нисходящем порядке), то главным приоритетом в обеспечении безопасности IoT является доступность. Исключение – область IoT потребительского класса, где основным приоритетом по-прежнему остается защита конфиденциальности и приватности…

Главное различие между традиционной кибербезопасностью и кибербезопасностью IoT заключается в том, что последняя ближе к операционным технологиям (OT), чем к информационным технологиям (IT)» ***(NIST разрабатывает стандарты безопасности для IoT // SecurityLabRu (https://www.securitylab.ru/news/491651.php). 20.02.2018).***

***

«…Основатель портала Techgage, публикующего обзоры и отзывы о технологических продуктах, блогер Роб Уильямс (Rob Williams) обнаружил в криптовалютном кошельке Jaxx проблемы с безопасностью. По словам Уильямса, Jaxx обеспечивает такой же уровень безопасности, как и большинство остальных offline-кошельков. Тем не менее, это касается только мобильных пользователей, позаботившихся о безопасности своих телефонов. Для пользователей Windows, Linux и Mac дела обстоят немного по-другому…

Подобно большинству приложений Jaxx хранит профиль пользователя в папке %APPDATA%, находящейся в скрытой по умолчанию папке пользователя. Созданная после инсталляции кошелька папка jaxx является весьма эффективным кэшем всей информации, необходимой для доступа к учетной записи. Ее содержимое само по себе не представляет интереса для злоумышленников, поскольку только прочтение файлов ничего не дает. Однако если взять содержимое папки и перенести его в такую же папку на другом компьютере, повторная аутентификация не потребуется…» ***(В криптокошельке Jaxx обнаружены проблемы с безопасностью // SecurityLabRu (https://www.securitylab.ru/news/491644.php). 20.02.2018).***

***

«Разработчики Flight Simulator Add-On встроили вредоносное программное обеспечение в игру, чтобы бороться с пиратством.

Если пользователь пытается установить неофициальную версию игры, вирус ворует его данные из кэша браузера Chrome и отправляет их на сервера FSLabs…

По замыслу разработчиков, это должно помочь в борьбе с распространением нелицензионных версий игры.

Основатель компании Fidus Information Security, занимающейся кибербезопасностью, сообщил, что этот способ борьбы с пиратством является одним из самых экстремальных…» ***(Разработчики компьютерной игры встроили в нее вирус // Gazeta.ua (https://gazeta.ua/ru/articles/science/_razrabotchiki-kompyuternoj-igry-vstroili-v-nee-virus/822011). 21.02.2018).***

***

«Развитие технологий искусственного интеллекта может привести к появлению новых форм киберпреступности, политических беспорядков и даже физического насилия в течение пяти лет, предупредила группа из 26 экспертов со всего мира…

В новом докладе эксперты в области науки, промышленности, а также представители благотворительных организаций описывают ИИ как "технологию двойного назначения" для военного и гражданского использования, сродни ядерной энергии, взрывчаткам и хакерским ПО…

Аналитики утверждают, что исследователи должны учитывать возможное злоупотребление ИИ в ходе своих исследований и работать над созданием надлежащих нормативных рамок для предотвращения вредоносного использования ИИ.

Если не соблюсти рекомендации, преступники могут воспользоваться ИИ в своих целях. Например, ИИ может автоматизировать обнаружение критических ошибок программного обеспечения или выбирать потенциальных жертв для финансовых преступлений. Кроме того, ИИ способен проводить атаки, используя методы социальной инженерии…

По мнению экспертов, защита, основанная на использовании искусственного интеллекта, не является панацеей, особенно, когда мы выходим за пределы цифрового мира. "Необходимо проделать большую работу по установлению правильного баланса в развитии ИИ и разработке улучшенных технических мер для проверки надежности систем. Кроме того, нужно удостовериться, что политическая структура адаптирована к новому миру, который мы создаем", - утверждают аналитики в докладе» ***(Ирина Фоменко. Развитие искусственного интеллекта может повысить уровень киберпреступности // InternetUA (http://internetua.com/razvitie-iskusstvennogo-intellekta-mojet-povsit-uroven-kiberprestupnosti). 22.02.2018).***

***

«Компания ARCHOS, европейский производитель мобильных устройств и «умных» гаджетов, представила на Всемирном мобильном конгрессе - 2018 кошелек для держателей криптовалют, который позволит защититься от хакерских атак. Archos Safe-T mini поступит в продажу в июне 2018 года по цене от €49,99…

ARCHOS Safe-T mini — это первая разработка R&D-команды ARCHOS, использовавшей для создания устройства собственную экспертизу в области холодного хранения данных. Производство ARCHOS Safe-T mini будет расположено во Франции.

Основные функции ARCHOS Safe-T mini в области кибербезопасности: генерирует и хранит секретный ключ в офлайн-режиме и не позволяет хакерам получить доступ к нему во время работы онлайн; выполняет все криптовалютные операции офлайн; экран устройства позволяет проверить детали транзакций перед их подтверждением (хакеры не смогут изменить детали операции без уведомления об этом владельца); обязывает программное обеспечение устанавливать PIN-код, поэтому получить доступ к устройству сможет только его владелец…» ***(На всемирном конгрессе в Барселоне представлено устройство для хранения криптокошельков с защитой от хакеров // TRISTAR.com.ua (http://tristar.com.ua/1/news/na_vsemirnom_kongresse_v_barselone_predstavleno_ustroistvo_dlia_hraneniia_kriptokoshelkov_s_zashitoi_ot_hakerov_9192.html). 27.02.2018).***

***

«Молодая израильская компания CyberX, которая специализируется на кибербезопасности в области "Интернета вещей", собрала еще 18 миллионов долларов во втором раунде финансирования, который состоялся сегодня, увеличив общую сумму инвестиций до 30 миллионов долларов.

Сегодняшний раунд возглавила компания Norwest Venture Partners. Вместе с ней, в торгах приняли участие текущие инвесторы Glilot Capital Partners, Flint Capital, Venture Capital и OurCrowd…» ***(CyberX: Специалист по кибер-безопасности собрал $30 млн. инвестиций // ISRAland (http://www.isra.com/news/212019). 27.02.2018).***

***

«…Несмотря на регулярные обновления в системе безопасности iPhone, полицейские теперь имеют доступ к любым телефонам благодаря «белым хакерам» израильской компании Cellebrite.

Эксперты по кибербезопасности компании Cellebrite сообщили, что им удалось обойти все защиты смартфона американской компании Apple — iPhone X.

Ккрупный подрядчик государственных американских компаний заявляет, что он нашел способ разблокировать практически любой iPhone. По всей видимости, это может стать важным достижением для правоохранительных органов и очевидной проблемой конфиденциальности для клиентов Apple.

В Cellebrite сообщили, что ее инженерам удалось найти способ обхода блокировок смартфонов, которые работают на базе программного обеспечения iOS 11, в том числе — iPhone X.

Именно эта модель гаджета и была успешно взломана экспертами кибербезопасности для получения необходимых данных Агентством Национальной Безопасности США еще в ноябре прошлого 2017 года…» ***(Хакерам удалось взломать все системы защиты iPhone // PaySpaceMagazine «доступно о платежах» (https://psm7.com/news/xakeram-udalos-vzlomat-vse-sistemy-zashhity-iphone.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 28.02.2018).***

***

«Уязвимость EternalBlue уже известна специалистам по кибербезопасности. Считается, что над ней работало Агентство национальной безопасности США, а ещё с её помощью компьютеры заражал шифровальщик WannaCry. Теперь, согласно отчёту компании Proofpoint, эксплойт EternalBlue (CVE-2017-0144) используется ботнетом Smominru для добычи криптовалюты Monero.

Согласно информации, предоставленной Proofpoint, Smominru орудует из-под операционных систем семейства Windows, и на данный момент он уже заразил более полумиллиона компьютеров по всему миру. Как правило, заражаются те ПК, где не установлены все необходимые обновления системы. Большинство заражённых компьютеров находится на территории России, Индии и Тайваня.

Хакеры задействовали по меньшей мере 25 машин для сканирования Интернета и поиска уязвимых компьютеров. Суммарных ресурсов всех заражённых ПК хватает, чтобы ежедневно зарабатывать для злоумышленников около 8500 долларов. На момент обнаружения мошенники смогли добыть более 9000 монет, что составляет более 3,6 миллиона долларов…» ***(Вячеслав Ларионов. Эксплойт АНБ помог вирусу-майнеру заработать более 3 миллионов долларов // Hi-News.ru (https://hi-news.ru/technology/eksplojt-anb-pomog-virusu-majneru-zarabotat-bolee-3-millionov-dollarov.html). 02.02.2018).***

***

«Эксперт по кибербезопасности Стивен Кантак обнаружил серьезную уязвимость в Skype, с помощью которой злоумышленник может как украсть данные с компьютера, так и полностью захватить над ним управление…

…Как говорит Кантак, взломщик может просто загрузить вредоносный DLL во временную директорию, а затем назвать его именем реально существующий файл вроде UXTheme.dll. А дальше все ограничивается лишь фантазией и нуждами хакера.

…по словам Кантака эту же уязвимость можно использовать не только на Win, но и на macOS и Linux. …эксперт уведомил Microsoft о проблеме еще в сентябре 2017 года. Из Microsoft ответили, что они видят баг, но не могут залатать его т. к. для этого придется чуть ли не писать код с нуля. Поэтому уязвимость устранили в новом клиенте восьмой версии Skype…» ***(Евгений Щербань. В Skype нашлась критическая уязвимость. Microsoft знает о ней уже 6 месяцев // gagadget.com (http://gagadget.com/announce/32774-vskype-nashlas-kriticheskaya-uyazvimost-microsoft-znaet-onej-uzhe-6mesyatsev/). 16.02.2018).***

***

«Cisco подтвердила попытки киберпреступников эксплуатировать критическую уязвимость в сетевом экране Cisco Adaptive Security Appliance (ASA)…

Брешь удостоилась наивысшей, 10-балльной оценки по системе CVSS. Ее первооткрывателем стал Цедрик Халбронн (Cedric Halbronn), исследователь из NCC Group.

В список пострадавших аппаратов входят:

- устройства промышленной безопасности Cisco ISA серии 3000;
- межсетевые экраны ASA серий 5500 и 5500-X;
- адаптивное виртуальное устройство безопасности Cisco ASAv;
- ряд устройств Firepower и программная защита Firepower Threat Defense.

В случае успешно проведенной атаки злоумышленник сможет перехватывать любой идущий через систему трафик, получив при этом административные привилегии и удаленный доступ к сети, сообщают эксперты из NCC. Однако «попытки воспользоваться брешью без подходящего эксплойта приведут к аварийному завершению работы сетевого экрана и могут оборвать сетевое подключение».

…брешь оставалась в тени целых семь лет…» (***Christopher Kanaracus. Cisco подтвердила атаки через уязвимость в сетевом экране // Threatpost (https://threatpost.ru/cisco-confirms-critical-firewall-software-bug-is-under-attack/24638/). 15.02.2018).***

***

«…Эксперты Positive Technologies Вячеслав Москвин и Антон Вайчикаускас выявили уязвимости в Ipswitch WhatsUp Gold. Это программное обеспечение предназначено для автоматического обнаружения сетевых ресурсов и их взаимосвязи, отслеживания состояния и доступности сети, а также для управления конфигурациями.

«Использование уязвимой версии WhatsUp Gold в промышленном предприятии может привести к киберинцидентам, в том числе к нарушению производственного процесса», — говорит руководитель отдела безопасности промышленных систем управления Positive Technologies Владимир Назаров…

Первая уязвимость (CVE-2018-5777) в Ipswitch WhatsUp Gold позволяет удаленному атакующему воспользоваться неправильной конфигурацией TFTP-сервера и выполнить произвольные команды в операционной системе самого сервера. Злоумышленник может получить доступ ко всей информации на сервере…

Вторая уязвимость (CVE-2018-5778) связана с недостаточной фильтрацией пользовательского ввода на некоторых веб-страницах WhatsUp Gold и возможностью выполнить SQL-инъекцию. …В результате атакующий может получить доступ к учетным данным для управления сетевым оборудованием, хранящимся в базе данных уязвимой системы.

Для устранения обнаруженных уязвимостей необходимо обновить WhatsUp Gold до версии не ниже WhatsUp Gold 2017 Plus Service Pack 2 (v.17.1.2)» ***(Positive Technologies обнаружила уязвимости в популярной программе управления***

сетью // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/290286/). 16.02.2018).

***

«Существенную дыру в безопасности системы для управления автозаправочными станциями обнаружили израильские специалисты по кибербезопасности. Идо Наор (Ido Naor) и Амихай Нейдерман (Amihai Neiderman) проанализировали исходный код программного обеспечения SiteOmat и нашли в нем несколько серьезных уязвимостей.

SiteOmat является частью пакета ForeSite израильской компании Orpak, который предназначен для контроля работы АЗС… Кроме того, SiteOmat входит в состав программного продукта ForeHB — комплексного решения для контроля за парком транспортных средств. При помощи веб-интерфейса пользователи программы SiteOmat могут удаленно подключаться к выбранной АЗС по локальной сети или через Интернет, чтобы контролировать настройки и оперативно управлять работой каждой колонки.

…При анализе выяснилось, что программа содержит бэкдор, позволяющий войти в систему с правами администратора, минуя стандартную процедуру авторизации (учетные данные для входа были жестко закодированы). Более того, для ряда процедур — например, изменения цены на топливо — не требовались права администратора. Исследователи смогли на практике получить доступ к одной АЗС, чей владелец согласился принять участие в эксперименте…

Среди возможных последствий, кроме уже упомянутого изменения цены, — полное отключение бензоколонки, перенаправление платежей, кража данных банковских карт клиентов и даже доступ к другим ИТ-системам в одной среде со скомпрометированной, например контроль за камерами видеонаблюдения.

В сентябре прошлого года Наор и Нейдерман сообщили Orpak о найденных уязвимостях, однако до сих пор не ясно, исправлены ли эти ошибки в актуальных версиях SiteOmat. Система эксплуатируется на 35 тысячах автозаправочных станций в 60 странах мира, а ПО для контроля за транспортными средствами установлено на 7 миллионах автомобилей…» ***(Anna Markovskaya. Тысячи АЗС по всему миру оказались уязвимыми // Threatpost (https://threatpost.ru/orpak-backdoor-allows-full-gas-station-control/24428/). 03.02.2018).***

***

«Две версии клиента uTorrent содержат уязвимость, которая дает хакеру возможность выполнять код на системе, получать доступ к загружаемым файлам и отслеживать историю загрузок.

Проблему обнаружил эксперт Google Project Zero Тэвис Орманди… Используя уязвимость, любой сайт, посещаемый пользователем, может захватить контроль над основными функциями клиента. Наибольшая угроза исходит от сайтов, которые могут задействовать уязвимость для того, чтобы загрузить вредоносный код в папку запуска Windows…

Нейтрализовать уязвимость пока нельзя, поэтому пользователи должны на время прекратить работу с uTorrent до того, как будут установки обновления» ***(С***

помощью уязвимости в uTorrent можно получить доступ к загружаемым файлам // SecureNews (https://securenews.ru/utorrent/). 21.02.2018).

***

«Google снова раскрыла уязвимости в ПО Microsoft до того, как компания выпустила патч. Microsoft изо всех сил пытается решить эту проблему.

Уязвимость влияет на динамическую компиляцию (JIT), используемую браузером Microsoft Edge при запуске JavaScript. JIT позволяет предугадать необходимый объем используемой памяти. Если злоумышленник знает об этом, он может поместить туда свой собственный код и забавляться тем, как Edge выполняет его команды странице.

Новость об уязвимости была опубликована в Project Zero 17 ноября 2017 года с обычным предупреждением о том, что подробности раскроют через 90-дней.

Позднее Google предоставил Microsoft дополнительные 14 дней.

Недавно появилось сообщение от Microsoft о том, что проблема оказалась более сложной, чем предполагалось ранее, и высока вероятность, что компания не сможет в срок выпустить патч…» ***(Google раскрыла уязвимости в ПО Microsoft до появления патча // SecureNews (https://securenews.ru/googlevsmicrosoft/). 20.02.2018).***

***

«Microsoft 13 февраля выпустила патчи для своей продукции, которые устраняют пятьдесят уязвимостей, в том числе четырнадцать критических.

В Outlook устранены две критические уязвимости. Первая ошибка позволяет дистанционно выполнять код. Используя его, хакер, прошедший авторизацию на атакуемой системе и имеющий права администратора, может полностью захватить контроль над системой…

Еще одна критическая уязвимость в Outlook также позволяет дистанционно выполнять код. Хакер может воспользоваться ею путем отправки специального электронного письма, которое заставит Outlook осуществить загрузку заранее сконфигурированного сообщения…» ***(Две критические уязвимости исправлены в Microsoft Outlook // ООО "Гротек" SecureNews (https://securenews.ru/outlook_3/). 14.02.2018).***

***

«…Согласно отчета компании Risk Based Security, в 2017 году число раскрытых уязвимостей увеличилось на 31,0% по сравнению с предыдущим годом… С web-сайтами связана половина (50,6%) уязвимостей, из которых 28,9% - проблемы межсайтового скриптинга (XSS).

В топ-десять поставщиков, в чьих продуктах были обнаружены уязвимости с оценкой от 9,0 до 10,0 по шкале CVSS, вошли Google (503 проблемы), SUSE (301), Canonical (285), Red Hat (274), SGP (257), Adobe (256), Mozilla (246), Samsung (228), Oracle (201) и Xerox (198)…

.

Хотя для большинства уязвимостей, обнаруженных в прошлом году (72,8%) были выпущены обновления или патчи в том или ином виде, 23,2% проблем в настоящее время остаются неисправленными.

В отчете также сказано, что лишь 1,7% от общего количества уязвимостей были обнаружены в продуктах SCADA, по сравнению с 2,8% в 2016 году…» ***(2017 год побил рекорд по числу обнаруженных уязвимостей // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=121548). 20.02.2018).***

***

«Специалисты компании в сфере кибербезопасности RedLock обнаружили, что производитель электромобилей Tesla стал жертвой хакеров, которые, пользуясь найденной уязвимостью в консоли Kubernetes от Google, получили доступ к облачной инфраструктуре компании в Amazon Web Services. Вычислительные мощности аккаунта в дальнейшем использовались для майнинга криптовалют…» ***(Облачные ресурсы Tesla использовали для майнинга крипто валют // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3557058?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). 21.02.2018).***

***

«Пользователь ресурса «Хабрахабр» под ником «dinikin» обнаружил уязвимость, которая позволяла получить список пассажиров рейсов Международных Авиалиний Украины — самого крупного авиаперевозчика страны…

Открыв в Google Chrome инструмент разработчика и изучив запросы к серверу, пользователь увидел, что данные о доступных местах сервером возвращаются. Также было замечено, что запрос, который возвращает список доступных мест, выполнялся во всех браузерах успешно, не смотря на то, что сессионные куки были доступны только в Google Chrome…

Таким образом, информация о пассажирах была доступна любому пользователю с любого устройства лишь по PNR коду…

Кроме этого, при похожем запросе для заказа места багажа, сайт МАУ сообщал ещё больше информации о пассажирах – к общей информации включалась ещё и дата рождения, при чем не об одном пассажире, а обо всех, включенных в данное бронирование (например, о семье)…

На странице оплаты, утверждается на «хабре», запрос также выполнялся во всех браузерах «без сессионных куков»…

После обращения пользователя в службу поддержки МАУ, на протяжении месяца все вышеуказанные уязвимости были устранены разработчиками» ***(Владимир Кондрашов. Крупнейшая авиакомпания Украины «делилась» списком пассажиров в сети – источник // InternetUA (http://internetua.com/krupneishaya-aviakompaniya-ukrain-delilas-spiskom-passajirov-v-seti-istocsnik). 27.02.2018).***

***

«…эксперт в области кибербезопасности Набил Ахмед обнаружил «смертельную» уязвимость в Windows, способную сломать любой компьютер.

Он утверждает, что с помощью бреши в системе защиты Windows можно вызнать Blue Screen of Death (BSOD), более известный как «синий экран смерти». С ее помощью любой компьютер можно вывести из строя, поскольку он перестанет включаться, так как операционная система отказывается запускаться.

Критическая уязвимость присутствует сразу в двух операционных системах – Windows 8.1 и серверной модификации Windows Server 2012 R2…

Вывести компьютер из строя эксперту удалось за счет уязвимости в протоколе SMBv3. Хуже всего то, что любой злоумышленник может дистанционно сломать операционную систему, в результате чего компьютер перестанет включаться…

Чтобы подтвердить свои слова Набил Ахмед выложил в сеть видеоролик с демонстрацией обнаруженной им уязвимости. Также он опубликовал специальный PoC-код, позволяющий любому желающему сломать компьютер на базе Windows. Восстановить его работоспособность можно будет только путем переустановки операционной системы, либо восстановлением из резервной копии» ***(Новая «смертельная» уязвимость в Windows позволяет сломать любой компьютер // Український телекомунікаційний портал (https://portaltele.com.ua/news/events/novaya-smertelnaya-uyazvimost-v-windows-pozvolyaet-slomat-lyuboj-kompyuter.html). 28.02.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…В начале января 2018 года группа специалистов в области компьютерной безопасности раскрыла данные о найденных ранее двух типах критических уязвимостей в современных процессорах — Meltdown и Spectre. Опасность уязвимостей заключается в том, что с их помощью вредоносная программа может читать содержимое кэша процессора, в том числе его областей, в которых хранятся данные других программ. Таким способом злоумышленник может украсть пароли или другую конфиденциальную информацию...

После раскрытия данных об уязвимостях большинство крупных производителей процессоров и программного обеспечения выпустили программные обновления, устраняющие уязвимости или сильно усложняющие их использование…

11 февраля группа исследователей из Принстонского университета и NVIDIA опубликовала статью с описанием новых вариантов использования обнаруженных в январе уязвимостей, которые они назвали MeltdownPrime and SpectrePrime. Интересно, что они нашли их …с помощью написанной ими программы…

С помощью этой программы исследователи обнаружили два новых варианта использования уязвимостей Meltdown и Spectre, основанные на атаке типа Prime+Probe…

Исследователи опубликовали код примера реализации атаки SpectrePrime в своей работе. Они отмечают, что, программная защита от таких атак не будет сильно отличаться от уже имеющихся обновлений для уязвимостей, обнаруженных в январе…» ***(Григорий Копиев. Обнаружены новые варианты уязвимостей Meltdown и Spectre // N+1 Интернет-издание (https://nplus1.ru/news/2018/02/15/spectreprime). 15.02.2018).***

***

«Компания Check Point Software Technologies представила линейку решений CloudGuard для защиты организаций от кибератак «Пятого поколения» на облачные приложения и инфраструктуру и запустила сервис CloudGuard SaaS, который обеспечивает защиту от атак на SaaS-приложения…

CloudGuard SaaS — это первый в отрасли пакет технологий для безопасности, разработанный для усовершенствованной защиты и предотвращения угроз в отношении SaaS-приложений. CloudGuard SaaS также предотвращает кражу пользовательских учетных записей и взлом приложений SaaS с помощью технологии ID-Guard, которая скоро будет запатентована.

Ключевые преимущества решения:

- Защита от угроз нулевого дня: Решение помогает обезопасить контент приложений SaaS от APT-атак и неизвестного вредоносного ПО «нулевого дня» с помощью технологий «песочницы», применяемых в режиме реального времени, а также технологий защиты от программ-вымогателей, ботов и постоянно обновляемой базы данных об угрозах в облаке.
- Технология защиты идентификации пользователей ID-Guard (в процессе получения патента): Решение обнаруживает и блокирует злоумышленников, которые пытаются получить доступ к учетным записям SaaS, а также отключает незарегистрированных пользователей и небезопасные устройства.
- Защита данных: Решение автоматически шифрует конфиденциальные данные, блокирует попытки несанкционированного обмена конфиденциальными файлами и помещает их в карантин.

CloudGuard IaaS (прежнее название vSEC) теперь является частью линейки CloudGuard. CloudGuard IaaS предлагает продвинутую защиту и предотвращение угроз «Пятого поколения» от атак на инфраструктуру и рабочие нагрузки всех ведущих публичных и частных облачных платформ…» ***(Облака под защитой // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5473963-Oblaka-pod-zashhitj.html#ixzz57v8wZx95). 09.02.2018).***

***

«Лаборатория Касперского» представила корпоративное решение нового поколения для моментального выявления угроз и реагирования на киберинциденты на конечных устройствах.

Продукт Kaspersky Endpoint Detection and Response (KEDR) непрерывно отслеживает любые аномалии и подозрительные процессы на рабочих местах сотрудников, представляет все собранные данные в удобном визуализированном виде, распознаёт угрозы и реагирует на инциденты. Таким образом, решение в значительной степени автоматизирует процесс поиска вредоносного ПО и вторжений в корпоративную сеть, сводя время ответной реакции на угрозу к минимуму. Компонент Kaspersky EDR тесно интегрирован с платформой для защиты от целевых атак Kaspersky Anti Targeted Attack Platform…

Kaspersky EDR позволит принципиально изменить ситуацию. В этом решении реализован гибкий и интеллектуальный подход к автоматическому распознаванию любых угроз (в том числе ещё неизвестных), а также своевременному и наиболее адекватному реагированию на них для предотвращения возможного ущерба и негативных последствий для организации. При этом всё управление осуществляется с помощью единого интерфейса…

Kaspersky EDR доступен как самостоятельный продукт, а также в составе комплексной платформы Kaspersky Threat Management and Defense, позволяющей компаниям получить полный визуальный контроль над всеми событиями в IT-инфраструктуре. Помимо Kaspersky EDR, эта платформа также включает в себя специализированное решение для борьбы с целевыми атаками — Kaspersky Anti Targeted Attack Platform — и аналитические сервисы, помогающие понимать особенности различных киберугроз…» ***(Выявить и блокировать киберугрозы можно моментально // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5476331-Vyyavit-i-blokirovat-kiberugrozy.html#ixzz57vKFwRwu). 21.02.2018).***

***

«…«Ростелеком» совместно с компанией NGENIX… представил новое облачное решение для защиты и ускорения веб-ресурсов…

Облачное решение позволяет корпоративным клиентам «Ростелекома» получить многоуровневую защиту веб-ресурсов от широкого спектра атак без раскрытия «чувствительных данных», таких как банковская тайна и персональные данные клиентов. В состав решения входит защита от DDoS-атак, эксплуатации уязвимостей веб-приложений и других противоправных действий киберпреступников (Web Application Firewall), ускорение сайта за счет использования сети доставки контента (CDN), а также защищенный распределенный сервис DNS. Облачное решение не требует подключения к определенному оператору связи, а также покупки оборудования и лицензий и содержания штата специалистов по информационной безопасности, что позволяет клиенту сфокусироваться на развитии своего бизнеса, а задачи по информационной безопасности передать на аутсорсинг…» ***(Облачное решение для защиты веб-ресурсов // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3559465?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). 27.02.2018).

***

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

Бистрова Б. В. Модернізація освітньої програми "Кібербезпека": реалії та перспективи / Б. В. Бистрова // Науковий вісник Мукачівського державного університету. Серія : Педагогіка та психологія. - 2017. - Вип. 2. - С. 22-24.

Представлено результати порівняльного аналізу освітніх програм вищих навчальних закладів США в галузі кібербезпеки. Висвітлено уявлення про реальний стан справ, отриманих зіставленням організації, технології, змісту і результатів навчання за схожими освітніми програмами при порівнянні підготовки бакалаврів з кібербезпеки в університетах України та США.

Шифр зберігання НБУВ: Ж25546/пед.

***

Вороненко І. В. Концептуальні засади щодо регулювання кіберпростору. Міжнародний аспект / І. В. Вороненко, К. Л. Тужик // Економіка. Менеджмент. Бізнес. - 2017. - № 4. - С. 73-80.

Досліджено теоретичні аспекти формування кіберпростору. Систематизовано основні положення міжнародних нормативно-правових норм, що регламентують функціонування та регулювання кіберпростору на міжнародному рівні. Здійснено аналіз рівня готовності щодо забезпечення результативного світового регулювання кіберпростором за допомогою глобального індексу кібербезпеки.

Шифр зберігання НБУВ: Ж73946.

***

Діордіна І.В. Напрями державної політики кібербезпеки / І.В. Діордіна // Прикарпатський юридичний вісник. - 2017. - Вип. 3 (18). - С. 112-117.

Здійснено аналіз нормативно-правових актів у безпековій сфері. Втокремлено ті норми, які безпосередньо стосуються державної політики кібербезпеки. Визначено основні напрями державної політики кібербезпеки. Виявлено чинники, які визначають державну політику кібернетичної безпеки та її основну мету. Запропоновано авторське розуміння категорії «кібернетичне суспільство».

Шифр зберігання НБУВ: Ж74200.

***

Діордіна І.В. Суб'єкти забезпечення кібербезпеки / Діордіна І.В. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2017. - Вип. 45(1). - С. 160-165.

Сформульовано авторське розуміння суб'єкта забезпечення кібербезпеки. Зосереджено увагу на необхідності передбачення відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури, дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави.

Шифр зберігання НБУВ: Ж68850/пр.

***

Живило Є.О. Стратегія кібероборони України / Живило Є.О. // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. - 2017. - Вип. 4. - С. 30-37.

Визначено пріоритети та шляхи удосконалення державної політики забезпечення кібербезпеки України. Запропоновано загальнодержавну модель побудови національної системи кібербезпеки.

Шифр зберігання НБУВ: Ж71640.

***

Збірник матеріалів Міжнародної науково-практичної інтернет-конференції "Облік, оподаткування і контроль: теорія та методологія", 30 червня 2017 р., Тернопіль : [тези доп.]. - Тернопіль : ТНЕУ, 2017. - 341 с.

Зі змісту:

- Лінський С.В. Економічна сутність витрат на інформаційну безпеку.

Шифр зберігання НБУВ: ВА815334.

***

Зернецька О. В. Глобальна комунікація : [монографія] / О. В. Зернецька. - Київ : Наукова думка, 2017. – 348 с.

У контексті революціних змін у галузі новітніх технологій, стрімкої диджиталізації, розвитку мережі Інтернет, глобальної блогосфери, соціальних медіа, мобільної телефонії тощо висвітлено роль глобальної комунікації у таких сферах життєдіяльності людства як культура, політика, економіка та кібербезпека. Проаналізовано еволюцію стратегій кібербезпеки США. Розглянуто соціальні мережі та кібербезпеку індивіда.

Шифр зберігання НБУВ: ВА815907.

***

Информационные технологии и безопасность : мат. XVII междунар. научно-практ. конф.- Вып. 17.- Киев, 2017.- 256 с.

Зі змісту:

- Баранов О.А. Інтернет речей (IoT): інтегральна безпека;
- Губська Д.О. Правові питання забезпечення інформаційної і кібернетичної безпеки платежів;
- Добровська С.В. Визначення публікаційної активності в наукових напрямках, які сприяють обороноздатності країни (захист інформації, комп'ютерна безпека);
- Кунченко-Харченко В., Огірко І., Огірко О. Інформаційні технології прогнозування та моделювання кібербезпеки.

Шифр зберігання НБУВ: Ж74360.

***

Камчатний М.В. Принципи обмеження ведення кібервійни / Камчатний М.В. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2017. - Вип. 45(2). - С. 152-158.

Досліджено наявні принципи обмеження ведення війни, можливість та доцільність їх застосування до кібервійн. Розглянуто основні підходи до формування нових обмежувальних принципів у сучасному кіберпросторі. Проаналізовано питання обмеження суб'єктів міжнародного права у методах та засобах ведення кібервійни.

Шифр зберігання НБУВ: Ж68850/пр.

***

Кива В. Ю. Аналіз існуючих методів кібернетичної розвідки інформаційно-телекомунікаційних мереж / В. Ю. Кива, Ю. С. Дрозд // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. - 2017. - № 3. - С. 62-66.

Розглянуто питання важливості забезпечення національної безпеки держави у кібернетичному просторі. Обгрунтовано актуальність та необхідність проведення розвідувальних заходів у кібернетичному просторі противника. Визначено етапи, складові та методи кібернетичної розвідки у кібернетичному просторі.

Шифр зберігання НБУВ: Ж73897.

***

Кібербезпека та інтелектуальна власність: проблеми правового забезпечення : матеріали міжнар. наук.-практ. конф. 21 квіт. 2017 р. - Київ, 2017. - Ч. 1. - 144 с.

Зі змісту:

- Доронін І.М. Правові аспекти стратегічного планування забезпечення кібербезбеки України в сучасних умовах;
- Фурашев В.М. Проблеми забезпечення права на об'єкт інтелектуальної власності в умовах кібербезпеки;
- Андрощук Г.О. Кібербезпека: тенденції в світі та Україні;
- Довгань О.Д. Проблеми правового забезпечення кібербезпеки в Україні;
- Солончук І.В. Правове регулювання забезпечення кібербезпеки;
- Гуцалюк М.В. Актуальні питання правового забезпечення кібербезпеки в Україні;
- Забара І.М. Кібербезпека Європейського Союзу: проблематика правового забезпечення;
- Каращук А. Забезпечення інформаційного суверенітету у кіберпросторі;
- Петряев С.Ю. Социальные риски киберсоциализации на пути к киберцивилизации;

- Петряєв О.С. Протидія інтернет-активності радикального ісламу як проблема кібернетичної війни;
- Дубняк М.В. Правове регулювання інформаційної взаємодії в процесі прийняття рішень як фактор забезпечення кібербезпеки;
- Мисливий В.А. Банківський кіберпростір як місце вчинення злочину.

Шифр зберігання НБУВ: В356872/1.

***

Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: матеріали міжнар. наук.-практ. конф. 21 квіт. 2017 р. - Київ, 2017. - Ч. 2. - 123 с.

Зі змісту:

- Єсипенко Ю.О. Інформаційна безпека та її об'єкти;
- Ліпенко Ю.О. Кіберзлочинність;
- Фарадж Д.Ю. Нагативний вплив кіберзлочинності на особисту інформаційну безпеку;
- Уліцька В.І. Кібертероризм: вигадка чи реальна загроза;
- Нагорний О.С. Кібертероризм як нова форма тероризму;
- Кузьмич М.А. Інформаційна небезпека: кібербуллінг;
- Мишаста Т.Ю. Кіберзлочин як один із найнебезпечніших видів злочинів.

Шифр зберігання НБУВ: В356872/2.

***

Колесніков А. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею / Андрій Колесніков, Марія Зяйлик // Актуальні проблеми правознавства. - 2017. - Вип. 1 (9). - С. 26- 29.

Досліджено проблематику визначення сутності кібербезпеки з урахуванням правової наказовості за кіберзлочин. Визначено основні ознаки суттєвого загострення загроз кіберзлочинності в Україні.

Шифр зберігання НБУВ: Ж70813.

***

Ляшенко П.А. Дослідження взаємозалежності понять соціальної та інформаційної безпеки з використанням Google Trends та Ahrefs /Ляшенко Павло Андрійович// Вісник Черкаського університету. Економічні науки. - 2017. - № 1. - С. 77-87.

Розглянуто гіпотезу стичності, взаємовпливу та взаємозалежності понять соціальної та безпеки за допомогою інструментів Google Trends та Ahrefs.

Шифр зберігання НБУВ: Ж69408/екон.н

***

Майданюк Н.В. Перспективи технологічної підтримки інформаційної безпеки в банківській справі /Майданюк Надія Володимирівна// Вісник Черкаського університету. Економічні науки. - 2017. - № 1. - С. 88-96.

Обгрунтовано доцільність застосування в банках симетричного та асиметричного методів шифрування даних для захисту банківської інформації.

Розглянуто питання ефективності захисту банківських інформаційних систем за допомогою криптографічних систем. Досліджено ситуацію вибору методу розподілу ключів. Показано, що вибір того чи іншого методу залежить від структури системи і технології оброблення даних.

Шифр зберігання НБУВ: Ж69408/екон.н.

***

Марків С. Історико-правовий аспект кібертероризму / Сергій Марків // Актуальні проблеми правознавства. - 2017. - Вип. 2 (10). - С. 103-106.

Доведено, що головною зброєю у боротьбі з кібертероризмом залишається законодавство, яке потребує подальшого вдосконалення.

Шифр зберігання НБУВ: Ж70813.

***

Матеріали всеукраїнської науково-практичної конференції "Державне управління в Україні: виклики та перспективи", 12-13 травня 2017 р. : [збірник]. - Запоріжжя, 2017. - 115 с.

Зі змісту:

- Островий О.В. Проблематика забезпечення кібернетичної безпеки України.

Шифр зберігання НБУВ: ВА815399.

***

Матеріали Міжнародної науково-практичної конференції "Інноваційний розвиток науки нового тисячоліття" (21-22 квітня 2017 року) : [зб. у 3 ч.]. - Ужгород, 2017. - Ч. 2. - 155 с.

Зі змісту:

- Махітько В.С., Полійчук М.В. Організація захисту інформації в банківських структурах;
- Покровська А.В. Низькотехнологічний тероризм як ключова загроза в епоху високих технологій.

Шифр зберігання НБУВ: В356850/2.

***

Негодченко В.О. Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України : монографія / В. О. Негодченко. - Харків, 2016. - 473 с.

Досліджено сутність та особливості адміністративно-правового забезпечення державної інформаційної політики органами Національної поліції України. Окрему увагу приділено діяльності органів поліції у сфері протидії кіберзлочинності.

Шифр зберігання НБУВ: ВА815326.

***

Петрик В. Використання спеціального програмного забезпечення для аналізу інформаційної агресії Російської Федерації проти України / В. Петрик, А. Давидюк // Information Technology and Security. - 2017. - Vol. 5, № 1. - С. 21-28.

Проаналізовано існуючі засоби інтелектуальної обробки даних та інформаційного протистояння у глобальній мережі Інтернет за допомогою спеціального програмного засобу “Support Ukraine”.

Шифр зберігання НБУВ: Ж74190.

***

Розвиток національної системи нормативно-правової інформації: комунікаційний та правовий аспекти (у контексті децентралізації влади в Україні) : матеріали наук.-практ. конф., 26 трав. 2017 р. - Київ : КПІ ім. Ігоря Сікорського : Політехніка, 2017. - 120 с.

Зі змісту:

- Буєва О.Ю. Забезпечення безпеки національного інформаційного простору Королівством Великої Британії.

Шифр зберігання НБУВ: ВА815749

***

Третя всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації», 02-06 вересня 2017 року : зб. тез. - Одеса : ОНАЗ, 2017. - 103 с.

Зі змісту:

- Дика Н.В., Одарченко Р.С., Шульга Б.С. Методи оцінки впливу та запобігання кібермоббінгу;
- Котелянець В.В., Смірнов О.А. Проблеми забезпечення кібербезпеки в сенсорних мережах;
- Одарченко Р.С. Підвищення рівня кібербезпеки сучасних стільникових мереж в Україні;
- Стайкуца Є.В., Дігов С.О., Бердніков О.М., Верстаков В.І. Аналіз ризиків корпоративного середовища з позиції міжнародних стандартів інформаційної безпеки;
- Харлай Л.О. Методи захисту інформації в оптичних мережах;
- Хлапонін Ю.С., Рудніцька О.В., Пальчик С.П. Інтелектуальні системи безпеки об’єктів критичної інфраструктури;
- Юдін О.Ю. Гнатюк С.Є. Аналіз вимог до елементів інформаційно-телекомунікаційних систем управління енергетичною інфраструктурою, які забезпечують кіберзахист.

Шифр зберігання НБУВ: ВА815397.

***

Чакрян В. Х. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки: автореф. дис. ... канд. техн. наук : 05.12.02 / Чакрян Вадим Хазарович ; Харків. нац. ун-т радіоелектроніки. - Харків, 2017. - 24 с.

Досліджено інформаційну безпеку потоку пакетів в процесі його динамічної маршрутизації в телекомунікаційній мережі шляхом урахування ризиків порушення конфіденційності, цілісності та доступності транзитних даних. Удосконалено математичну модель процесу передачі потоку пакетів в умовах кібератак щодо можливості проведення розрахунків про наявності атак типу

відмова в обслуговуванні на маршрутизатори мережі, шкідливих процесів на маршрутизаторах, які знижують пропускну здатність вузлу, чи взагалі виводять його з ладу, атак на перемаршрутизацію даних по не ефективним шляхам. Розроблено новий метод оцінки ризику інформаційної безпеки шляхів передачі потоку пакетів. Отримало подальший розвиток моделі одношляхової та багатошляхової маршрутизації потоку пакетів в телекомунікаційній мережі в умовах кібератак.

Шифр зберігання НБУВ: РА432186.

***

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

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