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

№ 11 (листопад)

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

«**Днепровский горсовет заключил меморандум о сотрудничестве со Службой безопасности Украины.** Его цель — расширение взаимодействия в сфере кибернетической безопасности и повышение уровня защищенности информационных, телекоммуникационных и информационно-телекоммуникационных систем мэрии…

MISP-UA — система с открытым программным кодом, созданная работниками Ситуационного центра обеспечения кибербезопасности Службы безопасности Украины для сбора и обработки информации об инцидентах кибербезопасности и обмена техническими данными об идентификаторах компрометации информационных систем объектов инфраструктуры. Платформа широко используется во всем мире, соответствует международным стандартам Европейского Союза и НАТО, а также применяется основными международными субъектами в сфере кибербезопасности — FIRST, CIRCL, CiviCERT, NATO NCI Agency. С помощью этой платформы Днепровский горсовет и Ситуационный центр СБУ в режиме реального времени смогут обмениваться технологической информацией о киберугрозах, что обеспечит повышение уровня безопасности и минимизирует время реакции на инциденты. Напомним, в июле этого года на базе Днепровской мэрии создали первый региональный Центр киберзащиты.» ***(СБУ займется кибербезопасностью Днепровского горсовета // «Новый формат» (https://nf.dp.ua/2018/11/sbu-zaymetsya-kiberbezopasnostyu-dneprovskogo-gorsoveta/). 14.11.2018).***

***

«Центральна виборча комісія планує створити окремий підрозділ для гарантування кібербезпеки під час виборів, повідомила секретар комісії Наталія Бернацька на першій прес-конференції нової ЦВК 13 листопада…

Втім, як зазначив заступник голови ЦВК Олег Конопольський, на відкриті вакансії ІТ-спеціалістів ще не було жодного охочого…» ***(ЦВК створить окремий підрозділ для гарантування кібербезпеки під час виборів // Західна інформаційна корпорація (https://zik.ua/news/2018/11/13/tsvk_stvoryt_okremyy_pidrozdil_dlya_garantuvannya_kiberbezpeky_pid_chas_1447155). 13.11.2018).***

***

«IT-специалисты Конституционного Суда Украины оставили возможность доступа к администрированию баз данных портала суда с любой точки земного шара. Потенциально это может привести к компрометации информации и использовании злоумышленниками Конституционного суда в информационно-психологических атаках.

Об этом на своей странице в Facebook сообщил эксперт по кибербезопасности Сергей Дяченко…

Эксперт уточняет: PhpMyAdmin используется, как правило, начинающими пользователями для облегчения администрирования баз данных, имеет многочисленные уязвимости, которые систематически обновляются. Среди специалистов PhpMyAdmin считается потенциально высокоопасным и может использоваться только локально…» ***(Владимир Кондрашов. Конституционный суд Украины оставил хакерам лазейку // Internetua (http://internetua.com/konstitucionnyi-sud-ukrainy-ostavil-hakeram-lazeiku). 22.11.2018).***

***

«Массовый взлом и последующая кража информации с планшетов Патрульной полиции Украины, а также атака на отказ в обслуживании могут быть реализованы уже в ближайшее время. Причина – в целом ряде критических уязвимостей в обеспечивающей инфраструктуре специализированного программного обеспечения LIS-M, закупленного для патрульной полиции. Более того, компания-поставщик данного оборудования имеет все признаки фиктивности…

Подробней о ситуации рассказал консультант по кибербезопасности Егор Папышев:

– Хактивисты Украинского кибералья́нса с помощью Kir Vaznitcky обнаружили дыры в серверах компании-разработчика софта для полиции (а именно, компании ООО "С.І.Т. ЦЕНТР "ВЕБ-КОНТИНЕНТ") несколько месяцев назад, сообщили о них в структуры СБУ и МВД, однако на протяжении длительного времени должной реакции не последовало. Сейчас ресурсы этой компании взломаны неизвестными хакерами. Как эти хакеры развивали свою атаку дальше - неизвестно, однако однозначно понятно, что обнаруженные уязвимости позволяли проломить всю эту специализированную систему LIS-M до основания, с последующим получением полного доступа к служебной информации патрульной полиции, – на своей странице в Facebook сообщил Егор Папышев…» ***(Владимир Кондрашов. Служебная информация Патрульной полиции Украины оказалась под угрозой // Internetua (http://internetua.com/sluzebnaya-informaciya-patrulnoi-policii-ukrainy-okazalas-pod-ugrozoi). 19.11.2018).***

***

«Центрвиборчком отримав від координатора проектів ОБСЄ в Україні комплекс обладнання і програмного забезпечення для посилення захисту Держреєстру виборців від кіберзагроз…

“Зокрема, Комісії передано системи для комплексного технічного захисту мережі ДРВ. Вони дозволять виявляти загрози, запобігати вторгненням і реагувати на можливі кібератаки…

Як уточнюють у ЦВК, передача обладнання стала важливим кроком в низці заходів, що проводяться Комісією для посилення кібербезпеки адміністрування виборів в Україні в рамках підготовки до загальнонаціональних виборів 2019 року…

Постачання зазначеного обладнання здійснено в рамках проекту “Посилення кібербезпеки і прозорості виборчих процесів в Україні”, що реалізується координатором проектів ОБСЄ за фінансової підтримки уряду Норвегії та місії США в ОБСЄ…» ***(ЦВК отримала від ОБСЄ обладнання для захисту від кібератак // 1NEWS (https://1news.com.ua/ukraine/tsvk-otrimala-vid-obsye-obladnannya-dlya-zahistu-vid-kiberatak.html). 28.11.2018).***

***

«З 28 листопада в 10 областях України запроваджується режим воєнного стану терміном на 30 днів. У переліку - Одеська, Миколаївська, Херсонська, Запорізька, Луганська, Донецька, Сумська, Харківська, Чернігівська, Вінницька області. Президент включив до Указу лише кілька заходів з 24-ох, передбачених у документі. Більшість - стосуються Збройних Сил України, Нацгвардії, СБУ та МВС, повідомляє ПІК з посиланням на офіційний сайт Херсонської ОДА.

Зокрема, підсилюються заходи із кібербезпеки, інформаційної безпеки, контррозвідувального, антитерористичного та контрдиверсійного режимів…» ***(Воєнний стан на Херсонщині: що треба знати кожному? // Інформаційне агентство «ПІК - Південна інформаційна Компанія» (https://pik.ua/news/url/vojennij-stan-scho-treba-znati-kozhnomu). 27.11.2018).***

***

«Интервью с Сергеем Демедюком о хакерах, пиратских сайтах, онлайн-казино и ситуации с Moneyveo…

— Чем занимается киберполиция, кроме расследования хакерских атак?

— Мы сосредоточены на четырех основных направлениях

Кибербезопасность — приоритетная задача подразделения. Противодействие распространению вредоносного ПО, кибератакам, распространению фишинговых писем — целенаправленным киберинцидентам по проникновению. Скрытый майнинг криптовалют тоже сюда относится. Мы причисляем его к вредоносным ПО. Потому что любая программа или скрипт, установленные на ПК без вашего ведома — вредоносные.

Преступления в сфере платежных систем — когда хакеры используют свои навыки, чтобы получить доступ к компьютеру бухгалтера или онлайн-банкингу и украсть деньги. Сюда входит также кардерство — манипуляции с операционными системами банкоматов и кража денег.

Интеллектуальная собственность — кроме выявления размещенного с нарушением авторских прав в интернете видео- и аудио-контента сюда также относятся электронные книги. Сегодня это одно из приоритетных направлений.

Противоправный контент — к нему относится распространение детской порнографии. Наша работа в этом направлении сосредоточена на раскрытии преступлений, связанных с созданием такого контента на территории Украины при участии украинских детей. Считаем это направление нашей деятельности очень важным. К противоправному контенту также относится продажа различных баз данных.

Помимо этого мы помогаем выявлять информацию о торговле оружием, наркотиками и другими запрещенными средствами. А также предложения взломать сайт, получить или перехватить конфиденциальную информацию. Помогаем раскрывать преступления другим подразделениям Нацполиции. И участвуем в международных кибероперациях.

— …в Украине наказание за киберпреступление — незначительное, и зачастую преступники отделываются штрафом. Какой же смысл их ловить тогда?

— Да, согласно Уголовному кодексу большинство преступников получают штрафные санкции, условные наказания, не более. Мы обязаны реагировать на правонарушения и привлекать преступника к ответственности по нашим законам. Однако они у нас на особом учете. Есть государства, где хакеров тоже ставят на учет…

В нашей стране так нельзя — нужны постановления суда. Права преступника защищаются законом больше, чем права правоохранителей. Но большинство хакеров у нас на учете и в основном они переходят на “белую сторону”. Помогают компаниям с ИТ-безопасностью, например.

— А бывало, чтобы вы поймали крутого хакера, а потом переманили работать в киберполицию?

— Я скажу так: иногда мы стараемся этих людей заинтересовать для работы в будущем на благо государства. Для этого есть много возможностей — и в правоохранительных органах, и в компаниях. Предлагая такую возможность, мы стараемся удержать наших граждан от противоправной деятельности. Если им интересна работа в сфере ИТ и наше предложение, почему и не работать? Они идут и работают.

— Какого возраста украинский хакер?

— Разного, но как правило начинается все еще в школьном возрасте. Мы уже не раз рассказывали о случаях, когда 16-17-летние ребята модифицировали вредоносное ПО, чтобы получить нужную им информацию. Когда человека тянет в эту сферу, он начинает экспериментировать…

— Давайте поговорим о направлении интеллектуальной собственности. Киберполиция закрыла в Украине сайты с пиратским контентом ex.ua и fs.to. Тем не менее, у нас в доступе куча других ресурсов. Почти сразу после вашей операции появился ex-fs. Вы говорили, что сложно бороться с пиратскими сайтами, когда серверы находятся вне Украины. Как же вы это делаете?

— Мы не можем убрать из интернета сам контент, даже если мы получим доступ к серверам, где этот контент хранится. Преступнику будет нетрудно заново все создать в будущем. Поэтому мы боремся с самими организаторами.

Они очень много зарабатывают на рекламе на своих сайтах. И мы подходим с этой стороны. Выявляем организаторов, откуда они получают деньги, и прекращаем эту деятельность. Это больно и влечет за собой более серьезную ответственность, чем за нарушение авторских прав.

Потому что это незадекларированные деньги и фактически это легализация денег, добытых в ходе преступной деятельности. За это можно получить до 8 лет лишения свободы.

Тут организаторы уже подумают. Потому что если попасться с таким второй раз, можно оказаться в месте лишения свободы с конфискацией всего имущества. Мы рассказываем о последствиях и люди от такой деятельности отходят.

— А как насчет онлайн-казино? Тоже ваша тема?

— В основном мы обращаем внимание на финансовые пирамиды, потому что из них потом получаются массовые мошеннические схемы. Онлайн-казино мы тоже выявляем в киберпространстве — оно запрещено на территории Украины.

— Как же тогда работает тот же Parimatch? Его рекламой даже метро обклеено. Это вызывает вопросы.

— До Parimatch мы тоже когда-нибудь дойдем. Мы закрывали их колл-центры по Украине, в Киеве в том числе. И продолжаем делать эту работу. Но чем более раскрученная компания, тем больше она использует средств по самозащите. И такие преступные группировки используют множество технических возможностей — зеркала, как я их называю…

— Получается, без возможности мониторинга и блокировки, Киберполиции приходится просто много раз переделывать одну и ту же работу? По сути, бороться с зеркалами и т.д.?

— Да, нам иногда приходится делать одну и ту же работу, чтобы прекратить деятельность противоправных ресурсов. Приведу пример борьбы с распространением наркотических средств. Как заблокировать такой сайт, если он находится в других странах, используя кучу зеркал?

Мы в государстве не можем этого сделать, но постоянные жалобы и претензии, почему мы этого не делаем, не прекращаются.

Поэтому мы должны в ближайшее время все-таки с законодателем решить эту проблему. И определить, каким образом мы будем взаимодействовать с операторами именно в данной сфере, — ограничении противоправного контента по отношению к нашим пользователям. Каким образом мы будем это делать – мы должны вместе обсудить. Мы свой способ предложили в этом законопроекте.

Некоторым он не нравится, и в связи с этим до сих пор, из года в год мы не можем его вынести даже в зал Верховной Рады…

— Какими технологиями вы пользуетесь? …на сколько процентов в реальности оснащенность Киберполиции соответствует представлениям киношников, в которых есть всякие крутые жучки и мониторы?

— …Для любого киберполицейского и хакера достаточно классного мощного девайса, с помощью которого он сможет делать многое. Ну, и интернет — чем более скоростной, тем лучше. И больше ничего ему не нужно. Самое главное — это мозг наших специалистов.

И Украина в этом случае является уникальной в Европе, потому что мы, наверное, впервые на базе полиции набрали на работу “белых” хакеров.

Как раз их ум и навыки продвинули нас вперед настолько, что мы в своих функциях и возможностях уже некоторые страны перегнали по линии кибербезопасности и киберпреступности. Потому что они (белые хакеры) сами пишут программное обеспечение, которое позволяет идентифицировать и выявлять вредоносное ПО…

— Вопрос по Moneyveo. Вы в курсе, что там происходит? Вы занимаетесь этой темой?

— Я могу сказать, что в Киберполицию от самих потерпевших не поступало ни одного заявления. К нам поступало несколько заявлений от самой Moneyveo, в которой нам сообщили, что к ним обращаются граждане, на которых кто-то якобы взял кредит. Мы этим занимаемся. Но проблема же здесь в самой Moneyveo. Компания была нацелена на предоставление услуг и раскрутку, но не сосредоточилась на своей безопасности, верификации этих документов…» ***(Глава Киберполиции: до Parimatch мы тоже когда-нибудь дойдем // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/270820-glava_kiberpolitsii_do_parimatch_my_tohe_kogda-nibudj_dojdem). 21.11.2018).***

***

«Государственная служба специальной связи и защиты информации Украины (Госспецсвязи) призывает госучреждения и предприятий критической инфраструктуры всех форм собственности принять меры для повышения уровня защиты своих информационно-телекоммуникационных систем и информационных ресурсов.

Об этом отмечается в сообщении госоргана.

"В случае возникновения киберугроз, нештатных ситуаций с признаками кибератак и киберинцидентив предлагаем немедленно обращаться в центр киберзащиты Госспецсвязи и правительственной команды реагирования на компьютерные чрезвычайные события CERT-UA", — отмечается в сообщении…» ***(В Госспецсвязи призвали все компании усилить киберзащиту // Goodnews.ua (http://goodnews.ua/technologies/v-gosspecsvyazi-prizvali-vse-kompanii-usilit-kiberzashhitu/). 26.11.2018).***

***

Національна система кібербезпеки

«У Дніпрі заступник голови СБ України Олег Фролов презентував перший регіональний центр забезпечення кібербезпеки, основними завданнями якої будуть реагування на кіберінциденти та кібератаки, цілями яких є державні електронні інформаційні ресурси та об'єкти критичної інфраструктури Дніпропетровської області…

Як повідомляється, створення регіонального центру є наступним кроком у розбудові національної системи кібербезпеки України у рамках другого етапу Угоди «Про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки»…

Центральний Ситуаційний центрй забезпечення кібербезпеки СБ України наразі фіксує збільшення як кількості кібератак, так і їх масштабності, що потребує відповідного реагування та дослідження. Крім цього російські спецслужби все частіше використовують кібератаки як складові заходів деструктивного інформаційно-психологічного пливу для інспірування протестних настроїв та

загострення суспільно-політичної обстановки в Україні. Дніпропетровська область є одним з найбільш індустріально розвинених регіонів України, що передбачає наявність на її території чималої кількості об'єктів критичної інфраструктури, де функціонують інформаційно-телекомунікаційні системи та автоматизовані системи управління технологічними процесами.

Усвідомлюючи загрози у кібербезпеці України з боку іноземних спецслужб для порушення сталого функціонування на території Дніпропетровщини стратегічних та ключових підприємств металургійної, гірничо-видобувної, хімічної, машинобудівної, фінансових та транспортних галузей, а також важливих об'єктів життєзабезпечення та паливно-енергетичного комплексу України, саме у Дніпрі створено перший регіональний центр забезпечення кібербезпеки. Для реагування на кібернетичні атаки регіональним центром, створеним на базі Управління СБ України у Дніпропетровській області, використовуватиметься платформа MISP-UA, що забезпечить обмін технологічною інформацією про реалізовані та потенційні кіберзагрози в режимі реального часу.

Ситуаційний центр забезпечення кібербезпеки СБ України до регіонального органу також передав найсучасніше обладнання. У подальшому планується створення таких центрів і в інших регіонах України…» ***(СБУ відкрила у Дніпрі перший регіональний центр кібербезпеки // Західна інформаційна корпорація (https://zik.ua/news/2018/11/22/sbu_vidkryla_u_dnipri_pershyy_regionalnyy_tsentr_kiberbezpeky_1453735). 22.11.2018).***

***

Правове забезпечення кібербезпеки в Україні

«Народні депутати підтримали закон, який посилює захист роботи ресурсів Центральної виборчої комісії від кібератак.

Проект Закону про внесення змін до додатка № 3 до Закону України «Про Державний бюджет України на 2018 рік» № 8496 під час ранкового засідання ВРУ… у другому читанні підтримали 253 обранці…

Як ідеться у пояснювальній записці, для посилення захисту інформації в інформаційно-телекомунікаційних системах ЦВК – ЄІАС «Вибори» та локальній обчислювальній мережі Комісії – слід здійснити низку заходів, зокрема: встановлення сучасного мережевого обладнання захисту інформації; встановлення системи збереження даних; модифікація комплексних систем захисту інформації та проведення їх державної експертизи; створення в Секретаріаті Комісії окремого підрозділу із кібербезпеки інформаційних ресурсів.

Загальна сума додаткових видатків становить 36,8 млн грн та 12,8 млн грн. На відповідну суму, майже 50 млн грн, зменшать видатки загального фонду за бюджетною програмою Субвенція з державного бюджету місцевим бюджетам на проведення виборів депутатів місцевих рад та сільських, селищних, міських голів…» ***(Напередодні виборів у Раді подбали про захист ЦВК від кібератак // Західна інформаційна корпорація***

(https://zik.ua/news/2018/11/22/naperedodni_vyboriv_u_radi_podbaly_pro_zahyst_tsvk_vid_kiberatak_1453597). 22.11.2018).

***

«Один із заходів Асоціації правників України із цікавою та оригінальною назвою «Кукіс – це не тільки печиво, а й дані відвідуваності сайту» був присвячений правовому регулюванню збирання, обробки, зберігання та поширення інформації про користувачів веб-сайтів.

Як зазначив Іларіон Томаров, радник, керівник практики інтелектуальної власності ЮФ «Василь Кісіль і Партнери» на початку заходу: «Загальновідомо, що веб-сайти збирають про нас інформацію, в тому числі, і за допомогою cookies. Це, так би мовити, наша плата за користування багатьма, в тому числі й безкоштовними, зручними сервісами, які стали невід'ємною частиною нашого життя».

Однак, як вони це здійснюють, для чого, чим це регулюється та як захистити права користувачів не зрозуміло. Наразі українське законодавство не приділяє окрему увагу даному питанню, водночас, завдяки загальним нормам про захист інформації про особу, її персональних та конфіденційних даних, уже існує судова практика із правового захисту користувачів Інтернету. Саме даній темі був присвячений захід…

Основним доповідачем виступив Юрій Карлаш, адвокат, патентний повірений ЮФ Petosevic, який для характеристики існуючих відносин в даній сфері обрав термін «випромінювання», оскільки користуючись веб-сайтами, ми своєрідним чином «випромінюємо» про себе інформацію.

Ці дані, навіть ті, що, на перший погляд, не несуть в собі можливість ідентифікувати особу та не є персональними, теж мають приховану цінність та у разі необхідності дають підстави для отримання певної інформації про особу.

Так відбувається, поміж іншого, завдяки великому, різноманітному масиву даних про особу, які обробляються комп'ютерними системами, а також завдяки прогресивним обчислювальним можливостям техніки (зокрема, шляхом обробки та співставлення). Таким чином, за допомогою вказаних характеристик, існує більша вірогідність досягти отримання цілісного образу користувача окремого веб-сайту шляхом його ідентифікації чи деанонімізації, ніж якби це здійснювалось за допомогою аналізу інформації з різних джерел…

Водночас, спікер відмічає, що у всіх інформаційних правовідносинах питання щодо охорони та таємниці приватного життя є досить важливим, однак не єдиним. При його розгляді, окрема увага приділяється визначенню юрисдикції вирішення спору щодо збору інформації - іншими словами, визначенню того, право якої держави слід застосовувати в конкретному випадку…

Підсумовуючи зазначене, спікер виділив наступні основні тези, які слід враховувати при користуванні cookies, веб-сайтами та мережею Інтернет загалом:

1) Завантаження cookies на пристрій користувача, який знаходиться в Україні, за загальним правилом зумовлює необхідність застосування законодавства України в частині обробки даних про користувача та обов'язковості (чи необов'язковості) отримання його згоди на це.

2) Якщо власник веб-сайту, який за допомогою cookies отримує інформацію про відвідувача веб-сайту, має витратити невиправдано велику кількість часу і докласти значних зусиль для ідентифікації особи відвідувача протягом строку зберігання даних, і, якщо ці дані формально підпадають під категорію конфіденційної інформації, такі дані не є персональними та не є конфіденційними і на них не поширюється Закон України "Про захист персональних даних", в тому числі і обов'язок отримання згоди на розповсюдження цих даних.» ***(Зозуля Наталія. Правовий погляд на cookies, або Як веб-сайти збирають інформацію про користувачів // "Українське право" (http://ukrainepravo.com/scientific-thought/legal_analyst/pravovyy-poglyad-na-cookies-abo-yak-veb-sayty-zbyrayut-informatsiyu-pro-korystuvachiv-/). 20.11.2018).***

***

Кібервійна проти України

«Міністерство з питань тимчасово окупованих територій зафіксувало здійснення хакерської атаки на сайт відомства впродовж 2-3 листопада… в результаті якої невідомі отримали доступ до панелі керування сайтом"…

Як зазначили у відомстві, використовуючи можливості панелі керування, були модифіковані деякі сторінки сайту МТОТ для розповсюдження спам-контенту. Наразі атаку вдалось зупинити, доступ до панелі керування сайту обмежено, модифіковані сторінки відновлені до останньої збереженої версії. Проводиться аналіз втраченої інформації…» ***(Євген Дем'янов. Сайт МінТОТ зазнав хакерської атаки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1761211-sayt-mintot-zaznav-khakerskoyi-ataki). 06.11.2018).***

***

«Голова Державної служби спеціального зв'язку та захисту інформації України Леонід Євдоченко прогнозує збільшення атак у кіберпросторі в контексті виборів у 2019 році…

Л.Євдоченко пояснив, що дії із захисту від кібератак перед виборами має бути спрямовано насамперед на захист персональних даних, баз даних та ресурсів Центральної виборчої комісії.

За його словами, Центр реагування на кіберзагрози в Україні співпрацює з більше ніж 300 такими командами в 60 країнах у всьому світі…» ***(У Держслужбі спецзв'язку України готові протистояти кібератакам напередодні виборів-2019 // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/543540.html). 08.11.2018).***

***

«Советник президента Украины, первый вице-президент Национальной академии наук Украины Владимир Горбулин заявил, что Украина в 2018 году

уже предупредила совершение двух мощных кибератак со стороны Российской Федерации.

Как передает корреспондент, об этом он сказал в Киеве на международной конференции "Уроки гибридного десятилетия: что нужно знать для успешного движения вперед" в Киеве.

"Россия пытается превратить Украину в своеобразный киберполигон, атакуя критическую инфраструктуру, финансовый сектор, энергетику, транспорт: "Прикарпатьеоблэнерго", министерство финансов, действие вируса NonPetya. Это та сфера, где мы выучили урок", - подчеркнул он…

В свою очередь заместитель секретаря Совета национальной безопасности и обороны Украины Александр Литвиненко заявил, что ведущее место в гибридной доктрине Кремля играют кибернетические средства, которые влияют не только на инструменты передачи информации, но и на содержание этой информации.

По мнению заместителя секретаря СНБО, гибридный подход Кремля базируется на выявлении, а порой создании и эксплуатации уязвимости противника.» ***(Советник Порошенко: РФ пытается превратить Украину в киберполигон // Телеграф (https://telegraf.com.ua/ukraina/obshhestvo/4692453-sovetnik-poroshenko-rf-pyitaetsya-prevratit-ukrainu-v-kiberpoligon.html). 07.11.2018).***

***

«Украинскому консультанту по кибербезопасности Егору Папышеву удалось проникнуть на «российскую фабрику троллей» и узнать некоторые подробности работы «кремлеботов» изнутри. Как оказалось, на российских ботофермах используют специальный софт для работы с социальными сетями, обучают сотрудников и готовят площадку для очередной информационной волны, "арендуя" реальные аккаунты украинцев в соцсетях.

Об этом Егор Папышев написал на своей странице в Facebook…

Масштабы происходящего, по его словам, «впечатляют неискушенного в "накрутках" и прочих приемах зрителя»:

– …У ботоводов детально налажены процессы работы и учета, отчетности, настроена инфраструктура и специализированный софт, – написал Папышев. – Они управляют своим ресурсом, постоянно актуализируют его и оперативно переключают на выполнение разных задач. Они занимаются обучением своих сотрудников. Они могут регистрировать сотни аккаунтов, создавать посты, лайкать, репостить, жаловаться на другие аккаунты, писать в сообщества, менять информацию в своих профилях, и всё это - массово, всего в пару кликов.

Папышев подчеркивает: ботофермы – это бизнес, который сегодня может «продвигать» одну персону, а завтра сделать «массовый вброс» фейковых новостей с перекрестными репостами и лайками, чтобы ударить по репутации другой…» ***(Владимир Кондрашов. Украинский хакер проник на «фабрику российских троллей» // Internetua (http://internetua.com/ukraindkiy-haker-pronik-na-fabriku-rossiiskih-trollei). 19.11.2018).***

***

«Експерти з кібербезпеки прогнозують посилення хакерських атак в Україні під час виборів у 2019 році…

Кіберзахист українських державних установ, військових і промислових об'єктів забезпечує Рада національної безпеки і оборони країни (РНБО).

Безпека виборів в Україні – принципове питання для цього органу, особливо на тлі спроб останніх років вплинути на вибори у США або на британський референдум щодо виходу з ЄС, які закидають Росії.

При Радбезі України працює національний координаційний центр кібербезпеки. У ньому представлені поліція, всі служби розвідки країни, СБУ, прокуратура – загалом десять відомств…

Для того, щоб припинити спроби втручання ззовні в парламентські і президентські вибори в Україні, США з 2017 року вже виділили Києву 10 мільйонів доларів. Це кошти на технічну підтримку ЦВК, виборчих дільниць, моніторингу підготовки та ходу виборів в 2019 році. Про це повідомили у посольстві США в Україні…

Крім того, партнерами Києва з кібербезпеки під час виборів стали також Трансатлантична комісія (ТК) і Атлантична рада, яку очолює Джон Гербст, колишній посол США в Україні. Він повідомив DW про створення спільної з Києвом робочої групи для моніторингу та допомоги в нівелюванні іноземного втручання в президентські вибори в Україні…

До робочої групи… входить відділ боротьби з дезінформацією під керівництвом чеського експерта Якуба Каленскі, відділ оцінки активності російської армії і ВМФ на чолі з експертом київського Центру Разумкова Олексієм Мельником. Буде в складі робочої групи і команда фахівців з кібербезпеки. Вже на початку грудня, планує Гербст, група має запрацювати наповну.» ***(Ольга Аверіна. Вибори – 2019: як Україна протистоятиме кібератакам // «Погляд» — незалежна інформаційна агенція (https://www.poglyad.tv/vybory-2019-yak-ukrayina-protystoyatyme-kiberatakam/). 24.11.2018).***

***

«Щонайменше чотири українські правозахисні, медійні та антикорупційні організації повідомили про спроби кібератаки на їх працівників.

На приватні та корпоративні Google-акаунти працівників 28 листопада надійшли повідомлення про те, що вони були атаковані зловмисниками, яких підтримує уряд. Назви організацій не називаються з метою безпеки. Як повідомляє Лабораторія цифрової безпеки, схожі повідомлення українські користувачі масово отримували у 2015-2016 роках, і подальше розслідування показало, що за ними стояли групи хакерів Fancy Bear, яких пов'язують із урядом Російської Федерації.

В компанії Google зазначили, що таких атак як ця зазнають менше ніж 0,1% користувачів Gmail. Утім, як саме здійснюється така атака не повідомляють, щоб про це не дізнались зловмисники…» ***(На українських правозахисників здійснили кібератаки в перший день воєнного стану – Лабораторія цифрової безпеки // MediaSapiens (https://ms.detector.media/web/cybersecurity/na_ukrainskikh_pravozakhisnikiv_zdiysni***

li_kiberataki_v_pershiy_den_voennogo_stanu_laboratoriya_tsifrovoi_bezpeki/). 29.11.2018).

***

Боротьба з кіберзлочинністю в Україні

«Небольшая украинская агрофирма лишилась более 150 тысяч гривен из-за несанкционированного вмешательства в работу интернет-банкинга. Мошенники перечислили украденные деньги на одну из криптобирж.

…Следователям удалось установить, что с карты «ОТП-Банка» в период с 9 июля 2018 по 9 августа 2018 были переведены средства с помощью Интернет ресурса wayforpay.com для пополнения баланса сайта «exmo.com» (так называемая «Международная биржа криптовалют»)…

Согласно материалам дела, следственный отдел Винницкого ОП ГУНП в Винницкой области занимается расследованием преступления, предусмотренного ч. 1 ст. 361 УК Украины («Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи»)…» ***(Владимир Кондрашов. Киберворы украли 150 тысяч у агрофирмы // Internetua (http://internetua.com/kibervory-ukrali-150-tysyacs-u-agrofirmy). 05.11.2018).***

***

«Два года лишения свободы получил безработный хакер, который вместе со знакомым сотрудником колл-центра «Ощадбанка» придумал, как воровать деньги с банковских карт. Схема лишила одно из клиентов государственного банка суммы в 224 тысячи гривен.

По версии следствия, уроженец Винницкой области, будучи студентом одного из местных техникумов по специальности обслуживание компьютерных систем и сетей, в период с сентября 2015 по февраль 2016 года создал вредоносную программу для несанкционированного вмешательства в работу автоматизированной системы АТ «Ощадбанк» и платежной системы «Portmone.com» для перевода чужих средств через электронные системы. Данная программа предназначена для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, и позволяет, зная номер и срок действия платежной карты, установить действующий CVV2 - код для платежной карты, что дает возможность обходить механизм проверки подлинности банковской карты по коду CVV2/CVC2…

Программа работала через систему Portmone.com: блокировалась одна гривна по карте с CVV2-кодами от 000 до 999 путем простого перебора. Когда блокировка удавалась, это означало, что CVV2-код верный. Чтобы знать, что одна гривна заблокирована, необязательно получать смс-сообщение, ведь благодаря Portmone.com в программе возвращался ответ.

Обвиняемый программу испытывал на данных, которые предоставлял ему товарищ, находящийся в колл-центре – он имел доступ к системе, видел номер карты и её срок действия…

Суд посчитал, что вина обвиняемого в совершении инкриминируемого ему уголовного правонарушения полностью нашла свое подтверждение в ходе судебного разбирательства, и квалифицировал его действия по ч. 2 ст. 361-1 УК Украины, то есть создание с целью использования вредоносного программного средства, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, причинивших значительный ущерб.

В итоге парень получил наказание в виде двух лет лишения свободы. Также его ожидает иск от «Ощадбанка» в рамках гражданского судопроизводства.

Отметим, что это довольно редкий случай, когда обвиняемый по такому преступлению не пошел на сделку со следствием и получил реальный, а не «условный» срок.» ***(Владимир Кондрашов. Хакера посадили на два года за кражу денег с карт клиентов «Ощадбанка» // Internetua (http://internetua.com/hakera-posadili-na-dva-goda-za-kraju-deneg-s-kart-klientov-osxadbanka). 01.11.2018).***

***

«…Працівники Київського управління Департаменту кіберполіції спільно зі слідчими Васильківського відділу поліції Київщини, за процесуального керівництва Києво-Святошинської прокуратури, викрили 24-річного мешканця Запоріжжя у створенні та адмініструванні піратського сайту «onemov.net».

Правоохоронці встановили, що молодик на веб-ресурсі «onemov.net» відтворював та розповсюджував аудіовізуальні твори, права на які належать компанії Universal City Studios LLLP (Universal), представником якої в Україні є Українськаантипіратська асоціація. Аудиторія відвідувачів сайту не обмежувалася кордонами України, оскільки більшість фільмів розміщених на цьому ресурсі відображалася англійською мовою. Пізніше фільми з’являлися російською та українською мовами…

Перевіряється причетність фігуранта до адміністрування та створення ще близько 10 піратських Інтернет-сайтів. Кримінальне провадження розпочато за ч. 3 ст. 176 (Порушення авторського права і суміжних прав) КК України…» ***(Кіберполіція припинила діяльність піратського сайту «onemov.net» // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-piratskogo-sajtu-onemovnet-5859/). 09.11.2018).***

***

«…Працівники Причорноморського управління Департаменту кіберполіції викрили мешканця Миколаєва у розповсюдженні шкідливого програмного забезпечення. За даним фактом поліція розпочала кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження

або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України.

…працівники кіберполіції встановили, що зловмисник з метою розповсюдження шкідливого програмного засобу створив декілька каналів на відеохостінгу «Youtube». На цих каналах він розміщував відеорекламу розважальних програм для комп'ютера, та у опису до відео надавав посилання, через яке користувач мав можливість завантажити таку програму. Натомість користувач завантажував шкідливе програмне забезпечення.

…Вирішується питання щодо оголошення підозри хакеру за ч. 2 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.» ***(Кіберполіція викрила розповсюджувача вірусу, замаскованого під розважальні програми // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-rozpovsyudzhuvacha-virusu-zamaskovanogo-pid-rozvazhalni-programy-4268/). 01.11.2018).***

***

«В среду, 7 ноября, неизвестные злоумышленники осуществили атаку повторного расходования на украинскую криптовалютную сеть Karbo [Карбованец].

Киберпреступникам удалось продать небольшое количество фальшивых монет в паре KRB/UAH на криптовалютной бирже Kuna, а затем вывести средства в биткойн на частный кошелек, сообщил изданию ForkLog основатель торговой площадки Михаил Чобанян.

В настоящее время биржа временно прекратила ввод/вывод KRB и оценивает возможность повторения атаки. По сообщению представителей Kuna, средства пользователей не пострадали.

По словам Чобаняна, разработчики блокчейн-сети Карбованец проинформировали о происходящем технический отдел биржи и было принято решение понаблюдать за развертыванием «атаки 51%». Полученный опыт операторы биржи намерены использовать для усиления безопасности площадки…» ***(Украинская блокчейн-сеть подверглась кибератаке // Goodnews.ua (http://goodnews.ua/technologies/ukrainskaya-blokchejn-set-podverglas-kiberatake/). 09.11.2018).***

***

«Киберполиция задержала хакера, который заразил вирусами почти 2 тыс. устройств с более 50 стран мира. Об этом сообщает Департамент киберполиции Национальной полиции Украины.

Хакером оказался 42-летний житель Львовской области…

Специалисты проанализировали вредоносное программное обеспечение и установили, что вирус оказывает полный удаленный доступ к подконтрольных компьютеров.

Хакер мог загружать и отгружать файлы, управлять автозагрузкой и службами, удаленно управлять реестром, устанавливать и удалять программы, делать скриншоты с удаленного экрана, перехватывать звук с микрофона и видео со встроенных или внешних камер.

"Кроме того, вирус DarkComet имеет кейлоггер (мониторинг нажатых клавиш), монитор буфера обмена, целый набор утилит для работы с сетью, а также предоставлял возможность злоумышленнику удаленно выключать и перезагружать пораженный компьютер. Программа использует бэк-коннект, то есть сама инициирует соединение с управляющей машиной", - сообщили в полиции…» ***(Украинский хакер взломал компьютеры в 50 странах мира // Gazeta.ua (https://gazeta.ua/ru/articles/science/_ukrainskij-haker-vzlamal-kompyutery-v-50-stranah-mira/871147). 23.11.2018).***

***

«Партия регионов заявляет, что на ее сайт, возобновивший работу 30 октября 2018 года, осуществляется ряд кибератак, которые каждый день обходятся недоброжелателям в сумму не менее 100 тыс. долларов…

«Против официального сайта Партии регионов развернулась настоящая кибервойна. За неделю количество запросов превысило 400 млн, а только, к примеру, за 19 ноября зафиксировано 67 млн атак. Работа сайта с момента возрождения партии вызывала негодование в рядах бывшего руководства и стоящих за ними олигархов. По всей видимости, смириться с тем, что рядовые члены партии смогли перехватить инициативу и задать новую стратегию развития, которая уже нашла отклик у многих единомышленников партии, для бывших руководителей оказалось невозможно», – говорится в сообщении пресс-службы.

Члены политсилы убеждены, что сайт терроризируют наемные хакеры…» ***(Партия регионов заявляет, что бывшее руководство атакует их сайт за $100 тысяч в день // RUpor.info (https://www.rupor.info/news/144035/partiya-regionov-zayavlyaet-chto-byvshee-rukovodstvo-atakuet-ih-sayt-za-100-tysyach-v-den). 26.11.2018).***

***

«Департамент киберполиции Национальной полиции Украины опубликовала инструкцию для пользователей по проверки операционной системы на наличие вируса DarkComet. Инструкцию обнародовали в Facebook.

"Рекомендуем проверить вашу операционную систему на наличие вируса DarkComet. Для этого необходимо: открыть командную строку: зажать клавишу "Windows" на клавиатуре, затем клавишу "R". Запустится окно "выполнить", в котором наберите "cmd" и нажмите ENTER или кнопку ОК. Далее, в открытой командной строке введите команду "netstat -nao" и нажмите ENTER. Вы увидите список соединений, среди которых вам нужно найти соединение с хостом 193.53.83.233 и портом 1604 или 81", - говорится в сообщении.

В случае, если пользователь найдет соединение с указанным IP адресом, в полиции рекомендуют связаться с ними через форму обратной связи.

Кроме того, при использовании компьютеров в киберполиции советуют:

- не работать и не запускать программы под учетной записью администратора системы;
- отказаться от программного обеспечения или его обновления, которое требует добавления в "список исключения" систем защиты компьютера;
- обновить антивирусное программное обеспечение и запустить полное сканирование системы и внешних носителей информации.

В случае получения тревоги от системы защиты компьютера (антивируса, фаервола и тому подобное) не следует препятствовать действиям по умолчанию антивируса или отключать автоматические обновления. Также правоохранители рекомендуют обновлять программное обеспечение и дополнительно проверять его на авторитетных ресурсах, предназначенных для анализа подозрительных файлов.» ***(Киберполиция предупредила украинцев о новом компьютерном вирусе: инструкция // Телеграф (https://telegraf.com.ua/tehnologii/4736382-kiberpolitsiya-predupredila-ukraintsev-o-novom-kompyuternom-viruse-instruktsiya.html). 23.11.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Країна-лідер у сфері розвитку та використання ІТ-технологій, Швеція… допомагає Україні підготуватись до президентських виборів, зокрема, у сфері кібербезпеки. Про це в коментарі УНН розповів Надзвичайний і Повноважний Посол Швеції в Україні, пан Мартін Хагстрьом…

"Ми щойно, лише у вересні, самі мали вибори, і ми провели велику роботу у Швеції перед нашими виборами. В даний час ведуться дискусії між нашими фахівцями та українськими фахівцями", - зазначив дипломат.

За його словами, в ході дискусій шведська сторона ділиться, зокрема, досвідом щодо роботи, проведеної шведським урядом щодо підготовки до виборів в країні…» ***(Саша Картер. Швеція та Україна проводять дискусії з кібербезпеки на тлі виборчих перегонів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1760457-shvetsiya-ta-ukrayina-provodyat-diskusiyi-z-kiberbezpeki-na-tli-viborchikh-peregoniv). 01.11.2018).***

***

«Координатор міжнародної політики з кібербезпеки у Міністерстві закордонних справ Польщі Марек Щигель заявив, що в Європейському союзі активно обговорюють запровадження механізму санкцій за проведення кібератак…

За його словами, наразі йдеться про звичайний набір інструментів ЄС для відповіді на порушення безпеки, такі як заборона на в'їзд, заморожування активів тощо…» ***(ЄС налаштований ввести санкції за кібератаки – МЗС Польщі // MediaSapiens***

(https://ms.detector.media/web/cybersecurity/es_nalashtovaniy_vvesti_sanktsii_za_kiberataki_mzs_polschi/). 08.11.2018).

***

«Україна в рамках угоди USAI ITI отримала допомогу з підвищення рівня кібербезпеки.

Також спільно з естонськими колегами розробили проект зі створення кіберлабораторії на базі однієї з військових частин ЗСУ. Про це заявив начальник військ зв'язку, начальник Головного управління зв'язку та інформаційних систем Генштабу ЗСУ Володимир Рапко…» ***(Створять кіберлабораторію на базі однієї з військових частин ЗСУ // manager (http://seabreeze.org.ua/stvoryat-kiberlaboratoriyu-na-bazi-odniyeyi-z-viyskovih-chastin-zsu/). 05.11.2018).***

***

«Другий раунд міжвідомчих українсько-американських консультацій у сфері гарантування кібербезпеки відбувся 5 листопада в Києві, повідомляється на офіційному сайті Міністерства закордонних справ України.

"У рамках заходу Україна та США підтвердили свої зобов'язання щодо гарантування відкритого, надійного та безпечного кіберпростору, домовившись про поглиблення двосторонньої співпраці у сфері кібербезпеки з метою боротьби з кіберзагрозами", - йдеться в повідомленні.

У МЗС зазначають, що підтвердженням виконання з боку США своїх зобов'язань є надання Україні технічної допомоги в розмірі $10 млн "для зміцнення кібербезпеки".

"Сторони також обговорили нові проекти допомоги, спрямовані на посилення кібербезпеки виборчих систем та критичної інфраструктури України, підтримку імплементації національної кіберстратегії України, посилення потенціалу реагування на кіберінциденти, підвищення рівня обізнаності у галузі кібербезпеки та проведення тренінгів у сферах кібербезпеки та цифрової криміналістики", - розповіли в українському зовнішньополітичному відомстві.

До складу делегації України увійшли представники МЗС, апарату РНБО, Міністерства оборони, Міністерства енергетики та вугільної промисловості, СБУ, Служби зовнішньої розвідки, Департаменту кіберполіції Нацполіції, Державної служби спеціального зв'язку та захисту інформації, Державної служби фінансового моніторингу, Національного банку, Національної виборчої комісії, Національного інституту стратегічних досліджень та Національної комісії з цінних паперів та фондового ринку.

До складу делегації США увійшли представники Державного департаменту, Міністерства оборони, Міністерства енергетики, Міністерства національної безпеки, Федерального бюро розслідувань та Агентства з питань міжнародного розвитку (USAID).» ***(Україна та США обговорили проекти посилення кібербезпеки виборчих систем і критичної інфраструктури // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/543252.html). 07.11.2018).***

***

«Вчера в своей речи на открытии 13-го Форума ЮНЕСКО по управлению Интернетом (IGF), президент Франции Эммануэль Макрон представил международное соглашение по принципам кибербезопасности. Под этим документом поставили подписи главы более 50 государств, 130 групп приватного сектора, 90 благотворительных организаций и учебных учреждений. Однако эти впечатляющие цифры не отражают истинной ситуации: в лагере неприсоединившихся к соглашению остаются самые ключевые для мировой кибербезопасности фигуры, включая Соединённые Штаты, Россию и Китай.

Не поддержали его и Иран с КНДР, которых обвиняют в создании и применении кибер-оружия, а также Израиль, занимающий лидирующее положение в индустрии кибербезопасности.

Парижский призыв к доверию и безопасности в киберпространстве (Paris Call for Trust and Security in Cyberspace) задуман как попытка привести к общему знаменателю разрозненные действия по созданию международных норм и законов, регулирующих вопросы кибернетических защиты и военных действий. На деле же он только углубил разрыв между либеральным миром и авторитарными сверхдержавами, ведущими политику ограничения свободы пользования технологиями Интернета.

Соглашение не обязывает принять какие-либо конкретные законы, оставившие под ним подпись лишь демонстрируют готовность следовать общим принципам, как-то:

- повышать уровень защиты от вредоносной онлайн-активности;
- защищать доступность и целостность Интернета;
- сообща остановить вмешательство в избирательные процессы;
- сотрудничать в борьбе с нарушениями интеллектуальной собственности через Интернет;
- предотвращать распространение вредоносных онлайн-программ и методов;
- улучшать безопасность цифровых продуктов и услуг, а также общую «кибер-гигиену»;
- сдерживать агрессивную деятельность онлайн-наёмников и негосударственных субъектов;

совместно работать над укреплением соответствующих международных стандартов…» ***(Призыв к доверию в киберпространстве принят без США, Китая и России // «Компьютерное Обозрение» (https://ko.com.ua/prizyv_k_doveriyu_v_kiberprostranstve_prinyat_bez_ssha_kitaya_i_rossii_126765). 13.11.2018).***

***

«НАТО поможет Украине обеспечить кибербезопасность на президентских выборах, заявил глава украинской миссии при альянсе Вадим Пристайко.

«Не просто готовы. Существует специальный трастовый фонд, который завершил первый этап. Страны НАТО вкладывают в это свои знания и средства,

руководит этим трастовым фондом Румыния», – сказал Пристайко в интервью «Интерфакс-Украина».

Он отметил, что определенные средства кибербезопасности, приборы и технологии уже переданы Украине, а именно МИД, СБУ и Укрспецсвязи.

На втором этапе, рассказал он, предусматривается помощь по защите серверов ЦИК для безопасного проведения выборов.

«Сейчас как раз специалисты из ЦИК, СБУ и Укрспецсвязи передали свои предложения НАТО, как аппаратную часть, так и финансовую. Могу сказать, что запросы довольно серьезные, сейчас страны-члены решают, как помочь Украине в тех объемах, которые требуются», – уточнил он…» ***(Киев обратился к НАТО за помощью на предстоящих выборах // 1NEWS.INFO (https://www.1news.info/kiev-obratilsya-k-nato-za-pomoshhyu-na-predstoyashhih-vyborah-631225). 13.11.2018).***

***

«США предоставили Украине помощь по повышению уровня кибербезопасности в Вооруженных силах Украины. Об этом сообщил начальник Главного управления связи и информационных систем Генштаба ВСУ Владимир Рапко.

…Помощь была предоставлена в рамках соглашения USA IT. На сегодняшний день ведутся работы по монтажу оборудования и инсталляции программного обеспечения в Центре оперативного реагирования на киберинциденты. "Этот проект одобрен большинством стран НАТО, сейчас мы ведем переговоры по финансированию этого проекта", - подытожил Рапко…» ***(США предоставили Украине новейшее оборудование по противодействию "бот-хакам" // Украинское рейтинговое агентство "УРА (href="http://ura-inform.com/ru/society/2018/11/10/ssha-predostavili-ukraine-novejshee-oborudovanie-po-protivodejstviju-bot-khakam). 10.11.2018).***

***

«Не антиросійська, а проестонська. Так охарактеризував політику Естонії у сфері безпеки головний виконавчий директор Міжнародного центру оборони та безпеки (ICDS) Дмитро Теперик від час зустрічі із українськими регіональними журналістами у Таллінні. Діяльність Центру Міжнародний центр оборони та безпеки є провідним аналітичним центром Естонії, що спеціалізується на тематиці оборони, безпеки та зовнішньої політики. Мета центру полягає у розвитку стратегічного мислення трансатлантичного співтовариства у відповідь на виклики безпеки в Північних і Балтійських країнах: від військової агресії та кібератак, до загроз соціального характеру та енергетичної безпеки. Щоб досягти мети, ICDS: – проводить два щорічні великі заходи з питань міжнародної оборони та безпеки – Міжнародну конференцію ім. Леннарта Мері (LMC) та Щорічну Балтійську конференцію з питань оборони (ABCD); – організовує Вищі курси з безпеки та оборони Естонії; – видає щомісячний журнал “Diplomaatia” з питань міжнародних відносин; – проводить різноманітні інформаційні заходи, щоб залучити відповідні аудиторії в Естонії, НАТО, ЄС та країнах-партнерах…

Центр не займається розвідкою, працює лише із відкритими даними та тими, що не є державною таємницею, а також не академічною установою. На сьогодні Центр налічує 21 працівника.

Співпраця із Україною Співпрацювати із Україною Центр почав ще із 2014 року, кошти на це спрямовує Естонія із державного бюджету. Ми працюємо не проти Росії, а тому, що нам цікаво щось робити разом…

У 2018 році Центр презентував рапорт результатів співпраці із 3 східними областями: Харківська, Луганська та Донецька. Однак програма до 2020 року передбачає залучення також Херсонської та Миколаївської областей. Ми створюємо в Маріуполі, Херсоні, Миколаєві та Сєвєродонецьку інформаційні хаби. Це не класичні тренінги. Ми хочемо проводити хакатони, будемо залучати студентів місцевих вузів, для того щоб разом шукати нестандартне рішення існуючих в регіоні проблем безпеки. Ми будемо працювати з міськими радами, цивільним активом…

До 2020 року експерти Центру виокремлюють три основні напрямки співпраці із Україною: кібербезпека, інформаційна безпека, комунікаційна безпека…

Про вплив Росії За словами Теперика, Росія, як не прикро визнавати, досі використовує Україну як полігон відпрацювання методів ведення підпільної війни – як впливати на суспільну думку…» ***(Олена Шаповал. Чого нам не можна робити – так це розслабитись і думати, що найгірше позаду, – експерт естонського Центру оборони та безпеки // Infomist (https://infomist.ck.ua/chogo-nam-ne-mozhna-robyty-tak-tse-rozslabytys-dumaty-shho-najgirshe-pozadu-ekspert-estonskogo-tsentru-oborony-ta-bezpeky/). 29.11.2018).***

***

«Відповідаючи на запитання журналістів після завершення зустрічі з Генеральним секретарем НАТО Єнсом Столтенбергом, голова українського парламенту наголосив, що дуже важливо отримати підтримку з боку НАТО у питанні кібербезпеки, особливо напередодні виборів…

За словами голови Верховної Ради, з Генсеком було обговорено широке коло питань, зокрема кібербезпеку. "І ми проговорили збільшення трастового фонду, через який НАТО допомагає України в питанні кібербезпеки", – розповів Парубій, повідомивши, що сторони домовилися про збільшення фінансування цієї лінії задля підтримки України…» ***(НАТО збільшить фінансову допомогу Україні в питанні кібербезпеки // UA|TV (https://uatv.ua/nato-zbilshyt-finansovu-dopomogu-ukrayini-v-pytanni-kiberbezpeky/). 28.11.2018).***

***

«…група чеських фахівців із кібербезпеки повернулася з прифронтової зони, де вони не лише ділилися своїм досвідом, але і уважно вивчали український…

Близько місяця тому чеські волонтери проїхали з низкою лекцій та тренінгів для всіх, кого цікавлять питання кібернетичної безпеки, майже по всій лінії

розмежування на Донбасі, починаючи з Маріуполя, і через Луганську область доїхали аж до Харкова…

Як каже Томаш Флідр, якщо раніше цю роботу група активістів робила безкоштовно, то тепер вони отримали ґрант від Вишеградського фонду, бо досвід, який має зараз Україна, є унікальним, і європейські організації зрозуміли, що напади на Україну не конче завершаться на українських кордонах…

Найважливішою інформацією для чехів Томаш Флідр назвав напади на критичну інфраструктуру України, яких було декілька і які показали, наскільки вразливими можуть бути головні об'єкти постачання електроенергії, якщо її вразить кібернетичний напад зловмисників…» ***(Марія Щур. Чеські спеціалісти з кібербезпеки проводили курси для українців на лінії фронту // Радіо Свобода (https://www.radiosvoboda.org/a/kiberbezpeka-ukrajina-chexija/29600746.html). 14.11.2018).***

***

«Глава департамента уголовного розыска национальной полиции Украины Сергей Князев и начальник главного управления полиции Индонезии Тито Карнаван договорились о расширении сотрудничества в области кибербезопасности…

Сотрудничество будет осуществляться путем обмена информацией и опытом в области полицейской деятельности…

Индонезийские представители подчеркнули, что сотрудничество в сфере кибербезопасности с Украиной еще больше укрепит и повысит готовность национальной индонезийской полиции к различным потенциальным кибератакам в стран.» ***(Украина расширит сотрудничество с Индонезией в области кибербезопасности // «Украина по-арабски» (http://arab.com.ua/ru/ukraina-rasshirit-sotrudnichestvo-s-indonezie-v-oblasti-kiberbezopasnosti). 21.11.2018).***

***

«21 листопада міністр оборони України Степан Полторак і державний секретар із питань оборони Великобританії Гевін Вільямсон домовилися поглибити співпрацю з протидії агресії Росії та гібридним загрозам.

За підсумками зустрічі в Лондоні вони прийняли спільну заяву, повідомляється на сайті Міноборони України.

Оборонні відомства зокрема наголосили, що агресія проти України зі сторони Російської Федерації є безпосередньою загрозою євроатлантичній безпеці та викликом існуючій системі міжнародних відносин й домовились поглибити співробітництво з протидії її злочинній діяльності та підривним діям проти заснованої на міжнародному праві системи безпеки на території України, у Великій Британії та інших країнах.

«Сторони погодилися щодо впровадження таких форм подальшої співпраці: підтримання постійного діалогу між оборонними відомствами двох держав; поглиблення співпраці в питаннях кіберзахисту, протидії гібридним загрозам та воєнної розвідки; збільшення консультативно-дорадчої допомоги Україні з боку Великої Британії; посилення воєнно-дипломатичного представництва Великої

Британії в Україні», —йдеться в заяві…». ***(Очільники оборонних відомств України та Британії домовилися протидіяти кіберзагрозам // MediaSapiens (https://ms.detector.media/web/cybersecurity/ochilniki_oboronnikh_vidomstv_ukraini_ta_britanii_domovilisya_protidiyati_kiberatakam_rf/). 21.11.2018).***

***

Світові тенденції в галузі кібербезпеки

«США, Китай и Россия отказались одобрить продвигаемое Францией соглашение, направленное на регулирование интернета и укрепление кибербезопасности, несмотря на то, что его поддержала 51 страна, в том числе все члены ЕС.

"Парижский призыв к доверию и безопасности в киберпространстве", с которым выступил президент Франции Эммануэль Макрон в понедельник, представляет собой попытку установить четкие правила применения кибер-вооружений.

На мероприятии, организованном ЮНЕСКО, французский лидер изложил свои устремления в целях укрепления международного регулирования интернета и усовершенствования сотрудничество по борьбе с кибератаками, зарубежным вмешательства в выборы, онлайн-цензурой и ненавистническими высказываниями.

Но отказ Вашингтона, Москвы и Пекина от подписания соглашения – это серьезный удар по инициативе…

Президент Макрон заявил, что намерен продолжать давление на США и другие страны, добиваясь подписания соглашения. Хотя администрация Трампа в настоящее время не поддерживает эту инициативу, американские технологические компании, такие как Google, Facebook и Microsoft, выступили "за".

Президент компании Microsoft Брэд Смит в понедельник выразил обеспокоенность в связи с тем, что в потенциале кибер-оружие может вызвать многосторонний конфликт…

Инициатива Макрона появилась после того как в 2017 году провалились переговоры в ООН, посвященные регулированию киберпространства – тогда ряд стран воспротивились установлению правил для передовых систем вооружений.

Новый договор между пятьдесят одной страной, подписанный также 218 компаниями, гласит, что технологические компании должны нести ответственность за "повышение доверия, безопасности и стабильности в киберпространстве".

Предполагается разработка других "совместных мер", направленных в том числе на предотвращение "злонамеренной кибер-деятельности" и кражи коммерческой тайны при помощи взлома и программного обеспечения".

Соглашение призвано также обеспечить безопасный доступ людей к интернету и предотвратить распространение вредоносного онлайн-программного обеспечения.» ***(The Telegraph: США, Россия и Китай отказываются поддержать инициативу Франции в области кибербезопасности // «Новости онлайн 24» (https://newsonline24.com.ua/the-telegraph-ssha-rossiya-i-kitaj-***

otkazyvayutsya-podderzhat-iniciativu-francii-v-oblasti-kiberbezopasnosti/). 14.11.2018).

***

«Кибербезопасность, скачок цен на энергоносители и провал национального руководства являются одними из крупнейших угроз для бизнеса в 2018 году…

Исследователи обнаружили значительные различия в восприятии рисков в разных регионах мира. Например, кибератаки считались риском номер один для руководителей в Европе и странах с развитой экономикой, в то время как крах правительства был главной проблемой для Латинской Америки…

Отчет Всемирного экономического форума показал, что опасения по поводу технологических рисков растут, а кибератаки называют главной проблемой для руководителей в трех из восьми охваченных регионов. В 2016 году только один регион — Северная Америка — назвал кибератаки самой большой угрозой для бизнеса…

По словам главы отдела глобальных рисков Zurich Insurance Group Лори Бейли, результаты исследования указывают на необходимость действий со стороны правительства.

"Кибератаки рассматриваются как риск номер один для ведения бизнеса на рынках, на долю которых приходится 50% мирового ВВП. Это наводит на мысль о том, что правительствам и предприятиям необходимо укреплять кибербезопасность, чтобы поддерживать доверие к высокоразвитой цифровой экономике", — заявила Бейли…» ***(Украина находится в наивысшей зоне рисков для государства // Goodnews.ua (http://goodnews.ua/technologies/ukraina-naxoditsya-v-naivysshej-zone-riskov-dlya-gosudarstva/). 13.11.2018).***

***

«Cisco обнародовала результаты отчета по кибербезопасности среди компаний малого и среднего бизнеса (SMB Cybersecurity Report), в котором приняли участие 1816 респондентов из 26 стран. По результатам исследования, более 53% небольших предприятий в 2018 году подвергались кибератакам, 20% из них заявили об ущербе в размере от 1 до 2,5 млн долларов. Данные получены в ходе исследования решений по обеспечению информационной безопасности Cisco 2018 Security Capabilities Benchmark.

В ходе исследования 53% респондентов заявили, что их компании подвергались вторжениям, повлекшим существенные финансовые издержки. Например, кибератаки часто провоцируют простой рабочих систем, в результате чего снижаются продуктивность и прибыльность бизнеса. По данным отчета, у 40% респондентов (предприятия с численностью 250-499 сотрудников) в прошлом году в результате серьезных атак случались 8-часовые простои. Как минимум половина систем пострадала в результате той или иной серьезной атаки у 39% респондентов.

Другие примечательные результаты отчета:

• 30% средних компаний сообщили, что вторжения обошлись им менее чем в 100 тыс. долл., тогда как 20% назвали суммы от 1 млн. до 2 499 999 долл.;

• компании СМБ (средний и малый бизнес) получают от систем безопасности до 5 тыс. уведомлений в день;

• средние компании расследуют 55,6% уведомлений;

• направленные на сотрудников атаки типа фишинга (79%), APT-угрозы (77%), вымогательское ПО (77%), DDoS-атаки (75%) и распространение BYOD (74%) являются для компаний СМБ пятью главными источниками проблем в области безопасности.

На фоне всеобщей озабоченности программами-вымогателями эксперты Cisco полагают, что значимость этой угрозы уменьшается в связи с тем, что все больше злоумышленников переключаются на незаконную добычу криптовалют (криптомайнинг). Привлекательность такого рода деятельности обусловлена тремя факторами: потенциально высокая доходность, невозможность отслеживания платежей и сравнительно невысокая тяжесть наказания в случае уголовного преследования…

Борясь с угрозами, компании инвестируют в технологии и кадры. При наличии достаточных кадровых ресурсов, прежде всего, решались бы следующие задачи:

• самый частый ответ — модернизация защиты оконечных точек с применением решений AMP/EDR (Advanced Malware Protection/Endpoint Detection and Response) — 19%;

• внедрение более совершенных приложений для защиты от веб-атак — 18%;

• внедрение технологии предотвращения вторжений, которая по-прежнему рассматривается в числе необходимых для отражения сетевых атак и внедрения эксплойтов — 17%...

Малым и средним предприятиям приходится сталкиваться с проблемами, обусловленными нехваткой квалифицированного ИБ-персонала, и они стараются максимально наращивать свои ограниченные ресурсы. Более половины компаний обращаются к партнерам по аутсорсингу за такими услугами, как рекомендации и консультации, реагирование на инциденты и мониторинг безопасности. В то же время такие задачи, как исследование угроз (Threat Intelligence), отдаются на аутсорсинг не столь часто (39%)…» ***(Медуна. Cisco представляет отчет по кибербезопасности среди предприятий малого и среднего бизнеса // <META> - Украина (http://pr.meta.ua/read/55428). 09.11.2018).***

***

«Страхование профессиональной ответственности перед третьими лицами (D&O) и киберстрахование тесно взаимосвязаны в условиях современных технологий и их влияния на бизнес-модели. Об этом сообщили в официальном заявлении Airmic, Marsh и AIG.

…руководители фирм должны понимать существующую тесную взаимосвязь защиты компании от кибернетического риска и собственной профессиональной ответственности.» ***(Риск профессиональной ответственности тесно связан с кибер рисками: отчет Airmic // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/risk-professionalnoy-otvetstvennosti-tesno-svyazan-s-kiber-riskami-otchet-airmic). 05.11.2018).***

***

«Безопасность пользователей все еще оставляет желать лучшего. Об этом говорится сразу в двух исследованиях, опубликованных компаниями eSentire и Proofpoint. И как указывают эксперты, несоответствие степени угрозы и уровня защиты пользователей может привести к серьезным утечкам данных либо к финансовым потерям как для отдельных лиц, так и для компаний…

Предприятия в два с половиной раза чаще становятся жертвами фишинговых атак со вторника по четверг, на каждых 33 сотрудника приходится одна фишинговая атака в квартал, а самый распространённый способ сокрытия вредоносного ПО – маскировка под «счет-фактуру». Об этом говорится в ежеквартальном отчете о киберугрозах eSentire 2018 Q2.

Исследователи указывают, из-за своей простоты и эффективности фишинг по-прежнему остается популярным и широко применяемым методом атаки. Чаще всего угрозы направлены на Office 365 и DocuSign, хотя общее количество попыток их использования уменьшилось. А с приближением праздничного сезона следует ожидать увеличения количества фишинговых электронных писем, замаскированных под корреспонденцию от UPS, eFax и FedEx, поскольку злоумышленники попытаются извлечь выгоду из растущего интереса к онлайн-покупкам.

Аналитики компании также отметили резкое увеличение количества атак на Microsoft Internet Information Services (IIS), с двух тысяч в первом квартале до 1,7 млн – во втором. Рост произошел в основном за счет взломанных серверов Tencent и Alibaba. Тренд получил продолжение и в третьем квартале. Кроме этого, Drupal и Oracle Web Logic подверглись атакам с использованием таких эксплойтов, как Drupalgeedon2 и EternalBlue. Наиболее распространенным выявленным вредоносным ПО стали Panda Banking Trojan и Emotet…

Потребителям по-прежнему не хватает понимания основ кибербезопасности. Об этом говорится в отчете Proofpoint, посвященному рискам, с которыми столкнулись пользователи в 2018 г. Для анализа эксперты компании использовали результаты опроса 6000 работающих взрослых, проведенного в Германии, Франции, Италии, Великобритании, США и Австралии.

Исследование показало, что многие респонденты имеют ограниченное понимание общих рисков кибербезопасности и не принимают достаточных мер для надлежащей защиты своих данных, устройств и систем. Так, более 60% не знают о программах-вымогателях, а 32% не понимают, что такое вредоносное ПО. 44% респондентов не защищают паролем свои домашние сети Wi-Fi, а 66% не изменили пароль, установленный по умолчанию на своих маршрутизаторах. 33% респондентов из США столкнулись с кражей личных данных и эта цифра превышает среднемировое значение более, чем в два раза.

Треть опрошенных заявили, что используют менеджер паролей. Из тех, кто этого не делает, 21% признались, что они применяют один или два пароля для всех своих учетных записей в интернете. Кроме того, 55% респондентов, чей работодатель предоставляет им устройство для использования дома, дают к нему доступ своим друзьям и членам семьи – разрешают проверять почту, общаться в

соцсетях, играть и заниматься шоппингом. Для фирм, сотрудники которых работают из дома или по схеме BYOD (bring your own device – принеси свое устройство), это может иметь серьезные последствия.

«Более 99% всех целевых кибератак опираются на использование человеческого фактора, и наш отчет указывает на пробелы в осведомленности пользователей о мерах безопасности. Они требуют немедленного реагирования для построения адекватной защиты, – рассказал Джо Феррара (Joe Ferrara), генеральный директор Wombat Security, одного из подразделений Proofpoint…». ***(В 99% кибервзломов виноваты сами пользователи // Goodnews.ua (http://goodnews.ua/technologies/v-99-kibervzlomov-vinovaty-sami-polzovateli/). 02.11.2018).***

***

«Согласно новому докладу Всемирного экономического форума (World Economic Forum, WEF), который был подготовлен совместно с Zurich Insurance Group и Marsh&McLennan, главным риском для бизнеса являются кибернетические атаки.

…в опросе приняли участие более 12,5 тысяч топ-менеджеров компаний из разных мировых регионов. Смысл опроса состоял в том, чтобы из перечня 30 видов глобальных рисков выделить наиболее серьезные для ведения бизнеса.

В результате выяснилось, что руководители североамериканских компаний единодушно на первое место по масштабности воздействия на бизнес поставили угрозу кибератаки…

WEF сообщает, что кибератаки воспринимаются главной угрозой также топ-менеджерами из европейских и азиатских компаний.» ***(Руководители мировых компаний назвали кибератаки главной угрозой для бизнеса // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/rukovoditeli-mirovyih-kompaniy-nazvali-kiberataki-glavnoy-ugrozoy-dlya-biznesa). 12.11.2018).***

***

«Призовой фонд в размере $18 тыс. разыграли команды экспертов в сфере этичного хакинга из России, Венгрии, Польши, Южной Кореи, Украины и Китая в минувшую пятницу. Розыгрыш прошел в рамках финала ежегодных международных соревнований CTFZONE, организованных дочерней компанией Сбербанка Bi.Zone, сообщили в пресс-службе Банка.

…мероприятие состоялось в рамках Международной конференции по практической кибербезопасности OFFZONE, проходившей в Москве 15-16 ноября. Ее организатором также выступила Bi.Zone.

В отборочном этапе соревнований… приняли участие более 1 тыс. команд из 50 стран. Однако в финальную часть вышли лишь лучшие 10 команд из России, Венгрии, Польши, Южной Кореи, Украины и Китая.

…перед ними стояла задача обнаружить в сервисах противников как можно больше слабых мест. Но это – не все. При этом нужно было с максимальной эффективностью отражать кибератаки соперников, которые также искали слабые места.

В результате первое место и $10 тыс. достались российской команде Bushwhackers. «Серебро» и $5 тыс. – опять же, нашим соотечественникам из LC⚡BC. «Бронзовые» же награды и $3 тыс. отправились вместе с командой p4 в Польшу…» ***(Лучшие эксперты в сфере этичного хакинга сразились на международном турнире в Москве // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3804637?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 19.11.2018).***

***

«Опрос, проведенный компанией по кибербезопасности Trend Micro, показал, что 86% ИТ-специалистов и экспертов в области безопасности во всем мире считают, что их организациям необходимо повысить уровень осведомленности об угрозах IoT…

Причина - в отсутствии знаний, растущем уровне угроз и проблемах безопасности, связанных с подключенными устройствами, которые ставят организации в компрометирующее положение.

Trend Micro опросил 1150 лидеров ИТ, которые выявили отсутствие кибербезопасности во многих организациях по всему миру, развертывающих проекты IoT для внедрения инноваций и цифровых трансформаций…

Управление уязвимостями и мониторинг аномального поведения являются главными требованиями для снижения риска компрометации устройств IoT. Trend Micro предлагает комплексный подход к защите сети для таких организаций, гарантируя необходимый уровень безопасности.

Согласно другому исследованию, проведенному Dynatrace в августе, хоть потребители по-прежнему заинтересованы в устройствах IoT, две трети из них признают, что они уже столкнулись с проблемами производительности и потенциальным риском.

Наиболее очевидным примером этой проблемы являются автономные автомобили, причем 85% обеспокоены тем, что эти транспортные средства могут выйти из строя, а 72% уверены, что программные сбои в них могут привести к серьезным травмам и летальным исходам. 84% заявили, что не будут ездить на автономных авто из-за страха программного сбоя.» ***(Ирина Фоменко. Мир не осознает угрозы от Интернета верей // Internetua (http://internetua.com/mir-ne-osoznaet-ugrozy-ot-interneta-vesxei). 23.11.2018).***

***

«…У 2018 році втрати бізнесу від кібератак становили 600 млрд дол, а до 2021 року світова економіка буде втрачати з вини кіберзлочинців 6 трлн дол на рік.

Такі цифри навів на зустрічі закритого клубу інвесторів iClub співзасновник і CEO екосистеми Hacken Дмитро Будорін, посилаючись на дані McAfee і Cybersecurity Ventures…

З огляду на темпи зростання кіберзлочинності, витрати на інформбезпеку — ІБ — теж збільшуються. У 2018 році вони становили 96 млрд дол, що на 17% більше, ніж у 2017 році… Як стверджує Будорін, цей ринок буде рости.

Підприємець також зазначає, що зараз важливо вкладати кошти в розробку інструментів та методів захисту, формування нових підходів. Причина проста: сфера кібератак розвивається швидше, ніж галузь ІБ, і, щоб мати "щит" завтра, виділяти кошти на його створення потрібно вже зараз…

…українська платформа етичного зламування має величезні перспективи на азійському ринку. У багатьох країнах регіону не довіряють американським платформам з політичних причин. Вибираючи між американською та європейською платформами, виберуть європейську (українську).

Ринок послуг і продуктів у сфері кібербезпеки зростає, тому що зростає ринок кіберзагроз. Оскільки "чорні" хакери зупинятися не збираються, навчання "білих" хакерів і робота з ними — дуже перспективний напрямок.

Україна має всі шанси стати європейським лідером у цій галузі та одним з ключових гравців у світі, але для цього потрібно максимально ефективно використовувати наявні напрацювання і не зупинятися ні на секунду.» ***(Ная Новак. Дорогі кіберзлочинці: що таке ринок кібербезпеки і чому він так швидко росте //Економічна правда (https://www.epravda.com.ua/publications/2018/11/20/642805/). 20.11.2018).***

***

«Служащие компаний не горят желанием инсталлировать на свои мобильные устройства приложения, предоставляемые работодателем, но одновременно с этим они все чаще устанавливают на своих рабочих местах программы, изначально ориентированные на использование в личных целях.

…Как говорится в отчете, опубликованном CCS Insight, 74% работников крупных организаций возражают против принудительной установки ПО для рабочих целей на свои гаджеты. В рамках этого исследования эксперты опросили представителей предприятий, расположенных в США и Западной Европе, для определения их отношения к таким цифровым технологиям, как искусственный интеллект и «умные помощники», мобильность бизнеса и устройств, а также по вопросам кибербезопасности, конфиденциальности и доверия.

В частности, выяснилось, что большинство респондентов возмущены идеей использования рабочих приложений на своих персональных устройствах из-за опасения, что работодатели могут следить за ними. По этой же причине 54% сотрудников сказали, что им будет некомфортно, если компания усилит мониторинг безопасности устройств и приложений на рабочем месте. Однако вместе с тем две трети опрошенных заявили, что доверяют своим нанимателям в вопросах конфиденциальности и защиты персональных данных.

Одновременно с этим авторы исследования отмечают, что, возможно, самым большим разочарованием для организаций в последние годы стал рост использования так называемых «теневых технологий» (Shadow IT – приложения и информационные системы, применяемые без ведома и одобрения ИТ-отделов компании). Поскольку границы между работой и личной жизнью становятся все

более прозрачными, сотрудники все чаще приносят потребительские или недорогие ИТ-решения на свои рабочие места.

Один из наиболее ярких примеров этой тенденции – рост числа общедоступных сторонних мобильных приложений, применяемых бизнесом. Согласно результатам опроса, WhatsApp в настоящее время является наиболее популярным приложением среди сотрудников компаний. О его использовании заявили 30% респондентов. Приложения под Microsoft Office 365 установлены у 29% опрошенных, G Suite от Google и Dropbox занимают третью позицию с 22% каждый. Amazon отметили 19%, а Skype и Facebook – 14% респондентов…

Кроме этого в отчете CCS Insight указывается, почти треть респондентов уже используют на своем рабочем месте цифровых помощников, таких как Amazon Alexa, Google Assistant, Microsoft Cortana и Apple Siri. Еще 51% рассматривают такую возможность…

Вместе с тем все больше компаний стремятся отойти от традиционной ИТ-среды на рабочем месте к более гибкой и мобильной стратегии организации рабочего пространства. 71% организаций уже внедрили или рассматривают возможность внедрения подхода «принеси свое устройство» (bring your own device – BYOD). Об этом говорится в совместном исследовании, опубликованном компаниями Capita и Citrix. Из тех предприятий, которые используют парадигму BYOD, 92% опрошенных считают, что это повысило производительность труда сотрудников, одновременно с этим 87% респондентов признали, что возросли и риски безопасности, 89% рассказали о росте нагрузки на ИТ-поддержку и 88% – о проблемах в управлении ИТ.

91% ИТ-директоров заявили, что пользовательский опыт важен для привлечения и удержания новых талантов, хотя в подавляющем большинстве организаций (83%) говорят, что они, как правило, узнают о таком ИТ-опыте сотрудников через звонки в службу поддержки.

И как указывается в отчете Cisco 2018 Security Capabilities Benchmark, в этом году более половины небольших предприятий подверглись кибератакам. 20% из них заявили об ущербе в размере от 1 до $2,5 млн, еще треть – что вторжения обошлись им не менее чем в $100 тыс. И, по мнению экспертов Cisco, пятью главными угрозами для компаний среднего и малого бизнеса стали: фишинговые атаки (79%), APT-угрозы и вымогательское ПО, (77%), DDoS-атаки (75%) и распространение BYOD (74%).» ***(Сотрудники компаний не хотят устанавливать рабочие приложения на личные гаджеты // Goodnews.ua (http://goodnews.ua/technologies/sotrudniki-kompanij-ne-xotyat-ustanavlivat-rabochie-prilozheniya-na-lichnye-gadzhety/). 25.11.2018).***

***

«Руководитель практик консалтинга в области кибербезопасности британской оборонной компании BAE Systems Робин Олдхэм представил исследование, проведенное совместно с межбанковской системой передачи информации и совершения платежей Swift. В отчете компаний говориться о влиянии кибератак на мировой финансовый рынок.

По словам Олдхэма, группы, совершающие целевые продолжительные атаки повышенной сложности (APT), все чаще работают от лица коммерческих организаций.

Жертвами банковских троянов всегда становятся клиенты банков. Растет уровень сложности этих атак из-за потенциально высокого вознаграждения создателей этих вирусов. Робин Олдхэм, руководитель практик консалтинга в области кибербезопасности BAE Systems

Согласно отчету BAE Systems и Swift, рынок капитала с его разнообразными структурами является особо уязвимым для киберпреступников. В частности, под большой угрозой находятся владельцы ценных бумаг…» ***(Названа следующая финансовая мишень для киберпреступников // Goodnews.ua (http://goodnews.ua/technologies/nazvana-sleduyushhaya-finansovaya-mishen-dlya-kiberprestupnikov/). 20.11.2018).***

***

«Страховой продукт под названием CyFly от международного страхового и перестраховочного брокера Willis Tower Watson предназначен специально для покрытия кибернетических рисков для аэропортов.

…Страховой продукт CyFly компания называет инновационным решением, которое доступно для клиентов во всем мире и включающее покрытие, которое не входит в традиционную программу киберстрахования.

В частности, страховой программой покрываются потери в результате перебоев в работе, сбоев, причиненных третьими лицами, в сетях которых используются аэропорты. Страховкой также покрываются расходы на подготовку претензий, штрафные санкции в сфере кибербезопасности и другое…» ***(Инновационный страховой продукт для киберзащиты аэропортов предлагает WTW // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/innovatsionnyiy-strahovoy-produkt-dlya-kiberzashhityi-aeroportov-predlagaet-wtw). 20.11.2018).***

***

«По мнению группы инженеров Айовского университета, практикуемое сейчас разделение кибератак на сети энергоснабжения по серьёзности на три уровня — высокий, средний и низкий — является недопустимо приблизительным.

Чтобы предложить на смену этому качественному подходу к оценке динамических и неопределённых рисков более точный, количественный метод, профессор компьютерных технологий Манимаран Говиндарасу (Manimaran Govindarasu) вместе с коллегами прибег к теории игр.

Задачей трёхлетнего проекта, на который Национальным научным фондом выделено 777 тыс. долл., будет разработка моделей для анализа и прогнозирования угроз, уязвимостей и последствий. Участники проекта уже имеют опыт применения математического аппарата теории игр к другим задачам, связанным с приложениями для дронов и кластеров роботов.

В конкретном случае энергосистемы, она может рассматриваться как поле игры между двумя противниками: операторами и хакерами. Первые хотят сохранить компьютеры и средства управления в безопасности за брандмауэрами с надёжными аутентификацией и механизмами контроля доступа. Вторые хотят обойти эту защиту и саботировать работу энергосистемы…

Игровые математические модели оперируют такими понятиями как «оптимальность» или «что лучшее я могу сделать?» в любом данном сценарии. В условиях ограниченных ассигнований на безопасность они представляют собой мощный инструмент для разработки стратегий защиты энергосистем.

Важными задачами проекта являются разработка практичного инструментария для индустрии, а также его адаптация для других кибер-физических инфраструктур, таких как нефте/газопроводы и транспортная сеть.» ***(В оценке опасности кибератак на энергосети поможет теория игр // «Компьютерное Обозрение» (https://ko.com.ua/v_ocenke_opasnosti_kiberatak_na_jenergoseti_pomozhet_teoriya_igr_126959). 28.11.2018).***

***

«Кибератаки, а также полная или частичная потеря данных воспринимаются топ-менеджерами как наиболее важные риски для деятельности компании вообще и репутационной составляющей старших менеджеров, в частности.

Об этом… известно из отчета компании по управлению рисками Willis Towers Watson, подготовленного совместно с юристами Allen&Overy.

Сообщается, что более половины публичных компаний в течение 2018 года испытали на себе либо хакерскую атаку, либо потерю данных. По сравнению с результатами 2017 года, когда этот показатель составил 30%, наблюдается значительное увеличение инцидентов, связанных с цифровой защитой данных.

Участники опроса считают, что риск кибератаки и потери данных являются разрушительными не только для бизнеса, но и вредят имиджу и профессиональной репутации руководителей высшего звена…» ***(Хакерские атаки и потеря данных — главные угрозы для бизнеса и репутации // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/hakerskie-ataki-i-poterya-dannyih-glavnyie-ugrozyi-dlya-biznesa-i-reputatsii). 27.11.2018).***

***

Сполучені Штати Америки

«…Исследователи по кибербезопасности обнаружили в открытом доступе сервер Палаты представителей США. Информацию об этом на своей странице в Facebook опубликовал специалист по кибербезопасности, ведущий разработчик компании ИТ Лаборатория Александр Галущенко…

– Сервер Палаты представителей США (палата Конгресса США) содержит множество внутренних документов, а также конфигурационные файлы, логины и

пароли к другим серверам (таким как joyce.house.gov, long.house.gov, neal.house.gov, carter.house.gov). И все это добро лежит в открытом доступе, – написал эксперт. – Из конфигурационных файлов следует, что все поддомены используют drupal и одну базу данных, к которой подключаются под пользователем root с паролем, который тоже утек...» ***(Владимир Кондрашов. Сервер Палаты представителей США доступен хакерам // Internetua (http://internetua.com/server-palaty-predstavitelei-ssha-dostupen-hakeram). 07.11.2018).***

***

«Секретарь штата Джорджия Брайан Кемп заявил, что начато расследование в отношении отделения Демократической партии США по подозрению в попытке взлома электронной системы регистрации избирателей…

Власти штата уже поставили об этом в известность ФБР, однако отмечается, что никаких доказательств кибератаки не предоставлено.

Демократы в ответ заявили, что эти "безобразные утверждения на 100% ложны" и являются примером злоупотребления властью секретаря Кемпа. Ранее его уже обвиняли Кемпа в превышении полномочий и конфликте интересов, призывая его уйти в отставку…» ***(Власти Джорджии обвинили демократов в кибератаке на систему регистрации избирателей // Информационное Агентство 112.ua (https://112.ua/mir/vlasti-dzhordzhii-obvinili-demokratov-v-kiberatake-na-sistemu-registracii-izbirateley-468478.html). 05.11.2018).***

***

«…Управление национальной защиты и программ Министерства внутренней безопасности США (NPPD) уже совсем скоро может получить новое название. Во вторник, 13 ноября, члены Палаты представителей Конгресса США единогласно проголосовали за принятие законопроекта, кодифицирующего деятельность NPPD и присваивающего управлению новое, более походящее название.

Согласно законопроекту, в связи с новыми задачами NPPD будет называться Агентством по обеспечению кибербезопасности и безопасности инфраструктуры (Cybersecurity and Infrastructure Security Agency, CISA). Сенат одобрил законопроект в октябре, и для окончательного его принятия документ должен быть подписан президентом Дональдом Трампом.

В настоящее время NPPD является главным органом, занимающимся обеспечением защиты правительственных сетей и критической инфраструктуры от киберугроз…» ***(Управление национальной защиты США получит более кибер-ориентированное название // SecurityLab.ru (https://www.securitylab.ru/news/496549.php). 16.11.2018).***

***

«Представники уряду США в останні декілька тижнів намагаються переконати свої країни-союзники не використовувати обладнання китайської компанії Huawei Technologies через загрозу кібератак…

Американські чиновники інформували своїх урядових колег та керівників телекомунікаційних компаній у дружніх країнах, де обладнання Huawei вже широко використовується, включаючи Німеччину, Італію та Японію, про те, що вони вбачають в китайському обладнанні ризики кібербезпеки…

Зокрема, представники уряду США розглядають питання фінансування телекомунікаційної сфери країн, що відмовляються від виробництва китайського обладнання.

США також розглядають питання щодо збільшення фінансової допомоги для розвитку телекомунікацій у країнах, які ухиляються від виробництва китайського обладнання…

Особливу увагу представники уряду США приділяють до країн, де знаходяться американські військові бази.

…у Сполучених Штатах вважають, що Китай може, завдяки своєму обладнанню у великих компаніях, проводити кібератаки або займатись електронним шпигунством у телекомунікаційній мережі.

Також у Вашингтоні побоюються, що КНР може зламати мережі, де встановлене дане обладнання.

Дані побоювання з'явились на тлі того, як країни по всьому світу готуються закупати обладнання для 5G — майбутнє покоління мобільних технологій.

…Сполучені Штати готові до холодної війни з Китаєм в разі, якщо Пекін не змінить свою політику…» ***(Ілля Нежигай. США переконують країни-союзники відмовитись від китайської техніки Huawei // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1763836-ssha-perekonuye-krayini-soyuzniki-vidmovitis-kitayskoyi-tekhniki-huawei). 23.11.2018).***

***

«Сооснователь Apple Стив Возняк представил проект «цифрового института» Woz U в октябре прошлого года. Онлайн-школа программирования предлагала людям без предварительной подготовки пройти курс и за 33 недели освоить разработку ПО, кибербезопасность или стать дата-аналитиком. Позднее создатели проекта планировали выйти в офлайн и открыть 30 школ в США.

Возняк обещал, что студенты Woz U будут на равных конкурировать с выпускниками американских вузов, а также смогут сохранить работу в условиях автоматизации.

Стоимость курса — $13 200. Однако… за такую цену студенты получили слабую учебную программу, в материалах которой постоянно встречаются фактические ошибки и опечатки, в том числе в строчках кода. Кроме того, тексты содержат гиперссылки на документы Microsoft и даже на статьи в Wikipedia…

По словам бывших сотрудников, руководство Woz U требовало привлекать как можно больше клиентов, не заботясь о качестве программы…» ***(Кирилл Иртлач. Цифровой университет Woz U обвинили в некачественной программе обучения // ITC.ua (https://itc.ua/blogs/tsifrovoy-universitet-woz-u-obvinili-v-***

nekachestvennoy-programme-obucheniya/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 28.11.2018).

***

Країни ЄС

«…В объединенном комитете по стратегии национальной безопасности парламента Великобритании подготовлен доклад с предложением ввести на уровне секретариата кабинета министров пост министра кибербезопасности, которому будет поручена организация мер по защите инфраструктуры страны от основных киберугроз. В настоящее время ответственность за это лежит на чиновниках более низкого уровня, тогда как главы соответствующих министерств лишь изредка проверяют их работу. Создание министерского поста позволит создать единую стратегию защиты инфраструктуры, полагают члены парламента. Министр кибербезопасности должен занять место в совете национальной безопасности и ему должны быть подотчетны отраслевые министерства…» ***(В британском парламенте обсуждают введение поста министра кибербезопасности // «Открытые системы» (https://www.computerworld.ru/news/V-britanskom-parlamente-obsuzhdayut-vvedenie-posta-ministra-kiberbezopasnosti). 21.11.2018).***

***

«Главы военных ведомств стран Евросоюза договорились о запуске новых проектов в сфере безопасности, сообщила пресс-служба Совета ЕС.

…страны ЕС согласовали обновленную версию рамочного документа по политике в сфере кибербезопасности. В частности, ЕС намерен во время учений «адекватным образом» отрабатывалась способность европейских структур «реагировать на кибернетические и гибридные кризисы»…» ***(Антон Антонов. Страны ЕС собрались создать Совместную разведывательную школу // Деловая газета «Взгляд» (https://vz.ru/news/2018/11/20/951383.html). 20.11.2018).***

***

«Рада ЄС у закордонних справах затвердила оновлену версію політики ЄС у сфері кібербезпеки.

"Оновлення дозволяє ЄС враховувати мінливі проблеми безпеки, оскільки первісна рамкова політика була прийнята в 2014 році. Воно визначає пріоритетні галузі кібероборони і роз'яснює ролі тих, хто бере участь у цьому процесі", - повідомила прес-служба Ради ЄС за підсумками його засідання в понеділок у Брюсселі.

У комюніке також наголошується співпраця ЄС, яка розширюється щодо посилення можливостей кібербезпеки.» ***(ЄС поновив політику кібербезпеки // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/546233.html). 20.11.2018).***

***

Китай

«Китай порушує досягнуті зі США двосторонні домовленості про відмову від діяльності, спрямованої на розкрадання електронної комерційної інформації, роблячи спроби дістати торгові секрети американських компаній. Із таким твердженням виступив у четвер старший радник зі стратегії кібербезпеки АНБ, екс-координатор Білого дому з питань кібербезпеки Роб Джойс…

Вищезазначені угоди були укладені в Вашингтоні у вересні 2015 року на зустрічі тодішнього президента США Барака Обами і голови КНР Сі Цзіньпіна. Як повідомляв Білий дім, США і Китай "погодилися, що ані в тій, ані в іншій країні уряд не стане займатися або свідомо підтримувати розкрадання за допомогою кіберзасобів інтелектуальної власності, включаючи торговельні секрети та іншу конфіденційну ділову інформацію, з метою створення конкурентних переваг для своїх компаній або комерційного сектора"…» ***(Самуїл Проскуряков. У АНБ США вважають, що Китай порушує угоди про відмову від комерційного кібершпигунства // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1761595-u-anb-ssha-vvazhayut-scho-kitay-porushuye-ugodi-pro-vidmovu-vid-komertsiynogo-kibershpionazhu). 09.11.2018).***

***

«Китайскую государственную компанию обвинили в краже коммерческих секретов американского производителя микросхем Micron Technology Inc… Министерство юстиции США активизирует действия против Китая, подозревая госкомпанию в экономическом шпионаже.

Согласно данным судебных документов, Fujian Jinhua Integrated Circuit Co. и тайваньской United Microelectronics Corp. уже предъявили обвинения в Калифорнии. Кроме того, США также требуют запретить экспорт в Америку любой продукции, произведенной этими компаниями с использованием коммерческой тайны.

Так, генеральный прокурор Джефф Сессион планирует объявить о новой инициативе в ответ на китайские попытки заполучить американскую технику и коммерческие тайны путем взлома или кражи инсайдерами…» ***(Ирина Фоменко. Китай украл у американской компании коммерческую тайну // Internetua (http://internetua.com/kitai-ukral-u-amerikanskoi-kompanii-kommercseskuua-tainu). 02.11.2018).***

***

Російська Федерація та країни ЄАЕС

«В конце прошлой недели депутаты-единороссы Адальби Шхагошев, Сергей Боженов, Олег Быков и другие их коллеги по фракции внесли в

Госдуму законопроект, который предусматривает создание кибердружин. Им надлежит мониторить Интернет и выявлять противоправную и запрещённую информацию. Эта новость вызвала в Рунете и за его пределами широкий общественный резонанс…

Судя по пояснительной записке, кибердружины будут искать данные, направленные на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды. Также в их сферу ответственности попадает запрещённая информация, за распространение которой предусмотрена административная или уголовная ответственность. Создавать кибердружины планируется в формате общественной организации по инициативе россиян, а принимать туда будут на добровольной основе с 18 лет. О том, как будет оплачиваться такая работа — не сообщается. Зато известно, что прокуратуру, следственные органы, органы государственной власти и местного самоуправления обяжут сотрудничать с кибердружинами…» ***(«Легализация киберстукачества» // РосКомСвобода (https://roskomsvoboda.org/42836/). 06.11.2018).***

***

«Компания «Ростелеком» создает единую платформу кибербезопасности, а также запускает первые три сервиса на ее основе… Согласно проекту, платформа будет функционировать на базе Ростелеком-Solar. Предполагается, что новая разработка обеспечит сетевую безопасность и защиту от киберугроз в формате сервисов, которые будут доступны через каналы связи «Ростелекома». Как заявили в компании, платформа построена на базе инновационной технологии программно-определяемых сетей (SD-WAN), она не имеет аналогов в России. Стартовый набор сервисов включает защиту от сетевых атак (Unified Threat Management), обеспечение безопасности электронной почты (Secure Email Gateway) и веб-приложений (Web Application Firewall). Стартовая емкость платформы будет составлять несколько тысяч подключений. «Стратегический вектор развития нашей компании заключается в том, чтобы стать цифровым партнером для населения, бизнеса и государства. Такой подход подразумевает создание экосистемы, состоящей из обширного набора телеком-услуг и цифровых сервисов высокого качества», — заявил Михаил Осеевский, президент ПАО «Ростелеком». «Платформа кибербезопасности является критически важным элементом такой экосистемы — она сможет гарантировать ее бесперебойную работу. <…> Единая платформа позволит нам достичь высокого уровня экономической эффективности в рамках каждой организации и повысить общий уровень защищенности российских компаний». Новая платформа ориентирована на массовую B2B-аудиторию. Она отличается от стандартных сценариев, когда сервис-провайдер управляет физическим оборудованием в центре обработки данных или на площадке заказчика. Единая платформа кибербезопасности будет иметь дело с виртуализованными объектами. Это позволит обеспечить полную управляемость, быструю масштабируемость и поддержку географически распределенной сети. Сервисная модель в этом случае позволит освободить заказчиков от финансовых и ресурсных затрат, которые ранее требовались на покупку, внедрение и поддержку решений. Более того, производительность каждого сервиса можно увеличить или

уменьшить практически мгновенно. Потребление сервисов осуществляется в режиме pay-as-you-grow. Это подразумевает, что заказчик определяет уровень своих возможностей и приобретет тот объем, который ему требуется на данный момент. На конференции также заявили, что в новую платформу инвестировали 1,5 миллиарда рублей за полтора года.

Специалисты Solar JCOS отвечают за подключение, настройку, эксплуатацию и поддержку в режиме 24/7. Как итог — существенно снизится стоимость владения сервисами платформы в течение 3-5 лет в сравнении с локальным использованием аналогичных решений.» ***(Олег Иванов. Ростелеком анонсировал единую платформу кибербезопасности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-11-14-1447/28028). 14.11.2018).***

***

«…28 ноября, канатную дорогу на Воробьевых горах в Москве закрыли из-за кибератаки.

Произошел этот инцидент лишь на третий день после открытия канатной дороги… В пресс-службе Московской канатной дороги (МКД) заявили, что кибернападение было зафиксировано в 14:00 мск, после чего было принято решение приостановить работу канатной дороги…» ***(Канатную дорогу в Москве закрыли в третий день работы // informing.ru (http://informing.ru/2018/11/28/kanatnuyu-dorogu-v-moskve-zakryli-v-tretiy-den-raboty.html). 28.11.2018).***

***

Інші країни

«Японский министр Ёситака Сакурада, отвечающий в кабмине за проблемы кибернетической безопасности в ходе дебатов в нижней палате парламента, передает информационное агентство Kyodo, признался, что не умеет пользоваться персональным компьютером.

В ответ на вопросы депутатов от оппозиции министр утверждал, что с ранней молодости упорно трудился, был сильно занят и не имел возможности овладеть компьютерной грамотностью. «Ну, а потом я вырос по службе и стал сам давать указания сотрудникам и секретарям,- гордо заявил член правительства. — Мне незачем теперь самому барабанить по клавиатуре компьютера».

Признание министра шокировало многих парламентариев. «Невозможно поверить в то, что именно этому человеку поручено такое дело, как кибернетическая безопасность», — заявил, в частности, оппозиционер Масато Имаи.

Сакурада при этом утверждал, что богатый политический опыт позволит ему без проблем заниматься поручениями. Однако на вопросы об организации защиты атомных электростанций от кибернетического терроризма он вынужден был признаться, что «деталями этой темы не владеет».

Оппозиция намерена требовать отставки министра.» ***(Министр кибербезопасности Японии признался, что не умеет пользоваться комп'ютером // Капитал (https://www.capital.ua/ru/news/120855-ministr-kiberbezopasnosti-yaponii-priznalsya-chto-ne-umeet-polzovatsya-kompyuterom). 14.11.2018).***

***

«Канадский производитель программного обеспечения BlackBerry собирается купить компанию Cylance, создающую решения для кибербезопасности…

По их данным, ведутся переговоры, а сделка может быть анонсирована на этой неделе (12-18 ноября 2018 года). Однако собеседники предупреждают, что окончательное соглашение пока не достигнуто, поэтому есть вероятность срыва продажи Cylance компании BlackBerry. Если сделка все же состоится, то BlackBerry может заплатить за приобретение до 1,5 млрд долларов. Сами компании пока воздерживаются от комментариев по запросам западных СМИ.

Cylance разрабатывает наделенные искусственным интеллектом продукты для предотвращения кибератак в компаниях. В июле 2018 года было представлено ПО Cylance Smart Antivirus, которое обеспечивает прогнозирующую безопасность для обнаружения и блокировки угроз, прежде чем они начнут работать, не влияя на производительность устройства или нарушая работу пользователя.

В Cylance говорят, что каждый день создается более 350 тысяч новых вредоносных программ, и традиционное антивирусное программное обеспечение просто не может идти в ногу с сегодняшней реальностью безопасности. Существующие способы решения проблемы основаны на технологиях, которые замедляют работу систем, бомбардируют пользователей всплывающими уведомлениями и требуют нарушения работы компьютера, чтобы начать обнаружение вредоносных программ. Cylance позиционирует свои продукты в качестве тех, которые минимально влияют на производительность устройств и которые просты в использовании…» ***(BlackBerry близка к покупке ИБ-компании Cylance // Goodnews.ua (http://goodnews.ua/technologies/blackberry-blizka-k-pokupke-ib-kompanii-cylance/). 14.11.2018).***

***

«Партнерство израильской компании Coronet, которая специализируется на киберзащите, с американским сервисом по размещению файлов Dropbox позволит привлечь миллионы новых пользователей для обеих фирм, считают эксперты.

В рамках партнерства платформа кибербезопасности Coronet, которая обнаруживает и блокирует подозрительное ПО, будет интегрирована во внутреннюю систему безопасности Dropbox.

В рамках партнерства Coronet будет предоставлять собственные функции безопасности Dropbox. Coronet фокусируется на предприятиях малого и среднего бизнеса.

«Этот сегмент рынка не может позволить себе безопасность корпоративного уровня, но мы можем предоставить достаточно сложный уровень защиты», - заявил соучредитель израильского проекта Дрор Ливер (Dror Liwer)…» ***(Израильская фирма по кибербезопасности Coronet начала сотрудничество с Dropbox // ISRAland Online Ltd (http://www.isra.com/news/222256). 09.11.2018).***

***

«Второй ежегодный обзор кибербезопасности, составленный исследовательской и консалтинговой фирмой Ovum для Silicon Valley FICO, свидетельствует о том, что 8 из 10 индийских компаний имеют страхование от киберрисков.

Высокий результат страхового покрытия кибербезопасности позволил Индии занять второе место, уступив только Великобритании по этому показателю (90%).

Следует отметить, что чуть меньше половины респондентов (48%) сообщили о всеобъемлющем страховом охвате кибер-рисков, что, по мнению исследователей, свидетельствует о достаточно высоких рисках для бизнеса в Индии.

В рамках исследования проведены телефонные опросы в 11 странах, в которых приняли участие руководители служб безопасности 500 компаний. 44% респондентов из Индии заявили, что при расчете страховых премий компании проводили детальный анализ своего профиля рисков, 17% опрошенных сообщили, что премии были основаны на неточном анализе, 32% — на средних показателях отрасли и 7% — на неизвестных факторах…» ***(Более 80% компаний в Индии обеспечены страхованием киберрисков – исследование // TRISTAR.com.ua - твой финансовый навигатор! (http://tristar.com.ua/1/news/bolee_80_kompanii_v_indii_obespecheny_strahovaniem_kiberriskov___issledovanie_10662.html). 07.11.2018).***

***

«Швейцарская страховая группа Zurich объявила о партнерстве со Всемирным экономическим форумом (ВЭФ) для борьбы с кибернетическими угрозами.

…Zurich, совместно с Глобальным центром кибербезопасности ВЭФ Zurich создает первую глобальную платформу для государственных и коммерческих структур, в том числе правительств, правоохранительных органов и экспертов в сфере кибербезопасности…» ***(Zurich присоединяется к Глобальному центру кибербезопасности ВЭФ // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/zurich-prisoedinyaetsya-k-globalnomu-tsentru-kiberbezopasnosti-vef). 28.11.2018).***

***

«Израиль обеспечит киберзащиту во время проведения встречи стран большой 20-ки, которая состоится в Аргентине с 30 ноября.

Министерство обороны Аргентины год назад подписало контракт с израильскими коллегами по предоставлению услуг кибербезопасности, хотя Израиль и не является членом группы G20. Этот контракт на сумму 5 миллионов

долларов предполагает работу двух групп реагирования на чрезвычайные ситуации в области информационной безопасности - CERT и CSIRT. 21 сентября обе страны подписали окончательное соглашение о реализации проекта…» ***(Израиль обеспечит кибербезопасность на встрече G20 в Буэнос-Айресе // ISRAland Online Ltd. (http://www.isra.com/news/222680). 21.11.2018).***

***

Протидія зовнішній кібернетичній агресії

«…В США готовят ответные меры против РФ на тот случай, если Кремль решится снова вмешаться в американские выборы.

…Минобороны США и разведывательные службы разработали специальный план противодействия возможной российской киберагрессии. Детали этого плана не разглашаются, но известно, что американские хакеры получили все необходимые разрешения для проведения превентивной кибератаки против РФ.

Сообщается, что превентивные действия американских хакеров будут применены в том случае, если будут обнаружены признаки, указывающие на попытку вмешательства со стороны РФ. При этом отмечено, что как агрессивные действия Российской Федерации будут расценены попытки хакеров сорвать регистрацию избирателей или подсчет голосов. Попытки РФ манипуляции общественным мнением, которые были зафиксированы ранее, не будут рассматриваться американцами в качестве повода для кибератаки.

В отчете также отметили, что разведывательные службы США в дальнейшем будут уделять больше внимания вопросу защиты от киберугроз…» ***(В США заявили о готовности нанести кибердудар по РФ // Судово-юридична газета (https://sud.ua/ru/news/abroad/128100-v-ssha-zayavili-o-gotovnosti-nanesti-kiberudar-po-rf). 02.11.2018).***

***

«Жодних цілеспрямованих кібератак проти проміжних виборів у США не було. Про це заявив заступник секретаря американського міністерства внутрішньої безпеки Кріс Кребс…

Секретар міністерства внутрішньої безпеки США Кірстен Нілсен за кілька годин до закриття виборчих дільниць заявила, що росіяни "тиснули за допомогою всіх можливих засобів і способів".

Утім, високопосадовці наполягають, що не було виявлено жодних доказів хакерських зломів виборчих систем…» ***(Юлія Шрамко. У США не помітили закордонних кібератак проти проміжних виборів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1761288-u-ssha-ne-pomitili-zakordonnikh-kiberatak-proti-promizhnikh-viboriv). 07.11.2018).***

***

«…За сбоем в работе международной системы навигации GPS во время учений НАТО Trident Juncture, может стоять Россия. Об этом 11 ноября заявил премьер-министр Финляндии Юха Сипиля…

Сбой в работе GPS военнослужащие зафиксировали в заполярных районах Финляндии 9 ноября. Военные предупредили Центр авианавигации о вмешательстве в ее работу. Предупреждение касалось территории от северных районов Рованиеми до норвежской границы и на восток от Киттиля до границы РФ.

Ранее похожие сбои зафиксировали в Норвегии. Тогда норвежцы заподозрили РФ во вмешательстве в работу спутниковых навигационных систем…» ***(В Финляндии подозревают Россию в кибератаках во время учений НАТО // LLC "UBT" (https://www.rbc.ua/rus/news/finlyandii-podozrevayut-rossiyu-kiberatakah-1542011566.html). 12.11.2018).***

***

«Федеральна служба безпеки РФ намагалася отримати доступ до баз даних візового центру TLScontact, що надає послуги з обробки заяв на візи в країни Шенгенської зони і Велику Британію.

Про це йдеться в розслідуванні групи Bellingcat і російського видання The Insider…

Розслідування базується на документах і свідченнях, отриманих від колишнього IT-співробітника TLScontact Вадима Мітрофанова (ім'я змінено), і мало на меті з'ясувати, зокрема, як отримали британську візу співробітники ГРУ РФ «Петров» і «Боширов», яких звинувачують в отруєнні Сергія Скрипаля і його дочки в Солсбері.

Пошук Bellingcat через корпоративні реєстри в Росії показав, що єдиною компанією, у якій формально працював «Боширов», була Kursor Ltd, московський «виробник медичного обладнання», яка була ліквідована через кілька місяців після того, як «Боширов» отримав свою фальшиву особистість в 2009 році.

Таким чином, він не міг підтвердити фінансову спроможність або наявність ділових зв'язків. Проте, неіснуючі особистості «Боширов» і «Петров» отримували візи до Британії, а також багаторазові шенгенські візи, за якими вони як мінімум чотири рази відвідали Британію і сім інших країн ЄС в період 2014-2018 років…» ***(Спецслужби Росії намагались зламати IT-систему візового центру Великої Британії, – Bellingcat // Західна інформаційна корпорація (https://zik.ua/news/2018/11/16/spetssluzhby_rosii_namagalys_zlamaty_itsystemu_vizovogo_tsentru_velykoi_1449825). 16.11.2018).***

***

«Facebook удалила еще 20 аккаунтов, в том числе и в принадлежащей ему соцсети Instagram в рамках борьбы со вмешательством в промежуточные выборы. Компания связала эти аккаунты с российской «фабрикой троллей».

Главы отдела кибербезопасности компании Натаниэль Глейхер рассказал, что некий сайт заявивший, что связан с российским Агентством интернет-исследований (IRA) (в США его называют «фабрикой троллей»), опубликовал список аккаунтов, которое создало IRA перед выборами. Он добавил, что Facebook

уже удалил большую часть этих учетных записей после внутреннего расследования, но все же уверенности во взаимосвязи сайта с IRA нет.

На прошлой неделе компания рассказала об удалении 30 аккаунтов в Facebook и 85 в Instagram. Сейчас их количество увеличилось до 36 и 99 соответственно…» ***(Facebook удалила 20 аккаунтов из-за подозрений в связях с российской «фабрикой троллей» // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3799114). 14.11.2018).***

***

«Комитет британского парламента в понедельник призвал правительство страны назначить ответственного за кибербезопасность на фоне растущих угроз со стороны враждебных государств, в частности, России.

Межпарламентский комитет по стратегии государственной безопасности в заявлении, опубликованном на сайте британского парламента, указал, что "враждебные государства начинают вести себя более агрессивно".

"Некоторые государства, в особенности Россия, начинают изучать пути для подрыва критической государственной инфраструктуры, в дополнение к шпионажу и краже интеллектуальной собственности", - говорится в заявлении комитета.

Также свои возможности для кибератак развивают и организованные криминальные группировки, отмечает комитет…

Члены комитета указали на необходимость "политического руководства" для инициатив по кибербезопасности критической инфраструктуры.

"Таким образом, мы призываем правительство назначить одного министра в секретариате кабмина, чтобы он взял на себя обязанности по созданию национальной (системы - ИФ) устойчивости (перед кибератаками - ИФ)", - заявляют члены парламента.

В британском правительстве, отвечая на призыв, заявили, что обеспечение безопасности критической инфраструктуры является приоритетом, и поэтому правительство инвестирует 1,9 млрд фунтов стерлингов в усовершенствование кибервозможностей, сообщает газета "Дейли Телеграф" со ссылкой на официального представителя правительства.» ***(В британском парламенте призвали Мэй уделить больше внимания кибербезопасности из-за России // Interfax-Azerbaijan (http://interfax.az/view/749633). 19.11.2018).***

***

«НАТО проводить в естонському місті Тарту навчання по відображенню кібератак під назвою «Кіберкоаліція»…

В НАТО називають ці навчання «одними з найбільших у світі», у них беруть участь близько 700 ІТ-фахівців і програмістів – не тільки військові, але і представники ділових кіл, розробники програмного забезпечення, виробники техніки та інформаційні гіганти.

Вчення «Кіберкоаліція» спрямовані на підготовку фахівців з кіберзахисту з країн Північноатлантичного альянсу і перевірку їх здібностей забезпечувати захист інформаційних мереж НАТО, так і їх рідних країн.

У ході навчань буде відпрацьовано відображення хакерських атак і проведення військових операцій в кіберпросторі проти можливого противника.» ***(НАТО проводить масштабні навчання з кібербезпеки в Естонії // Західна інформаційна корпорація https://zik.ua/news/2018/11/29/nato_provodyt_masshtabni_navchannya_z_kiberbezpeky_v_estonii_1458573). 29.11.2018).***

***

«Поведінка Росії на міжнародній арені серйозно непокоїть членів НАТО й організація планує згадати про це в резолюції «Посилення стримування НАТО на сході».

Про «безвідповідальну поведінку» РФ йдеться у проекті резолюції…

«Асамблея схвильована все більш активною й безвідповідальною поведінкою Росії, що виявляється у формі кібератак, використання сили проти сусідів, незаконного застосування хімічних речовин для замаху на вбивство на території одного з членів Альянсу, а також підступного підриву Москвою демократичних інституцій та принципів шляхом втручання у вибори й проведення дезінформаційних кампаній», — стверджується у документі.

В резолюції також звернули увагу на те, що Росія у своїх стратегічних документах називає НАТО противником і вбачає у діях Альянсу загрозу. «Асамблея усвідомлює, що зміни у російських доктринах в період між 2010 та 2014 роками визначили НАТО де-факто супротивником і що Росія вважає дії Альянсу у Центральній та Східній Європі прямими загрозами російським національним інтересам», — констатували в НАТО…» ***(У НАТО занепокоєні через російські кібератаки // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_nato_zanepokoeni_cherez_rosiyski_kiberataki_y_gotuyut_rezolyutsiyu/). 19.11.2018).***

***

Створення та функціонування кібервійськ

«Кібернетичне командування США (U.S. Cyber Command) придумало як підвищити власні можливості в нинішніх кібервійнах. Воно оголосило про регулярну публікацію вірусів, троянців та інших типів шкідливих програм, що використовуються у кібератаках. Зразки поміщатимуть на популярну базу VirusTotal, з якою співпрацюють майже усі антивіруси світу».

Публікація кіберзброї в загальнодоступних базах типу VirusTotal зробить її неефективною. «Це схоже на приклад нової стратегії США, – коментує фахівець з кібербезпеки Брюс Шнайер. – Публікуючи шкідливе ПЗ, США змушують їх постійно знаходити і використовувати нові уразливості».

Експерти кажуть, що спецслужби розсекречуватимуть кіберінструменти противника не одразу. Публікація відбуватиметься лише після того, як спецслужбовці США усестороннє дослідять та вивчать зразки, проведуть необхідну

розвідувальну та оперативну роботу. Коли з кіберінструмента отримають усі можливі відомості, його зроблять доступним громадськості через базу VirusTotal.

Кібернетичне командування США збирається діяти максимально публічно, широко інформуючи про зловмисне програмне забезпечення інших спецслужб. Дізнаватися про нові зразки можна буде через твіттер-аккаунт USCYBERCOM Malware Alert.

Нині там вже знаходиться два приклади кіберзброї. Це файли rpcnetp.dll і rpcnetp.exe, які відносяться до класу «дроппер». Вони є компонентом кіберзброї, і використовуються для доставки основного навантаження, наприклад бекдора Computrace хакерської групи APT28/Fancy Bear. Сам Computrace є зараженою версією комерційного програмного забезпечення LoJack від компанії, яка раніше називалася Computrace (зараз – Absolute). Воно захищає лептоп при крадіжці та допомагає відстежити його місцезнаходження.» ***(Євген Корольов. Пентагон пробує новий інструмент кіберборотьби: він розсекречуватиме кіберзброю противників // Tech Today (https://techtoday.in.ua/news/pentagon-probuye-noviy-instrument-kiberborotbi-vin-rozsekrechuvatime-kiberzbroyu-protivnikiv-106062.html). 12.11.2018).***

***

Кіберзахист критичної інфраструктури

«Конгресс США принял закон о создании ведомства, которое будет гарантировать защиту инфраструктуры страны от цифровых угроз.

В Министерстве внутренней безопасности США создадут отдельное агентство по кибербезопасности и безопасности инфраструктуры. Об этом говорится в распространенном в среду, 14 ноября, сообщении министерства.

Отмечается, что закон о создании агентства по кибербезопасности был принят Нижней палатой конгресса США…

Документ ранее был согласован верхней палатой, теперь он отправится на подпись президенту США Дональду Трампу…» ***(США создают агентство по кибербезопасности // ua-ru.info (http://ua-ru.info/news/134429-ssha-sozdayut-agentstvo-po-kiberbezopasnosti.html). 14.11.2018).***

***

«Президент США Дональд Трамп подписал закон о создании Агентства по кибербезопасности и защите инфраструктуры, сообщается на сайте Белого дома. Новую структуру планируется создать на базе Министерства внутренней безопасности (МВБ). Она будет разделена на три департамента: по кибербезопасности, по безопасности инфраструктуры и по коммуникациям в условиях чрезвычайных ситуаций…

Закон о создании агентства был одобрен Палатой представителей США 13 ноября…». ***(Дональд Трамп создал Агентство по кибербезопасности на базе МВБ США // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3804207). 17.11.2018).***

***

«Авіакомпанії і аеропорти світу в цілому вклали 3,9 млрд доларів в забезпечення кібербезпеки в 2018 році, проте зберігаються труднощі з впровадженням конкретних заходів запобігання кіберзлочинів.

Про це йдеться в дослідженні компанії SITA "Кібербезпека на авіатранспорті в 2018 році"…

В середньому авіакомпанії збільшили частку витрат на ці цілі з 7% загального бюджету на IT в 2017 році до 9% у 2018 році, а аеропорти – з 10% до 12%.

Згідно з результатами проведеного опитування, 89% директорів з інформаційних технологій авіакомпаній в наступні три роки планують реалізувати масштабні ініціативи в сфері кібербезпеки. У 2017 році таких CIO було помітно менше – 71% респондентів.

В аеропортах серйозно зайнятися кібербезпекою планують 95% опитаних. Пріоритетом для більш ніж половини (57%) керівників залишається захист операційних систем та процесів з метою забезпечити безперервність діяльності.

Основні статті витрат і для авіакомпаній, і для аеропортів – навчання персоналу (76%), виконання регуляторних вимог (73%), а також управління доступом (63%).

Однак в дослідженні виділено додаткові напрямки, які потребують уваги в найближчі роки: профілактичний моніторинг і захист мереж, забезпечення безпеки корпоративного хмарного середовища та інтернету речей (IoT), а також захист від внутрішніх загроз, включаючи витік даних.» ***(Авіакомпанії і аеропорти світу витрачають мільярди на кібербезпеку // 1NEWS (https://1news.com.ua/svit/aviakompaniyi-i-aeroporti-svitu-vitrachayut-milyardi-na-kiberbezpeku.html). 29.11.2018).***

***

«…Оператори енергомережі декілька днів поспіль відновлювали електропостачання після кібернападу… так видання Wired описало частину реалістичного експерименту на федеральному американському рівні, у якому було задіяно більше сотні експертів, які спеціалізуються на енергомережах та кібербезпеці.

Агенція новітніх розробок Міноборони США Darpa провела масштабний експеримент з поновлення енергопостачання після кібернападу під назвою «чорний старт».

Для реалістичності, навчання проводились на острові Плам – федеральній дослідницькій установі, де дослідники охопили частину острова власною енергомережею…

Навчання стосувались поновлення енергопостачання для критично важливого об'єкту. Таким активом в реальному житті може бути лікарня, або військова база, або інший об'єкт, робота якого не може зупинятись у надзвичайній ситуації…

Інструменти захисту, розроблені в результаті навчань можуть знадобитись в надзвичайних ситуаціях…» ***(Пентагон протестував кібернапад на енергомережі***

на спеціальному острові // "Українські медійні системи" (https://glavcom.ua/world/observe/pentagon-protestuvav-kibernapad-na-energomerezhi-na-specialnomu-ostrovi-545310.html). 16.11.2018).

***

Захист персональних даних

«В інтернеті у вільному доступі викладена інформація про 257 тисяч користувачів Facebook, у 81 тисячі акаунтів доступні навіть приватні повідомлення. Хакери, які стоять за витоком, стверджують, що всього у них є дані 120 млн чоловік. Розслідування Facebook показало, що зловмисники використовували шкідливі розширення для браузерів…

Найактивніше представлена Україна…: 47 тисяч користувачів. Росію як країну проживання вказали 12 тисяч чоловік. Всього на сайті майже 200 розділів по країнах, у вибірці є акаунти з Великої Британії, США, Бразилії та країн СНД…» ***(Анастасія Ткачук. Хакери зламали тисячі акаунтів українців у Facebook // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1760601-khakeri-zlamali-tisyachi-akauntiv-ukrayintsiv-u-facebook). 02.11.2018).***

***

«Eurostar сбросил пароли своих пользователей после обнаружения попыток взлома учетных записей клиентов.

Компания уведомила пострадавших о хакерской атаке, а других пользователей – о вынужденной блокировке аккаунтов, а также необходимом сбросе данных.

Eurostar отказался рассказать, был ли взлом успешным, однако сообщил, что платежные данные остались нетронутыми…

Атака была совершена между 15 и 19 октября и связана с "небольшим количеством" IP-адресов…» ***(Ирина Фоменко. Хакерам не удалось взломать одного из крупнейших перевозчиков // Internetua (http://internetua.com/hakeram-ne-udalos-vzlomat-odnogo-iz-krupneishih-perevozcsikov). 01.11.2018).***

***

«Данные клиентов «Акадо», среди которых юридические и физические лица, оказались в свободном доступе – об этом в своем блоге на Medium написал сотрудник Фонда борьбы с коррупцией Владислав Здольников. По его словам, их имена, названия и контактные данные оказались в базе данных RIPE Network Coordination Centre – одной из пяти организаций, занимающихся распределением IP-адресов в Европе и СНГ.

Здольников утверждает, что через базу данных RIPE, вводя IP-адреса, используемые головной компаний «Акадо», «Комкор», можно узнать фамилию, имя, отчество пользователя или название организации, адрес, контактный телефон.

По словам блогера, он нашел адреса расположения подключенных «Комкором» камер наблюдения департамента информационных технологий (ДИТ) Москвы, банков, контакты жителей элитного поселка Жуковка.

В 20.00 в пятницу при вводе IP-адресов в базу данных RIPE такая информация уже не выдавалась.

«Акадо» ведет внутреннюю проверку этой информации, сообщила его представитель Светлана Белых…» ***(Валерий Кодачигов. Данные клиентов «Акадо» оказались в открытом доступе. Они обнаружились в базе регистратора IP-адресов RIPE // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/articles/2018/11/02/785557-akado). 02.11.2018).***

***

«Разработан закон о защите данных потребителей в США, который предусматривает тюремное заключение на срок от 10 до 20 лет за сокрытие утечек личных данных

Сенатор США от штата Орегон Рон Уайден работает над законопроектом о защите пользовательских данных, аналогичным европейскому GDPR. Марк Цукерберг и руководители других крупных IT-компаний обязаны отчитываться насчет использования и хранения данных пользователей, а если они попытаются скрыть факт утечки конфиденциальной информации, то должны сесть в тюрьму, полагает сенатор.

В настоящее время проект документа под названием «Закон о защите данных потребителей» (Consumer Data Protection Act, CDPA) находится на стадии разработки, однако Уайден уже опубликовал его рабочую версию для общественного обсуждения. Кроме этого, на сайте Уайдена сказано:

«Сегодняшняя экономика — это гигантский пылесос, который собирает вашу личную информацию: что вы читаете, куда вы ходите, что вы покупаете и с кем вы разговариваете — все это засасывается в базы данных корпораций. Но рядовые американцы слишком мало знают о том, как их данные собираются, используются и как ими делятся».

.Уайден предлагает прекратить эту практику, дав новые полномочия Федеральной торговой комиссии. Все компании, чей годовой доход превышает $1 млрд, а также те, которые собрали данные более чем 50 млн пользователей, должны будут каждый год отчитываться перед правительством о предпринятых мерах по защите этих данных.

В документе содержатся обязательные для выполнения минимальные требования по защите конфиденциальности и обеспечению кибербезопасности. В случае их невыполнения компаниям грозит штраф в размере до 4% от годового дохода.

Ответственность за отчеты будет лежать лично на генеральных директорах, старших директорах по обеспечению конфиденциальности данных или старших директорах по информационной безопасности компаний.

В отчетах должно сообщаться, обеспечивает ли компания (и каким образом) выполнение требований CDPA. За сокрытие утечек или предоставление ложных сведений директорам будет грозить до 20 лет лишения свободы. Документ

предлагает Федеральной торговой комиссии разработать и ввести в действие систему «Do Not Track» («Не отслеживать»), позволяющую пользователям отказываться от предоставления компаниям своих персональных данных.

CDPA запрещает компаниям отказывать в предоставлении услуг пользователям, решившим не раскрывать свои персональные данные. В случае отказа пользователя от предоставления своих данных компании получат право взимать с него плату в денежном эквиваленте.

Согласно законопроекту, пользователи получат право узнавать, какую персональную информацию о них собирает компания и с кем ею обменивается.

В случае принятия закона в Федеральной торговой комиссии будет создано более 175 новых рабочих мест для сотрудников, в чьи обязанности войдет наблюдение за обеспечением конфиденциальности данных пользователей.» ***(В США могут ввести уголовное наказание для глав IT-компаний за утечки персданных // РосКомСвобода (https://roskomsvoboda.org/42827/). 06.11.2018).***

***

«…В среду, 31 октября, компания Google сообщила о добавлении четырех новых функций для защиты учетных записей пользователей от хакерских атак. Новые функции позволяют не только защитить учетную запись до и после авторизации в ней пользователя, но и восстановить после взлома.

Как пояснил директор по продукции Google Джонатан Скелкер (Jonathan Skelker) в блоге компании, первая из четырех функций срабатывает еще до того, как пользователь начнет вводить свой логин и пароль. По его словам, в будущем авторизоваться в учетной записи Google будет невозможно, если в браузере отключен JavaScript. Дело в том, что Google использует JavaScript для проверки заходящих на страницу авторизации пользователей. При отключенном JavaScript злоумышленник может обойти эту проверку.

Изменения коснутся лишь очень незначительной доли пользователей (около 0,01%), но станет серьезным препятствием для ботов, поскольку большая их часть запускается через браузеры, где JavaScript отключен для повышения производительности.

Вторая функция безопасности касается вредоносных приложений, установленных пользователями на Android-устройства. Google намерена воспользоваться данными интегрированного с Google Play сканера Google Play Protect и создать список вредоносных приложений, присутствующих на устройствах пользователей. Уже в ближайшие недели список появится в пользовательских учетных записях Google в разделе Google Security Checkup.

Третья функция связана со сторонними приложениями и сайтами, которым пользователь в прошлом дал разрешение на доступ к данным учетной записи Google. Все подобные сторонние сайты и приложения будут собраны в список, который также появится в разделе Google Security Checkup.

Четвертая функция предназначена для использования после взлома учетной записи злоумышленниками. Она уже работает и представляет собой набор процедур для восстановления доступа и защиты скомпрометированного профиля. Кроме того, с ее помощью жертва взлома может проверить финансовую активность

в Google Pay и наличие новых файлов в Gmail и на Google Диске.» ***(Google объявила о добавлении новых функций для защиты учетных записей // SecurityLab.ru (https://www.securitylab.ru/news/496241.php). 01.11.2018).***

***

«Израильская компания ClearSky, которая специализируется на кибербезопасности, заявляет, что хакеры пытались продать в "темной" сети данные 62 миллионов избирателей в США накануне выборов в Сенат.

Пул данных включает информацию об избирателях из 17 разных штатов. Он продается на одном из крупнейших рынков в так называемой Darknet на сайте Dream Market. Например, пакет данных о 1,7 миллионах избирателях в Арканзасе продается за 10 долларов или 0,001647 биткойна.

В пакетах информации есть полные имена избирателей, их ID, текущие и прошлые адреса, даты их рождения, пол и номера телефонов.

Боаз Долев (Boaz Dolev), генеральный директор ClearSky, объясняет, что уже в июне этого года стало известно о том, что пул данных об американских избирателях просочился в Интернет, но его выставили на продажу только накануне выборов.» ***(Израильская фирма обнародовала попытку продать данные 62 миллионов избирателей в "темной" сети // ISRAland Online (http://www.isra.com/news/222125). 06.11.2018).***

***

«Хакеры выставили на продажу в интернете похищенные ими данные банковских карт 244 тыс. клиентов авиакомпании British Airways…

Эксперты Flashpoint обнаружили, что хакеры выставили на продажу в теневом сегменте интернета похищенные данные банковских карт клиентов British Airways по цене от £6,94 ($9) до £38,58 ($50) за одну карту. По оценке экспертов компании, продажа этих данных могла принести хакерской группировке до £ 9,4 млн ($12,19 млн). Во Flashpoint полагают, что кибератаку совершила хакерская группировка Magecart, которая, по утверждению Daily Mail, якобы имеет российское происхождение.

British Airways в сентябре информировала, что в результате хакерской атаки данные карт сотен тысяч ее пассажиров оказались доступны злоумышленникам. Жертвами хакеров могли оказаться все, кто бронировал билеты или оплачивал иные услуги на сайте или через приложение авиакомпании в период с 21 августа по 5 сентября этого года.

Изначально British Airways опасалась, что были похищены данные кредитных карт 380 тыс. клиентов. Однако по итогам проведенного авиакомпанией расследования выяснилось, что хакерам удалось получить доступ к данным 244 тыс. карт.» ***(Хакеры выставили на продажу данные кредиток клиентов British Airways // Капитал (https://www.capital.ua/ru/news/120885-khakery-vystavili-na-prodazhu-dannye-kreditok-klientov-british-airways#ixzz5WuBCI0ul). 14.11.2018).***

***

«По мере того, как весь мир адаптируется к положениям «Общего регламента по защите данных» (GDPR) и все больше внимания уделяется неприкосновенности частной жизни и обеспечению безопасности, ведущие европейские эксперты по информационной безопасности все еще не уверены в способности этой отрасли обеспечить безопасность критической инфраструктуры, корпоративных сетей и персональных данных.

Последний аналитический отчет Black Hat Europe, озаглавленный Трудные задачи в области кибербезопасности, стоящие перед Европой (Europe's Cybersecurity Challenges), подробно раскрывает причины, не дающие ведущим европейским экспертам по информационной безопасности спокойно спать по ночам. В отчете представлены мнения более чем 130 респондентов; кроме того, раскрываются темы, связанные с GDPR, неприкосновенностью частной жизни, непростыми задачами, стоящими перед отраслью в настоящее время, а также перспективами, ожидающими европейцев в ближайшие годы…

Хотя респонденты отмечают, что введенный в действие в мае этого года «Общий регламент по защите данных» (GDPR) занимает по важности первое место, появляются сомнения в его потенциальной эффективности. Без сомнения, изменения были проведены для выполнения требований GDPR – 70% опрошенных подтвердили, что обладают достаточными ресурсами для реализации инициатив GDPR. Однако достаточно интересно то, что лишь более трети опрошенных полностью уверены, что их организации соответствуют требованиям GDPR. Кроме того, среди считающих, что GDPR может помочь защитить персональные данные, менее четверти считают, что помощь будет существенной…

По мере того, как GDPR вступает в полную силу и пользователи видят новостные заголовки о неправильном обращении социальных сетей с персональными данными, эксперты по безопасности все более внимательно относятся к задачам, стоящим при защите частной жизни. Одним из основных проблемных вопросов является использование коммерческими организациями данных, позволяющих идентифицировать личность. Почти 60% респондентов приводят сведения о случаях сбора и/или продажи персональных данных компаниями и социальными сетями, не обеспечивающими должным образом защиту частной жизни, и считают это самой серьезной угрозой безопасности персональных данных. Эти опасения вынудили более 40% экспертов по информационной безопасности разработать план по минимизации собственного использования социальных сетей; кроме того, многие из них рекомендуют и другим пользователям и подразделениями компаний поступать так же.

Год спустя европейская критическая инфраструктура все еще вызывает опасения

Около двух третьих опрошенных экспертов по безопасности (65%) полагают, что в течение ближайших двух лет произойдет крупномасштабная атака на критическую инфраструктуру многих европейских стран. Указанная выше цифра показывает, что число обеспокоенных такой атакой не уменьшилось по сравнению с прошлогодним опросом. Основное опасение связано с киберугрозой со стороны крупных государств, таких как Россия и Китай: 30% опрошенных считают, что

основную угрозу представляют крупные государства, а 17% опрошенных называют организованную преступность, заинтересованную в финансовой выгоде…

Как и в прошлом году, низкий уровень защиты Европы связан с недостаточным финансированием, отсутствием у специалистов необходимых технических средств и неэффективными технологиями. 42% респондентов считают, что самым слабым звеном в средствах защиты являются конечные пользователи, которые нарушают политики информационной безопасности и которых легко обмануть при атаках, основанных на использовании социальной психологии. В то же время 20% опрошенных винят в провале стратегий по информационной безопасности недостаток навыков; кроме того, менее половины респондентов считают, что располагают достаточными финансовыми средствами для противостояния современным угрозам…» ***(Недоверие к GDPR, отсутствие конфиденциальности в соцсетях, угроза атак на критическую инфраструктуру в масштабах страны // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5545270-Nedoverie-k-GDPR-otsutstvie-konfide.html). 14.11.2018).***

***

«Появился телеграм-бот, при помощи которого можно получить полный перечень данных о владельце автомобиля.

…По номеру автомобиля предлагается узнать информацию о владельце. В зависимости от того, сколько вы приведете новых пользователей на данный канал-телеграм, вам предоставится максимально полная информация о владельце ТС».

Как выяснилось, фактически любой желающий может получить перечень данных о владельце автомобиля. Особо усердные могут заполучить даже адрес владельца транспортного средства…» ***(Паспорт, адрес, телефон: данные миллионов украинцев продают в сети // "Судово-юридична газета" (https://sud.ua/ru/news/ukraine/128788-pasport-adres-telefon-dannye-millionov-ukraintsev-prodayut-v-seti). 15.11.2018).***

***

«Попадание данных в открытый доступ из-за неправильной конфигурации S3 стало серьезной проблемой.

В Amazon Web Services появились новые функции безопасности для защиты пользовательских учетных записей от случайных утечек данных, связанных с неправильной конфигурацией бакетов S3.

Начиная с 15 ноября, владельцам учетных записей AWS открыт доступ к четырем новым функциям на панели управления в разделе «Настойки общественного доступа для этого аккаунта» («Public access settings for this account»). С их помощью можно установить настройки по умолчанию для доступа ко всем бакетам в учетной записи.

Новые настройки отменят все существующие или вновь создаваемые списки управления доступом и политики. Владельцы учетных записей смогут устанавливать их как для бакетов, которые будут создаваться впредь, так и для уже существующих бакетов. Эти настройки станут своего рода «мастер-

переключателем», предотвращающим случайное открытие бакетов владельцами учетных записей и их сотрудникам/разработчиками…» ***(Новые функции в AWS защитят от случайных утечек данных // SecurityLab.ru (https://www.securitylab.ru/news/496597.php). 20.11.2018).***

***

«Бразильская Федерация промышленности Сан-Паулу (FIESP) допустила утечку информации из трех своих баз данных. В утекших записях содержались имена, электронные и физические адреса, идентификационные карты, номера социального страхования и телефонные номера.

…исследователь безопасности Боб Дяченко (Bob Diachenko) обнаружил три базы данных, доступных через поиск Elasticsearch, 12 ноября текущего года. Крупнейший источник насчитывал 34,8 млн входов. Данные находились в открытом доступе в течение нескольких дней…

Согласно заявлению FIESP, базы данных не содержали паролей, а какие-либо свидетельства неправомерного использования хранящихся в БД данных отсутствуют. Для расследования инцидента организация обратилась за помощью к неназванной компании, специализирующейся на кибербезопасности…» ***(Крупнейшее объединение промышленников в Бразилии допустило утечку даннях // Goodnews.ua (http://goodnews.ua/technologies/krupnejshee-obedinenie-promyshlennikov-v-brazilii-dopustilo-utechku-dannyx/). 27.11.2018).***

***

«Компания Dell сбросила пароли пользователей сайта Dell.com в связи с инцидентом, который коснулся безопасности этого ресурса. В частности, 9 ноября компания обнаружила и остановила в своей сети неавторизованную активность. Отмечается, что неизвестные хакеры хотели похитить данные клиентов Dell, включая их имена, электронные адреса и хэши паролей. Обнаружив активность вредоносного характера, компания сразу же приняла ответные шаги, а также обратилась к независимым исследователям по безопасности для проведения расследования. По результатам предварительного расследования случившегося, не выявило каких-либо свидетельств того, что злоумышленникам удалось осуществить задуманное. Однако не исключено, что киберпреступники все же могли похитить некоторую информацию из внутренней сети. Соблюдая меры предосторожности, Dell на всякий случай сбросила все пароли пользователей сайта Dell.com. Компания не раскрывает подробности о том, как злоумышленникам удалось проникнуть в сеть и сколько пользователей было затронуто инцидентом. При этом в Dell уверили своих клиентов в полной сохранности их банковских карт и номеров социального страхования. На работу продуктов и сервисов компании инцидент не оказал никакого влияния.» ***(Dell сбросила пароли пользователей из-за возможной кибератаки // Интернет-портал PaySpace Magazine (https://psm7.com/security/dell-sbrosila-paroli-polzovatelej-iz-za-vozmozhnoj-kiberataki.html). 29.11.2018).***

***

«Сервис по заказу такси Uber оштрафован в Великобритании и Нидерландах в общей сложности на $1,17 млн из-за кибератаки 2016 года, в результате которой персональные данные миллионов клиентов и десятков тысяч водителей могли оказаться в руках хакеров.

…штраф в Великобритании составил 385 тыс. фунтов стерлингов ($491 тыс.), в Нидерландах - 600 тыс. евро ($679 тыс.).

По данным британского Управления уполномоченного по вопросам информации (ICO), злоумышленники, получившие доступ к системам Uber, могли выгрузить данные около 2,7 млн клиентов и 82 тыс. водителей сервиса в Великобритании. Нидерландские власти говорят об утечке данных 174 тыс. подданных королевства.

По всему миру утечка коснулась имен, адресов и телефонов 50 млн клиентов и 7 млн водителей Uber. Руководство Uber выплатило хакерам $100 тыс. за уничтожение данных и замалчивало этот инцидент больше года.» ***(Uber оштрафовали в Великобритании и Нидерландах на $1,17 млн из-за кибератаки 2016 года // Интерфакс-Украина (https://interfax.com.ua/news/economic/548715.html). 27.11.2018).***

***

«Взлом, в результате которого были похищены 808 тыс. электронных адресов и более 1,8 млн имен пользователей, обернулся немецкой соцсети штрафом в размере 23 тыс. евро за нарушение недавно принятого Общего регламента по защите данных (GDPR).

В июле нынешнего года платформа nuddels.de стала жертвой кибератаки. Неизвестные похитили данные с серверов соцсети и опубликовали их в открытом виде на Pastebin и Mega. По словам сотрудников компании, инцидент затронул всех пользователей, имевших учетную запись в сервисе или зарегистрированных в чате по состоянию на 20 июля 2018 года.

Как оказалось позднее, соцсеть хранила конфиденциальные данные пользователей, в том числе пароли, без какой-либо защиты. В связи с этим, власти обязали сайт nuddels.de заплатить штраф за нарушение требований GDPR. Данный случай является первым в Германии, когда компанию привлекли к ответственности за нарушение GDPR, вступившего в силу в Евросоюзе в мае нынешнего года…» ***(Соцсеть из Германии получила штраф за нарушение GDPR // Goodnews.ua (http://goodnews.ua/technologies/socset-iz-germanii-poluchila-shtraf-za-narushenie-gdpr/). 27.11.2018)***

***

Кіберзлочинність та кібертероризм

«Іранський міністр з телекомунікацій Мохаммад Джавад Азері Жахромі та його заступник Хамід Фатахі заявили, що на їх країну здійснюється кібератака…

Міністр з телекомунікацій Ірану Мохаммад Джавад Азері Жахромі та його заступник Хамід Фатахі звинуватили в атаці Ізраїль і повідомили, що під «роздачу» попала іранська комунікаційна інфраструктура.

У Міністерстві закордонних справ Ізраїлю відмовилися коментувати повідомлення іранських посадовців…» ***(Іран заявив про кібератаку на свої комунікації з боку Ізраїля // Західна інформаційна корпорація (https://zik.ua/news/2018/11/05/iran_zayavyv_pro_kiberataku_na_svoi_komunikatsii_z_boku_izrailya_1441427). 05.11.2018).***

***

«Эксперты по кибербезопасности из компании Japan Digital Design, являющейся подразделением японской финансовой корпорации Mitsubishi UFJ Financial Group (MUFG), сообщили, что они, возможно, обнаружили информацию о злоумышленниках, укравших с крипто-биржи Zaif $60 млн…

Согласно Japan Digital Design, она изучала перемещение активов с момента инцидента на бирже и обнаружила "источник" атаки, после того как активы в криптовалюте Monacoin начали перемещаться во второй половине прошлого месяца.

Компания отмечает, что передала полученную информацию властям…

Аналитики публично не раскрывают добытую ими информацию, как и ее масштаб, однако отмечают: "В ходе расследования утечки виртуальной валюты был проанализирован платёжный канал с применением статического анализа блокчейна. Путём установки ноды виртуальной валюты после утечки виртуальной валюты мы подтвердили, можем ли получить улики, такие как IP-адрес источника и т.д. Мы также собрали полезные данные, чтобы подтвердить точность информации и стоимость отслеживания"…» ***(Хакеры украли 60 млн долларов с японской крипто-биржи Zaif // “Багнет” (http://www.bagnet.org/news/economics/380751/hakery-ukrali-60-mln-dollarov-s-yaponskoy-kripto-birzhi-zaif). 06.11.2018).***

***

«Тысячи конфиденциальных документов, относящихся к атомным электростанциям и исправительным учреждениям, были похищены с серверов одной из французских компаний…

Согласно сообщениям в СМИ, инцидент имел место еще в июне нынешнего года. Неизвестные злоумышленники взломали серверы компании Ingerop и похитили порядка 65 ГБ данных. По данным немецкой телерадиокомпании NDR, в общей сложности было похищено 11 тыс. файлов из десятка проектов.

Помимо прочего, в руках у злоумышленников оказались схемы расположения камер видеонаблюдения в одной из французских тюрем строго режима, документы, касающиеся захоронений ядерных отходов на северо-востоке Франции, а также персональная информация более 1 тыс. сотрудников Ingerop. Некоторые похищенные документы также имеют отношение к французской АЭС Фессенхайм, расположенной неподалеку от границы с Германией.

Часть похищенных данных была обнаружена следователями на арендованном сервере в Дортмунде (Германия). Ведется следствие. По словам представителей Ingerop, они уведомили об инциденте своих затронутых утечкой клиентов и предприняли меры по усилению кибербезопасности.» ***(Киберпреступники похитили тысячи документов АЭС и тюрем // Goodnews.ua (http://goodnews.ua/technologies/kiberprestupniki-poxitili-tysyachi-dokumentov-aes-i-tyurem/). 03.11.2018).***

***

«Международный финансовый гигант HSBC стал жертвой кибератаки с использованием украденных учетных данных. Этот инцидент произошло в прошлом месяце. Сообщается, что в период с 4 по 14 октября к некоторым учетным записям пользователей был получен несанкционированный доступ. Атака затронула только клиентов HSBC в США, и только 1% от всех американских клиентов. Однако точное количество пострадавших неизвестно. В результате инцидента злоумышленникам удалось похитить имена, адреса и даты рождения пользователей, а также такую банковскую информацию, как номера и балансы счетов, история транзакций и номера счетов получателей… Такая атака основывается на автоматизированном подборе к учетным записям соответствующих паролей, полученных в результате прошлых утечек. Весьма странно, что клиенты HSBC могли стать жертвами подобной атаки, ведь банки обычно используют двухфакторную аутентификацию, и простой брутфорс сработать не должен. В качестве компенсации HSBC предложил пострадавшим клиентам бесплатную услугу мониторинга кредитной истории и защиты от кражи личности в течение одного года.» ***(Хакеры похитили данные клиентов ведущего финансового холдинга // Интернет-портал PaySpace Magazine (https://psm7.com/security/xakery-poxitili-dannye-klientov-vedushhego-finansovogo-xoldinga.html). 07.11.2018).***

***

«…Аналитический центр компании InfoWatch составил дайджест утечек, произошедших в результате действий руководителей.

Недавно в США некоммерческий фонд Green Beret Foundation, созданный для защиты интересов военнослужащих спецназа и членов их семей, подал в суд на бывших членов руководящего состава. В фонде утверждают, что исполнительный директор Дженнифер Пакетт (Jennifer Paquette) и глава финансовой службы Мелисса Пучино (Melissa Pucino) заблокировали другим сотрудникам доступ к информационным сервисам, в том числе сведениям о 40 тыс. контактов фонда. Кроме того, руководители перед своим уходом скопировали ряд конфиденциальных данных. Этим действиям предшествовало увольнение обоих топ-менеджеров…

Бывшего высокопоставленного сотрудника корейской сети беспошлинной торговли Lotte Duty Free обвинили в передаче секретной информации конкурентам из компании DFS. В судебных документах отмечается, что человек по фамилии Ли (Lee) уволился из Lotte вскоре после неудачных притязаний на более высокую

должность. Вскоре после этого Ли отправился в Гонконг, где передал представителям DFS конфиденциальную информацию, касающуюся развития бизнеса в других странах. В частности, речь идет о концессионном контракте Lotte Duty Free с аэропортом Гуама на сумму порядка $150 млн.

Весьма чувствительными для репутации компании оказываются случаи, когда руководитель использует персональные данные клиентов с целью наживы. Например, в американском штате Пенсильвания был разоблачен директор окружного агентства по чрезвычайным ситуациям. Используя персональные данные уволившегося сотрудника, руководитель открыл в банке кредитную карту и использовал ее для совершения покупок.

Отдельную категорию нарушителей среди топ-менеджеров составляют высокопоставленные политики. Их действия в отношении конфиденциальной информации могут нанести серьезный ущерб системе национальной безопасности. В Алжире к пятилетнему тюремному заключению приговорен бывший депутат Ахмед Белкасми. Экс-парламентарий признан виновным в передаче информации иностранному государству. В частности, Белкасми скомпрометировал закрытые отчеты по вопросами безопасности, экономики и политического устройства. Также он делился секретными сведениями о здоровье президента республики, его перемещениях и текущей деятельности. Что интересно, Белкасми сдала его собственная жена.» ***(Как данные утекают по вине руководителей // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5544167-Kak-dannye-utekayut-po-vine-rukovod.html#ixzz5WuiQRWCy). 12.11.2018).***

***

«…Аналитический центр компании InfoWatch составил дайджест утечек из гостиничных сетей.

В октябре сеть отелей Radisson уведомила участников своей программы лояльности об утечке личной информации. Скомпрометированными оказались такие данные, как имена, адреса, страны проживания, адреса электронной почты, номера телефонов и номера партнерских карт. Согласно предварительной информации, злоумышленники обманным путем получили доступ к учетным записям ряда сотрудников отелей и смогли похитить конфиденциальные сведения. О числе пострадавших не сообщается, но представители Radisson уверяют, что скомпрометированы данные «менее 10%» участников программы лояльности.

Одну из крупнейших в истории Китая утечек информации испытал гостиничный холдинг Huazhu Group. В даркнете обнаружена информация 130 млн постояльцев отелей: имена, телефонные номера, адреса электронной почты, данные банковских карт и сведения о бронировании номеров. Предположительно, утечка произошла через незащищенный канал при загрузке базы данных на GitHub. Анонимные торговцы предлагали купить полную базу за 8 биткойнов (около $54 тыс.), но после того, как инцидент получил огласку в СМИ, снизили цену до 1 биткойна.

Летом хакеры атаковали сервера системы Fastbooking, которая предоставляет услуги бронирования для более чем 4000 отелей в 40 странах. Одним из пострадавших партнеров названа японская сеть Prince Hotels. Добычей

киберпреступников стали около 125 тыс. записей персональных данных: имена, адреса и платежная информация.

В особой зоне риска находятся посетители отелей, использующие публичные Wi-Fi-сети. Это излюбленный канал для злоумышленников. Взломав сеть, хакер может похитить идентификационные данные или перехватить пароль для входа в мобильный банк…» ***(Как из гостиниц утекают данные постояльцев // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5542885-Kak-iz-gostinicz-utekayut-dannye.html).*** 06.11.2018).

***

«…По данным DeviceLock, цена «пробивки» абонентских и банковских данных в теневом Интернете сильно выросла… «Пробивка» — это предоставление информации, нарушающее тайну и тайну переписки. Кража данных абонентов у сотовых операторов выросла на 25%. «Пробивка» в банке увеличилась более чем на 50%: выписки клиентов предлагаются по цене от 8 тыс. руб. за месяц или от 10 тыс. руб. за полгода.

При этом стоимость баз данных и сканов документов осталась прежней. Они применяются большей частью для спама и телефонного мошенничества и потому не приносят крупных доходов, пояснили в DeviceLock. Так, базы персональных данных по всем регионам России, содержащие Ф.И.О., пол, телефон, полные паспортные данные, СНИЛС, адрес регистрации и проживания за 2017–2018 годы продаются о по 20–25 коп. за одну запись.

Цены на «пробивку» выросли, потому что увеличился риск для продавцов данных и из-за операций правоохранительных органов по борьбе с ними, считают в DeviceLock. Делая «заказы», оперативники выявляют цепочку от продавца до похитителя информации. Однако уже похищенные «спасти» никак нельзя: здесь требуются превентивные меры, в первую очередь в виде внедрения DLP-систем (программы для предотвращения утечек конфиденциальной информации за пределы корпоративной сети)…» ***(Цены на украденные персональные данные растут // «Открытые системы» (https://www.computerworld.ru/news/Tseny-na-ukradennye-personalnye-dannye-rastut). 22.11.2018).***

***

Діяльність хакерів та хакерські угруповування

«Австралійське оборонне підприємство Austral заявило про хакерську атаку, в результаті якої були викрадені особисті справи співробітників. Вкрадені дані, включаючи адреси електронної пошти співробітників і номери мобільних телефонів, частково були опубліковані в інтернеті з метою вимагання, однак Austral вже заявила, що ні за яких обставин “не реагуватиме на спроби шантажу з боку злочинців”

… хакерська атака торкнулася тільки австралійського офісу Austral.

Міністерство оборони Австралії підтвердило факт злому системи безпеки Austral, але також відзначило, що “фактів, які підтверджують крадіжку технологій

або секретної інформації, не виявлено”…» ***(Самуїл Проскуряков. Невідомі хакери зламали систему безпеки австралійського оборонного підприємства Austral // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1760567-nevidomi-khakeri-zlamali-sistemu-bezpeki-avstraliyskogo-oboronnogo-pidpriyemstva-austral). 02.11.2018).***

***

«Група хакерів зламала низку верифікованих акаунтів й розмістила через них оголошення, в яких використовувались логотип Tesla та постать відомого підприємця Ілона Маска.

Серед тих, чиї акаунти зламали шахраї, були британський фешн-ритейлер Matalan, кінодистриб’ютор Pathe UK та американське видавництво Pantheon Books, повідомляє BBC. Вони запустили платне просування дописів у Twitter, аби їх побачили більше користувачів у соцмережі. Зараз більшість дописів були видалені.

Хакери змінювали зображення у зламаних акаунтах та їх назви, імітуючи сторінку Ілона Маска. Оскільки до цього профілі отримали позначку про верифікацію (синя галочка на сторінці), деяких людей це ввело в оману. Зловмисники почали поширювати з псевдо-сторінок пости про те, що зараз Ілон Маск проводить акцію з роздачі біткоїнів. Для того, аби долучитися до неї, потрібно перевести невелику суму в криптовалюті на вказаний рахунок. На момент, коли обман розкрили, користувачі встигли перевести на віртуальний гаманець шахраїв суму в близько 180 тисяч доларів…» ***(Шахраї видали себе за Ілона Маска в Twitter та виманили 180 тисяч доларів у користувачів // MediaSapiens (https://ms.detector.media/web/cybersecurity/shakhrai_vidali_sebe_za_ilona_maska_v_twitter_ta_vimanili_180_tisyach_dolariv_u_koristuvachiv/). 07.11.2018).***

***

«Федеральная антимонопольная служба (ФАС) подверглась хакерской атаке…

«Это была полноценная хакерская атака. Началось с массовой рассылки на адреса ФАС вируса, который ворует служебные логины и пароли», — рассказали в ФАС.

Хакерская атака началось в среду вечером, затронув центральный аппарат ведомства и территориальные органы.

Вместе с тем были атакованы информационные ресурсы ФАС, предположительно с целью взлома, отметил представитель службы.

Специалисты по информационной безопасности отреагировали оперативно, пострадавших в результате атаки нет, добавили в ФАС.

Злоумышленники создали для атаки на ведомство персональный вирус, рассказала в Facebook начальник управления общественных связей ФАС Ирина Кашунина.

Она опубликовала скриншот «вирусного» письма, где отправителем значится Federal Antimonopoly Service, а в теме указано: «Ожидающее уведомление: Федеральная Антимонопольная служба делится с вами файлом»…» ***(Екатерина***

Симикян. В ФАС рассказали о хакерской атаке на ресурсы службы // (https://rb.ru/news/fas-hacker-attack/). 15.11.2018).

***

«…Агентство Bloomberg опубликовало ошеломляющую новость об экстраординарной хакерской атаке на оборудование, которая осуществлялась китайскими агентами, финансируемыми государством. В статье "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" («Большой взлом: Как Китай при помощи крошечного чипа проникал в американские компании») говорилось об успешном встраивании Народно-освободительной армией Китая крошечных чипов в материнские платы серверов компании Super Micro. Впоследствии эти чипы компрометировали системы, предоставляя к ним доступ…

Super Micro – один из крупнейших в мире производителей подобного оборудования, поставляющий свою продукцию министерству обороны США, министерству внутренней безопасности, НАСА, Конгрессу и многим крупнейшим мировым компаниям. По утверждению Bloomberg, в конечном итоге атака затронула почти 30 компаний…

В Bloomberg заявили, что одной из жертв хакерского взлома оборудования стала компания Apple.

Apple действительно на протяжении многих лет время от времени использовала в своих ЦОДах оборудование Super Micro…

По сведениям Bloomberg, Apple развернула около 7 тыс. серверов Super Micro, после чего служба безопасности обнаружила крошечные скрытые дополнительные чипы. Утверждается, что Apple выявила взломанные серверы в 2015 году и сообщила об этом в ФБР, однако конкретные подробности не разглашались. По информации неназванного чиновника, Apple не позволила правительственным структурам получить доступ к своей инфраструктуре и оборудованию…

Bloomberg публикует реакцию на свою публикацию со стороны Amazon, Apple, Super Micro и китайского министерства иностранных дел. Подробный ответ Apple сводится к отрицанию всех ранее сделанных выводов:

…Apple никогда не обнаруживала никаких вредоносных чипов, аппаратных манипуляций и уязвимостей ни на одном из серверов. Мы никогда не обращались в ФБР и прочие агентства по поводу инцидентов такого рода. Нам неизвестно о проводимом ФБР расследовании, и мы не поддерживаем контактов с правоохранительными органами…

Заявление Apple практически не оставляет простора для разночтений. Компания утверждает, что «никогда не обнаруживала ни вредоносных чипов, ни манипуляций с оборудованием, ни уязвимостей, преднамеренно встроенных в серверы». Все это имеет совершенно однозначную трактовку…

В Bloomberg, со своей стороны, сообщают о получении информации от трех инсайдеров Apple и четырех из шести чиновников, подтвердивших, что Apple была жертвой…» ***(Джейсон Кросс. В Apple опровергли публикацию Bloomberg о китайских хакерах // «Открытые системы»***

(https://www.computerworld.ru/articles/V-Apple-oprovergli-publikatsiyu-Bloomberg-o-kitayskih-hakerah). 12.11.2018).

***

«Американская компания Palo Alto Networks, занимающаяся системами кибербезопасности, заявила об обнаружении нескольких кибератак со стороны хакерской группы APT28, также известной как Fancy Bear или Sofacy, якобы имеющей отношение к России.

Palo Alto Networks обнаружили образец зараженного документа, использовавшегося в фишинговых рассылках группы в октябре и начале ноября нынешнего года для «ряда государственных структур, в том числе в Северной Америке, Европе и странах бывшего СССР». Таким образом хакеры могут получить информацию с компьютера получателя.

По информации компании, APT28 известны «постоянным развитием своих механизмов». Так Palo Alto Networks обратили внимание, что компания начала использовать программу, которую эксперты назвали Cannon. Программа уникальна тем, что имеет «невысокий» шанс обнаружения…» ***(США обвинили российских хакеров в новых атаках // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3805957). 21.11.2018).***

***

«На российские банки снова совершена крупная хакерская атака, об этом сообщила компания Group-IB. Объектами нападений стали более 50 игроков банковского рынка, в том числе, по некоторым данным, не менее трех организаций из первой «тридцатки». Акция была проведена в виде массовой рассылки так называемых фишинговых писем, причем они были отправлены от имени Центробанка.

Эксперты отмечают, что в результате подобных атак страдают, как правило, не клиенты банков, а сами кредитные организации, из которых могут быть выведены деньги. Причем это может произойти не сразу, а через три-четыре недели. К нынешнему нападению следует отнестись очень серьезно, отметил заместитель руководителя лаборатории по компьютерной криминалистике Group-IB Сергей Никитин: «Опасность данной атаки в том, что, во-первых, она происходила как бы от имени ФинЦЕРТа и ЦБ, то есть люди видели адрес отправителя и доверяли ему. Проблема номер два — эти рассылки шли сотрудникам самых разных банков. Антивирусы не детектировали эти вложения, и могли помочь только решения класса "песочницы", которые заранее открывают все вложения писем и проверяют, что происходит. Третья опасность в том, что, к сожалению, во многих банках не стоят своевременные обновления, в том числе офисного пакета, операционных систем, из-за чего заражение происходит очень масштабно, заражаются другие компьютеры в банках»…» ***(Андрей Загорский. Хакеры адресовали письма российским банкам. Что известно о последней крупной кибератаке // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3803702). 16.11.2018).***

***

«Хакерську групу APT29 підозрюють в атаці на урядові агентства і приватні компанії в США. Хакери розсилають заражені листи від імені працівниці держдепу…

Атака була розпочата 14 листопада. Хакери, які є імовірно членами групи APT29, і котрі, як підозрюють, працюють на Службу зовнішньої розвідки Росії, розсилають електронні листи від імені співробітниці держдепартаменту США Сюзан Стівенсон. Одержувачам пропонується завантажити листи, написані нібито співробітницею держдепу Хізер Науерт.

При відкритті листів встановлюється шкідлива програма, яка забезпечує хакерам широкий доступ до комп'ютера користувача, розповів представник FireEye.За словами співрозмовника агентства, атаки зазнали понад 20 клієнтів FireEye, в тому числі військові агентства, правоохоронні органи, підрядники Пентагону, медійні компанії і фармацевтичні фірми. CrowdStrike і FireEye не уточнили, які саме організації було атаковано і скільком з них завдано збитків.

Російська компанія з розробки антивірусного софту Kaspersky Lab підтвердила, що ці атаки були здійснені хакерами APT29, які не виявляли активності з минулого року…» ***(Російських хакерів підозрюють у розсиланні листів від імені держдепу США // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/270125-rosijsjkih_hakeriv_pidozrjujutj_u_rozsilanni_listiv_vid_imeni_derhdepu_ssha). 17.11.2018).***

***

«Хакеры научились взламывать старые iPhone и Mac с помощью поддельных сайтов, незаметно заменяя букву доменного имени. Об этом рассказали эксперты в области кибербезопасности Tencent Security Xuanwu Lab в блоге компании.

Исследователи утверждают, что в устаревших версиях браузера Safari некоторые символы из Юникода отображаются так же, как и обычные буквы. В частности, латинская буква d в поисковой строке будет выглядеть в точности, как символ dum. Причем пользователи не заметят разницу и не смогут распознать поддельную ссылку.

Брешь в системе безопасности устаревшей версии браузера позволяет мошенникам подделывать страницы популярных сайтов, в которых используется буква d: LinkedIn, Dropbox, Reddit, WordPress и множество других. После того, как жертва авторизируется в фейковом сервисе, злоумышленники получат их данные от оригинальной страницы.

Найденная специалистами уязвимость угрожает владельцам смартфонов и компьютеров от Apple, на которых не установлены последние обновления ОС. Среди потенциально опасных устройств эксперты отметили iPhone с версией iOS 11.4.1 и старше, а также iMac и MacBook с прошивками macOS High Sierra до 10.13.5. Чтобы не стать жертвами мошенников, специалисты посоветовали владельцам устаревших гаджетов обновить версию ОС до самой актуальной.» ***(Владельцы старых iPhone оказались под угрозой взлома // Goodnews.ua***

(http://goodnews.ua/technologies/vladelcy-staryx-iphone-okazalis-pod-ugrozoj-vzloma/). 21.11.2018).

***

«Два дня подряд хакеры атакуют Сбербанк, но только сегодня кредитное учреждение об этом сообщило… По словам заместителя председателя правления Станислава Кузнецова, речь идет о беспрецедентной кибератаке.

Серию мощнейших хакерских атак зафиксировали специалисты Сбербанка в среду и четверг. Согласно подсчетам, было не менее шести нападений. Удалось отследить, что атаки совершались через спутник с более чем 100 серверов из шести стран.

Станислав Кузнецов заявил, что кибератаки сильно беспокоят руководство банка. За два дня длительность DDoS-атак составила 1,5 часов.

«Одна из атак длилась около 27 минут. Это беспрецедентная по длительности атака, которая осуществлялась с помощью новых технологий с применением технологии спуфинга и сокрытия адресов отправителя», – поведал заместитель председателя правления Сбербанка. Он подчеркнул, что киберпреступники – настоящие профессионалы. Атака была проведена на высоком уровне, на ресурсы банка и его работу не повлияла. Главное, что интересовало хакеров – уровень защиты Сбербанка. Именно его они интенсивно исследовали в течение двух дней подряд…» ***(Сбербанк сообщил о беспрецедентной кибератаке // informing.ru (http://informing.ru/2018/11/30/sberbank-soobschil-o-besprecedentnoy-kiberatake.html). 30.11.2018).***

***

«Хакеры осуществили кибератаки на Бундестаг, Бундесвер и посольства в Берлине, подозрения снова ведут в Россию…

У депутатов Бундестага хакеры взломали электронную почту. При этом их интересовали партийные, а не парламентские аккаунты политиков. Последняя атака произошла 14 ноября.

Немецкое Федеральное ведомство по защите конституции (BfV) подозревает в атаках хакеров из группировки Snake (также известна под названиями Turla и "Уроборос"), которую немецкие власти связывают с российскими спецслужбами, говорится в материале. Какие данные удалось получить хакерам, пока неизвестно…» ***(В Германии - кибератаки на депутатов, посольства и Бундесвер. Подозревают хакеров РФ // Европейская правда (https://www.eurointegration.com.ua/rus/news/2018/11/30/7090061/). 30.11.2018).***

***

«Специалисты Trend Micro подготовили отчет о деятельности северокорейской хак-группы Lazarus. Исследователи предупреждают, что с середины сентября текущего года группировка заражает бэкдорами финансовые учреждения в странах Латинской Америки.

По словам экспертов, данные атаки перекликаются с деятельностью Lazarus в 2017 году, когда группа атаковала азиатские страны. Сейчас злоумышленники так

же используют в атаках файл FileTokenBroker.dll и тот же модульный бэкдор, который уже был замечен аналитиками ранее.

Малварь группы состоит из трех компонентов, каждый из которых отвечает за выполнение различных целей: AuditCred.dll/ROptimizer.dll играет роль загрузчика, который запускается как служба, Msadoz.dll – это сама зашифрованная бэкдор-малварь, а Auditcred.dll.mui/rOptimizer.dll.mui представляет собой конфигурационный файл вредоноса.

Проникнув в систему, преступники с помощью своего бэкдора получают возможность выполнять самые разные вредоносные задачи. Они могут: собирать различные данные о системе и похищать файлы, загружать дополнительную малварь, запускать или останавливать процессы, внедрять вредоносный код в запущенные процессы, удалять файлы, задействовать обратный шелл, прокси и так далее.

Эксперты Trend Micro предупреждают, что эта вредоносная кампания Lazarus сложна и опасна, равно как и другие кампании группы. Исследователи подчеркивают, что обнаруженная ими малварь намерено борется как с обнаружением, так и с удалением из системы (например, лоадер и файл конфигурации расположены в %windows%system32, тогда как сам бэкдор скрывается в другой директории, %Program Files%Common FilesSystemado)… «***(Северокорейские хакеры атакуют банки в Латинской Америке // Goodnews.ua (http://goodnews.ua/technologies/severokorejskie-xakery-atakuyut-banki-v-latinskoj-amerike/). 26.11.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«Сотрудники компании кибербезопасности McAfee Labs выявили новое российское ПО для криптоджекинга под названием WebCobra, тайно майнящее на компьютерах своих жертв криптовалюты Monero и Zcash.

По данным сотрудников McAfee Labs, приложение WebCobra, имеющее российское происхождение, тайно устанавливает майнеры Cryptonight или Claymore, в зависимости от конфигурации компьютера жертвы. В частности, на системах x86 это ПО встраивает код майнера Cryptonight, запускающий контроль над ходом процесса, а на системах x64 вирус изучает конфигурацию GPU, после чего скачивает и запускает майнер Zcash Claymore с удалённого сервера.

Хотя, по сведениям специалистов, ПО было разработано и впервые получило распространение в России, они выявляли его по всему миру: больше всего им оказались заражены компьютеры в Бразилии, Южной Африке и США.» ***(«Сетевая кобра»: компания Макафи выявила российский вирус, майнящий Monero и Zcash // BIGFIN (https://bigfin.net/14/11/2018/setevaja-kobra-kompanija-makafi-vyjavila-rossijskij-virus-majnjashhij-monero-i-zcash/). 14.11.2018).***

***

«Криптоджекинг с каждым днем становится все более и более продвинутым. Недавно специалисты компании The Next Web выяснили, что киберпреступники придумали внедрять скрытый майнер в инсталлятор ОС «Виндовс».

Вирус передается на машину в качестве файла MSI. Важно то, что установщик «Виндовс» является легитимным приложением. Учитывая это, у жертвы нет никаких подозрений в том, что имеется опасность для ПК. Потенциально вредоносное ПО обходит даже антивирусные программы…

На этом киберпреступники не останавливаются. В инсталляторе есть скрипт, противодействующий антивирусным программам. При этом повышается вероятность заражения машины другими вредоносными приложениями.

Чтобы специалисты по кибербезопасности не смогли проанализировать действие вируса и придумать «противоядие», в майнинговый модуль вложен механизм самоуничтожения. Эксперты предполагают, что это дело рук хакеров из РФ, так как инсталляционная программа на русском языке.» ***(Анастасия Чабанюк. С инсталлятором «Виндовс» идет в комплекте скрытый майнер // BitBet.news (https://bitbet.news/novosti-kriptovalyut/s-installjatorom-vindovs-idet-v-komplekte-skrytyj-majner/).***

***

«Лукас Стефанко, эксперт по кибербезопасности, нашел в Google Play приложения, которые помогали кибермошенникам воровать пароли от электронного банкинга и криптовалютных бирж. Лукас Стефанко утверждает, что в приложении Easy Rates Converter, которое предназначено для определения курсов валют, содержится вредоносная программа. Этот вирус замаскирован под обновление Adobe Flash. После скачивания приложения вирус ждет, когда пользователь откроет онлайн-банкинг или официальную страницу криптовалютной биржи, чтобы открыть фейковую страницу для входа в свой аккаунт. Таким образом хакеры воруют и используют данные клиентов. Эксперт пожаловался на приложение и его уже убрали из Google Play. Похожие приложения были обнаружены в Android app store. Стефанко советует читать комментарии перед установкой программ, так как обычно пострадавшие пользователи оповещают о скрытых угрозах.» ***(В Google Play нашли угрозу для клиентов онлайн-банкинга и криптобирж // Интернет-портал PaySpace Magazine (https://psm7.com/googlepay/v-google-play-nashli-fishingovye-prilozheniya.html). 05.11.2018).***

***

«Пользователи во всём мире стали чаще сталкиваться с вредоносным ПО, предназначенным для кражи денег через онлайн-доступ к банковским счетам.

Согласно внутренней статистике «Лаборатории Касперского», по итогам третьего квартала количество попыток запуска подобных зловредов на цифровых устройствах увеличилось на 41,5% по сравнению с предыдущим трёхмесячным периодом.

О том, что финансовые киберугрозы набирают силу, говорит и тот факт, что на протяжении всего 2018 года растёт число мобильных банковских троянцев. На текущий момент их доля среди всех мобильных угроз составляет почти 4,5%, при этом в начале года этот показатель был в три раза меньше. Наибольшее же число пользователей, столкнувшихся с банковскими троянцами на Android-устройствах, в третьем квартале было зафиксировано в России – эксперты связывают это с массированными атаками Asacub, пик которых пришёлся на конец лета и начало осени и преимущественно затронул русскоязычных пользователей.

С другой стороны, получить деньги своих жертв злоумышленники по-прежнему пытаются с помощью программ-шифровальщиков. И хотя, по подсчётам «Лаборатории Касперского», количество обнаруженных в третьем квартале модификаций шифровальщиков оказалось заметно ниже, чем в предыдущие три месяца, общее число атакованных ими пользователей в итоге выросло на 39%. Примечательно, что более чем на четверти устройств (29%) был обнаружен печально известный WannaCry, что говорит о том, что существенная доля пользователей так и не установила закрывающее уязвимость обновление, выпущенное полтора года назад…

В среднем же, по оценке «Лаборатории Касперского», в третьем квартале приблизительно каждый пятый компьютер в мире подвергся как минимум одной веб-атаке. Чуть большую долю компьютеров (23%) затронули локальные угрозы, распространяемые не через интернет, а с помощью съёмных устройств, например, USB-флешек.» ***(Число банковских зловредов выросло почти в полтора раза // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5544899-Chislo-bankovskix-zlovredov-vyroslo.html). 14.11.2018).***

***

«Експерти центру CERT-UA спільно зі Службою зовнішньої розвідки України виявили нові модифікації шкідливого програмного забезпечення Pterodo на комп'ютерах державних органів України.

На думку експертів CERT-UA такі програми, імовірно, є підготовчим етапом для проведення кібератаки…

Цей вірус, назва якого походить від латинської назви птеродактиля, збирає дані про систему, регулярно відправляє їх на командно-контрольні сервери і очікує подальших команд.

Основною відмінністю цієї версії від попередніх є можливість інфікування системи через флеш-накопичувачі та інші знімні носії інформації.» ***(На комп'ютерах держорганів України виявили шкідливу програму, через яку можлива кібератака // Західна інформаційна корпорація (https://zik.ua/news/2018/11/21/na_kompyuterah_derzhorganiv_ukrainy_vyyavyly_shkidlyvu_programu_cherez_yaku_1452649). 21.11.2018).***

***

«Google удалил 13 приложений из Google Play в эти выходные после обнаружения в них вредоносного ПО…

Приложения загружали в общей сложности 560 000 тысяч раз, прежде чем их удалили из Google Play. 13 программ разработал один и тот же человек – Луис О. Пинто, подделав их под гоночные игры.

Когда пользователь, загрузив игру, пытался ее запустить, то ему это не удавалось, в то же время вредоносное ПО все равно устанавливалось на телефон или планшет.

Указанные приложения "скрывают" себя и свои иконки после запуска, и просят пользователей установить на устройство дополнительный APK под названием "Game Center".

Два приложения вошли в топ-игр Google Play, прежде чем были удалены…» ***(Ирина Фоменко. Очередной прокол: полмиллиона пользователей закачали вирусы из Google Play под видом приложений // Internetua (http://internetua.com/ocserednoi-prokol-polmilliona-polzovatelei-zakacsali-virusy-iz-google-play-pod-vidom-prilojenii). 27.11.2018).***

***

«…Нова версія відомого банківського троянця TrickBot, що з'явився у 2016 році, стала збирати інформацію про функціонування та збої операційної системи Microsoft Windows. Ці дані надає функція Reliability Analysis Component (RAC). Вона веде журнал про стабільність Windows, встановлення програмного забезпечення, оновлення, помилки в ОС і додатках, а також про апаратні збої.

Дані агент RACAgent збирає щогодини і зберігає їх у локальній папці C:\ProgramData\Microsoft\RAC\. Цю опцію можна відключити через «Планувальник завдань».

Експерти вважають, що зібрані відомості про стабільність роботи комп'ютера можуть використовуватися для фішингу. Вони також можуть підказати хакерам слабкі місця в системі для подальшої атаки.

TrickBot останнім часом активно поширюється у вигляді фальшивих повідомлень від банку Lloyds Bank. Листи нібито виходять з адреси donotreply@lloydsbankdocs.com, а шкідливий код міститься в макросі у вкладеному файлі Microsoft Word. Документ також містить логотип антивірусної компанії Symantec, щоб переконати користувача, що він пройшов перевірку на шкідливе ПЗ, проте як мінімум 30 антивірусів ідентифікують цей файл як шкідливий.» ***(Євген Корольов. Хакери почали збирати дані про збої комп'ютерів, експерти з кібербезпеки не знають, навіщо // Tech Today (https://techtoday.in.ua/news/hakeri-pochali-zbirati-dani-pro-zboyi-komp-yuteriv-eksperti-z-kiberbezpeki-ne-znayut-navishho-106838.html). 28.11.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Европол подвел итоги девятого этапа глобальной операции In Our Sites (IOS), направленной на пресечение торговли поддельными товарами и пиратской продукцией. Совместные усилия правоохранительных органов 26 государств, Национального координационного центра по защите интеллектуальной собственности США (NIPRCC) и других организаций привели к закрытию более 33 тыс. сайтов, продававших контрафакт.

Управление антипиратской кампанией осуществляла Координационная коалиция по вопросам защиты интеллектуальной собственности (IPC3), входящая в состав Европола. Как сообщили ее представители, благодаря совместной работе представителей брендов, силовых ведомств и общественных организаций удалось отключить на 13 тыс. доменов больше, чем в 2017 году. Специалисты полагают, что такой результат обусловлен комплексным подходом Европола к борьбе с торговлей контрафактной продукцией.

Помимо закрытия криминальных сайтов, правоохранительным органам удалось задержать 12 подозреваемых в пиратстве, а также арестовать более €1 млн на счетах киберпреступников в банках и электронных платежных системах. Специалисты IPC3 также сообщают о блокировке майнинг-ферм, принадлежавших злоумышленникам.

Важным элементом борьбы с распространением контрафакта является информационная кампания Don't F***(ake) Up, призванная рассказать покупателям об опасности приобретения подделок. В рамках программы пользователям объясняют, как отличить сайт-клон от легитимного ресурса, а также дают рекомендации по выявлению фальшивых приложений и аккаунтов в социальных сетях…» ***(Egor Nashilov. Борцы с контрафактом заблокировали более 33 тыс. сайтов // Threatpost (https://threatpost.ru/europol-dont-fake-up-initiative-blocks-33k-counterfeit-sites/29405/). 27.11.2018).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Исследователи компании Armis, занимающейся обеспечением безопасности устройств интернета вещей, сообщили об обнаружении двух опасных уязвимостей Bluetooth Low Energy (BLE) чипов, производимых компанией Texas Instruments.

Эти чипы широко используются, в частности, в точках доступа для корпоративных сетей производства Cisco Systems, Meraki (принадлежит Cisco) и Aruba Networks, вместе удерживающих не менее 70% рынка этих устройств. Кроме того, BLE-чипы от Texas Instruments применяются в таких медицинских устройствах как водители сердечного ритма и инсулиновые помпы, а также во множестве устройств интернета вещей.

Уязвимости получили общее название BLEEDINGBIT. Первая из них, CVE-2018-16986, может быть проэксплуатирована для повреждения памяти с последующим установлением полного контроля над системой. Причем атакующий не должен быть авторизован в сети, однако должен находиться поблизости от уязвимого устройства, на котором включен BLE-модуль и активирован режим сканирования. В этом случае для успешной атаки достаточно отправки на устройство специально созданного вредоносного пакета. (В компании Cisco назвали такое сочетание условий маловероятным, отметив, что на ее устройствах BLE-модуль по умолчанию не включен, а режим сканирования не активирован.) Уязвимость CVE-2018-7080 представляет собой бэкдор, используемый в процессе производства для беспроводной загрузки прошивки. Ее эксплуатация подразумевает использование предустановленного пароля.

Компания Texas Instruments уже выпустила обновление ПО, устраняющее уязвимость CVE-2018-16986. В отношении CVE-2018-7080 представители компании ограничились рекомендацией производителям устройств: отключить функцию беспроводной загрузки прошивки, поскольку она необходима лишь на стадии сборки и тестирования.» ***(Обнаружена опасная уязвимость BLEEDINGBIT // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5542780-Obnaruzhena-opasnaya-uyazvimost-BLE.html#ixzz5WukeTIVe). 06.11.2018).***

***

«В ряде решений для управления производственными процессами от компании Siemens выявлены множественные уязвимости, в том числе проблемы, позволяющие удаленно выполнить код или вызвать отказ в обслуживании устройства. Уязвимости затрагивают продукты Siemens IEC 61850 System Configurator, DIGSI 5, DIGSI 4, SICAM PAS/PQS, SICAM PQ Analyzer, SICAM SCC, SIMATIC, SIMATIC WinCC и SCALANCE S.

Решения Siemens IEC 61850 System Configurator, DIGSI 5, DIGSI 4, SICAM PAS/PQS, SICAM PQ Analyzer подвержены уязвимости (CVE-2018-4858), позволяющей извлечь ограниченный объем данных из системы либо выполнить произвольный код с разрешениями пользователя Microsoft Windows. Степень опасности проблемы оценена в 4,2 балла по шкале CVSS v3.

В продуктах Siemens SIMATIC, SIMATIC WinCC , SIMATIC S7 , SIMATIC STEP 7 , SIMATIC IT Production Suite выявлено в общей сложности 6 уязвимостей, позволяющих внедрить произвольный HTTP-заголовок, вызвать сбой в работе устройства, восстановить пароли, обойти аутентификацию на уровне приложения или извлечь файлы с устройства. Степень опасности проблем варьируется от 4 до 7,7 баллов по классификации CVSS v3.

Модули сетевой безопасности серии SCALANCE S содержат уязвимость (CVE-2018-16555), предоставляющую возможность осуществления XSS-атак. Для успешной атаки злоумышленнику потребуется заставить пользователя нажать на вредоносную ссылку.

Наиболее опасные уязвимости обнаружены в модульных программируемых контроллерах серии SIMATIC S7-400 (CVE-2018-16556 и CVE-2018-16557). С их помощью атакующий может вызвать отказ в обслуживании устройства. Для

восстановления работы может потребоваться переустановить вручную или перепрошить устройства. Опасность проблем оценена в 7,5 и 8,2 балла по шкале CVSS v3 соответственно.» ***(В промышленных продуктах Siemens обнаружены опасные уязвимости // ООО "Гротек" (http://itsec.ru/newstext.php?news_id=125587). 15.11.2018).***

***

«Из-за слабой культуры кибербезопасности промышленные системы управления продолжают оставаться легкими целями для хакеров. Эксперты CyberX подготовили отчет, в котором подсказывают, что здесь происходит не так, и предлагает наилучшие пути для исправления ситуации.

До 40% промышленных объектов имеют хотя бы одно подключение к общедоступному Интернету

Отсутствие подключения критически важных систем остается эффективным способом снижения вероятности атаки. Отсутствие связи с Интернетом означает, что для выполнения необходимых им операций инициаторы атак должны находиться непосредственно на объекте. Однако многие компании не обеспечивают такой изоляции. Более трети промышленных объектов имеют по крайней мере один канал связи с Интернетом. Поисковые инструменты (например, Shodan) упрощают обнаружение устройств, не обладающих надежной защитой и позволяющих атакующим легко вторгаться в промышленные сети. А для того чтобы проникнуть в систему, вполне достаточно и одного канала.

По крайней мере одну беспроводную точку доступа имеют 16% объектов, а у 84% есть хотя бы одно устройство, к которому можно обращаться удаленно. И то, и другое является дополнительной лазейкой для проникновения атакующих.

На 53% объектов установлены устаревшие версии Windows

У промышленных объектов зачастую имеются встроенные системы, обновлять которые достаточно сложно, не говоря уже о том, чтобы сменить установленную там операционную систему. Устаревшие и уже неподдерживаемые версии Windows не содержат исправлений для новых уязвимостей, формирующих в системе безопасности значительные пробелы. Более половины промышленных объектов, мониторинг которых осуществляет CyberX, имеют устаревшие и неподдерживаемые версии Windows.

Поддержка Windows Vista истекла в 2017 году, XP – в 2014-м. Жизненный цикл Windows 8 подошел к концу в 2016 году (у 8.1 еще осталось немного времени), а Windows 7 будет списана со счетов в 2020-м. Хотя компании и могут получить от Microsoft расширенную поддержку, стоит это дорого и представляется всего лишь временным решением.

В 69% сетях промышленных систем используются незашифрованные пароли…

«Обычно они связаны с унаследованными устройствами, которые не поддерживают современные безопасные протоколы, такие как SNMP v3 или SFTP», – говорится в отчете.

57% объектов не имеют систем антивирусной защиты с автоматическим обновлением сигнатур…

Промышленные системы сегодня действительно небезопасны, но еще сильнее беспокоит отсутствие какого-либо прогресса в этой области. «За прошедший год в отрасли мало что изменилось», – говорится в отчете CyberX. Единственное, где по сравнению с прошлогодним исследованием произошли существенные изменения – это уменьшение числа объектов с унаследованными системами Windows. Их доля сократилась с 76% в 2017 году до 53% в 2018-м…

Зачастую промышленным системам уже немало лет. Поскольку вносить в них коррективы слишком сложно и дорого, на протяжении многих лет они сохраняются в неизменном виде. Исследование CyberX показало, что чаще всего на промышленных предприятиях используется Modbus, протокол последовательной связи, впервые опубликованный компанией Modicon (ныне Schneider Electric) в 1979 году.

Это создает дополнительные трудности для мониторинга, поскольку традиционные инструменты, проектировавшиеся для корпоративных ИТ-сетей, не видят протоколов наподобие Modbus TCP, а значит, организации не знают, что делается в их сети. Опрос, проведенный «Лабораторией Касперского», показал, что у почти половины предприятий нет инструментов для выявления атак на их устройства промышленных систем управления…» ***(2019: Что будет с безопасностью промышленных систем управления и Интернета вещей // «Открытые системы» (https://www.computerworld.ru/articles/2019-Chto-budet-s-bezopasnostyu-promyshlennyh-sistem-upravleniya-i-Interneta-veschey). 15.11.2018).***

***

«Ставшие привычными для граждан технологии мобильных и онлайн-банков крайне уязвимы для хакеров, выяснили специалисты по кибербезопасности Bi.Zone. Злоумышленники могут воспользоваться, например, слишком продолжительной сессией клиента в мобильном банке или подобрать трансакцию под пароль, а не наоборот. Риски высоки более чем в половине работающих в РФ мобильных банков, и клиентам остается только проявлять предусмотрительность.

О самых распространенных уязвимостях мобильных и онлайн-банков рассказал на конференции OFFZONE 2018 ведущий специалист по тестированию на проникновение Bi.Zone (дочерняя структура Сбербанка, специализирующаяся на кибербезопасности) Аркадий Литвиненко. По его словам, используемая сейчас рассылка одноразовых паролей в СМС-сообщениях для подтверждения входа в личный кабинет в онлайн-банке или мобильном банке — это «порочный путь», который может привести к хищению. Проблема в безопасности передачи самого пароля: по поддельной доверенности и скану паспорта жертвы можно получить дубликат сим-карты. Есть и сравнительно недорогие устройства (от $700) для перехвата СМС-сообщений. И, по словам Аркадия Литвиненко, это далеко не единственная уязвимость.

Так, в большинстве банков для подтверждения трансакций используются одноразовые пароли из СМС из четырех цифр, при трижды неверно введенном пароле трансакция блокируется. «Но можно перебирать трансакцию под пароль (например, 5555), то есть создать множество операций по списанию средств со

счета клиента, при подборе 16 тыс. трансакций вероятность угадать пароль — 99%»,— отмечает эксперт.

Конечно, клиент банка может не заметить 16 тыс. СМС от банка с одноразовым паролем разве что ночью или в отпуске, когда не пользуется телефоном постоянно, но это не исключено, отмечают эксперты.

Получить доступ к личному кабинету в онлайн-банке злоумышленники могут, если клиент, к примеру, прошел по ссылке в фишинговом письме или случайно загрузил вредоносное программное обеспечение, отмечает руководитель лаборатории практического анализа защищенности Центра информационной безопасности «Инфосистемы Джет» Лука Сафонов.

По данным Positive Technologies, по итогам 2017 года компания выявила критически опасные уязвимости более чем в половине онлайн-банков. При этом недостатки авторизации выявляли в 63% случаев…

По данным Positive Technologies, уязвимости в 52% мобильных банков позволяли расшифровать, перехватить и подобрать учетные данные для доступа в мобильное приложение или обойти процесс аутентификации. Данные для взлома мобильных банков активно продаются в даркнете, отмечают в Positive Technologies. При этом средняя стоимость «входа» в мобильный банк составляет $22.

Впрочем, доля систем дистанционного банковского обслуживания, в которых обнаруживаются критически опасные уязвимости, снижается с каждым годом. Если в 2015 году уязвимости высокого уровня риска содержались в 90% проанализированных систем, а в 2016 году — в 71%, то по итогам 2017-го уже только в 56%, указывают в Positive Technologies. Тем не менее клиентам необходимо знать о возможных рисках и проявлять предусмотрительность (см. справку).» ***(Вероника Горячева. Хакеры держат дистанцию. Удаленное банковское обслуживание уязвимо для хищений // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3805158). 20.11.2018).***

***

«Популярные смарт-часы, отслеживающие геолокацию детей, настолько легко взломать, что их должны снять с продажи…

MiSafes Kid's Watcher Plus - это GPS-устройство для мониторинга местоположения ребенка и звонков, которое используют тысячи родителей в Великобритании.

Исследователи обнаружили серьезные недостатки безопасности в продукте, в том числе использование незашифрованных данных. Так, хакеры могут загружать программное обеспечение для отслеживания местоположения ребенка, слушать его разговоры и звонить ему, притворяясь родителями…

Смарт-часы MiSafes, впервые вышедшие на рынок в 2015 с ценой в 9 фунтов стерлингов, имеют функцию GPS, которая обновляется в реальном времени и отслеживает предыдущие местоположения. Часы также позволяют осуществлять звонки…» ***(Ирина Фоменко. Смарт-часы, которые отслеживают местоположение ребенка, могут взломать преступники // Internetua (http://internetua.com/smart-csasy-kotorye-otslejivauat-mestopolojenie-rebenka-mogut-vzlomat-prestupniki). 16.11.2018).***

***

«Второй год подряд Mozilla публикует руководство по подаркам, отмечая опасные и безопасные с точки зрения ИБ продукты.

…По мнению ИБ-экспертов, худшим подарком с точки зрения безопасности данных являются игрушки с выходом в интернет…

Второй год подряд Mozilla публикует руководство по подаркам под названием « Privacy Not Included » («Приватность в комплект не входит»). В руководстве с точки зрения ИБ описаны десятки самых популярных подарков. Список нынешнего года включает в себя семьдесят наименований, начиная от «умных» колонок и заканчивая устройствами для вакуумной готовки.

Совместно с организацией Internet Society and Consumers International компания Mozilla также опубликовала список минимальных требований безопасности и отметила соответствующие им продукты.

Подключенные к интернету продукты могут считаться заслуживающими доверие, если в них реализовано шифрование, присутствует механизм автоматической установки обновлений безопасности, надежно защищены пароли, уязвимости исправляются по мере их обнаружения, а пользовательские соглашения написаны доступным языком.

Из семидесяти включенных в руководство подарков Mozilla одобрила тридцать три, в том числе Nintendo Switch, Google Home и Harry Potter Kano Coding Kit. Как самые небезопасные с точки зрения защиты данных компания отметила семь продуктов. В список попал прибор для вакуумной готовки Anova Precision Cooker, селфи-дрон DJI Spark Selfie Drone, дрон Parrot Bebop 2 и как минимум одна видео-няня.» ***(Mozilla опубликовала список небезопасных с точки зрения ИБ подарков // SecurityLab.ru (https://www.securitylab.ru/news/496529.php). 15.11.2018).***

***

«Представители социальной сети Facebook объявили, что увеличивают вознаграждение, которое с 2011 года выплачивается ИБ-исследователям за найденные уязвимости. Теперь «белые» хакеры смогут получить $40 тыс. за описание способа взлома учетных записей без привлечения пользователя. Если минимальное взаимодействие с хозяином аккаунта все же потребуется, то награда составит $25 тыс. Такие условия будут действовать и для других продуктов компании — WhatsApp, Instagram и Oculus.

При этом исследователям не придется раскрывать, как именно они обошли защиту, в которой задействован механизм Link Shim, предотвращающий переходы по сомнительным ссылкам. После каждого клика по внешнему URL, Link Shim сверяется со списком вредоносных и фишинговых сайтов, чтобы убедиться, что пользователя не перенаправили на подозрительный ресурс. Кроме того, он сканирует контент в почтовой рассылке Facebook на наличие вредоносного содержимого.

Социальную сеть интересуют любые ошибки, которые могут привести к захвату учетных записей пользователей, вне зависимости от того, в какой форме

это произойдет — прямая кража данных, утечка маркеров доступа или возможность подключения к текущей сессии…» ***(Egor Nashilov. Компания Facebook повысила премии багхантерам // Threatpost (https://threatpost.ru/facebook-offers-up-to-40k-dollars-for-bugs/29382/). 23.11.2018).***

Технічні та програмні рішення для протидії кібернетичним загрозам

«За допомогою нової програми дослідники допомагають правоохоронним органам боротися з шахраями, які крадуть дані електронних поштових скриньок

Як пише Eurek Alert, новий інструмент візуальної аналітики значно прискорює досудові розслідування і виділяє критичні посилання.

Правоохоронним органам часто не вистачає ресурсів для ідентифікації кіберзлочинців, які продовжують активну діяльність щодо електронного листування користувачів.

Для вирішення питання дослідницька група з Нью-Йоркського університету разом з компанією Agari розробила програму "Бігль" (Beagle) - візуальний аналітичний інтерфейс, який може працювати з безліччю листів, підсумовувати дані з них, виділяти загальні риси.

Вчені наголосили, що програма добре систематизує дані, які правоохоронці часто не помічають - час відправлення листа, місце розташування жертв, ключові слова та шаблони шахраїв…» ***(Американські вчені розробили дієву програму для боротьби із кібершахраями // Espreso.tv (https://espreso.tv/news/2018/11/05/amerykanski_vcheni_rozrobyly_diyevu_programu_dlya_borotby_iz_kibershakhrayamy). 05.11.2018).***

***

«Несмотря на то что Microsoft официально не объявила о поддержке протокола WPA3, в сборке Windows 10 SDK 18272, также известной как 19H1, появилось несколько API, поддерживающих новый стандарт безопасности Wi-FI.

Новый стандарт безопасности беспроводной связи был представлен летом 2018 года. WPA3 использует одновременную аутентификацию равноправных элементов (Simultaneous Authentication of Equals, SAE) — новую технологию проверки подключаемых устройств, устойчивую перед атаками с переустановкой ключа (Key Reinstallation Attacks, KRACK). SAE основана на принципе, согласно которому каждая из сторон может независимо от другой отправить как запрос на соединение, так и удостоверяющую информацию.

Предыдущее поколение стандарта WPA2-Personal использовало технику PSK (Pre-Shared Key), основанную на алгоритме валидации путем сообщения пароля после «обмена четырьмя рукопожатиями» — именно в него вмешивался злоумышленник методом KRACK и на третьем «рукопожатии» перехватывал ключ.

Технология SAE предназначена для личных устройств и обеспечивает безопасность даже при использовании слабых паролей. Для передачи информации по корпоративным сетям в WPA3-Enterprise по умолчанию предусмотрено 128-битное шифрование, однако при желании можно задействовать кодирование в 192 бита…» ***(Dmitry Nazarov. В Windows 10 может появиться поддержка WPA3 // Threatpost (https://threatpost.ru/windows10-may-support-wpa3/29141/). 13.11.2018).***

***

«На этой неделе компания Cisco выпустила 16 обновлений безопасности, которые закрывают множество брешей в разных продуктах. Четыре уязвимости являются критическими, еще одной присвоен высокий уровень опасности, а 11 остальным— средний. Помимо этого, вендор признал, что во время проверки качества сборки ПО разработчики забыли удалить из ряда продуктов специально внедренный эксплойт.

Один из патчей касается библиотеки Commons FileUpload фреймворка Struts 2.3.36 или более ранних версий. О бреши стало известно из опубликованного Apache Struts Team 5 ноября бюллетеня безопасности, хотя впервые ее обнаружили еще два года назад. Выяснилось, что исправление уязвимости CVE-2016-1000031, вышедшее летом 2017 года, не было учтено при выпуске новых сборок.

Баг позволял злоумышленникам удаленно выполнить код и манипулировать файлами. Производитель рекомендовал заменить файл библиотеки вручную и проверить системы на наличие его копий. В связи с этим Cisco изучает свои продукты и услуги, чтобы определить, какие из них может затрагивать эта уязвимость. На данный момент CVE-2016-1000031 обнаружена только в USC RMS — системе управления маломощными беспроводными точками доступа (микросотами). Список будет пополняться по мере продвижения исследования. Отслеживать изменения можно на странице бюллетеня.

Другое важное исправление касается критической уязвимости CVE-2018-15394, вызванной небезопасной конфигурацией. Эта брешь в консоли управления системой мониторинга StealthWatch может позволить удаленному злоумышленнику обойти процесс аутентификации и пользоваться правами администратора. Баг затрагивает продукты линейки Cisco Stealthwatch Enterprise выпусков 6.10.2 и более ранних.

Еще одна серьезная брешь была найдена в серии коммутаторов Cisco Small Business. CVE-2018-15439 также позволяет удаленному злоумышленнику обойти аутентификацию на устройстве и получить права администратора…

Четвертая из критических брешей, CVE-2018-15381, касается выполнения команд в модуле Cisco Unity Express. Ошибка связана с десериализацией Java-объектов в интерфейсе вызова удаленных методов (RMI). Успешный эксплойт может позволить злоумышленнику выполнить на устройстве произвольные команды с root-привилегиями. Баг затрагивает все выпуски Unity Express до 9.0.6 включительно…» ***(Dmitry Nazarov. Cisco пропатчила 16 уязвимостей в своих продуктах // Threatpost (https://threatpost.ru/cisco-patched-16-vulnerabilities-in-products/29090/).*** 09.11.2018).

***

«Разработчик решений в области информационной безопасности представил обновленные программы для защиты от криптоджекинга и других атак.

По данным Avast, количество атак, для которых применяется вредоносный код для майнинга в браузере, меняется вслед за колебаниями курсов криптовалют. Киберпреступники планируют свою деятельность с учетом популярности цифровых активов, считают аналитики компании. За последние несколько месяцев число атак снизилось — вместе со стоимостью большинства цифровых денег. Одной из причин этого являются расходы киберпреступников: им нужно поддерживать собственные сайты, разрабатывать новые уловки и обслуживать командные серверы. Поэтому майнинг прибылен только в определенное время…

Между тем 41% россиян не обеспокоены тем, что их устройства могут использоваться для незаконной добычи криптовалюты, выяснили в Avast. 32% и вовсе считают, что они не могут стать жертвами криптоджекинга, потому что не владеют майнинг-фермами и не занимаются добычей криптовалюты. При этом 82% опрошенных о такой угрозе в принципе слышали.

Для защиты от криптоджекинга и других атак (в том числе, мобильных угроз, уязвимостей устройств Интернета вещей и др.), а также оптимизации производительности компьютеров в Avast представили новые версии Avast Cleanup для ПК и Mac. Улучшенные программы обнаруживают рекламные приложения, пробные версии программ, панели инструментов и другое лишнее предустановленное ПО.

Avast Cleanup для ПК формирует список всех установленных программ с присвоенным им рейтингом, составленном на основе эвристических алгоритмов, рекомендательного механизма Avast, а также облачного пользовательского рейтинга. Если какая-либо программа вызывает сомнения, ее можно поместить в «карантин». Функция «Спящий режим» временно замораживает всю фоновую активность приложения, что повышает производительность ПК. Avast Cleanup для Mac предлагает новую функцию Photo Cleaner, которая позволяет обнаружить некачественные фотографии и дубликаты и предлагает рекомендации по их удалению.

Также компания выпустила новую версию антивируса Avast 2019. Обновленная программа предлагает режим «Не беспокоить», защиту персональных данных и распознавание угроз с помощью искусственного интеллекта.

Функция «Не беспокоить» позволяет не отвлекаться на оповещения от различных сервисов во время работы. Благодаря ей вредоносный код не может просматривать и изменять файлы. Искусственный интеллект находит фишинговые сайты путем автоматической проверки URL-адреса сайта на наличие подозрительных маркеров, метаданных домена и проверки визуальных деталей сайтов. Интеллектуальное сканирование в состоянии отслеживать вирусы, сетевые проблемы и т.д. одновременно – процесс запускается одним щелчком.

Новая версия Avast 2019 доступна для Avast Free Antivirus, Avast Internet Security и Avast Premier. Avast Free Antivirus защищает от программ-вымогателей, криптоджекинга, шпионских программ, фишинга, вредоносных URL-адресов в

Интернете и вложений. Программа предупреждает об угрозах безопасности в домашней сети с помощью Wi-Fi Inspector и предлагает управление паролями через Avast Пароли. Она тоже имеет режим «Не беспокоить» и использует искусственный интеллект для блокировки продвинутых фишинговых атак. Avast Internet Security помимо этого предоставляет расширенную защиту от программ-вымогателей, запуск файлов в безопасной среде, брандмауэр и защиту от спама. Avast Premier ко всему прочему дает защиту от слежки через веб-камеру…» ***(Мелиса Савина. Avast: активность криптомайнеров увеличивается на волне роста крипто валют // «Открытые системы» (https://www.computerworld.ru/articles/Avast-aktivnost-kriptomaynerov-uvelichivaetsya-na-volne-rosta-kriptovalyut). 06.11.2018).***

***

«…На минувшей неделе Федеральное управление по информационной безопасности Германии (Bundesamt für Sicherheit in der Informationstechnik, BSI) опубликовало рекомендации и минимальные требования по обеспечению безопасности маршрутизаторов…

По мнению ведомства, необходим «управляемый уровень безопасности» и защитные функции, которые «должны быть реализованы в дизайне и активированы по умолчанию». Для защиты домашних маршрутизаторов и устройства класса SOHO (Small office/Home office) в документе предлагаются следующие меры:

Установить ограничение LAN/Wi-Fi до DNS, HTTP/HTTPS, DHCP/DHCPv6 и ICMPv6, с публичного интерфейса должен быть доступен минимальный набор сервисов (CWMP для конфигурации, SIP, если есть поддержка VoIP, и ICMPv6);

Закрыть гостевым Wi-Fi сервисам доступ к настройкам устройства;

Установить шифрование WPA2 в качестве минимального значения по умолчанию, использовать надежный пароль, в котором будут исключены упоминания производителя, модели или MAC-адреса;

Установить стойкую парольную защиту на интерфейс настроек, использовать HTTPS, если это доступно в интерфейсе WAN;

Сделать обязательным использование межсетевого экрана;

Возможность удаленной конфигурации должна быть отключена по умолчанию, удаленная настройка должна быть доступна только через зашифрованное, авторизованное сервером соединение;

Контролируемые пользователями обновления прошивки с возможностью уведомления о доступности патча.

В рекомендациях также указывается, что сброс настроек к заводским должен возвращать настройки безопасности к первоначальному значению, а все персональные данные должны удаляться с устройства.

Участники команды OpenWRT и сообщества Chaos Computer Club (CCC) раскритиковали идеи ведомства, отметив, что BSI пропустило два важных аспекта. Во-первых, производители должны информировать пользователей о том, как долго они намерены выпускать обновления безопасности для своих продуктов. Во-вторых, у владельцев устройств должна быть возможность устанавливать пользовательское ПО даже после «окончания официальной поддержки». Кроме

того, идея предоставить пользователям минимальный уровень безопасности недоработана - на самом деле уровень защиты будет зависеть от производителей (при условии, что они будут следовать директиве), подчеркивают специалисты.» ***(Немецкие власти разработали правила защиты маршрутизаторов // SecurityLab.ru (https://www.securitylab.ru/news/496607.php). 21.11.2018).***

***

«Підрозділ кібербезпеки компанії Alphabet, Jigsaw, розробив продукт, покликаний забезпечити максимальну безпеку даних у поєднанні з простотою установки і використання. По суті, це проект компанії Google, так що про якість продукту можна не переживати. Він розрахований на людей, що не мають глибоких технічних знань – журналістів та активістів, вимушених працювати в умовах цензури.

Часто у таких умовах користувачі покладаються на різних провайдерів сервісів VPN, але не мають можливостей перевірити, наскільки даються тими гарантії безпеки даних відповідають реальності. До того ж, раніше експерти з безпеки повідомили, що більшість VPN-сервісів не гарантують конфіденційність, так що і їм не варто довіряти. Нехай вони і змінюють ваше фактичне розташування в мережі, але за перегляд ваших історій браузера і відвіданих сайтів ніхто не відповідає.

На відміну від них, приватний VPN Outline, створений Jigsaw, це продукт з відкритим кодом, аудит якого проводить некомерційна консультаційна організація Radically Open Security.

Клієнтські додатки доступні для платформ iOS, Android, Windows, macOS, Chrome OS, так що можна сміливо завантажувати і не боятися злому, якщо ви довіряєте Google.» ***(Цензури не уникнути: Google представила новий сервіс // znaj.ua (https://znaj.ua/techno/190292-cenzuri-ne-uniknuti-google-predstavila-noviy-servis). 26.11.2018).***

***

«Компания Adobe выпустила внеплановое обновление безопасности, устраняющее критическую уязвимость (CVE-2018-15981) в версиях Flash Player для Windows, Mac и Linux. Воспользовавшись уязвимостью, злоумышленник может добавить вредоносный код в файл .swf, внедрить его на интернет-страницу и скрыто установить вредоносное ПО на устройства, с которых посещалась данная страница.

У Adobe нет четкого графика релиза патчей, неделю назад компания уже выпустила обновления безопасности, устраняющие ряд уязвимостей раскрытия информации в продуктах Flash Player, Acrobat, Reader и Photoshop CC. Выход нового патча через столь короткий промежуток говорит о том, что речь идет о довольно опасной уязвимости.

Пользователям рекомендуется обновиться до версии Flash Player 31.0.0.153 и более поздних как можно скорее. Учитывая множественные уязвимости, которые то и дело обнаруживаются в плагине, многие специалисты в области кибербезопасности советуют удалить Flash Player или хотя бы отключить его по

умолчанию.» ***(Adobe выпустила экстренный патч для уязвимости в Flash Player // Goodnews.ua (http://goodnews.ua/technologies/adobe-vypustila-ekstrennyj-patch-dlya-uyazvimosti-v-flash-player/). 22.11.2018).***

***

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

Х науково-практична конференція «Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО», 9-10 листопада 2017 року : (доп. та тези доп.). - Київ, 2017. - 283 с.

Зі змісту:

- Грохольський Я.М., Грохольський Р.Я., Шелепенко О.Ю. Проблемні аспекти фільрації сигналів;
- Євецький В.Л., Попов В.В., Гуменюк Н.О. Система захисту інформації на основі нейронної мережі;
- Куцаєв В.В., Терещенко Т.П., Козубцов І.М. Спеціальне програмне забезпечення по виявленню шкідливого програмного контенту в інформаційно-телекомунікаційних системах ЗС України;
- Макарчук О.М., Марченко О.В. Види комп'ютерних атак та методи їх виявлення;
- Татьянін В.В., Кириченко Т.В. Криптографічний захист інформації в системах зв'язку та управління. CASPER – захищений носій ключової інформації;
- Успенський О.А., Колісник Є.М. Методика побудови системи захисту комп'ютерної мережі на основі розподіленого сканування портів;
- Цуркан В.В., Гирда В.А., Пахольченко Д.В., Канарський Ю.В. Аналіз процесу виявлення «тролів» у соціальних мережах;
- Цуркан В.В., Дуденко О.В. Отримання даних з відкритих джерел у глобальній мережі Інтернет;
- Цуркан В.В., Легенький Р.О., Сільницький А.О. Порівняльна характеристика систем виявлення вторгнень у комп'ютерні мережі;
- Цуркан В.В., Мітін С.В., Мельник О.Ю. Аналіз процесу тестування на проникнення у комп'ютерні системи та мережі.

Шифр зберігання НБУВ: СО35923.

***

Актуальні питання протидії злочинності в сучасних умовах: вітчизняний та зарубіжний досвід = Актуальные вопросы противодействия преступности в современных условиях: отечественный и зарубежный опыт = Current issues of combating crime: national and international experience : матеріали II Міжнар. наук.-практ. конф., (15 берез. 2018 р., Дніпропетр. держ. ун-т внутр. справ). - Дніпро, 2018. - 479 с.

Зі змісту:

- Риб'янець С.А., Соболь О.І. Інформаційна безпека в мережі Інтернет;
- Южека Р.С. Проблемні питання протидії кіберзлочинності в Україні.

Шифр зберігання НБУВ: ВА824791.

***

Актуальні проблеми державотворення, правотворення та правозастосування : матеріали наук. семінару, (9 груд. 2016 р., Дніпропетр. держ. ун-т внутр. справ). - Дніпро : Ліра, 2017. - 479 с.

Зі змісту:

- Малиновський В.О. Ознаки сучасної кіберзлочинності;
- Шматкова А.В. Проблеми національного законодавства у сфері боротьби із кіберзлочинністю;
- Яковлєва Ю. Основні проблеми захисту персональних даних в мережі Інтернет.

Шифр зберігання НБУВ: ВА824788.

***

Бердиченко І.О. Правове забезпечення кібернетичної безпеки України : навч. посіб. / І. О. Бердиченко. - Полтава, 2018. - 126 с.

Узагальнено нові теоретичні здобутки та існуючу практику протидії кібернетичній злочинності в Україні. Грунтуючись на наукових узагальненнях учених-правознавців та власних практичних розробках, автор пропонує своє бачення розв'язання низки складних дискусійних у теорії кримінального права та кримінології питань, зокрема стосовно правових засобів та методів протидії кібернетичній злочинності в Україні.

Шифр зберігання НБУВ: ВА824548.

***

Богославський М.Ю. Організація зберігання електронних архівів банку як забезпечення протидії кібератакам / М.Ю.Богославський // Науковий вісник Полтавського університету економіки і торгівлі. Серія : Економічні науки. - 2017. - № 5. - С. 180-186.

Розглянуто особливості сучасного стану та нормативно-правові акти, які регулюють зберігання архівів програмно-технологічного комплексу банку відповідно до вимог НБУ. Обгрунтовано важливість інформаційної безпеки банку. Доопрацьовано функціонал архівного підрозділу банку та доповнено його визначення в контексті засад формування електронних архівів та їх здатності протидіяти сучасним кіберзагрозам.

Шифр зберігання НБУВ: Ж70791/Екон.н.

***

Бура Т. В. Поняття та кримінологічна характеристика кіберзлочинності / Т. В. Бура, Н. М. Білик // Соціально-гуманітарний вісник. - 2018. - Вип. 22. - С. 52.

Розглянуто підходи до визначення поняття кіберзлочину.

Шифр зберігання НБУВ: Ж74326.

***

Бурдаков В.М. Синергія та темподинаміка вдосконалення моделі кібернетичних загроз ядерних об'єктів / В.М.Бурдаков, В.Г.Кононович, І.В. Кононович // Адаптивні системи автоматичного управління. - 2018. - № 1. - С. 23-36.

Сформульовано принципи побудови проектної моделі кіберзагроз автоматизованим системам технологічного й адміністративного управління. Складено перелік проектних кіберзагроз із урахуванням цільової діяльності підприємства, особливостей і вразливостей об'єктів ядерної чфери. Розроблено формалізовану дискретну математичну модель періодичного вдосконалення переліку проектних кіберзагроз.

Шифр зберігання НБУВ: Ж63671.

***

Державне бюро розслідувань: на шляху розбудови : матеріали Міжнар. наук.-практ. конф., 16 черв. 2018 р., м. Одеса. - Одеса : Юридична література, 2018. - 430 с.

Зі змісту:

- Самойленко О.А. Проблеми розслідування злочинів, пов'язаних із використанням обстановки кіберпростору (в контексті діяльності Державного бюро розслідувань).

Шифр зберігання НБУВ: ВА824799.

***

Дімітрова Н. М. Основні види кіберзлочинів та причини, що їх породжують / Н. М. Дімітрова, Н. М. Білик // Соціально-гуманітарний вісник. - 2018. - Вип. 22. - С. 50.

Висвітлено причини, що породжують кіберзлочинність, та фактори що на неї впливають.

Шифр зберігання НБУВ: Ж74326.

***

Економічна та інформаційна безпека: проблеми та перспективи : матеріали Міжнар. наук.-практ. конф., (м. Дніпро, 27 квіт. 2018 р.). - Дніпро, 2018. - 274 с.

Зі змісту:

- Волков Ю.М. Проблема підготовки фахівців кібербезпеки для органів Національної поліції;
- Гаврилюк Р.В. Сучасні тенденції протидії кіберзлочинам;
- Пушак Я.Я., Марченко О.М. Проблемні аспекти запобігання та протидії кіберзлочинності в Україні;
- Рудий Т.В., Сеник В.В., Кулешник Я.Ф. Інформаційно-аналітична діяльність Національної поліції України у протидії кіберзлочинності як аспект кібербезпеки держави;

- Тулупов В.В., Спориш Є.Ю. Захист систем відеоспостереження від витоку інформації;
- Федорова Н.Є. Шляхи подолання кіберзлочинності як форма прояву інформатизації суспільства;
- Шеломенцев В.П. Кіберзагрози у законодавстві України.

Шифр зберігання НБУВ: ВА824790.

***

Інтернет речей: проблеми правового регулювання та впровадження : матеріали наук.-практ. конф., 24 жовт. 2017 р. - Київ : КПІ ім. Ігоря Сікорського : Політехніка, 2017. - 237 с.

Зі змісту:

- Яременко О.І. Правові проблеми кіберзахисту національної критичної інфраструктури України в контексті європейської інтеграції;
- Ткачук Т.Ю. Тіньовий інтернет: співвідношення можливостей й загроз;
- Некіт К.Г. Інтерент речей та інформаційна безпека: деякі правові проблеми;
- Огородников Д.В. Методи зовнішнього втручання у технології передачі даних Інтернет речей;
- Забара І.М. Інтернет речей: вплив на розвиток права Європейського союзу (концептуальні підходи до питань кібербезпеки);
- Коваленко Л.П., Горбунова А.Р. Щодо основних завдань кіберполіції в сфері забезпечення інформаційної безпеки України.

Шифр зберігання НБУВ: ВА822591.

***

ІТ-право та цифрове суспільство : матеріали Всеукр. конф. до 20-річчя НУ "ОЮА", м. Одеса, 24 листоп. 2017 р. - Одеса : Юридична література, 2017. - 117 с.

Зі змісту:

- Кузьма О.П. Щодо питання визначення основних загроз, які виникають під час використання соціальних мереж;
- Мазур М.М. Кібербулінг та неповнолітні: сучасні правові проблеми;
- Саушкіна О.Р. Кіберсквотинг: способи захисту від порушень;
- Третьякова А.С. Тенденції боротьби з кіберправопорушеннями в цивільних правовідносинах: постановка питання.

Шифр зберігання НБУВ: ВА824797.

***

Криміналістичні та кримінально-процесуальні засоби оптимізації досудового розслідування : матеріали ІІІ Дистанц. наук. конф. до 20-річчя НУ ОЮА та 170-річчя Одес. шк. права, м. Одеса, 11 груд. 2017 р. - Одеса : Юрдична література, 2017. - 260 с.

Зі змісту:

- Мирошниченко Ю.В. Способи шахрайства в мережі Інтернет;

- Пастущак О.В. Перспективи пошуку та встановлення особи злочинця в кіберпросторі.

Шифр зберігання НБУВ: ВА824978.

***

Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки / Круглов В.В. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Державне управління. - 2018. - Т. 29, № 3. - С. 57-61.

Проаналізовано можливості забезпечення кібербезпеки шляхом використання механізмів державно-приватного партнерства, а саме захист критичної інфраструктури, забезпечення надійного доступу до Інтернет-мережі, регулювання технічної безпеки, проведення обміну інформацією щодо загроз, здійснення допомоги щодо вирішення ситуацій, пов'язаних із загрозами.

Шифр зберігання НБУВ: Ж70795/Держ.упр.

***

Матеріали IV Міжнародної науково-практичної конференції «Право: історія, теорія, практика» (22-23 лютого 2018 року). - Харків, 2018. - 119 с.

Зі змісту:

- Нескороль Н.В. Цифрові права людини в аспекті захисту персональних даних у мережі Інтернет.

Шифр зберігання НБУВ: ВА823811.

***

Правова реформа: концепція, мета, впровадження : зб. наук. пр. : матеріали VIII Міжнар. наук.-практ. конф. (Київ, 23 листоп. 2017 р.). - Київ : Ніка-Центр, 2017. - 479 с.

Зі змісту:

- Демченко П. Правові основи кібернетичної безпеки як гарантія безпеки виборчого процесу в Україні.

Шифр зберігання НБУВ: ВА824187.

***

Радиш О. В. Профілактика і протидія комп'ютерної злочинності як комплексний підхід для безпеки України / О. В. Радиш, Н. М. Білик // Соціально-гуманітарний вісник. - 2018. - Вип. 22. - С. 44-45.

Розглянуто загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання кіберзлочинності.

Шифр зберігання НБУВ: Ж74326.

***

Ричка Д.О. Модель комп'ютерних злочинів / Ричка Д.О. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2018. - Вип. 49(2). - С. 122-125.

Розглянуто суб'єкт злочинів у сфері електронно-обчислювальних машин, систем та комп'ютерних мереж. Проведення аналізу ознаки комп'ютерних злочинців надало змогу вивести типову модель комп'ютерних злочинців.

Шифр зберігання НБУВ: Ж68850/пр.

***

Теоретико-правові основи формування та розвитку інформаційного суспільства : матеріали наук.-практ. конф., 29 листоп. 2017 р. - Київ : КПІ ім. Ігоря Сікорського : Політехніка, 2017. - 225 с.

Зі змісту:

- Яременко О.І. Кіберпростір як об’єкт правового регулювання.

Шифр зберігання НБУВ: ВА822592.

***

Шемчук В.В. Основні напрями міжнародного співробітництва у сфері кібербезпеки / Шемчук В.В. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки. - 2018. - Т. 29(68), № 2. - С. 125-130.

Виходячи із аналізу чинного національного законодавства, міжнародно-правових актів, міжнародної експертної діяльності, функціонування деяких міжнародних організацій, виокремлено пріоритети міжнародного співробітництва у сфері кібербезпеки з метою забезпечення ефективної системи кібербезпеки.

Шифр зберігання НБУВ: Ж70795.

***

Якість і безпека. Сучасні реалії : матеріали наук.-практ. конф., 14-15 берез. 2018 р. - Вінниця : ВНТУ, 2018. - 198 с.

Зі змісту:

- Заєць В.І., Кобилянська І.М. Загрози у кіберпросторі;
- Мисько Ю.О., Колган В.А. Попередження небезпек інформаційного простору;
- Ковальчук В.В., Кобилянський С.О. Тенденції захисту від кіберзлочинів;
- Гоголкіна А.О. Захист даних в сфері телекомунікаційних послуг.

Шифр зберігання НБУВ: СО35943.

***

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.