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

№ 12 (грудень)

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

«Електронні реєстри і бази даних в Україні не достатньо захищені від витоку інформації, тому користувачу слід убезпечувати себе дублюванням документів на паперових носіях. Про це повідомив член громадської ради при Державній адміністрації спеціального зв'язку та захисту інформації, голова правління ГО "Асоціація учасників ринку бездротових мереж передачі даних" Олег Соболєв…

За його словами, Україна доволі швидко рухається у напрямку переходу на електронний документообіг, вводить, зокрема, електронний підпис, різноманітні бази даних, однак у зв'язку із цим виникає багато ризиків…» ***(Марія Мамаєва. Електронні реєстри і бази в Україні не достатньо захищені – експерт // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1766320-elektronni-reyestri-i-bazi-v-ukrayini-ne-dostatno-zakhischeni). 06.12.2018).***

***

«Украинские хактивисты обнаружили серьезные проблемы с безопасностью, которые могли повлечь за собой утечку в открытый доступ около 2,2 терабайт медицинской информации, принадлежащей столичному Центру детской кардиологии и кардиохирургии.

Информацию об этом на своей странице в Facebook опубликовал пользователь под ником Lurca Tier…

По состоянию на 14-00 12 декабря уязвимость уже закрыта.

…в открытом доступе находилось около 2,2 терабайт информации о пациентах, включая рентгеновские снимки, записи о пациентах, данные флюорографии, МРТ, УЗИ и т.д.

Сведений о том, что из-за уязвимости данные могли похитить злоумышленники, нет.» ***(Владимир Кондрашов. Медицинские данные детей центра кардиохирургии были на грани "утечки" // Internetua (http://internetua.com/medicinskie-dannye-detei-centra-kardiohirurgii-byli-na-grani-utecski). 12.12.2018).***

***

«За підсумками засідання Трансатлантичної цільової групи з питань виборів в Україні й громадянського суспільства, представник Німецького фонду Маршалла в США Джонатан Катц наголосив, що для майбутніх президентських та парламентських виборів в Україні сьогодні існує ціла низка викликів.

…вибори, заплановані в Україні на наступний рік, викликають особливе занепокоєння у зв'язку з намаганнями Росії втрутитися в процес.

"Росіяни робили такі спроби як у передвиборчий період, так і безпосередньо в день голосувань", – попередив Джонатан Катц.

Представник фонду зазначив, що насамперед це питання кібербезпеки, однак у цьому контексті США та інші країни заходу взаємодіють з Україною…» ***(У США***

повідомили, що загрожує майбутнім виборам в Україні // 5 канал (https://www.5.ua/polityka/u-ssha-povidomyly-shcho-zahrozhuie-maibutnim-vyboram-v-ukraini-183373.html). 20.12.2018).

***

«У Центрі управління навчанням учасників виборчих процесів при ЦВК за сприяння Міжнародної фундації виборчих систем в Україні (IFES) протягом грудня пройшли десять тренінгів з кібергігієни, у яких взяли участь 169 членів ЦВК - працівники Секретаріату Комісії та Служби розпорядника Державного реєстру виборців.

…серія тренінгів завершила сертифікацію ЦВК з кібергігієни. Ця інноваційна програма була розроблена експертами IFES з метою сприяння безпечній та відповідальній кіберповедінці та обізнаності в галузі кібербезпеки. При цьому вона стала першою у своєму роді, яку міжнародна організація запропонувала в Україні та світі…

У ході подальшої підготовки до виборів Президента України 31 березня 2019 року подібні тренінги будуть запропоновані широкому колу учасників виборчого процесу, зокрема, членам окружних виборчих комісій, працівникам органів адміністрування ДРВ (Державний реєстр виборців), представникам організацій громадянського суспільства…» ***(Іра Костюченко. ЦВК провела цикл тренінгів з кібербезпеки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1768922-tsvk-provela-tsikl-treningiv-z-kiberbezpeki). 20.12.2018).***

***

«Для внесення змін до державних реєстрів рейдери наймають хакерів та підробляють ключі нотаріусів…

Про це розповіла Член Ради Нотаріальної палати України, голова комісії Національної палати України з питань протидії кіберзлочинності під час антирейдерського форуму «Бізнес проти знищення держави», організованого ГО «Бізнес-Варта» Наталія Козаєва… «Державний реєстр речових прав працює на комп'ютерах, де встановлено Windows 2007, державні нотаріуси працюють за технікою, якій більше, як 10 років. Отримуємо листа від міністерства юстиції, відкриваємо, не знаємо, що це підробка, і на комп'ютер приходить вірус. Потім нотаріус іде у відпустку, повертається, дізнається, що з її ключем хакери переоформили право власності невідомі люди… Ні одного хакера кіберполіція не спіймала. Коштів від держави на оновлення техніки ми не отримували», - розповідає Наталія Козаєва.

В Україні існує 250 реєстрів, хакерське втручання до яких може завершитися рейдерським захопленням. І кожним з них займається окрема компанія, яка його підтримує. На це держава затрачає 3 млрд грн на рік. За документами, саме на цих організаціях має лежати відповідальність за електронну безпеку реєстрів, а також єдиний доступ для нотаріусів, реєстраторів та уповноважених до онлайн-роботи представників органів місцевого самоврядування, - пояснив Олександр Данченко, народний депутат України, Голова комітету ВРУ з питань інформатизації та

зв'язку, бізнес-омбудстмен ГО «Бізнес-Варта». На практиці – за безпеку відповідають нотаріуси. Останні - не лише не мають ІТ-підготовки, але і не можуть відслідковувати, чи під час робочого дня або за ранок, поки не були на роботі, хакер не заходив до реєстру – такі технічні звіти у програмі не передбачені…» ***(Рейдери стали користуватися послугами хакерів // ІАС Аграрії разом (https://agrarii-razom.com.ua/news-agro/reyderi-stali-koristuvatisya-poslugami-hakeriv). 07.12.2018).***

***

«Защищенность нотариусов и регистраторов от атак хакеров остается на недостаточном уровне, несмотря на определенные меры по защите государственных реестров. Нотариусы уверены, что для обеспечения кибербезопасности нотариусов нужны комплексные решения с четкой позицией государства.

Об этом шла речь в ходе круглого стола на тему «Кибербезопасность нотариусов и государственных реестров Украины: риски, инструменты и методы решения проблемы», который состоялся 11 декабря в Киеве…

При обсуждении проблем входа злоумышленников в реестры член Совета Нотариальной палаты Украины, председатель комиссии НПУ по вопросам противодействия киберпреступности Наталия Козаева отметила, что на данный момент не существует единых правил сертификации рабочего места регистратора. Конечно же, некоторые требования к программному обеспечению и техники присутствуют, но на практике очень часто нотариусы используют один компьютер и для работы в реестрах, и для пользования электронной почтой, Интернетом и тому подобное.

Из положительных тенденций можно отметить то, что после перехода регистраторов в 2017 году на защищенные ключи количество случаев несанкционированного доступа уменьшилось в разы, и уже в 2018 году такие случаи были единичными. Важно и то, что многие нотариусы сейчас переходят на постоянные IP-адреса. Но проблематика и риски остаются, ведь регистраторы и нотариусы — юристы, а не «айтишники»…

Еще одна существенная проблема — когда нотариусы выявляют незаконные регистрационные действия, совершенные третьими лицами, в них нет законодательного механизма для защиты владельца. По мнению нотариуса, эту проблему следует решать качественно и безболезненно, чтобы не увеличивать цепочку пострадавших людей.» ***(Нотариусы обсудили пути обеспечения кибербезопасности // Закон и Бизнес (https://zib.com.ua/ru/print/135655-notariusi_obsudili_puti_obespecheniya_kiberbezopasnosti.html). 12.12.2018).***

***

«Украинских чиновников решили наказать за пренебрежение элементарными правилами кибергигиены. Информацию о том, что украинские государственные информационные ресурсы могут быть подвержены более чем 4,7 тысячам так называемых «дорков», опубликовал эксперт по кибербезопасности, ведущий разработчик компании ИТ Лаборатория Александр Галущенко. Он также

призвал воспользоваться перечнем всем желающим и опубликовать обнаруженные данные в открытом доступе…

Опубликованный экспертом перечень Google Dork Queries (специфических запросов к поисковику, помогающих раскрыть общедоступные, но скрытые от посторонних глаз данные), по задумке, призван раскрыть реальное положение дел в безопасности украинских государственных веб-сервисов.

– Полную ответственность за все обнаруженные уязвимости несут хозяева сайтов и организации, осуществляющие контроль и надзор в сфере своей компетенции, а также те, кто обеспечивают защиту государственных ресурсов, – рассказал Александр Галущенко… – Я опубликовал этот перечень для того, чтобы привлечь внимание к проблеме низкой подготовки и уровня сотрудников, отвечающих за свой сектор работы…

Александр Галущенко отметил, что речи о взломе или каком-то несанкционированном доступе не идет: все уязвимости можно обнаружить благодаря обычному поиску через тот же Google. Как отмечает эксперт, найденные таким образом дыры – это, в первую очередь, свидетельство халатного отношения администраторов и чиновников к своей работе…» ***(Владимир Кондрашов. Украинцев призывают проучить «специалистов по кибербезопасности» // Internetua (https://internetua.com/ukraincev-prizyvauat-proucsit-specialistov-po-kiberbezopasnosti-). 24.12.2018).***

***

Національна система кібербезпеки

«Подразделения кибернетической безопасности Вооруженных сил Украины перешли на боевой режим работы. Об этом заявил начальник Войск связи ВСУ - начальник Главного управления связи и информационных систем Генерального штаба ВСУ генерал-майор Владимир Рапко на брифинге…

По его словам, основным направлением деятельности подразделений является защита информационно-телекоммуникационных систем ВСУ от внешних и внутренних угроз.

Рапко также добавил, что с 2014 года зафиксировано интенсивное увеличение количества кибератак различной степени сложности, направленных на нарушение функционирования системы управления и связи ВСУ.

Однако подразделения кибербезопасности выработали четкие алгоритмы реагирования на различные случаи кибернетических угроз или атак, как правило, это DDoS атаки на системы и распространение вредоносных программ…» ***(Анастасия Очеретнюк. Киберподразделения ВСУ переведены в боевой режим // ООО "Национальные информационные системы" (http://podrobnosti.ua/2274818-kiberpodrazdelenija-vsu-perevedeny-v-boevoj-rezhim.html). 18.12.2018).***

***

«…На заседании во вторник, 18 декабря, Комитет Верховной Рады Украины по вопросам информатизации и связи рассматривал законопроект №8608 «О внесении изменений в некоторые законы Украины».

Полторы страницы проекта закона авторства Кабинета Министров – на данный момент единственный законопроект, который предусматривает возложение на Государственную службу специальной связи и защиты информации Украины обязанностей по хранению резервных копий информации и сведений государственных электронных информационных ресурсов.

– Также с целью нормализации необходимости создания резервных копий и определения перечня органов, на которых эта норма распространяется, в Закон Украины «Об основных принципах обеспечения кибербезопасности Украины» добавляется норма, которой на государственные органы, воинские формирования, образованные в соответствии с законами Украины, государственные предприятия, учреждения и организации возлагается обязанность по созданию резервных копий и определяется, что установление порядка передачи, хранения и доступа к резервным копиям будет определяться Кабинетом Министров Украины, – говорится в пояснительной записке к документу.

По словам Главы Госспецсвязи Леонида Евдоченко, который представлял документ от имени Кабмина, проект закона разрабатывался с целью обеспечить резервное копирование критической информации в стране…

К документу у ИТ-комитета Рады возникли замечаний в два раза больше, чем текста в самом законопроекте. Так, депутаты предлагают не вносить изменения в Закон Украины «Об основах обеспечения кибербезопасности Украины». Дело в том, что предложенные изменения предполагают создание всеми субъектами государственного сектора – от министерств до предприятий – резервных копий всей электронной информации (от веб-сайта до бухгалтерии, включая реестры и базы данных) и передачу этих копий в ГСССЗИ.

– Во-первых, это физически невозможно. Нужно будет вложить огромные деньги в те же сервера. Во-вторых, такой подход неприемлем с точки зрения безопасности хранения и неотвратимости потери информации в случае физического уничтожения… – прокомментировал Александр Данченко…

Во время обсуждения законопроекта у депутатов возник вполне логичный вопрос: во сколько обойдется бюджету копирование, передача копий и их хранение на ресурсах ГСССЗИ. На этот вопрос четкого ответа Леонид Евдоченко дать не смог. Дело в том, что законопроект утверждает, что дополнительных трат из бюджета не потребуется, хотя на деле всё немного сложнее.

Как стало известно, ГСССЗИ уже освоила 120 миллионов гривен, за счет которых создала условия для хранения резервных копий ресурсов госучреждений

– Я могу только сказать, какие цифры на сегодня. В бюджете 2018 года на создание дата-центра для хранения копий было заложено около 120 миллионов гривен. Что касается остальных министерств и ведомств, то эти средства заложены в их бюджеты на 2019 год для того, чтобы можно было привести всё к единому формату и передавать в Госспецсвязи для резервного хранения, – сообщил Леонид

Евдоченко. – Действует Закон об основах обеспечения кибербезопасности Украины, в нем легализована Национальная телекоммуникационная сеть, одной из функций которой является передача информации между государственными органами власти. Практически эта функция будет завершена до конца года – 20 декабря мы принимаем первый этап этой работы. То есть фактически транспорт мы обеспечили. Что же касается средств для того, чтобы передавать эти копии в ГСССЗИ, – сейчас суммы просчитываются, но это не будут «миллиарды».

…руководитель Госспецсвязи не исключает того факта, что построенных на данный момент его ведомством мощностей может не хватить для хранения всех резервных копий. На какой объем рассчитано хранилище – секретная информация, но Евдоченко намекнул, что «речь идет о терабайтах».

Не смотря на кажущуюся простоту, по мнению нардепа Юрия Мороко, законопроект в той редакции, в которой он зашел в парламент, может с треском провалиться в Раде. Причины тому – не только несогласованность терминологии, множественные замечания самого ИТ-комитета, но и отсутствие подробного описания «финансового вопроса», ведь депутатов в сессионном зале чаще всего волнует именно этот вопрос – сколько документ будет стоить бюджету. На данный момент законопроект Кабмина ответа на него дать не может.

В результате длительных прений вокруг судьбы законопроекта члены Комитета, понимая необходимость принятия законопроекта, и, в то же время, проблемы самого законопроекта, решили поддержать документ в первом чтении с учетом замечаний. Такое решение позволит нардепам официально направить свои замечания и ожидать, что документ в Кабмине всё-таки доработают.» ***(Государство потратило 120 миллионов на пустой дата-центр // Goodnews.ua (http://goodnews.ua/technologies/gosudarstvo-potratilo-120-millionov-na-pustoj-data-centr/). 19.12.2018).***

***

Кібервійна проти України

«Сполучені Штати вважають, що російська влада намагається в тому числі за допомогою операцій в кіберпросторі підривати демократичні інститути України і в зв'язку з цим останнім часом в значній мірі зосереджують свою підтримку Києву на зміцнення кібербезпеки. Про це повідомив у вівторок представник Держдепартаменту високого рангу в Брюсселі під час брифінгу для журналістів.

…"росіяни, і особливо російський уряд", "бачать Україну як вразливу мету і намагаються різними шляхами підривати впевненість в її демократичних інститутах". "(Ми бачимо) значну активність Росії в кіберпросторі", — стверджував він.

"Значна частина нашої останньої за часом допомоги (Києву) була націлена на зміцнення оборонних можливостей України в кіберпросторі…", — сказав представник зовнішньополітичного відомства…» ***(Олексій Супрун. Держдеп: США концентрують свою допомогу Україні на зміцненні кібербезпеки //***

Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1766068-derzhdep-ssha-kontsentruyut-svoyu-dopomogu-ukrayini-na-zmitsnenni-kiberbezpeki). 04.12.2018).

***

«Співробітники СБУ блокували спробу російських спецслужб провести масштабну кібератаку на інформаційно-телекомунікаційні системи Судової влади України…

"Фахівці СБУ зафіксували, що кібератака розпочалася через розсилку електронною поштою заражених вірусом підроблених бухгалтерських документів. Після відкриття файлів на комп'ютери приховано завантажувалось шкідливе програмне забезпечення для несанкціонованого втручання до судових інформаційних систем та викрадення службової інформації", - йдеться у повідомленні.

Як зазначили у СБУ, встановлено, що "виявлена вірусна програма з'єднувалась з контрольно-командних серверів, які мають, зокрема, російські IP-адреси". За висновками фахівців, задум спецслужб РФ полягав у блокуванні сталого функціонування судової інформаційної системи України…» ***(Євген Дем'янов. СБУ запобігла кібератаці на українські суди з боку Росії // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1765978-sbu-zapobigla-kiberatatsi-na-ukrayinski-sudi-z-boku-rosiyi). 04.12.2018).***

***

«Украинский гидрометцентр взломали неизвестные хакеры, понимающие кириллицу. Уязвимость позволила злоумышленникам воровать данные гидрометцентра и получить полный контроль над почтовым сервером учреждения.

Информацию о том, что Украинский гидрометцентр был взломан, опубликовал на своей странице в Facebook консультант по кибербезопасности Егор Папышев…

В Украинском гидрометцентре… сообщили, что знают об атаке, но она якобы произошла ещё полгода назад, уязвимость уже давно закрыта, а делом занимается Департамент киберполиции. Тем не менее, как сообщил Егор Папышев, уязвимость была ещё актуальна по состоянию на 3 декабря этого года.

– Скомпрометирована вся служебная переписка конкретного ведомства. У злоумышленников был полный доступ к размещению информации, её отправке по служебным каналам, – уточнил эксперт…

По его словам, хакеры могли использовать доступ к почте для искажения информации и отправки недостоверных сведений, например, в ГСЧС…» ***(Украинский гидрометцентр взломали русскоязычные хакеры // Goodnews.ua (http://goodnews.ua/technologies/ukrainskij-gidrometcentr-vzlomali-russkoyazychnye-xakery/). 19.12.2018).***

***

«Служба безопасности Украины подтвердила, что скупкой аккаунтов украинцев в социальных сетях под видом маркетингового агентства занималось скандально известное российское «Агентство Интернет Исследований», больше известное как «ольгинская фабрика троллей»…

В свежем сообщении Службы безопасности Украины говорится о том, что «Агентство Интернет Исследований» собиралось использовать аккаунты украинцев для дестабилизации ситуации в стране.

– Накануне президентских и парламентских выборов в Украине в 2019 году к гражданам нашей страны от этой российской «фабрики троллей» начали поступать предложения якобы от коммерчески заинтересованных лиц. У них за денежное вознаграждение украинским пользователям предлагается предоставить временный доступ к так называемому рекламному кабинету аккаунтов в социальных сетях «Facebook» и «Twitter» для якобы распространении через них таргетинговой рекламы и продвижения коммерческих интересов, – объясняют в СБУ. – На самом деле полученные представителями страны-агрессора права доступа к аккаунтам украинцев в социальных сетях будут использованы спецслужбами РФ для проведения разведывательно-подрывной деятельности, манипулирования общественным сознанием, вмешательства в предвыборные процессы, а также распространения антиукраинских материалов, направленных на дестабилизацию общественно-политической обстановки в государстве.

СБУ просит в случае получения предложений продать или передать в аренду свой аккаунт в социальных сетях, сообщать на горячую линию СБУ.» ***(В СБУ подтвердили, что "российские тролли" покупают аккаунты украинцев в соцсетях // Politica.com.ua (http://politica.com.ua/v-sbu-podtverdili-chto-rossijskie-trolli-pokupayut-akkaunty-ukraincev-v-socsetyax/). 16.12.2018).***

***

«Россия "готовила почву" для совершенного в ноябре захвата кораблей ВМС Украины, предприняв крупную кибератаку и запустив кампанию по дезинформации против Украины, согласно сообщениям одной из компаний, специализирующейся на кибербезопасности, и представителя ЕС.

…появилось заявление частной компании, занимающейся кибербезопасностью, в котором утверждается, что Москва провела серию кибератак на украинские правительственные серверы, нацеленную на сбор разведывательных данных, которые могли быть использованы для захвата кораблей. В отдельном порядке комиссар по вопросам безопасности ЕС заявил, что Кремль развернул сложную "кампанию дезинформации", призванную "смягчить общественное мнение" накануне захвата украинских кораблей.

На этой неделе американская компания Stealthcare заявила, что две хакерские группы, Carbanak и Gamaredon Group, по предположениям, спонсируемые российскими спецслужбами, провели кибератаки против Украины. Первая волна атак, которая произошла в октябре этого года, была сосредоточена на фишинговой кампании, нацеленной на государственные органы Украины и других стран Восточной Европы.

По данным Stealthcare, компьютеры жертв этих атак выполняли “важные функции”, которые перешли к удаленным субъектам, занимавшимся кражей и передачей данных. Во время следующей атаки в ноябре, всего за несколько дней до кризиса в Керченском проливе, была проведена установка программы, обеспечивающей хакерам доступ через “черный ход” к компьютерным серверам, принадлежащим украинским государственным органам.

По словам компании Stealthcare, эти две атаки, предоставили хакерам доступ к “информации, которая могла быть […] уместна при планировании” военно-морского кризиса 25 ноября. Компания добавила, что “нет никаких сомнений в том, что это была разведывательная операция под руководством Кремля по подготовке к кризису в Керченском проливе”.

Между тем в понедельник британский дипломат Джулиан Кинг, который в настоящее время является комиссаром Европейского Союза по безопасности, заявил, что Россия “подготавливала почву” для кризиса в Керченском проливе” посредством системной информационной кампании по распространению фальшивых новостей, которая “длилась более года”. Эта кампания, по утверждению Кинга, включала использование социальных сетей для распространения ложных слухов, таких как заявления о том, что украинское правительство заразило Черное море бактериями, вызывающими холеру…» ***(IntelNews: Российские шпионы "предприняли масштабную кибератаку на Украину" накануне военно-морского инцидента // «Новости онлайн 24» (https://newsonline24.com.ua/intelnews-rossijskie-shpiony-predprinyali-masshtabnuyu-kiberataku-na-ukrainu-nakanune-voenno-morskogo-incidenta/). 13.12.2018).***

***

«Кремль планирует вмешательство в избирательный процесс в Украине по нескольким каналам, заявил экс-посол США в Украине, директор Евразийского центра при Атлантическом совете США Джон Хербст. Эксперт допустил, что в преддверии выборов от РФ следует ожидать актов агрессии и кибератак. «Я уверен, что Россия планирует мультиканальное вмешательство в предвыборный процесс в Украине, как это было в Крыму в феврале 2014 года. Мы уже видим локальную агрессию на земле и на море. Без сомнения, будут цифровые атаки, акции массовой дезинформации, будут попытки создавать псевдоавтономные образования, как это было с попыткой создать Одесскую народную республику, к сожалению, предполагаю продолжение заказных убийств активистов накануне выборов», - указал он…» ***(РФ планирует «мультиканальное вмешательство» в украинские выборы, – экс-посол США // ua.today (http://ua.today/news/politics/rf_planiruet_multikanalnoe_vmeshatelstvo_v_ukrainskie_vybory_eks_posol_ssha). 21.12.2018).***

***

«Сотрудники СБУ блокировали попытку спецслужб РФ провести масштабную кибератаку на информационно-телекоммуникационные системы судебной власти Украины.

По данным ведомства, кибератака началась через рассылку по электронной почте зараженных вирусом поддельных бухгалтерских документов. После открытия файлов на компьютеры скрыто загружалось вредоносное программное обеспечение для несанкционированного вмешательства в судебные информационные системы и похищения служебной информации.

Сотрудники СБУ установили, что обнаруженная вирусная программа загружалась с контрольно-командных серверов, которые имеют, в частности, российские IP-адреса. По заключению специалистов, замысел спецслужб РФ заключался в блокировании устойчивого функционирования судебной информационной системы Украины.

Благодаря совместным с Государственной судебной администрацией и Госспецсвязи мероприятиям удалось локализовать негативные последствия кибератаки и предупредить ее дальнейшее развитие. СБУ как ключевая структура по обеспечению национальной безопасности продолжает реализовывать комплекс необходимых мер по защите критической информационной структуры государства.» ***(СБУ блокировала попытку кибератаки спецслужб РФ на информационно-телекоммуникационные системы судебной власти Украины // РепортерUA (https://reporter-ua.com/2018/12/05/341231_sbu-blokirovala-popytku-kiberataki-specsluzhb-rf-na-informacionno). 05.12.2018).***

***

Боротьба з кіберзлочинністю в Україні

«Кіберполіція зафіксувала в Україні випадки розповсюдження вірусу, замаскованого під повідомлення від державних установ…

За даними правоохоронців, вказане шкідливе програмне забезпечення націлене на користувачів операційної системи MS Windows.

"Спеціалісти з кіберполіції 11 грудня почали фіксувати факти розповсюдження цього шкідливого програмного забезпечення. Загалом, воно було націлене на користувачів, які є приватними нотаріусами України", - розповіли у прес-службі [кіберполіції].

Додається, що для надсилання шкідливого програмного забезпечення правопорушники використовували поштові сервіси українських компаній та що "повідомлення із шкідливими додатками надходили начебто від імені державних установ, зокрема судів різних інстанцій"…» ***(Ілля Нежигай. Кіберполіція попередила про розповсюдження нового вірусу // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1767334-kiberpolitsiya-poperedila-pro-rozpovsyudzhennya-novogo-virusu). 12.12.2018).***

***

«Причерноморское управление киберполиции Департамента киберполиции Национальной полиции Украины вышло на след гражданина Украины, который осуществляет распространение и сбыт вредоносных программ. По данным киберполиции, данное ПО используется для

несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи…

Основываясь на информации киберполиции, следователем Приморского ОП Одессы 27 апреля открыто уголовное производство по признакам уголовного преступления, предусмотренного ч.2 ст. 361 УК Украины …

27 октября по месту жительства продавца вирусов был проведен обыск…» ***(Владимир Кондрашов. Киберполиция вышла на след продавца вирусов // Internetua (http://internetua.com/kiberpoliciya-vyshla-na-sled-prodavca-virusov). 13.12.2018).***

***

«У 2018 році підрозділами Національної поліції України було викрито майже тисячу кіберзлочинів…

"У цьому році підрозділом виявлено близько 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій. З них майже тисяча – злочини, вчинені у сфері кібербезпеки", – повідомив голова Нацполіції Сергій Князєв під час підсумкового річного звіту.

Голова Нацполіції додав, що серед успішних операцій – затримання організатора бот-мережі Avalanche, викриття учасника міжнародного хакерського угрупування Cobalt, участь в припиненні діяльності міжнародної хакерської групи FIN7…» ***(Крістіна Попова. Поліція цього року викрила майже тисячу кіберзлочинів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1768946-mayzhe-tisyachu-kiberzlochiniv-bulo-vikrito-politsiyeyu-v-2018-rotsi). 20.12.2018).***

***

«В 2018 году Нацполиция разоблачила тысячи преступлений в сфере кибербезопасности. Об этом сообщили в пресс-службе ведомства.

Всего раскрыто около 6000 преступлений, совершенных в сфере использования высоких информационных технологий.

Среди успешных операций — задержание организатора бот-сети Avalanche, разоблачения участника международной хакерской группировки Cobalt, участие в прекращении деятельности международной хакерской группы FIN7.» ***(Одесситам на заметку: полицейские раскрыли шесть тысяч киберпреступлений // Волнорез (http://volnorez.com.ua/novosti/odessitam-na-zametku-policejskie-raskryli-shest-tysyach-kiberprestuplenij.html). 21.12.2018).***

***

«Специалисты кибербезопасности ПриватБанка сообщили о появлении в Украине новой мошеннической схемы с использованием поддельных писем о “случайном” переводе денег и поддельных сайтов, внешне напоминающих веб-сайт Приват24.

По данным специалистов банка, уже зафиксированы случаи, когда клиентам банка через различные каналы коммуникаций (мессенджеры, электронную почту и

т.д.) приходит сообщение о пополнении карты неизвестным лицом на несколько тысяч гривен. Далее мошенники предлагают перейти по ссылке на фальшивую квитанцию с фишинговым сайтом Приват24.

ПриватБанк предупреждает своих клиентов не открывать такие сообщения от мошенников и не реагировать даже на самые заманчивые сообщения о неожиданных денежных переводах. Также ни в коем случае нельзя вводить свои логин и пароль на поддельных банковских сайтах. Настоящий Приват24 находится только по одному адресу www.privat24.ua.» ***(Украинцев предупредили о новом виде мошенничества с использованием поддельных писем // Goodnews.ua (http://goodnews.ua/technologies/ukraincev-predupredili-o-novom-vide-moshennichestva-s-ispolzovaniem-poddelnyx-pisem/). 20.12.2018).***

***

«В течение года полицейские предотвратили распространение четырех массовых кибератак на территории Украины

Национальная полиция Украина в этом году раскрыла почти 1000 преступлений, совершенных в сфере кибербезопасности. Об этом на отчетной пресс-конференции сообщил председатель Национальной полиции Сергей Князев.

«В этом году подразделение (Департамент киберполиции - ред.) выявило около 6 тыс. преступлений, совершенных в сфере использования высоких информационных технологий. Из них почти тысяча - это преступления, совершенные в сфере кибербезопасности. Среди успешных операций - задержание организатора бот-сети Avalanche, разоблачение участника международной хакерской группировки Cobalt», - сказал Князев…

«Продолжается борьба с пиратством. В течение года пресечена деятельность более 40 пиратских сайтов. Также в рамках международного сотрудничества было разоблачено 8 транснациональных хакерских группировок и принято участие в более 30 международных операциях», - добавил Князев…» ***(С начала года Нацполиция раскрыла почти 1000 киберпреступлений // "Українські медійні системи" (https://glavcom.ua/ru/news/s-nachala-goda-nacpoliciya-raskryla-pochti-1000-kiberprestupleniy-554877.html). 20.12.2018).***

***

«…в Кривом Роге 20-летнему юноше было вручено подозрение о совершении им правонарушения: ему вменяют создание и распространение интернет-вируса…

В ходе следствия установлено, что юноша разработал компьютерный вирус и пытался с его помощью заработать денег. С личного электронного ящика он распространял эту программу случайным пользователям, а после того как люди открывали письмо — вирус начинал действовать и передавал информацию с компьютера жертвы на другой сервер. Так, одно из таких писем пришло жительнице города Сумы.

Кроме того, хакер разместил в сети Интернет объявление о продаже созданной им вредоносной программы и вскоре появился клиент, желающий приобрести вирус. За свою разработку юный гений попросил сумму в 1100 гривен,

половина из которых составлял аванс, а после получения денег — переслал покупателю желаемый файл…» ***(Евгений Гессен. 20-летнего хакера задержали за торговлю вирусом // «Відкритий» (https://opentv.media/20-letnego-hakera-1zaderzhali-za-torgovlyu-virusom/). 19.12.2018).***

***

«…В Национальном агентстве по вопросам предотвращения коррупции заявили о рассылке неизвестными на адреса электронной почты государственных служащих вирусных писем от имени ведомства…

Сказано, что письма приходили с логотипом Нацагентства и в них предлагалось пройти анкетирование…

Отправлены письма были с адреса umiko@hamaichi.co.jp...

"Обращаем внимание, что сообщения от Национального агентства поступают исключительно из домена gov.ua", - отметили в ведомстве. (Почту госслужащих атаковали от имени НАПК - заявление // Информационное агентство ЛІГАБізнесІнформ (https://news.liga.net/politics/news/pochtu-gosslujaschih-atakovali-ot-imeni-napk---zayavlenie). 13.12.2018).

Группа хакеров украла данные с сайта Министерства Европы и иностранных дел Франции, созданного для граждан, выезжающих за границу. В 2010 МИД Франции создал службу Ariane, которая позволяет людям, планирующим поездку за границу, зарегистрироваться онлайн, в частности, для получения информации о безопасности, сообщили ведомстве.

"Личные данные, зарегистрированные при регистрации на платформе Ariane, были украдены. Эти данные могут быть использованы не по назначению, но ограничены по своему действию, поскольку информация не включает конфиденциальную, финансовую информацию или информацию, которая может раскрыть места назначения поездок, объявленных в Ariane", - говорится в сообщении внешнеполитического ведомства Франции.

Дипломаты сообщили о том, что предприняли немедленные меры для предотвращения повторения подобных атак.

Сервис Ariane продолжает работать. В МИД не сообщили, откуда хакеры могли осуществить кибератаку…» ***(Хакеры украли данные в МИД Франции // «Зеркало недели. Украина» (https://zn.ua/WORLD/hakery-ukrali-dannye-v-mid-francii-303029_.html). 13.12.2018).***

***

«Працівники Київського управління Департаменту кіберполіції спільно зі слідчими поліції Полтавщини, за процесуального керівництва Полтавської місцевої прокуратури, викрили хакера у поширенні шкідливого програмного забезпечення.

Оперативники встановили, що для унеможливлення ідентифікації молодик використовував орендовані віртуальні сервери. Модифікований ним вірус був призначений для несанкціонованого втручання в роботу комп’ютерів та збору персональної і білінгової інформації (паролі, логіни, куки, данні по гаманцях криптовалют, файли з інформацією) на заражених персональних комп’ютерах…

На даний час проводяться заходи, спрямовані на ідентифікацію власників інфікованої вірусами електронно-обчислювальної техніки.

Триває досудове розслідування розпочате за ч.1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Зловмиснику загрожує до двох років позбавлення волі.» ***(Кіберполіція виявила хакера, який поширював у мережі вірус-стіллер // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-viyavila-xakera-yakij-poshiryuvav-u-merezhi-virus-stiller/). 24.12.2018).***

***

«…В Украине и мире продолжается распространение шифровальщика #Scarab через массовые рассылки фишинговых писем на русском или украинском языках (возможно с ошибками)», - сообщили в пресс-службе CERT-UA.

Более того, эксперты также предложили вариант подобного вирусного письма.

"Здравствуйте! Невозможно связаться с вами по телефону. Посылаю повторно вчерашний акт сверки", - говорится в тексте фитингов сообщения.

Например, после запуска вируса на компьютере запускается специальный процесс, который приводит к полному блокированию техники. После этого он начинает требовать оплату в виде биткоинов.» ***(Украинцов предупреждают об опасном компьютерном вирусе // Gazeta.ua (https://gazeta.ua/ru/articles/science/_ukraincov-preduprezhdayut-ob-opasnom-kompyuternom-viruse/876465). 22.12.2018).***

***

«…Працівники Подільського управління Департаменту кіберполіції, за участі детективів Хмельницького відділу поліції, співробітників СБУ в Хмельницькій області та працівників військової прокуратури Хмельницького гарнізону, викрили 36-річного мешканця Хмельницького у втручанні до комп'ютерної мережі бухгалтерського обліку державних органів та підприємств.

Працівники кіберполіції встановили: чоловік є працівником приватного підприємства, що обслуговує державні об'єкти, в тому числі і військові частини. До його обов'язків входили реалізація, встановлення та обслуговування програмного забезпечення бухгалтерських та облікових систем. Крім того, чоловік реалізовував, встановлював та обслуговував програмне забезпечення бухгалтерських та облікових систем, яке входить до санкційного списку.

Порушуючи вимоги договірних зобов'язань, він таємно отримував доступ до даних працівників цих підприємств, реєстраційних номерів їх облікових карток платників податків тощо…

Триває досудове розслідування розпочате за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. Зловмиснику загрожує до шести років

ув'язнення з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.» ***(Кіберполіція викрила чоловіка у незаконному втручанні в бази даних державних установ та їх накопиченні // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-nezakonnomu-vtruchanni-v-bazy-danyx-derzhavnyx-ustanov-ta-yix-nakopychenni-3851/). 25.12.2018).***

***

«Главное следственное управление Национальной полиции Украины с июня этого года расследует уголовное производство по фактам несанкционированного вмешательства в работу электронно-вычислительных машин, совершенного по предварительному сговору группой лиц…

По версии следствия, начиная с 2017 года неустановленная группа лиц, действуя по предварительному сговору, совершает несанкционированное вмешательство в работу компьютерных сетей, а именно веб-ресурсов, которые предоставляют пользователям услуги управления электронными кошельками криптовалют. Злоумышленники создают визуально похожие веб-ресурсы реально существующих сайтов управления криптовалютными активами и, благодаря невнимательности пользователей, получают доступ к логинам и паролям, воруя в дальнейшем с кошельков жертв криптовалюты.

Как один из эпизодов противоправной деятельности неизвестных мошенников, в определении суда фигурирует ресурс «bockchein.com» – клон сервиса blockchain.info…

Уголовное дело открыто по факту совершения преступления, предусмотренного ч.2 статьи 361 Уголовного кодекса Украины. Злоумышленникам «светит» от трех до шести лет лишения свободы.» ***(Владимир Кондрашов. Создателям фейковых сайтов обмена криптовалют светит шесть лет тюрьмы // Internetua (https://internetua.com/sozdatelyam-feikovyh-saitov-obmena-kriptovaluat-svetit-shest-let-tuarmy). 27.12.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Україна отримає фінансову підтримку на наукові проекти через Український науково-технологічний центр за напрямками: кібербезпека… Відповідне рішення прийняла Адміністративна рада Українського науково-технологічного центру (УНТЦ)…

"…Це рішення дозволить Україні залучити додаткові кошти під наукові дослідження та розробки з кібербезпеки. Саме їх результати дозволять і Україні, і усім нашим партнерам проваджувати нові, ефективні рішення для протидії одній з найбільших нинішніх загроз людства", - зазначив заступник міністра освіти і науки України, представник України в Адміністративній раді УНТЦ Максим Стріха…» ***(Марія Мамаєва. Кібербезпека, знищення хімвідходів та дослідження Дунаю:***

під що отримали гроші українські вчені // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1766447-kiberbezpeka-znischennya-khimvidkhodiv-ta-doslidzhennya-dunayu-pid-scho-otrimali-groshi-ukrayinski-vcheni). 06.12.2018).

***

«Україна бачить всі можливості для взаємодії з НАТО у межах трастового фонду з кібербезпеки для вирішення питання кіберзахисту, враховуючи безперервні атаки РФ в українському кіберпросторі. Про це заявила віце-прем'єр-міністра з питань європейської та євроатлантичної інтеграції України Іванни Климпуш-Цинцадзе під час зустрічі із заступником Генерального секретаря НАТО з нових викликів безпеці Антоніо Міссіролі у Брюсселі…

В уряді за підсумками зустрічі додали, що, враховуючи безперервні атаки РФ в українському кіберпросторі, зокрема, на системи функціонування державного управління, а також потенційні ризики зовнішнього втручання у хід виборчого процесу, допомога союзників та спроможності трастового фонду з кібербезпеки є нагальною потребою для України…» ***(Крістіна Попова. Україна хоче використати трастовий фонд НАТО для кіберзахисту від РФ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1768915-cherez-bezperervni-ataki-rf-ukrayina-potrebuye-nagalnoyi-dopomogi-soyuznikiv-z-kiberbezpeki). 20.12.2018).***

***

«Провідний B2B-акселератор Європи Startup Wise Guys із головним офісом в Естонії оголосив в Україні набір на програму з розвитку стартапів у сфері кібербезпеки та штучного інтелекту. Програма називається CyberNorth і розрахована на пошук проектів у цій сфері у 10 різних європейських країнах

Українські стартапи будуть боротися за право взяти участь разом із кандидатами з-понад 10 країн Європи. Програма проводиться за підтримки Міністерства оборони Естонії. Протягом 3 міс акселераційної програми із кібербезпеки їм допомагатимуть понад 150 менторів та інвесторів. Українці-переможці отримають фінансування до €30 тис з можливістю додаткових інвестицій…» ***(Людмила Кліщук. Українці зможуть подаватися до естонського стартап-акселератора // Na chasi (https://nachasi.com/2018/12/18/akselerator-iz-kiberbezpeky/). 18.12.2018).***

***

«Уряд України та Європейська комісія підписали Угоду про фінансування Програми технічного співробітництва 2018 року

Відповідний документ підписали на полях 5-го засідання Ради асоціації Україна-ЄС…

У рамках угоди ЄС виділить 37 млн євро для реалізації Угоди про асоціацію з ЄС і для допомоги українським установам у зміцненні поваги до демократичних принципів, прав людини та основних свобод

Зазначається, що допомогу ЄС надасть за трьому основними пріоритетами. Зокрема, гроші спрямують на зміцнення інституційної спроможності українських органів влади імплементувати законодавчі норми ЄС в українське законодавство та забезпечити виконання положень Угоди про асоціацію у таких напрямках: довкілля, транспорт, енергетика, санітарний та фітосанітарний контроль, бухгалтерський облік, стандартизація, електронна комунікація, кібербезпека…» ***(ЄС надасть Україні 37 млн євро на втілення Угоди про асоціацію // Espreso.tv (https://espreso.tv/news/2018/12/17/yes_nadast_ukrayini_37_mln_yevro_na_vtilennya_ugody_pro_associaciyu). 17.12.2018).***

***

«Фахівці Головного управління зв'язку та інформаційних систем Генштабу ЗСУ та представник Головного штабу оборони збройних сил Італії полковник Феліче де Роза обговорили перспективи спільних тренувань фахівців з кібербезпеки…

Італійський полковник відзначив високий рівень організації підготовки курсантів та слухачів інституту, потужну наукову та матеріально-технічну базу для підготовки фахівців у сфері кібернетичної безпеки. Він також розповів українським військовим про те, як збройні сили Італії організовують національну систему кібербезпеки та як вона функціонує.

Обговорили представники України та Італії й подальше двостороннє співробітництво.» ***(Україна й Італія спільно тренуватимуть "кібервоїнів" – подробиці // 5 канал (https://www.5.ua/suspilstvo/ukraina-ta-italiia-spilno-trenuvatymut-kibervoiniv-182852.html). 12.12.2018).***

***

«Україна посилюватиме взаємодію з Литвою в реформуванні оборонного сектору, серед актуальних питань співпраці також енергетична безпека, інвестиції, кібербезпека…

Про це президент Петро Порошенко сказав під час спільної з президентом Литовської Республіки Далею Грібаускайте заяви для ЗМІ у Києві…

Також, за словами Порошенка, серед актуальних питань двосторонньої співпраці енергетична безпека, економічне та інвестиційне співробітництво, кібербезпека…» ***(Україна посилить співпрацю з Литвою в реформуванні сектору оборони // Західна інформаційна корпорація (https://zik.ua/news/2018/12/07/ukraina_posylyt_spivpratsyu_z_lytvoyu_v_reformuvanni_sektoru_oborony_1465061). 07.12.2018).***

***

«Європейський Союз зацікавлений у поглибленні співпраці з Україною у сфері кібербезпеки. Про це заявила Віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України Іванна Климпуш-Цинцадзе за результатами зустрічі з Віце-президентом Єврокомісії з питань Єдиного цифрового ринку Андрусом Ансіпом у Брюсселі 5 грудня.

Віце-прем’єр-міністр зазначила, що нагальним завданням для України є захист від кібератак, мішенню яких неодноразово ставали об'єкти критичної інфраструктури країни. “Посилена співпраця між Україною та ЄС могла б створити міцну платформу для протистояння кібератакам”, – зазначила Іванна Климпуш-Цинцадзе. Зокрема, Україна зацікавлена у залученні до роботи Агентства з питань мережевої та інформаційної безпеки Європейського Союзу (ENISA), до діяльності Європейського центру досліджень та компетенції з кібербезпеки, а також до тренінгів ЄС щодо координації механізмів спільного реагування ЄС та держав-членів на масштабні інциденти та кризові ситуації в галузі кібербезпеки.

Андрус Ансіп заявив, що Євросоюз готовий до поглиблення співпраці з Україною у сфері кібербезпеки. “Жодна країна не здатна самостійно ефективно протидіяти кібератакам. Ми маємо об'єднати наші сили”, – наголосив Єврокомісар.

Він також зазначив, що, зважаючи на взаємопов'язаність, яка сьогодні існує у світі, кібератака проти однієї країни неминуче впливає на інші. Зокрема, він нагадав про вірус “NotPetya”, деструктивний вплив якого відчули далеко за межами України.

Сторони погодилися, що посилення кібербезпеки України та поглиблення співпраці у цій сфері відповідає інтересам і ЄС, і України.

Віце-прем’єр-міністр зазначила, що цифрова економіка є однією з пріоритетних у співпраці України з Європейським Союзом. “За три роки постійного діалогу з європейською стороною в рамках “Східного партнерства” нам вдалося досягнути значного прогресу в цій сфері”, – підкреслила Іванна Климпуш-Цинцадзе.

Віце-прем’єр-міністр запропонувала закріпити співпрацю з ЄС у цій галузі шляхом узгодженого робочого плану. За її словами, такий план буде зосереджений на оновленні додатків Угоди про асоціацію, що стосуються цифрової економіки, а також низки додаткових заходів, запропонованих українською стороною у Дорожній карті щодо інтеграції цифрових ринків України та ЄС…» ***(У ЄС розуміють: кібербезпека України – це їхня безпека, – Іванна Климпуш-Цинцадзе // Агенція інформації та аналітики (https://galinfo.com.ua/news/u_yes_rozumiyut_kiberbezpeka_ukrainy__tse_ihnya_bezpeka__ivanna_klympushtsyntsadze_302515.html). 06.12.2018).***

***

«Великобритания и Польша договорились "усилить оборону и безопасность, чтобы противостоять новым угрозам, таким как кибератаки и враждебная активность России"…

"Сегодня мы договорились о продвижении в ряде ключевых областей, в том числе о начале совместных консультаций по вопросам кибербезопасности и по России в начале следующего года", - рассказал глава МИД Великобритании Джереми Хант.

Он добавил, что стороны подчеркнули желание "сделать НАТО эффективным инструментом для отображения этих вызовов"…» ***(Великобритания и Польша договорились расширить диалог по противодействию России // Украина***

сегодня (http://ukr-today.com/politics/372588-velikobritanija-i-polsha-dogovorilis-rasshirit-dialog-po-protivodejstviju-rossii.html). 21.12.2018).

***

Світові тенденції в галузі кібербезпеки

«Согласно новым данным, опубликованным этической хакерской платформой Bugcrowd, внештатные хакеры могут зарабатывать более 500 000 долларов в год на поиске уязвимостей и сообщении об этих проблемах компаниям, таким как Tesla и правительственных организациям - типа Министерства обороны…

Хакеры работают над четко определенным контрактом для конкретной компании и получают вознаграждение, когда они могут найти изъян в сетевой части компании. Сколько им платят, зависит от того, насколько серьезна решенная ими проблема.

Компании все чаще ищут альтернативы для тестирования кибербезопасности, говорит генеральный директор Bugcrowd Кейси Эллис. По некоторым оценкам, к 2021 году могут остаться открытыми до 3,5 миллионов рабочих мест .

В прошлом году компания увидела крупнейшую выплату за один эксплойт - 113 000 долларов за ошибку, обнаруженную в крупной компании, выпускающей техническое оборудование, сказал Эллис. Согласно данным, выплаты выросли на 37 процентов в годовом исчислении в 2018 году.

Согласно исследованию, половина этических хакеров - или экспертов по безопасности, нанятых для проникновения в сети и компьютерные системы от имени их владельцев - сообщили о том, что они работают на полную ставку. Около 80 процентов сказали, что усилия помогли им найти работу в области кибербезопасности. По словам Эллиса, средние ежегодные выплаты для топ-50 хакеров составили около 145 000 долларов…

IJet и Tesla платят хакерам от 1000 до 15000 долларов за поиск проблем, в зависимости от серьезности проблемы. Mastercard выплачивает до 3000 долларов. В октябре министерство обороны заключило контракты с «Взломом Пентагона» для Bugcrowd и HackerOne для их краудсорсинговых программ.» ***(Дмитрий Сизов. Наемные хакеры спасают IT компании от реального взлома // Internetua (http://internetua.com/naemnye-hakery-spasauat-it-kompanii-ot-realnogo-vzloma). 13.12.2018).***

***

«…Компания Trend Micro выпустила отчет под названием «MAPPING THE FUTURE», посвященый ключевым угрозам и тенценциям кибербезопасности в 2019 году.

По прогнозам специалистов, наиболее распространенной угрозой как среди потребителей, так и бизнеса станут фишинговые атаки. Кроме того, в информационном пространстве появится больше неизвестных киберугроз; атаки при помощи социальной инженерии заменят распространение эксплойтов;

продолжатся атаки на учетные записи знаменитостей и массовое использование похищенных данных.

В 2019 году киберпреступники будут применять больше скрытых методов атак, также получат распространение целенаправленные атаки, в том числе с помощью искусственного интеллекта. По прогнозам аналитиков, некорректная настройка параметров безопасности во время миграции в облако приведет к росту числа утечек данных, а злоумышленники будут использовать облачные сервисы для добычи криптовалюты.

Киберпреступники будут бороться за доминирование в «войне червей» для IoT-устройств; появятся первые случаи, когда пожилые люди станут легкими жертвами атак через IoT и смарт-устройства для здоровья. Предоставление возможности сотрудникам работать из дома может обернуться угрозой для безопасности предприятий, в частности благодаря росту популярности концепции BYOD, предупреждают эксперты…» ***(Trend Micro опубликовала прогноз по угрозам безопасности в 2019 году // SecurityLab.ru (https://www.securitylab.ru/news/496968.php). 13.12.2018).***

***

«…в октябре Thoma Bravo за $2,1 млрд выкупила активы компании Imperva, а в ноябре за $950 млн стала собственницей компании Veracode, которую выкупила у Broadcom. Также, если верить неофициальной информации, Thoma Bravo сделала интересное предложение о поглощении компании Symantec.

Новой покупкой Thoma Bravo обещает стать та самая McAfee, которая наполовину освободилась от Intel, а в виде другой половины принадлежит TPG Capital. Согласно утечкам от осведомлённых источников, Intel и TPG находятся на раннем этапе переговоров о продаже всех акций McAfee в собственность Thoma Bravo. В то же время источник предупреждает, что переговоры могут ничем не закончиться. Все стороны возможного обсуждения отказались комментировать данный слух.» ***(McAfee снова может сменить владельца // Goodnews.ua (http://goodnews.ua/technologies/mcafee-snova-mozhet-smenit-vladelca/). 18.12.2018).***

***

«Согласно данным Cisco, подавляющее большинство профессионалов (92%), использующих решения Интернета вещей в управлении производственными процессами, намерены уделять обеспечению информационной безопасности своих систем повышенное внимание. Они понимают необходимость использования IP-сетей, но при этом отдают себе отчет, что такое подключение сильно увеличивает площадь для кибератак.

Тем не менее, около 44% инцидентов информационной безопасности на предприятиях вообще выпадают из поля зрения ответственных специалистов, а из 56% исследованных событий действительно неложными срабатываниями оказались 34%, однако примерно по половине из них никаких мер принято не было. Причиной этого является нехватка ресурсов и квалификации персонала для адекватного анализа и реагирования на инциденты. В этой ситуации не является

панацеей даже передача обеспечения информационной безопасности на аутсорсинг, поскольку провайдеры таких услуг сами испытывают дефицит квалифицированных специалистов.

Как отмечают специалисты Cisco, для исправления ситуации необходимо начать активное использование искусственного интеллекта и повысить степень автоматизации обеспечения безопасности по всей цепочке, от обнаружения угроз до расследования инцидентов. Среди подходов к автоматизации процессов есть уже давно зарекомендовавшие себя, например, машинное обучение для составления «белых» списков, обнаружения в трафике вредоносных сигнатур и других индикаторов компрометации, а также статистическая обработка больших объемов данных для выявления отклонений от стандартных профилей поведения или признаков известных атак.

В сетях постоянно увеличивается доля зашифрованного трафика и в этом году она колеблется между 60% и 70%. Однако межсетевые экраны нового поколения, работающие на уровне трафика приложений, не в состоянии разбирать такой трафик и выявлять в нем угрозы. Поэтому злоумышленники активно используют шифрование трафика между вредоносными программами, внедренными в атакованную инфраструктуру, и центрами управления ими. Cisco научилась обнаруживать вредоносные активности в зашифрованном трафике: ее сетевое оборудование работает как датчики, передающие в системы аналитики информацию о том, какие алгоритмы использованы для шифрования трафика, какими цифровыми сертификатами подписаны сеансы связи узлов перед передачей данных, куда шифрованный трафик направлен и т.д. Эти данные дополняются информацией системы обнаружения вторжений Talos, что, как заявляют в Cisco, без расшифровки с вероятностью выше 99% выявлять вредоносный характер зашифрованного трафика.

Построенная на основе машинного обучения аналитика данных позволяет выявлять вредоносные серверы, расположенные на публичных облачных ресурсах для последующего их блокирования. Например, средство защиты веб-трафика Cisco Cognitive Threat Analytic обменивается данными с другими средствами обеспечения безопасности, повышая тем самым общий уровень защиты. Сотни собираемых параметров того или иного события после обработки аналитическими ресурсами позволяют оценить, таит ли оно реальную угрозу и является ли признаком атаки на конкретную компанию или рыночный сегмент, специфические операционные системы или оборудование управления производством.» ***(Cisco: защита промышленных систем IoT требует использования ИИ // «Компьютерное Обозрение» (https://ko.com.ua/cisco_zashhita_promyshlennyh_sistem_iot_trebuet_ispolzovaniya_ii_127179). 17.12.2018).***

***

«Генеральная ассамблея ООН подавляющим большинством голосов одобрила российскую резолюцию, содержащую кодекс поведения государств в интернете. Этот документ не является юридически обязывающим, но создает условия для выработки международной конвенции по информационной

безопасности. Москва добивалась принятия такой резолюции 20 лет. Однако большинство западных стран ее инициативу не поддержали.

Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» была поддержана 119 государствами, 46 стран проголосовали против, 14 воздержались…

Российская резолюция призывает государства придерживаться 13 принципов, предполагающих использование киберсредств «исключительно в мирных целях». Государства, как сказано в документе, не должны огульно обвинять друг друга в противоправных действиях в интернете, а все подобные претензии должны быть «обоснованными». Страны не должны позволять использовать свою территорию и инфраструктуру для осуществления кибератак, а также самим атаковать при помощи киберсредств критически важную инфраструктуру друг друга (АЭС, системы управления транспортом и водоснабжением и т. д.). Кроме того, государства обязуются не вставлять «закладки» — скрытые коды — в IT-продукцию, производимую на их территории.

Рабочей группе открытого состава предстоит обсудить эти принципы и, возможно, составить на их основе проект юридически обязывающей конвенции ООН по международной информационной безопасности. Присоединиться к работе сможет любая страна, при этом решения группа должна принимать консенсусом. Этот механизм по задумке Москвы должен прийти на смену созданной в 2004 году по инициативе РФ группе правительственных экспертов ООН. В нее в разное время входило 20–25 государств, и именно она выработала те принципы, которые Россия включила в свою резолюцию. Однако в 2017 году члены старой группы разругались, и с тех пор она парализована.

США и их союзники хотят восстановить прежний механизм, поэтому проголосовали против новой российской идеи. Американская контррезолюция будет вынесена на рассмотрение Генассамблеи ООН до конца месяца. Россия ее не поддержит, но, скорее всего, она тоже будет одобрена большинством голосов, поскольку большинство стран предпочитают не сориться ни с Москвой, ни с Вашингтоном. Между тем принятие двух конкурирующих резолюций и создание двух механизмов дальнейшей работы только углубит раскол международного сообщества по вопросам, связанным с кибербезопасностью, и отдалит перспективу выработки общепризнанных правил поведения стран в этой сфере.» ***(Елена Черненко. Россия зашла в ООН со своим киберуставом // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3821853?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 07.12.2018).***

***

Сполучені Штати Америки

«Погана кібербезпека залишає США відкритими для ракетних нападів. За словами спостерігача з Пентагону, збої в кібербезпеці підвищують загрозу «смертельних ракетних ударів»

У доповіді, датованій 10 грудня, яку оприлюднили лише у п'ятницю, підводяться підсумки восьмимісячного розслідування, проведеного Управлінням Генерального інспекції Пентагону. Звіт інспектора виявив незашифровані флешки, класифіковані сервери без блокувань і невиправлені комп'ютерні помилки, починаючи з 1990 року.

Кібербезпека втрачає базову значимість зарахунок нехтування шифруванням класифікованих флеш-накопичувачів і нездатність встановити фізичні блокування на критично важливих комп'ютерних серверах, що робить Сполучені Штати уразливими для смертельних ракетних атак, говориться в новому звіті внутрішнього спостерігача Міністерства оборони…

Насамперед, найбільш тривожним з того, що виявила перевірка, є те, що мережеві адміністратори в трьох з п'яти установ не займались усуненням відомих вразливостей, зокрема навіть тими, які були відмічені з боку американського кібер-командування як "потенційно серйозні з необхідністю негайного вирішення".» ***(Погана кібербезпека залишає США відкритими для ракетних нападів, - Пентагон // Агенція інформації та аналітики (https://galinfo.com.ua/news/pogana_kiberbezpeka_zalyshaie_ssha_vidkrytymy_dlya_raketnyh_napadiv__pentagon_303536.html). 18.12.2018).***

***

«Минобороны США сообщило, что в рамках мероприятия по поиску уязвимостей Hack the Air Force 3.0 более тридцати «белых хакеров» заработали $130 000. Всего исследователям удалось обнаружить более 120 уязвимостей. Эту акцию министерство проводило совместно с платформой HackerOne. Стартовало мероприятие 19 октября, а закончилось 22 ноября, — продлилось более четырех недель. По сути, Hack the Air Force 3.0 представляло собой самую масштабную кампанию по поиску багов, организованную правительством США. В программе приняло участие в районе 30 так называемых «белых хакеров» (white hat hackers). Теперь же Минобороны опубликовало результаты и подвело итоги конкурса…». ***(Олег Иванов. Хакеры нашли более 120 багов в системах ВВС США, заработали $130 000 // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-12-21-1447/28409). 21.12.2018).***

***

«Согласно отчету Министерства обороны США, несколько тщательно охраняемых объектов, которые являются частью Системы противоракетной обороны США (BMDS), не внедрили основные методы кибербезопасности…

Генеральный инспектор Министерства обороны США обнаружил, что в пяти местах на военных базах США имелись серьезные недостатки в области безопасности, которые могли позволить хакерам получить доступ к компьютерной сети BMDS.

BMDS — это система ПРО США, предназначенная для перехвата иностранных ракет, прежде чем они взорвутся на территории США.

Следователи обнаружили проблемы, в том числе уязвимость в компьютерной сети, которую впервые выявили американские военные в 1990 году, но до сих пор не устранили.

Сотрудники также нашли видеозапись, где видно, как военнослужащий получает доступ к тщательно охраняемому компьютерному объекту, просто открывая незапертую дверь и проходя мимо сослуживцев.

Авторы отчета написали, что нарушение было "серьезной угрозой безопасности персонала". В докладе также отмечается, что сотрудники, которым был предоставлен доступ к компьютерным сетям, не обращались за ним надлежащим образом.

Персонал, работающий с компьютерными сетями, должен использовать многофакторную аутентификацию, которая включает использование карт безопасности и токенов для доступа к сетям, чтобы снизить риск взлома.

Но отчет показал, что люди, работающие над системой ПРО, обычно использовали только имя пользователя и пароль, причем один сотрудник делал это в течение семи лет. В защищенных сетях не было программного обеспечения, предназначенного для выявления и прекращения попыток взлома…» ***(Система противоракетной обороны США оказалась без киберзащиты // Goodnews.ua (http://goodnews.ua/technologies/sistema-protivoraketnoj-oborony-ssha-okazalas-bez-kiberzashhity/). 18.12.2018).***

***

«Не так давно в США имел место скандал, связанный с тем, что многие крупные компании, такие как Amazon, Apple и другие, плюс некоторые военные подрядчики с 2015 года закупали вычислительную технику, в которой были использованы "нестандартные" комплектующие.

Исследования, проведенные специалистами Флоридского института проблем кибербезопасности (Florida Institute for Cybersecurity Research, FICS), указывают на то, что это все является кибератакой нового типа…

Более того, специалисты FICS уже разработали новую технологию, позволяющую выявлять и противодействовать атакам такого типа. Созданная ими полуавтоматическая система позволяет определить наличие "аномалий", требующих пристального внимания, в электронном устройстве любой сложности. От сложности устройства только зависит время, через которое новая система выдает результат, и это время может колебаться от нескольких секунд до нескольких минут.

В новой системе используются блоки формирования оптических изображений, микроскопы, рентгеноскопия и искусственный интеллект. При помощи всего этого система способна произвести анализ печатной платы устройства, установленных на ней чипов и других компонентов с целью поиска любых несоответствий с изначальным дизайном.

Работа системы начинается с проведения высококачественной съемки верхней и нижней сторон анализируемой печатной платы. Полученные данные пропускаются через предварительно обученную систему искусственного интеллекта, которая идентифицирует все компоненты и соединений между ними.

Рентгеновские технологии позволяют заглянуть вглубь печатной платы, обнаружить соединения на промежуточных слоях и даже компоненты, которые могут быть скрыты внутри платы вместо их установки на поверхности.

В результате работы системы получается серия двухмерных снимков, которые затем "сшиваются" в одну трехмерную карту печатной платы и установленных компонентов. И сейчас эта система успешно справляется с составлением карты больших печатных плат, имеющих до 12 внутренних слоев. В конце концов, реальная трехмерная карта сравнивается с трехмерной картой, построенной на базе данных изначального проекта. Естественно, что такое сравнение позволяет выявить все несоответствия, наличие недостающих, лишних чипов и соединений, при помощи которых реализуются шпионские недокументированные функции…» ***(Новая технология позволит рассекретить любую аномалию в электронике за минуты // "Багнет" (http://www.bagnet.org/news/tech/384303/novaya-tehnologiya-pozvolit-rassekretit-lyubuyu-anomaliyu-v-elektronike). 14.12.2018).***

***

Країни ЄС

«Єврокомісія, Європейська Рада та Європарламент дійшли згоди у політичному рішенні щодо прийняття Акту з кібербезпеки. Завдяки документу значно посилиться мандат європейської агенції з кібернетичної безпеки (ENISA)…

Документ має сприяти країнам-членам ЄС краще взаємодіяти при попередженні та виявленні кібернетичних загроз та координації відповідних дій щодо цих кібератак. Акт з кібернетичних безпеки включає систему сертифікації для онлайн послуг та відповідних споживчих гаджетів.» ***(Ілля Нежигай. Євросоюз збільшить протидію кіберзагрозам // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1767331-yevrosoyuz-zbilshit-protidiyu-kiberzagrozam). 11.12.2018).***

***

«Європарламент (ЄП) на пленарному засіданні в Страсбурзі визначив зовнішньополітичні та безпекові пріоритети Євросоюзу на наступний рік. Вони прописані в прийнятій євродепутатами резолюції, йдеться на сайті ЄП…

Одним з основних пріоритетів для Європи називається протистояння кіберзагрозам, що йдуть від Росії…» ***(Олексій Супрун. Європарламент назвав пріоритетною метою боротьбу з російською кіберзагрозою // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1767547-yevroparlament-nazvav-prioritetnoyu-metoyu-borotbu-z-rosiyskoyu-kiberzagrozoyu). 13.12.2018).***

***

«После многочисленных обвинений со стороны различных государств китайская технологическая компания Huawei решила дать свой ответ. Техногигант принял решение инвестировать около двух миллиардов долларов в обеспечение кибербезопасности. Таким образом, как заявили в самой компании, Huawei хочет раз и навсегда решить вопросы, связанные с обвинениями в угрозе национальной безопасности, которую якобы несут продукты техногиганта. Помимо этого, решение вложить дополнительные средства в кибербезопасность связано еще и с поставкой оборудования по технологии 5G — Huawei уже заключила 25 коммерческих контрактов. «Мы уже поставили более 10 000 базовых станций для 5G, что наглядно демонстрирует надежность компании», — цитирует China Daily одного из топ-менеджеров Huawei первого призыва Ху Хоукуня (он же Кен Ху). «Мы откроем Центр прозрачности в Брюсселе, это случится приблизительно в первом квартале следующего года. Такой шаг поможет нашим клиентам понять — на продукты компании можно положиться»…» ***(Олег Иванов. Huawei отвечает на обвинения вложением $2 млрд в кибербезопасность // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-12-19-1447/28382). 19.12.2018).***

***

«Влада КНР вкрай незадоволена заявами американського уряду про хакерські атаки і розкраданні мережевої інформації, нібито причетних до китайських держорганів…

«Китайський уряд займає незмінну і однозначну позицію з питань мережевої безпеки. Китай виступає рішуче за безпечний інтернет, твердо бореться з розкраданнями інформації через інтернет в будь-яких їх проявах», — йдеться в заяві, опублікованій на офіційному сайті зовнішньополітичного відомства…

«Звинувачення в так званій інтернет-крадіжці відносно двох громадян КНР і відповідний ”позов" — дії, які серйозно порушують норми міжнародного законодавства, завдають серйозної шкоди китайсько-американським відносинам ... Китай висловлює з цього приводу рішучий протест, а також жорстке подання на адресу США…» ***(Ілля Нежигай. МЗС Китаю висловив ноту протесту США за звинувачення в хакерстві // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1769091-mzs-knr-visloviv-protest-ssha-za-zvinuvachennya-na-adresu-kitayu-v-khakerskikh-rozkradannyakh). 21.12.2018).***

***

Російська Федерація та країни ЄАЕС

«До Держдуми Росії внесли законопроект про відключення від світової мережі та автономну роботу російського сегменту інтернету…

У пояснювальній записці автори підкреслюють, що враховували "агресивний характер прийнятої у вересні 2018 року стратегії національної кібербезпеки США".

На думку російських парламентаріїв, в ній міститься принцип "збереження миру силою", а Росія "бездоказово" звинувачується в хакерських атаках.

Російський законопроект, зокрема, передбачає централізоване управління трафіком та технічне обмеження доступу до ресурсів із забороненою інформацією.

У законопроекті зазначається, що таким чином створюється можливість для мінімізації передачі за кордон даних, якими обмінюються між собою російські користувачі. Для цього будуть визначені точки підключення російських мереж до зарубіжних…

Крім цього, в російських мережах повинні встановити технічні засоби, що визначають джерело трафіку. Ці засоби повинні будуть при необхідності обмежити доступ до ресурсів із забороненою інформацією не лише за мережевими адресами, а й шляхом заборони пропуску трафіку.

Для роботи російського сегмента інтернету в ізольованому режимі буде створена національна система DNS.» ***(Інквізиція в мережі: у Путіна готуються відсікти рунет від світової павутини // znaj.ua (https://znaj.ua/world/194968-inkviziciya-v-merezhi-u-putina-gotuyutsya-vidsikti-runet-vid-svitovoji-pavutini). 14.12.2018).***

***

«На территории России несколько хакерских группировок собирают данные российских граждан в интересах других стран, чтобы затем в отношении них можно было ввести санкции, сообщил на конференции AntiFraud Russia глава компании Group IB Илья Сачков…

По словам Ильи Сачкова, задача таких хакеров заключается не в том, чтобы «воровать деньги из банка», а в том, чтобы «пополнять санкционные американские списки». Для сбора информации используются не только банки, но и компании из разных секторов, их партнеры и подрядчики, которых проще взломать, чтобы добраться до необходимых данных, добавил он.

Источник РБК на рынке кибербезопасности рассказал, что «два или даже три подобных случая в России, когда таким образом вводили санкции, уже точно были». По его словам, хакеры проникают в банки, чтобы выявлять их клиентов, против которых можно было бы ввести санкции. «Они изучают в первую очередь их счета, а также объемы и направления транзакций», — рассказал он.

По данным Group IB, такие хакерские группы работают не только в России, в топ-3 стран происхождения самых активных проправительственных хакерских групп входит Китай, Северная Корея и Иран…» ***(Group IB рассказала о сборе хакерами данных для санкций против россиян // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3822035?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 07.12.2018).***

***

«Digital Revolution часто цитируют Виктора Цоя, а свой первый твит «настало время освободить Рунет» они сопроводили треком рэпера Влади

Хакеры из группы Digital Revolution утверждают, что взломали сервер НИИ «Квант», принадлежащего ФСБ. Опубликованные ими документы описывают систему мониторинга соцсетей, основная цель которой — анализ протестных настроений. Такую систему «Квант» в качестве субподрядчика уже реализует в Казахстане…

В октябре 2018 года они пообещали наказать тех, кто, по их мнению, «превращают интернет в тюрьму» — российские спецслужбы, правоохранительные органы и Роскомнадзор.

1 декабря группа дала понять, что взломала сервер научно-исследовательского института «Квант».

Закрытый институт в спальном московском районе Ховрино в 1970-е годы создавал первые советские ЭВМ, в 2008 году его перевели в ведение ФСБ.

В доказательство взлома «цифровые революционеры» выложили скриншоты, на которых видны названия папок и список администраторов на сервере «Кванта». Публикацию они сопроводили хештегом #квантнаш…

Кроме того, они изменили код официального сайта «Кванта»: при заходе на него появлялось изображение собак в балахонах — одного из символов «цифрового сопротивления» блокировкам мессенджера Telegram.

В настоящий момент сервер «Кванта» отключен вместе с сайтом и корпоративной почтой…

«Квант» — не случайная жертва хакеров. НИИ упоминался на сайте WikiLeaks как один из клиентов итальянской компании Hacking Team. Исходя из той утечки, в 2012-2014 годах «Квант» мог приобрести у компании несколько шпионских программ, среди которых, по данным Forbes, была Remote Control System («Удаленная система контроля»), позволявшая отслеживать действия на зараженных устройствах: делать снимки с экрана, подключаться к веб-камере и микрофону, перехватывать переписку и пароли.

За создание подобных программ «Репортеры без границ» объявили Hacking Team «врагами интернета». По данным ESET, итальянцы продолжают создавать шпионские программы, пользующиеся спросом у авторитарных режимов…

19 декабря хакеры из Digital Revolution опубликовали на своем сайте четыре документа объемом более 300 страниц. Они посвящены системам мониторинга СМИ и соцсетей, к разработке которых, исходя из их слов, мог быть причастен «Квант…». ***(Андрей Сошников , Андрей Захаров. Самообучаемая нейронная сеть ФСБ проанализировала «путинско-сечинский застой» // hpib.life (http://hpib.life/samoobuchaemaya-nejronnaya-set-fsb-proanalizirovala-putinsko-sechinskij-zastoj/). 22.12.2018).***

***

«В первой половине 2018 года доля атак на компьютеры автоматизированных систем управления (АСУ) технологическим процессом в России составила 44,7%, а в мире — 41,2% (выросла на 3,5 п.п.). Россия вошла в топ-20 стран по проценту атакованных компьютеров АСУ ТП. В целом доля атакованных компьютеров АСУ растет, что связано с общим повышением вредоносной активности и увеличением цифровизации предприятий. Различным

организациям важно помнить: отсутствие подключения устройств к сети вовсе не гарантирует их защищенности от киберугроз. Исследования «Лаборатории Касперского» показывают, что злоумышленники могут успешно атаковать множество промышленных компаний, даже используя простые техники атаки, известное вредоносное ПО, фишинговые письма, а также методы социальной инженерии и сокрытия вредоносного кода в системе. В этом году мы зафиксировали волну фишинговых писем с вредоносными вложениями, нацеленных преимущественно на промышленные компании в России. Вредоносная программа, используемая в атаках, устанавливала в систему легитимное ПО для удаленного администрирования, которое позволяло злоумышленникам получать удаленный контроль над атакованными системами. Также были предотвращены множественные попытки атак с использованием RAT (программ для удаленного администрирования) в технологических сетях компаний. В основном они были направлены на технологическую сеть автомобилестроительной или сервисной компании, в частности на компьютеры, предназначенные для диагностики двигателей и бортовых систем грузовиков и тяжелой техники. Потенциальный ущерб от кибератаки на промышленную инфраструктуру может быть грандиозным. Показательна статистика за 2017 год, согласно которой средние затраты для компаний, столкнувшихся с киберинцидентом, составили $347,6 млн. Очень интенсивно растет список уязвимостей, найденных в решениях для промышленного IoT, и пока нет эталонов его безопасной архитектуры…» ***(Алексей Петухов. Вопрос цены // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3821732?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 07.12.2018).***

***

«…В связи с появлением новых угроз информационной безопасности Министерства иностранных дел РФ в ведомстве будет создан новый отдел, занимающийся вопросами ИБ. Об этом в понедельник, 17 декабря, заявил постпред РФ в Вене Михаил Ульянов…

По словам Ульянова, в настоящее время министерство активно занимается вопросом информационной безопасности. У России есть немало сторонников, отметил постпред, «так что процесс идет». Тем не менее, говорить о результатах пока еще рано…». ***(В МИД РФ будет создан новый департамент по вопросам ИБ // SecurityLab.ru (https://www.securitylab.ru/news/497035.php). 18.12.2018).***

***

Інші країни

«Довольно-таки неприятный прецедент может произойти в Австралии, власти которой решили принять новый закон, согласно которому различные IT-компании обязаны содействовать правоохранительным органам и по первому требованию предоставлять доступ к зашифрованным данным.

Документ поддержали обе палаты парламента, теперь его должен подписать генерал-губернатор Австралии. Оппозиционная Лейбористская партия согласилась отозвать свои поправки к проекту при условии, что парламент рассмотрит их в следующую сессию в 2019 году.

Законопроект направлен на борьбу с терроризмом, организованной преступностью и педофилией, утверждают в правительстве. Премьер-министр Скотт Моррисон заявил, что 95% людей, которые находятся под наблюдением правоохранительных органов, используют сервисы с функцией шифрования переписки. В результате правоохранительные органы «не видят и не слышат», заключил советник правительства по кибербезопасности Аластер МакГиббон…

Закон затронет такие компании, как Google, Facebook, Apple и прочие. Полиция и спецслужбы получат право требовать от технологических компаний ключи шифрования, а также возможности бэкдора, которые позволят самостоятельно получать доступ к устройствам и сервисам. Компании при этом не смогут уведомлять пользователей о сотрудничестве с правоохранительными органами.

Для того, чтобы избежать злоупотреблений, полномочия правоохранительных органов будут ограничены — они смогут требовать такие инструменты только при расследовании тяжких преступлений и только при наличии ордера.

За неисполнение требований компаниям грозят штрафы в размере до 10 млн австралийских долларов ($7,3 млн), а сотрудникам, которые отказались помочь получить данные предполагаемых преступников, — тюремные сроки.

С законопроектом несогласны члены ассоциации Digital Industry Group, в которую входят Google, Facebook, Apple, Amazon и Twitter. В сообщении ассоциации говорится, что законопроект «противоречит европейскому законодательству о защите данных и ставит под угрозу безопасность приложений и систем, которыми каждый день пользуются миллионы австралийцев». ***(«Давайте сделаем австралийцам безопасное Рождество!»: о передаче ключей шифрования государству // РосКомСвобода (https://roskomsvoboda.org/43631/). 07.12.2018).***

***

«…Национальное управление по кибернетике и информационной безопасности Чехии предостерегло операторов связи от использования программного обеспечения и техники производства китайских компаний Huawei и ZTE, поскольку они могут представлять угрозу безопасности пользователей.

«Обнаруженные свидетельства активности этих компаний в Чехии и по всему миру вызывают обоснованное беспокойство о существовании потенциальных рисков использования технических и программных инструментов, предоставляемых клиентам в целях поддержки интересов Китая», - говорится в сообщении ведомства. При этом в документе не приводятся какие-либо конкретные доказательства шпионажа.

«Китайские законы требуют от частных компаний, базирующихся в Китае, сотрудничества с разведывательными службами, поэтому их внедрение в главные государственные системы может стать угрозой», - заявил директор национального агентства Душан Навратил (Dusan Navratil)…

Чехия стала еще одной страной, выразившей обеспокоенность по поводу рисков использования оборудования Huawei и ZTE…» ***(Чехия сочла оборудование Huawei и ZTE угрозой безопасности // SecurityLab.ru (https://www.securitylab.ru/news/497045.php). 18.12.2018).***

***

«Премьер Чехии Андрей Бабиш запретил работникам администрации правительства использовать мобильные телефоны, произведенные китайской фирмой Huawei

Подобный шаг также готовит Министерство промышленности и торговли…

Поводом для такого решения стало обнародованное ранее предупреждение со стороны Национальном управлении по вопросам кибернетической и информационной безопасности, согласно которому использование аппаратного и программного обеспечения, производимого фирмами Huawei и ZTE, представляет угрозу для национальной безопасности.

В Управлении заявили, что китайские законы требуют, чтобы частные компании, базирующиеся в Китае, сотрудничали с разведывательными службами, поэтому их внедрение в главные государственные системы может стать угрозой.

В Huawei отвергли утверждение, что продукты компании могут представлять угрозу чешской безопасности…» ***(Администрации правительства Чехии запретили пользоваться гаджетами Huawei //DsNews (http://www.dsnews.ua/world/administratsii-pravitelstva-chehii-zapretili-polzovatsya-19122018083500). 19.12.2018).***

***

«Про компанії Huawei та ZTE ходять недобрі поголоси. Нібито вони збирають дані для Китаю. Достеменно стверджувати так ми не можемо, але країни одна за одною починають відмовлятися від їхніх послуг. Хоча, як відомо, Huawei – це найбільший у світі виробник телекомунікаційного обладнання. Ще в листопаді, Австралія та Німеччина, виключили його з конкурсу на отримання тендера з будівництва мереж 5G. США та Великобританія теж відмовились.

Тепер і Японія має намір заборонити на державному рівні придбання обладнання у китайських компаній. Таким чином, вони хочуть посилити захист від кібератак та витоків персональних даних. Найближчим часом, японський уряд перегляне правила закупівель обладнання і тоді стане відома доля китайських компаній. Але висновки можна зробити вже зараз, хоч би з того, що Японія перебуває в тісному контакті з США у багатьох галузях, включно з кібербезпекою.» ***(Грицина Вікторія. Японія теж відмовляється від послуг Huawei та ZTE // Pingvin.Pro (https://pingvin.pro/gadgets/news-gadgets/yaponiya-proty-huawei-ta-zte.html). 07.12.2018).***

***

«Розвідувальні служби Росії стояли за торішніми кібератаками, спрямованими на чеське міністерство закордонних справ. Про це повідомила чеська служба безпеки BIS…

У своїй доповіді BIS заявила, що "дві окремі атаки на чеське міністерство закордонних справ почасти є роботою групи хакерів APT28, яка пов'язана з російським урядом і звинувачується у минулих нападах у Німеччині та Сполучених Штатах".

"Усі висновки ясно показують, що це була кібершпигунська кампанія Turla, що походить від ФСБ, російської розвідки і APT28/Sofacy, яка приписується російській військовій розвідці, ГРУ", - йдеться у річному звіті.

Як повідомляється, зловмисники отримали доступ до більш ніж 150 поштових скриньок співробітників МЗС країни, копіюючи електронні листи і вкладення…» ***(Юлія Шрамко. Чехія звинуватила РФ у кібератаках на МЗС // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1765793-chekhiya-zvinuvatila-rf-u-kiberatakakh-na-mzs). 03.12.2018).***

***

«…запрет правительства США на программное обеспечение «Лаборатории Касперского» был подписан. Запрет, вписанный в Закон о защите национальной обороны на 2018 год (NDAA), запрещает использовать антивирусное программное обеспечение, созданное российской фирмой по кибербезопасности…

Закон применяется как к гражданскому населению, так и к военному.» ***(vanburen. Дональд Трамп подписал закон о запрете ПО «Лаборатории Касперского» // HiTechNews (https://hitechnews.biz/programmy/trump-podpisal-zakon-o-zaprete-po-laboratorii-kasperskogo.html). 13. 12.2018).***

***

«Контролируемые Кремлем фейковые аккаунты в Twitter активизировались против французского президента Эммануэля Макрона и на фоне протестов “желтых жилетов” во Франции начали распространять ложную и неподтвержденную информацию…

Как рассказали в Альянсе обеспечения демократии, в котором отслеживает активность кремлевских ботов и пророссийскую деятельность, Макрону удалось избежать кибератак во время выборов в 2017 году. Тогда за попытками дискредитировать Макрона, как считается, стояли прокремлевские группы.

Сейчас же, по данным ресурса, в Twitter активно освещают протесты во Франции 600 пророссийских учетных записей. Российские боты пишут, что французская полиция якобы находится на грани мятежа и готова стать на сторону протестующих.» ***(Кремлевские боты начали атаковать Макрона в Twitter //***

АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/274233-kremlevskie_boty_nachali_atakovatj_makrona_v_twitter). 09.12.2018).

***

«Хакеры, предположительно работающие по заданию Министерства государственной безопасности Китая, взломали сети американских технологических компаний Hewlett Packard Enterprise и IBM, а затем воспользовались полученными сведениями для атаки на их клиентов…

Эти атаки, как предполагается, часть кампании, названной Cloudhopper и направленной против американских, британских и немецких компаний. Компании, занимающиеся кибербезопасностью, и различные государственные учреждения говорят о такой кампании с 2017 года, не называя при этом конкретные компании, против которых она была направлена. Атаки направлены прежде всего на так называемых поставщиков удаленных услуг, хакеры хотели получить доступ к сетям таких компаний, чтобы через них получить доступ к сетям и конфиденциальной информации компаний-клиентов. В IBM заявили, что у них нет сведений о том, что какие-либо конфиденциальные корпоративные данные были скомпрометированы. Hewlett Packard отказалась комментировать ситуацию…» ***(Яна Рождественская. Reuters: Китай подозревают в хакерской атаке на Hewlett Packard и IBM // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3840510?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 21.12.2018).***

***

«Турецьким фахівцям вдалося запобігти кібератаці, націленій на штаб командування збройних сил країни, повідомив у середу президент Туреччини Реджеп Таїп Ердоган.

"Програмне забезпечення під назвою Octopus, яке ми розробили в Туреччині, запобігло кібератаці на штаб командування збройних сил", - наводить газета Daily Hurriyet слова турецького лідера. Він розповів про ситуацію, виступаючи на Науково-технічній дослідницькій раді в Анкарі.

Ердоган зазначив, що кібератаки представляють сьогодні одну з "найбільших загроз, які послаблюють національну безпеку і право людини на таємницю особистого життя"…» ***(Ердоган повідомив про запобігання кібератак на турецьке військове командування // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/555790.html). 26.12.2018).***

***

Створення та функціонування кібервійськ

«Міністерство національної оборони Польщі завершує роботу над створенням військ оборони кіберпростору…

Одним з нових проектів є військові сили, які захищатимуть кіберпростір…

"…Ми також консолідуємо установи, які підлягають міністерству національної оборони, відповідальні за кібербезпеку. До таких дій нас зобов'язано рішенням саміту НАТО у Варшаві", – сказав міністр національної оборони Польщі Маріуш Блащак…» ***(Юлія Шрамко. Польща створить війська кібероборони // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1766148-polscha-stvorit-viyska-kiberoboroni). 05.12.2018).***

***

«Японія планує оснастити війська Національних Сил Самооборони новими технологіями, які б могли здійснювати кібернетичні атаки…

На сьогодні японським оборонним відомством розробляється відповідне положення, яке необхідно до кінця року…

…таке рішення прийнято через стрімкий розвиток комунікаційних мереж та особливу важливість кібернетичного простору в умовах сучасного веденнях бойових дій. Відповідно до японської конституції зброя буде заборонена для використання в наступальних цілях, тому Сили Самооборони Японії зможуть використовувати технології виключно у відповідь на кібератаки по країні…» ***(Ілля Нежигай. Японія планує використовувати кіберзброю при самообороні // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1765575-yaponiya-planuye-vikoristovuvati-kiberzbroyu-pri-samooboroni). 02.12.2018).***

***

Кіберзахист критичної інфраструктури

«Опубликовано третье издание «Руководство по кибербезопасности на борту кораблей».

…Корабли сталкиваются с теми же проблемами с кибербезопасностью, что и представители других отраслей. В связи с этим было выпущено специальное руководство по обеспечению кибербезопасности на борту кораблей.

«Руководство по кибербезопасности на борту кораблей» («Guidelines on Cyber Security onboard Ships») является третьим изданием, одобренным конгломератом, в который входит 21 международная ассоциация и отраслевая группа. В документе представлены рекомендации по обеспечению безопасности бортовых IT-систем, а также приведены примеры возможных последствий, которыми чреваты нарушения этих рекомендаций…

Помимо вредоносного ПО, инфицирующего критически важные системы управления судном, корабли также подвержены атакам программ-вымогателей. Иногда они атакуют используемые кораблем системы и серверы непосредственно во время рейса. Не всегда вина за заражение лежит на команде корабля – в некоторых случаях инцидент случался на стороне партнеров. В документе также описываются случаи, когда владельцы судов платили выкуп вымогателям.»

(Морские суда часто подвергаются кибератакам // SecurityLab.ru (https://www.securitylab.ru/news/497004.php). 14.12.2018).

***

Захист персональних даних

«Google обнаружил ошибку в обновлении софта, из-за которого сторонние разработчики могли получить доступ к персональным данным более 50 млн пользователей Google +. В связи с этим процесс закрытия соцсети перенесли с августа на апрель 2019 года…

Тестирование выявило ошибку в работе API Google+, которую в компании «быстро исправили».

В течение шести дней разработчики приложений могли запрашивать закрытые данные профиля пользователей.

На текущий момент известно, что ошибка затронула около 52,5 млн пользователей, в том числе данные об именах, адреса электронной почты, род занятий, возраст и другое.

Кроме того, приложения с доступом к данным профиля Google+, также имели доступ к закрытым данным профиля, которые были переданы с согласия другого пользователя.

Ошибка не дает разработчикам доступ к финансовым данным, национальным идентификационным номерам, паролям и другой информации, обычно используемой с целью мошенничества или кражи личных данных…» ***(Екатерина Симикян. Google сообщил о планах ускорить закрытие Google+ из-за утечки данных более 50 млн пользователей // Rusbase (https://rb.ru/news/google-utechka/). 11.12.2018).***

***

«Расследование кражи личных данных 500 млн клиентов Marriott показало, что к этому инциденту могут быть причастны хакеры, связанные с правительством Китая…

К такому выводу пришли частные следователи, которых наняла сеть отелей. Они обнаружили, что при взломе системы бронирования Starwood использовались методы, которые китайские хакеры применяли и в других атаках.

Источники предполагают, что украденная информация может быть использована властями Китая для шпионажа. При этом не исключен вариант, что к взлому причастна и другая группа киберпреступников, так как часть приемов, которые применялись при атаке на Starwood, выкладывалась в интернет…» ***(Анна Полякова. В краже персональных данных гостей Marriott заподозрили правительство Китая // Rusbase (https://rb.ru/news/v-krazhe-zapodozrili-kitai/). 06.12.2018).***

***

«В наши дни наиболее актуальными угрозами в сфере информационной безопасности являются потеря данных и утечка информации, вызванные действиями организованной преступности. Большинство таких атак происходит с помощью популярных моделей вымогательства, таких как шифровальщики или криптоджекинг , обе из которых являются достаточно простыми и эффективными способами получения требуемого результата…

Сегодня мы говорим с Брайаном Хонаном, основателем Ирландской службы отчетности и информационной безопасности (IRISS), первой в Ирландии компьютерной группы реагирования на чрезвычайные ситуации (CERT, Computer Emergency Response Team). Журнал SC назвал его Человеком года в информационной безопасности, а в 2016 году он был включен в Зал славы Infosecurity Europe…» ***(Брайан Хонан: "Раньше было 2-3 утечки данных в месяц. Теперь – 2-3 в день" // SecurityLab.ru (https://www.securitylab.ru/blog/company/PandaSecurityRus/345300.php). 06.12.2018).***

***

«Злоумышленники могут использовать контрольные вопросы в Windows 10 для сохранения присутствия на взломанной системе.

Киберпреступники, атакующие компьютеры под управлением Windows, как правило стремятся заполучить на атакуемой системе права администратора. Когда желаемые права получены, сохранить их помогут контрольные вопросы, считают эксперты.

В ходе своего выступления на конференции Black Hat Europe исследователи компании Illusive Networks продемонстрировали новый метод сохранения присутствия на взломанной системе с помощью контрольных вопросов в Windows 10. Контрольные вопросы были добавлены в ОС в апреле нынешнего года и предназначены для большего удобства пользователей…

По словам исследователя Магала База (Magal Baz), контрольные вопросы облегчают жизнь администратору, но также ставят его под угрозу. Если администратор забыл свой пароль, авторизоваться в учетной записи Windows будет невозможно, и для возобновления доступа потребуется переустановка системы. Контрольные вопросы избавляют от необходимости переустанавливать Windows…

Тем не менее, с точки зрения безопасности контрольные вопросы еще более ненадежны, чем пароли. У них нет срока давности, к ним не предъявляются требования по сложности и в большинстве случаев они никогда не меняются. Кроме того, зачастую ответы на контрольные вопросы можно легко найти в соцсетях…» ***(Контрольные вопросы в Windows 10 могут использоваться как бэкдор // SecurityLab.ru (https://www.securitylab.ru/news/496848.php). 06.12.2018).***

***

«Американский социальный сервис обмена знаниями Quora сообщил о кибератаке на свои системы. В результате хакерам удалось получить доступ к личным данным более 100 млн пользователей, рассказал в блоге компании создатель сервиса Адам д'Анджело…

Компания проводит внутреннее расследование причин инцидента. Quora также уведомила о кибератаке правоохранительные органы.

По словам основателя сервиса, хакеры могли получить доступ к сведениям об учетных записях пользователей, например, имена, адреса электронной почты, зашифрованные пароли, а также данные, переданные из других сетей при авторизации.

Помимо этого кибератака затронула публичные данные, в том числе вопросы, ответы, комментарии и предложения.

По мере проведения расследования Quora предпринимает дополнительные меры для улучшения безопасности, уведомляя о кибератаке пользователей, чьи данные были скомпрометированы…» ***(Екатерина Симикян. Сервис обмена знаниями Quora сообщил об утечке личных данных более 100 млн пользователей // Rusbase (https://rb.ru/news/quora-utechka-dannyh/). 04.12.2018).***

***

«Неизвестные взломали принтеры по всему миру, разослав сообщение с предложением провести «самую вирусную кампанию в истории»…

В твиттер-аккаунте printeradvertising (в настоящее время доступ к аккаунту ограничен), который, предположительно, является автором рассылок, также появилось сообщение о проведении кампании…» ***(Анастасия Марьина. Неизвестные взломали принтеры по всему миру, разослав рекламу своих услуг по взлому // Rusbase (https://rb.ru/news/vzlom-printery-mir/). 03.12.2018).***

***

«Кіберзлочинність сьогодні поширена в різних формах, але однією з найстаріших і найнебезпечніших є атака типу Man-In-The-Middle (MITM). Дослівно це перекладається як «людина посередині», тобто коли злочинець виступає в ролі посередника при передачі інформації. Цей тип кіберзлочину є розповсюдженим та руйнівним…

Суть атаки man-in-the-middle доволі проста: злочинець таємно перехоплює трафік з одного комп’ютера та відправляє його кінцевому одержувачу, попередньо прочитавши та змінивши на свою користь.

Атаки MITM надають злочинцю можливість робити такі дії як підміна криптовалютного гаманця для викрадення коштів, перенаправлення браузера на шкідливий веб-сайт або ж просто пасивний збір інформації з метою її подальшого злочинного використання.

Кожного разу, коли третя сторона перехоплює інтернет-трафік, це можна ідентифікувати як атаку MITM. Такі дії зовсім неважко зробити злочинцеві навіть без належної автентифікації. Наприклад, загальнодоступні мережі Wi-Fi є гарним джерелом для MITM, оскільки ні маршрутизатор, ні підключений комп’ютер не перевіряють її ідентичність.

У випадку публічної атаки через мережу Wi-Fi зловмисник повинен перебувати поблизу та під'єднатися до тієї самої мережі, або ж просто мати комп'ютер в мережі, здатний перехоплювати трафік. Не всі атаки MITM вимагають, щоб зловмисник фізично знаходився поруч зі своєю жертвою, оскільки існує велика кількість штамів зловмисного програмного забезпечення, яке здатне викрасти трафік та підмінити інформацію в будь-якому місці, де є можливість інфікувати комп'ютер жертви.

Боротьба з атаками MITM вимагає використання певної форми автентифікації кінцевої точки, наприклад TLS або SSL, яка застосовує ключ ідентифікації, що в ідеалі не може бути підробленим. Слід зазначити, що методи автентифікації стають все більш сильними, що веде до наскрізного шифрування деяких систем.

Двофакторний метод автентифікації є одним з прикладів підвищеного захисту проти атак MITM…

Інтернет речей (IoT) стає все більш популярною метою для атак типу MITM, оскільки число пристроїв зростає швидко, і технології безпеки просто не встигають за ними. IoT-пристрої також потенційно можуть надсилати великі обсяги особистої інформації про індивідуальних користувачів та компаній, що робить викрадення трафіку перспективною справою для кіберзлочинців.

Корпорації, що працюють з технологією Industrial Internet of Things (IIoT), стикаються з особливим ризиком з боку атак MITM з причини слабкого захисту конфіденційної інформації, до якої мають доступ машини IIoT. Атака типу MITM на системи IIoT може призвести до зупинки виробництва, маніпуляцій з продуктом, що виготовляється, з метою зробити його менш якісним чи безпечним, а також до викрадення пропрієтарної інформації, яку використовують машини IIoT у виробничому процесі…» ***(Атаки типу Man-In-The-Middle: що треба знати кожному // Blog Imena.UA (https://www.imena.ua/blog/man-in-the-middle/). 14.12.2018).***

***

«Вопрос кибербезопасности постепенно выходит на первый план для большинства стран мира. К такому выводу пришли специалисты компании Trend Micro…

В Trend Micro считают, что такой распространенный вид мошенничества, как фишинг, в следующем году приобретет новые масштабы. Старая схема хорошо себя зарекомендовала, а пользователи никак не научатся игнорировать подозрительные письма в электронной почте.

Нехитрая уловка позволяет взламывать даже компьютеры правительственных учреждений, похищать важные документы и вести слежку за высокопоставленными чиновниками.

«ПЕРЕЙДИТЕ ПО ССЫЛКЕ». Количество фишинговых атак за последние три года возросло на целых 3800%. В 2019 году станет еще больше сообщений с видео. Если вы попытаетесь посмотреть видеоролик, вам порекомендуют обновить плеер. При скачивании обновления вирус проникнет в компьютер пользователя.

ЧАТ-БОТЫ. Любители соцсетей и мессенджеров столкнутся с чат-ботами, зараженными вредоносными программами. При помощи «взломанных» ботов злоумышленники будут проникать в домашние сети и похищать личные данные пользователей (пароль от онлайн-банкинга, почты, аккаунта в соцсети).

ПСЕВДОБАНКИНГ. Только соцсетями хакеры не ограничатся. Под угрозой – боты, обслуживающие онлайн-банкинги. Такие псевдопомощники, представляясь работниками финучреждений, будут предлагать пользователю пройти по опасной ссылке. После этого злоумышленники получат доступ к банковским данным пользователей.

ФЕЙК НЬЮЗ. На государственном уровне угрозой №1 можно назвать фейковые новости. В Trend Micro отмечают, что особо ожесточенные кибератаки ждут те страны, где должны состояться выборы. Под ударом – Украина, Польша, Греция, ЮАР, Нигерия, Индия и Индонезия.

НОВАЯ БОРЬБА. В ответ на киберугрозы государства вынуждены будут ужесточить контроль за хакерами и киберпреступностью в целом. ООН от обсуждения международного Договора о кибербезопасности перейдет к его принятию. Вероятно, в организации кибератак будут обвинять Россию, Северную Корею и Китай. Все соцсети ждет еще более пристальное внимание со стороны спецслужб.» ***(Гарченко. Опасность в сети: какие киберугрозы поджидают нас в 2019 году // ETCETERA.MEDIA (https://etcetera.media/opasnost-v-seti-kakie-kiberugrozyi-podzhidayut-nas-v-2019-godu.html). 22.12.2018).***

***

«Производитель решений для обеспечения информационной безопасности Fortinet опубликовал исследование, посвященное киберугрозам в ближайшие годы.

По словам экспертов, многие преступные организации оценивают технологии атак не только с точки зрения их эффективности, но и учитывают затраты на их разработку, модификацию и реализацию. Таким образом, для остановки некоторых атак достаточно сменить сотрудника, модернизировать процессы и технологии. Одним из решений для организаций является внедрение новых стратегий и технологий, таких как машинное обучение и автоматизация, для выполнения утомительных и трудоемких задач, которые обычно требуют высокой степени контроля и участия человека

Такие новые стратегии защиты могут повлиять на стратегии киберпреступников, заставляя их модернизировать методы атак и прилагать больше усилий для развития. Учитывая все более широкое использование машинного обучения и автоматизации, мы можем заявлять, что киберпреступное сообщество, скорее всего, будет придерживаться описанных ниже стратегий. И специалистам в сфере кибербезопасности также придется им следовать.

Цена эксплойтов "нулевого дня" всегда была довольно высокой, прежде всего из-за времени, усилий и навыков, необходимых для их обнаружения. Но по мере развития технологии ИИ такие эксплойты перестают быть крайне редким явлением и превращаются в предмет торговли…

Значительное развитие изощренных атак на базе технологии роевого интеллекта приближает нас к реальности больших групп ботов, которые называются "роевыми" сетями. Это новое поколение угроз будет использоваться для создания огромных роевых сетей, состоящих из интеллектуальных ботов, которые могут работать совместно и автономно. Такие роевые сети не только повысят требования к технологиям корпоративной защиты, но, как и в случае с обнаружением угроз "нулевого дня", окажут существенное влияние на базовую бизнес-модель киберпреступников.

В итоге развитие технологий обнаружения эксплойтов и методологий атак приведет к кардинальному изменению бизнес-моделей, используемых киберпреступным сообществом. В настоящее время экосистема киберпреступности ориентирована главным образом на людей. За определенную плату профессиональные хакеры разрабатывают специальные эксплойты и даже новые модели, например "программы-вымогатели как услуга"». ***(Fortinet представила прогноз по киберугрозам // Goodnews.ua (http://goodnews.ua/technologies/fortinet-predstavila-prognoz-po-kiberugrozam/). 09.12.2018).***

***

«Приближающиеся рождественские каникулы, по оценкам специалистов в сфере киберстрахования, связаны с увеличением количества кибератак на предприятия всех отраслей, но наибольший риск праздничный период представляет для компаний-ритейлеров, для которых риск взлома увеличивается на 35%.

Как выяснил УкрСтрахование из отчета Cyber in Focus, подготовленного специалистами североамериканского страховщика Chubb, за период с 2011 года количество страховых требований в сфере киберзащиты увеличилось на 116%.

Комментируя результаты отчета, исполнительный вице-президент Chubb Майкл Таненбаум подчеркнул особенность кибер-рисков в зависимости от отраслевой принадлежности и масштаба компании. «Располагая результатами наблюдений более чем за 20 лет, Chubb может помочь клиентам глубже понять риски, которые больше всего влияют на их конкретную организацию и отрасль», — сказал он.

Кроме сезонного риска для компаний розничной торговли, в отчете также говорится об увеличении в это время года количества фишинговых атак с помощью кредитных карт.» ***(В праздничные дни количество кибератак возрастает на 35%: отчет Chubb // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/v-prazdnichnyie-dni-kolichestvo-kiberatak-vozrastaet-na-35-otchet-chubb). 21.12.2018).***

***

«Польща вважає кібершпигунство порушенням міжнародного права

Польща стурбована заявою ЄС щодо випадків комерційного кібершпигунства, ймовірно пов'язаних з Китаєм…

"Польща стурбована випадками комерційного кібершпигунства, зокрема тих, які наші партнери пов'язують з Китаєм, що суперечить заснованому на правилах

міжнародному порядку та підриває стабільність кіберпростору", - йдеться у заяві…» ***(Польща стурбована повідомленнями про кібершпигунство Китаю // «РБК-Україна» (https://www.rbc.ua/ukr/news/polsha-obespokoena-soobshcheniyami-kibershpionazhe-1545408487.html). 21.12.2018).***

***

«Пользователь Twitter под псевдонимом @TheHackerGiraffe взломал 50 тыс. принтеров и заставил их печатать листовки с призывом подписаться на YouTube-канал известного видеоблогера PewDiePie.

29 ноября модели принтеров самого разного предназначения, начиная от многофункциональных устройств в крупных компаниях и заканчивая портативными принтерами для печати чеков на автозаправках, вдруг стали печатать рекламу YouTube-канала PewDiePie. Проблема затронула только подключенные к интернету устройства со старой прошивкой и активированным портом для печати.

Способ осуществления кибератаки… заключается в отправке атакуемому принтеру с помощью автоматизированных скриптов сообщения для печати. Для этого на устройстве должны быть включены порты IPP (Internet Printing Protocol), LPD (Line Printer Daemon) и 9100.

Как сообщил @TheHackerGiraffe на форуме Reddit, он взломал только 50 тыс. принтеров, хотя мог с легкостью взломать 800 тыс., в настоящее время доступных через интернет. В ходе атаки взломщик использовал инструмент Printer Exploitation Toolkit (PRET). Инструмент был выпущен в начале прошлого года вместе с подробным описанием шести уязвимостей в 20 моделях принтеров…» ***(Фанат популярного видеоблогера заставил 50 тыс. принтеров печатать рекламу своего кумира // Goodnews.ua (http://goodnews.ua/technologies/fanat-populyarnogo-videoblogera-zastavil-50-tys-printerov-pechatat-reklamu-svoego-kumira/). 04.12.2018).***

***

«Американская компания Agari, специализирующаяся на разработке решений кибербезопасности, обнаружила (.pdf) список 35 тыс. финансовых директоров и 15 тыс. сотрудников финансовых отделов различных компаний, составленный группой хакеров London Blue. Хакеры намеревались использовать этих людей, многие из которых работают в очень крупных компаниях и банках, для фишинговых атак.

Хакеры из London Blue базируются в Нигерии, осуществляя фишинговые атаки по всей Западной Европе и в США. Они покупают личные данные людей, у которых наверняка есть деньги, и засылают тем электронные письма с каких-либо знакомых этим людям адресов с просьбой немедленной отправки денежного перевода, убедительно формулируя причину такой необходимости и указывая не вызывающую подозрений сумму (средний размер запрашиваемого перевода составляет $35 тыс.). Несмотря на высокую информированность сотрудников компаний и банков о подобных мошенничествах, хакерам нередко удается ввести их в заблуждение, сообщает Agari. На каждые 100 писем приходится 3,97

результативного ответа. По данным ФБР, которые приводит Agari, такого рода мошенничества обошлись компаниям в $12 млрд с 2013 года.

В докладе Agari отмечается, что в обнаруженном ее специалистами списке потенциальных объектов фишинговых атак больше половины людей работают в США, остальные — в Великобритании, Испании, Финляндии, Нидерландах, Мексике и ряде других стран. Судя по списку, больше всего хакеров интересуют люди, работающие в сфере финансовых услуг, чуть меньше — в строительстве, на рынке недвижимости, в здравоохранении.» ***(Алена Миклашевская. Группа хакеров London Blue составила список 50 тысяч своих потенциальных жертв // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3820140?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). 04.12.2018).***

***

Діяльність хакерів та хакерські угруповування

«…Хакери протягом трьох років мали доступ до дипломатичних переписок Євросоюзу, що дозволило їм завантажити тисячі секретних повідомлень.

…злом виявила компанія Area 1, що працює в сфері кібербезпеки. Вона передала виданню понад 1 100 перехоплених повідомлень…

Як повідомляється, у викрадених матеріалах відображено занепокоєння Європи щодо «непередбачуваної адміністрації Трампа», в тому числі відчуття ЄС, що негативне ставлення американського лідера до блоку «створило значну невпевненість». Матеріали також виявляють труднощі, з якими стикається Євросоюз при взаємодії з Росією і Китаєм, а також його занепокоєння з приводу ризику відродження ядерної програми Ірану. У числі повідомлень виявилися доповідні записки про розмови з лідерами Саудівської Аравії, Ізраїлю та інших країн, що поширювались всередині ЄС.

Отримана хакерами інформація була конфіденційною, але мала низький статус секретності. …більш секретні документи зберігаються в іншій системі…» ***(ЗМІ: хакери три роки читали листування європейських дипломатів // "Українські медійні системи" (https://glavcom.ua/world/observe/zmi-hakeri-tri-roki-chitali-listuvannya-jevropeyskih-diplomativ--554695.html). 20.12.2018).***

***

«Підтримувані Іраном хакери атакували особисті електронні поштові скрині чиновників Казначейства США в той час, коли президент Сполучених Штатів Дональд Трамп запровадив санкції проти Тегерана…

Фірма з кібербезпеки Certfa виявила хакерську групу, відому як Charming Kitten, яка протягом останнього місяця намагалася отримати доступ до особистих поштових акаунтів чиновників з допомогою фішинг-кампанії.

За повідомленнями, хакерська група також переслідувала видних діячів, які підтримують, принуждающих або виступають проти Ядерної угоди з Іраном. Серед тих, кого переслідували, були іноземні експерти з ядерної зброї і співробітники аналітичних центрів Вашингтона.

АР повідомляє, що дослідники безпеки змогли ідентифікувати деяких людей, на яких була націлена кампанія, після того як хакерська група випадково залишила сервер доступним в Інтернеті.

У звіті, опублікованому в четвер, дослідники Certfa написали, що хакери, мабуть, зібрали інформацію про тих, хто зазнав нападу, до початку атак…» ***(Іранські хакери зламали особисту пошту чиновників Казначейства США – АР // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/iranski-hakeri-zlamali-osobistu-poshtu-chinovnikiv-kaznacheystva-ssha-ap-296920_.html). 13.12.2018).***

***

«Хакеры осваивают все новые сферы: в следующем году переключатся на смартвещи

В 2019 году хакеры смогут влиять как на мировую экономику, меняя курсы валют, так и на нашу личную жизнь, "залезая" в устройства, которые мы используем ежедневно: например, в "умные" часы и мелкую бытовую технику. Эксперты отмечают, что в 2018 году киберпреступники проявляли беспрецедентную активность: за первые 3 квартала 2018 года число кибератак выросло на треть по сравнению с прошлым годом, сообщили в компании Positive Technologies. Также в компании отметили рост промышленного шпионажа. В других компаниях, занимающихся кибербезопасностью, наблюдали схожие тренды…

"Умным" городам бояться сдедует больше всего: где автоматизировано практически все, там больше и поле деятельности для хакеров. Инструкцию по взлому чего-либо можно купить в даркнете, поэтому при большом желании любой хакер может проникнуть в электронные системы транспортной инфраструктуры и ЖКХ.

"По мере проникновения умных устройств в различные сферы нашей жизни - ЖКХ, транспорт - можно ожидать инциденты, направленные уже непосредственно на жителей и инфраструктуры умных городов с возможными экономическими и социальными последствиями", - говорят эксперты.

Среди трендов киберугроз также и обход биометрии. Главная проблема в том, что хакеры научились использовать обнаруженные уязвимости до того, как компании успевают отреагировать и выпустить обновления…» ***(Любовь Мельникова. "Умные города" начнут атаковать своих жителей в 2019 году // ESGROUP (https://ubr.ua/ukraine-and-world/technology/umnye-horoda-nachnut-atakovat-svoikh-zhitelej-v-2019-hodu-3878998). 21.12.2018).***

***

«Согласно служебной записке, которую на этой неделе получили все сотрудники НАСА, в октябре 2018 года Национальное управление по аэронавтике и исследованию космического пространства подверглось

хакерской атаке. Неизвестные злоумышленники смогли получить доступ к одному из серверов, где хранилась информация о бывших и действующих сотрудниках, включая даже их номера социального страхования.

Инцидент произошел еще 23 октября 2018 года, и не совсем ясно, почему сотрудникам сообщили о случившемся только спустя два месяца. Вероятно, огласку просили отложить представители правоохранительных органов, расследовавшие инцидент. Также сообщается, что к расследованию были привлечены специалисты по кибербезопасности федерального уровня.

Тем не менее, пока НАСА неизвестны ни точные цели злоумышленников, ни количество пострадавших сотрудников. Поэтому в служебной записке абсолютно всех, кто работал (увольнялся, переводился) в управлении в период с июля 2006 по октябрь 2018 года, простят соблюдать осторожность и принять контрмеры на случай возможного мошенничества. В настоящее время штата НАСА насчитывает порядка 17 300 человек.

Представители НАСА подчеркивают, что расследование случившегося займет немало времени, но уверяют, что инцидент не коснулся данных, связанных с миссиями и проектами НАСА.» ***(NASA подверглось кибератаке и допустило утечку данных сотрудников // Goodnews.ua (http://goodnews.ua/technologies/nasa-podverglos-kiberatake-i-dopustilo-utechku-dannyx-sotrudnikov/). 19.12.2018).***

***

«Хакеры, связанные с КНР, за последние полтора года значительно усилили попытки кибервзлома электронных систем компаний, работающих подрядчиками ВМС США… такие атаки подчеркнули уязвимость систем ВМС и работающих на них по контракту гражданских компаний, послужив импульсом к проведению Вашингтоном масштабных проверок в области кибербезопасности. Как отмечает издание, хакерам, в частности, предположительно, удалось похитить засекреченную информацию, имеющую отношение к новейшим военным технологиям США. В одном случае злоумышленники, по данным источников издания, смогли получить доступ к данным, связанным с секретными чертежами сверхзвуковых противокорабельных ракет, которые планировалось устанавливать на американских подлодках. Как пишет The Wall Street Journal, связанные с КНР хакеры атакуют все виды ВС США, однако наиболее активные попытки взлома предпринимаются в отношении именно ВМС, а также ВВС США. Атакам подвергаются, в основном, их компании-подрядчики, как крупные, так и небольшие, которым зачастую не хватает ресурсов для того, чтобы должным образом защитить свои компьютерные сети от взлома, отмечает издание. Также злоумышленники выбирают в качестве целей лаборатории при университетах и других научных заведениях, где проводятся военные исследования и разрабатываются новейшие технологии для использования ВМС и другими видами ВС США… министр ВМС США Ричард Спенсер отдал приказ провести проверку сетей подотчетного ему вида вооруженных сил на наличие уязвимостей перед кибератаками…» ***(Китайские хакеры усилили кибератаки в отношении компаний-подрядчиков ВМС США // информационный портал "ua.today"***

(http://ua.today/news/world/kitajskie_hakery_usilili_kiberataki_v_otnoshenii_kompanij_podryadchikov_vms_ssha). 16.12.2018).

***

«В декабре 2018 года антивирусная компания "Лаборатория Касперского" сообщила о кибератаках на европейские банки. Новая хакерская кампания получила название DarkVishnya.

В рамках кибератак, которые произошли в 2017-2018 годах, злоумышленники использовали гаджеты с установленным вредоносным ПО. Устройства внедряли в здания банков или физически подключали к корпоративным сетям. Это могли быть ноутбуки или небольшие одноплатные компьютеры, а также спецустройства для проведения USB-атак.

В ходе атак киберпреступники пытались получить доступ к общим сетевым папкам, веб-серверам и т. п. Украденные данные они использовали для подключения к серверам и рабочим станциям, предназначенным для осуществления платежей или содержащим другую полезную для злоумышленников информацию. После успешного закрепления в инфраструктуре финансового учреждения хакеры использовали легитимное ПО для удаленного управления.» ***(Хакеры атакуют банки через прямое подключение к корпоративным сетям // Goodnews.ua (http://goodnews.ua/technologies/xakery-atakuyut-banki-cherez-pryamoe-podklyuchenie-k-korporativnym-setyam/). 11.12.2018).***

***

«Появился первый пострадавший от фишинговой рассылки партнерам Юнистрим-банка с взломанного хакерами почтового сервера кредитной организации… им стал банк «ВТБ Грузия». По предварительным результатам расследования, там вскрыли фишинговое письмо от экс-партнера, в результате чего 14 декабря хакеры вывели средства. Круг потенциальных жертв может быть шире, отмечают эксперты, однако выявить их непросто, особенно при трансграничных атаках.

…Сейчас идет расследование инцидента, которое показало, что хакеры проникли в сеть банка через фишинговое письмо, полученное от бывшего партнера «ВТБ Грузия» Юнистрим-банка…

По словам экспертов по кибербезопасности, обычно расследование инцидента длится несколько месяцев. И если по итогам факт проникновения в банк через письмо Юнистрим-банка будет доказан, то это может иметь серьезные последствия для всего рынка денежных переводов в целом…» ***(Вероника Горячева, Ксения Дементьева. Дорогое письмо бывшему партнеру // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3836720?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 21.12.2018).***

***

«Основатель хакерской группы «Шалтай-Болтай» Владимир Аникеев намерен создать компанию, которая буде заниматься вопросами информационной безопасности… Аникеев не исключил, что возможно, что будет использоваться бренд «Шалтай-Болтай» и «Анонимного интернационала».

Владимир Аникеев рассказал, что будет совладельцем компании, но имена партнеров и объем инвестиций не назвал. По его словам, компания будет создавать многоуровневую защиту от взломов. При этом выпускать свое программное обеспечение не планируется из-за слишком высокой стоимости. В работе компании он намерен «использовать знания некоторых реалий темной стороны, того, как эти люди (хакеры) работают».

Также господин Аникеев сообщил, что планирует запустить несколько анонимных Telegram-каналов. «Я нахожусь в России, в Питере, в Москве. Даже если не верить в мои моральные качества, что я сейчас на стороне добра, то можно поверить в здравый смысл. Нарушать закон, находясь здесь, не совсем правильно»,— заверил он…» ***(Лидер «Шалтая-Болтая» займется обеспечением кибербезопасности // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3829522?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 14.12.2018).***

***

«Хакеры атаковали российские предприятия с помощью поддельных почтовых ящиков госкомпаний. Злоумышленники рассылали письма с вложенными копиями документов или служебными записками. Под эти файлы был замаскирован троян, который создавал платежные поручения. О схемах рассказала компания Group-IB, которая специализируется на кибербезопасности. Всего хакеры успели послать 11 тыс. вредоносных писем. Жертвами стали транспортные и промышленные организации, а также банки. По оценкам экспертов, в среднем из-за каждой атаки юрлицо теряло около 1,1 млн руб.

Такая сумма ущерба говорит о массовости атаки, пояснил руководитель российской практики услуг по информационной безопасности PwC Роман Чаплыгин…». ***(Евгений Плотников. Хакеры взяли госкомпании массовостью атак // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3821789?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). 06.12.2018).***

***

«Невідомі хакери викрали особисті дані близько тисячі громадян КНДР, які втекли до Південної Кореї, повідомили в південнокорейському міністерстві об'єднання. Походження атаки встановлюється.

Міністерство виявило витік і повідомило, що зловмисники отримали доступ до бази даних агентства з питань переселення. Хакери викрали інформацію про імена, дати народження й адреси проживання перебіжчиків.

Агентство, на яке здійснили атаку, входить у мережу з 25 таких же інститутів, які допомагають вихідцям із КНДР з пошуком роботи, медичним забезпеченням і юридичною підтримкою. Співробітники агентств побоюються, що витік може поставити під загрозу родичів перебіжчиків, які залишаються в Північній Кореї…» ***(У Південній Кореї викрали особисті дані перебіжчиків із КНДР // Радіо Свобода (https://www.radiosvoboda.org/a/news-pivdenna-korea-perebizhchyky-hakerska-ataka/29681367.html). 28.12.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«Специалисты по кибербезопасности обнаружили вирус, воздействующий на устройства на базе Android…

Пользователи скачали зараженные приложения из магазина Google Play. Вредоносный код получил название Andr/Clickr-AD. Он генерирует постоянный переход по рекламным ссылкам вне зависимости от желания владельца смартфона и таким образом быстро разряжает устройство.

Издание отмечает, что если пользователь принудительно закрывает программу, то она затем открывается сама через 3 минуты.

Всего вирусом было заражено 20 приложений, общее число скачиваний и установок превышает 20 миллионов. Сейчас они все удалены из Google Play.

Постадавшим пользователям рекомендуется запустить антивирусную программу и сбросить свои гаджеты до заводских настроек, однако при этом информация, хранившаяся на устройстве, будет потеряна.» ***(Анастасия Марьина . Обнаружен вирус, разряжающий смартфоны на Android // Rusbase (https://rb.ru/story/virus-android/). 18.12.2018).***

***

«Користувачам смартфонів та інших гаджетів на операційній системі Android слід остерігатися нової шкідливої програми. На цей раз він маскується під додаток, яке здатне оптимізувати заряд смартфона, збільшуючи його автономність. Звичайно ж, цього не робить. До речі, він потрапляє в смартфони за допомогою фейкових магазинів і інших додатків.

Виявив цей Android-троян експерт в області кібербезпеки антивірусної компанії ESET Лукас Стефанко.

Так, після установки програма сканує пристрій на предмет наявності додатку PayPal, потім запитує доступ до спеціальних можливостей, і в підсумку ховає свою піктограму на робочому столі. Після цього користувач отримує повідомлення з рекомендацією увійти в обліковий запис PayPal для перевірки даних з метою безпеки.

І вже після входу в додаток, вірус перераховує 1 тисячу доларів з рахунку, тим самим залишаючи власника без грошей. У випадку, якщо у вас немає платіжної системи в смартфоні, він вивчає паролі та інші дані до ваших облікових записів…» ***(Новий вірус заражає Anroid-девайси, Google не діє // znaj.ua***

(https://znaj.ua/techno/194496-noviy-virus-zarazhaye-anroid-devaysi-google-ne-diye). 13.12.2018).

***

«Фахівцями з кібербезпеки було заявлено про виявлення нового шкідливого майнера Монеро, який вміє розвиватися. Сама по собі система здатна заробляти на працю користувачів мережі, причому робить це непомітно для всіх. Знахідка виявилася більше 6 місяців тому. У той час вона приховано добувала тематичну криптовалюту.

На даний момент, програма вже оновлює саму себе, а також усуває "конкурентів" на ПК жертви. Непомітно для самого власника пристрою, система здатна використати продуктивність комп'ютера для видобутку криптовалют. Подібні характеристики шкідливої програми виключають її виявлення антивірусами, так що недосвідчений користувач не здатний виявити і видалити вірус на своєму пристрої.

Фахівці з'ясували, що майнер призначається для серверів, використовуючи практично всю їх потужність. Також, є відомості, що працює ЗА для особистого пулу майнер, що підвищує анонімність…» ***("Чорні майнери" знову заражають комп'ютери: як уникнути пастки // znaj.ua (https://znaj.ua/techno/191931-chorni-mayneri-znovu-zarazhayut-komp-yuteri-yak-uniknuti-pastki). 03.12.2018).***

***

«Специалисты антивирусной компании McAfee представили новое исследование, отдельные моменты которого по-настоящему удивляют. Согласно их отчету, компания фиксирует 480 новых IoT-вредоносов каждую минуту. Эксперты считают, что к такой ситуации привели годы, на протяжении которых разработчики уделяли гораздо больше внимания внедрению новых возможностей в ущерб безопасности. Таким образом, на рынке появилось огромное количество уязвимых устройств. Первым звоночком, что что-то не так была атака ботнета Mirai в 2016 году… В настоящее время атаки на IoT-устройства являются самым обыденным способом проникнуть в целевую сеть. Специалисты McAfee заявили, что в третьем квартале 2018 года 480 новых вредоносов для IoT-устройств появлялись каждую минуту. Более того, количество новых семплов увеличилось на 53%. «Киберпреступники стараются извлечь максимальную выгоду из уязвимостей, как новых, так и старых. Эффективность злоумышленников значительно повысилась благодаря тому, что на подпольных форумах стало гораздо больше сервисов для организации атак», — заявил эксперт Кристиан Бик.» ***(Олег Иванов. Эксперты фиксируют 480 новых IoT-вредоносов каждую минуту // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-12-21-1447/28410). 21.12.2018).***

***

«Специалисты в области кибербезопасности из компании TrendMicro обнаружили вредоносный код в опубликованных в соцсети Twitter мемах. О

новом методе работы хакеров сообщается в отчете, опубликованном на сайте компании.

Вредная программа под названием TROJAN.MSIL.BERBOMTHUM.AA получала команды из кода, содержащегося в опубликованных в Twitter картинках. Изображения использовались в качестве средства связи с оператором вредоносной программы. После заражения компьютера вирус мог делать снимки экрана жертвы или воровать личные данные.

Злоумышленники создали аккаунт в Twitter заблаговременно: посты появились в нем еще в октябре. На данный момент учетная запись деактивирована. Как происходит заражение устройств жертв и кто контролирует атаки, неизвестно.

Вероятно, преступники использовали такой уникальный способ контролировать атаки из-за того, что антивирусное программное обеспечение в большинстве случаев не помечает обращение к сайту Twitter опасным.» ***(Хакеры начали прятать вирусы в мемах // Goodnews.ua (http://goodnews.ua/technologies/xakery-nachali-pryatat-virusy-v-memax/). 19.12.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Министерство юстиции США объявило о захвате 15 доменов, ассоциируемых с предоставлением услуг по проведению DDoS-атак. Одновременно на Аляске и в Калифорнии были предъявлены обвинения трем предполагаемым операторам таких сервисов. Им инкриминируют пособничество в совершении преступлений, предусмотренных Законом о мошенничестве и злоупотреблениях с использованием компьютерных технологий (Computer Fraud and Abuse Act).

В пресс-релизе Минюста отмечено, что за последние пять лет число специализированных DDoS-сервисов, зачастую именуемых booter или stresser (от boot и stress — создавать нагрузку), заметно возросло. За умеренную плату они предлагают подписчикам готовые инструменты для проведения атак и с этой же целью сдают в аренду ботнеты, облегчая задачу начинающим преступникам.

Разгромная акция, подготовленная сотрудниками ФБР совместно с зарубежными коллегами, состоялась 19 декабря — за неделю до Рождества, которое дидосеры неизменно отмечают серией атак против игровых сообществ. Заручившись ордером, ФБР захватило домены 15 booter- и stresser-сервисов, в том числе critical-boot.com, ragebooter.com, downthem.org и quantumstress.net.

В тот же день в Лос-Анджелесе были оглашены обвинения, выдвинутые против Мэтью Гэтрела (Matthew Gatrel) и Хуана Мартинеса (Juan Martinez) — операторов Downthem и Ampnode. Первый сайт специализировался на DDoS-услугах, второй предоставлял клиентам ресурсы для создания таких сервисов. Согласно материалам дела, с октября 2014 года по ноябрь 2018-го услугами

Downthem воспользовались более 2 тыс. подписчиков, которые провели или попытались провести свыше 200 тыс. атак.

Судебный процесс на Аляске начался неделей раньше. Ответчиком по делу о пособничестве дидосерам здесь выступает 23-летний Дэвид Букоски (David Bukoski) из Пенсильвании. Собранные свидетельства указывают на то, что он являлся оператором Quantum Stresser, запущенного в 2012 году. По состоянию на конец ноября этот сервис насчитывал свыше 80 тыс. подписчиков; за последний год он использовался для проведения более 50 тыс. DDoS-атак, в том числе на Аляске и в Калифорнии.

В расследовании, завершившемся захватом доменов и арестами, принимали участие сотрудники ФБР и британского Управления по борьбе с преступностью, киберполицейские Нидерландов, эксперты Akamai, Bell Aliant, Cloudflare, Flashpoint, Google, Oath Inc., Oracle, Palo Alto Networks, SpyCloud, ShadowDragon, PayPal, представители Riot Games и американской Ассоциации производителей ПО и компьютерных игр, а также исследователи из Кембриджского университета…» ***(Maxim Zaitsev. Теневой DDoS-бизнес несет потери // Threatpost (https://threatpost.ru/law-enforcement-shuts-down-fifteen-ddos-for-hire-services/30208/). 21.12.2018).***

***

«В США обвиняют двух китайцев в 45 кибератаках на крупные компании и госучреждения страны…

В прокуратуре заявляют, что хакеры Чжу Хуа и Джан Шилуном были членами группировки, известного как Advanced Persistent Threat 10 Red Panda, Stone Panda и CVNX. Обвиняемые работали в компании Huayhing Haitei Science and Technology Development Co в городе Тяньцзинь…

Хакеры осуществляли кибератаки с участием сотрудников китайских служб госбезопасности в течении последних десяти лет.

Китайцев обвиняют в краже данных крупных компаний, работающих в различных сферах промышленности, а также интеллектуальной собственности и конфиденциальных деловых данных. Как отмечается, киберпреступники также взломали базы данных ВМС США и украли личную информацию более 100 тыс. военнослужащих.

Кроме того, хакеров обвиняют во взломе компьютеров, связанных с Лабораторией реактивного движения NASA…» ***(США обвинили китайских хакеров в кибератаках // NewsOboz - последние новости в Украине и мире (http://newsoboz.org/it_tehnologii/ssha-obvinili-kitayskih-hakerov-v-kiberatakah-20122018211849). 21.12.2018).***

***

«…Министерство юстиции США предъявило обвинения двум гражданам Ирана, которых обвиняют в масштабных кибератаках. Фарамарз Шахи Саванди и Мохаммад Мехди Шах Мансури ответственны за создание вируса-вымогателя SamSam.

Сообщается, что иранцы смогли получить $6 млн от 200 своих жертв, среди которых числятся не только рядовые пользователи, но и целые американские города — Атланта и Ньюарк.

Из-за этого инцидента Министерству финансов пришлось впервые наложить санкции на биткоин-кошельки, так как все средства, полученные хакерами в качестве выкупа, хранились именно на них.

SamSam начал заражать компьютеры в 2015 году, специализируясь на атаках на больницы и объекты инфраструктуры. Как и другие вирусы-вымогатели, SamSam блокировал компьютер пользователя и требовал за дешифровку денежный выкуп в биткоинах, причем сумма иногда доходила до десятков тысяч долларов. Как утверждает следствие, через кошельки обвиняемых прошло свыше 7 тыс. транзакций.

Как заявил прокурор США Крейг Карпенито, главной целью Саванди и Мансури были не деньги.

«Они пытались навредить нашим учреждениям и критической инфраструктуре. Они пытались посягнуть на наш образ жизни», — заявил Карпенито…

К сожалению, как часто бывает в подобных случаях, правосудие над преступниками может и не свершиться — они пока не задержаны…

Как пояснил специалист технического сопровождения сервисов ESET Russia Андрей Ермилов, SamSam — это не столько вирус, сколько таргетированные атаки на организации с уязвимостью в сети. Злоумышленники выискивали такие сети, проникали в них по RDP [протокол удаленного рабочего стола]. После этого начинался второй акт, где они получали права доменного администратора. Для этого использовалась целая комбинация инструментов, в том числе и довольно известный Mimikatz. Получив права администратора, злоумышленники завершали атаку, разворачивая шифраторы на все ПК в сети…

Специалисты Check Point описали вирус-вымогатель SamSam еще в 2016 году. Он может быть доставлен на компьютер различными способами — один из них использует уязвимость Windows, которая не требует от пользователя открыть зараженный файл или перейти по ссылке. Злоумышленники могут запустить программу-вымогатель удаленно после обнаружения незакрытой уязвимости на сервере и проникновения в сеть. После проникновения, используя те же уязвимости, вирус-вымогатель распространяется по локальной сети и заражает другие устройства.» ***(Хаос на улицах: как хакеры остановили работу городов // Goodnews.ua (http://goodnews.ua/technologies/xaos-na-ulicax-kak-xakery-ostanovili-rabotu-gorodov/). 01.12.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Военнослужащие США используют два уязвимых Android-приложения, потенциально открывающие противникам доступ к конфиденциальным данным.

Речь идет о приложениях KILSWITCH (Kinetic Integrated Low-Cost Software Integrated Tactical Combat Handheld) и APASS (Android Precision Assault Strike Suite). Обе программы отображают спутниковые снимки окружающей местности, в том числе объекты, цели миссии, а также находящихся поблизости противников и союзников. Они являются своего рода современной альтернативой картам и рациям. С помощью приложений военные могут координировать свои действия через специальный мессенджер и даже вызывать подкрепление с воздуха всего в несколько тапов по экрану.

Согласно опубликованному 20 декабря отчету генерального инспектора ВМС США, в KILSWITCH и APASS содержатся опасные уязвимости, открывающие противнику доступ к данным. Подробности об уязвимостях не приводятся, однако, как сообщается в отчете, чиновники ВМС не проконтролировали распространение обоих приложений и своевременно не предупредили военных об опасности, грозившей им почти год.

В отчете также сказано, что KILSWITCH и APASS предназначены исключительно для использования в учебных целях и не одобрены для использования во время боевых действий. «Кибербезопасность не была в приоритете у разработчиков приложений», так как программы изначально создавались для использования только во время учений, отмечается в отчете.

Благодаря удобному интерфейсу и полезным функциям приложения стали чрезвычайно популярными, и не только у американских, но и у иностранных военных. Однако руководство ВМС не позаботилось о том, чтобы донести до солдат истинное предназначение программ. Во время боевых действий военным следует отказаться от KILSWITCH и APASS, а вместо них использовать приложение ATAK» ***(Android Tactical Assault Kit), одобренное Минобороны США для применения в военных действиях. (Военные США используют уязвимые Android-приложения // Goodnews.ua (http://goodnews.ua/technologies/voennye-ssha-ispolzuyut-uyazvimye-android-prilozheniya/). 21.12.2018).***

***

«Компания Google решила привлечь ученых и экспертов в области кибербезопасности для сокращения числа уязвимостей операционной системы Android, организовав исследовательскую программу ASPIRE… Цель ASPIRE состоит в создании новых технологий обеспечения конфиденциальности, которые

окажут непосредственное влияние на развитие экосистемы Google в перспективе ближайших пяти лет…

Благодаря ASPIRE в Маунтин-Вью рассчитывают нивелировать негативные последствия, которые несет в себе открытость Android. Чтобы проект оказался эффективным, Google планирует создать несколько независимых экспертных советов, обеспечив таким образом максимальный охват всех недоработок и уязвимостей операционной системы. При этом поучаствовать в совершенствовании Android вне рамок ASPIRE смогут не только ученые, но и рядовые добровольцы. Достаточно отправить Google соответствующую заявку.

Планы по совершенствованию Android, которые Google строит на ближайшую пятилетку, могут свидетельствовать о том, что компания не намеревается отказываться от эксплуатации «зеленого робота». Поэтому все слухи о скорой замене Android на Fuchsia, скорее всего, так и останутся слухами без претензии на какую-либо объективность…» ***(Google привлечет ученых для повышения безопасности Android // Goodnews.ua (http://goodnews.ua/technologies/google-privlechet-uchenyx-dlya-povysheniya-bezopasnosti-android/). 12.12.2018).***

***

«Уязвимости в домашних зарядных станциях для электромобилей позволяют злоумышленникам осуществлять кибератаки с целью причинения физического ущерба. Как сообщается в недавнем отчете специалистов «Лаборатории Касперского», опытный киберпреступник может взломать зарядную станцию и отключить питание электромобиля или даже вызвать возгорание.

Электромобили стремительно набирают популярность, однако инфраструктура бесплатных зарядных станций по-прежнему малоразвита. В связи с этим пользователи все чаще покупают домашние зарядные устройства, которые можно установить непосредственно в гараже. Однако, по словам специалистов, эти устройства уязвимы к кибератакам.

Для начала исследователи «Лаборатории Касперского» проанализировали на наличие уязвимостей приложение ChargePoint Home, позволяющее удаленно управлять процессом зарядки. Как оказалось, злоумышленник может зарегистрировать в приложении нового пльзователя, подключить устройство к смартфону через Bluetooth, настроить параметры сети Wi-Fi для беспроводного подключения и завершить процесс регистрации, отправив ID нового пользователя и GPS-координаты смартфона конечному устройству. Это позволит атакующему в любое время вмешиваться в процесс зарядки и не давать электромобилю заряжаться, в результате чего его владелец может понести серьезные убытки, в том числе материальные.

Добавить в приложение нового пользователя без ведома настоящего владельца не составляет особого труда. После регистрации в приложении обойти механизм аутентификации очень просто. Злоумышленник может внедрить код JTAG в процедуру верификации пароля и успешно пройти аутентификацию с недействительным паролем.

Помимо прочего, зарядные станции оснащены встроенным сервером с включенным интерфейсом CGI, поверженным целому ряду уязвимостей. Две из них затрагивают код, ответственный за загрузку на устройство файлов из разных папок в зависимости от параметров строки запроса. Несколько уязвимостей переполнения буфера в стеке были обнаружены в коде, используемом для отправки зарядной станции различных команд, а еще одна – в коде, для выгрузки с устройства системных реестров.

«Все это дает атакующему возможность управлять процессом зарядки путем подключения к сети Wi-Fi», – пояснили исследователи. Теоретически, злоумышленник может увеличить силу тока и временно отключить часть домашней электросети и даже вызвать возгорание от перегрева.

Исследователи сообщили об уязвимостях разработчикам ChargePoint Home, и в настоящее время они уже исправлены.» ***(Зарядные станции для электромобилей уязвимы к кибератакам // Goodnews.ua (http://goodnews.ua/technologies/zaryadnye-stancii-dlya-elektromobilej-uyazvimy-k-kiberatakam/). 19.12.2018).***

***

«Тысячи, а то и больше, серверов Jenkins уязвимы к атакам с целью захвата контроля, похищения данных и майнинга криптовалюты. Атаки возможны благодаря двум уязвимостям, позволяющим повысить привилегии до администратора или авторизоваться на сервере с недействительными учетными данными.

Проблемы обнаружили специалисты компании CyberArk и частным образом сообщили о них команде Jenkins. Хотя патчи были выпущены еще прошлым летом, тысячи уязвимых серверов Jenkins по-прежнему доступны через интернет.

Уязвимость CVE-2018-1999001 позволяет с помощью вредоносных ученых данных заставить сервер перенести свой файл config.xml из домашней директории в другое место. Если атакующему удастся вызвать аварийное завершение работы или перезагрузку сервера, сервер загрузится с настройками конфигурации по умолчанию, то есть с отключенными функциями безопасности. В таком случае любой жалеющий сможет авторизоваться на сервере и получить права администратора, открывающие доступ к корпоративному исходному коду и даже позволяющие вносить в него изменения и встраивать бэкдоры в приложения.

Вторая уязвимость CVE-2018-1999043 позволяет злоумышленнику создавать в памяти сервера временные записи пользователя, дающие ему возможность в определенный отрезок времени авторизоваться на сервере с недействительными учтенными данными.» ***(Тысячи серверов Jenkins уязвимы к кибератакам // Goodnews.ua (http://goodnews.ua/technologies/tysyachi-serverov-jenkins-uyazvimy-k-kiberatakam/). 18.12.2018).***

***

«Исследователи из Cisco Talos Group предупреждают пользователей, что популярные зашифрованные приложения обмена сообщениями Telegram, WhatsApp и Signal поддерживают конфиденциальность связи, так как

частично делегируют безопасность операционным системам, на которых они работают. Хотя протоколы MT и Signal, используемые тремя приложениями для обмена сообщениями, способны обеспечивать безопасность данных при передаче, они не отвечают требованиям защиты состояния приложения и пользовательской информации, говорится в отчете Cisco Talos Group. И это связано с тем, что мессенджеры делегируют безопасность операционной системе на которой работают.

Указывая на уязвимости в структуре пользовательского интерфейса для приложений, такие как удаленная ошибка в Electron, о которой было сообщено в январе 2018 года и которая затронула Signal, Slack и Skype, исследователи Talos говорят, что приложения могут быть скомпрометированы атаками по сторонним каналам. Частично проблема заключается в том, что пользователи, не являющиеся техническими специалистами, верят, что приложения имеют одинаковый уровень безопасности на всех платформах, когда некоторые из них более рискованны, чем другие.

Пользователям не сообщают об этом, и при этом они не получают достаточную информацию, чтобы принять обоснованные решения относительно риска, допускающего определенные настройки на их устройствах. Ранее в этом году исследователи Cisco Talos Group проанализировали вредоносную программу Telegrab, которая захватывает сессии пользователей Telegram. Имея доступ к сеансам, злоумышленники могут создавать теневые сеансы, которые копируют сообщения и изображения, отправленные или полученные жертвами. Исследователи указали, что на Telegram теневые сеансы могут быть установлены без предупреждений пользователя об установленных теневых сеансах.

В тоже время мессенджеры Signal и WhatsApp отображают подобные уведомления при создании теневых сессий, но злоумышленники могут обойти предупреждения и получить доступ к контактам и сообщениям…» ***(Милош Восковец . Telegram, WhatsApp и Signal открыты для кибератак // Bad Android (https://bad-android.com/news/42625-telegram-whatsapp-i-signal-otkryty-dlya-kiberatak). 11.12.2018).***

***

«В інтернет-браузері Google Chrome знайшли вразливість, за якою можна перезавантажувати процесори комп'ютерів, повністю виводячи їх з ладу. Тепер користувачі ПК під загрозою, як і їх дані, які з легкістю можна вивантажити незаконно і непомітно.

Дану загрозу виявив експерт з кібербезпеки з компанії Microsoft Жером Сегура. За його словами, помилка працює в кілька етапів і використовується хакерами досить хитро. Користувач отримує нібито системне повідомлення про шкідливий програмному забезпеченні. Вийти з браузера після такого повідомлення можливо тільки через «Диспетчер задач" Windows, який і робить всю брудну роботу за хакерів.

При відкритті диспетчера завдань Chrome починає навантажувати процесор ПК фіктивною роботою по обробці фонових процесів, витрачаючи в результаті всі ресурси системи і виводячи її з ладу. При цьому навіть диспетчер перестає

працювати, і закрити шкідливий сайт не вийде. Хакери користуються моментом, і крадуть особисті дані з ПК користувача, який нічого не підозрює в цей момент.

Google вже повідомили, що працюють над усуненням помилок і подякували колезі з Microsoft за оперативне виявлення уразливості. Варто відзначити, що в інших сервісах подібних помилок немає...» ***(У Google Chrome знайшли лазівку для хакерів, дані під загрозою // znaj.ua (https://znaj.ua/techno/198156-u-google-chrome-znayshli-lazivku-dlya-hakeriv-dani-pid-zagrozoyu). 27.12.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…Компания Microsoft запустила программу по разработке алгоритма, который сможет предсказывать, какие типы компьютеров на базе Windows вероятнее всего могут быть заражены вредоносным ПО. Проект запущен совместными усилиями исследовательской команды Microsoft, Северо-Восточного университета и Технологического института штата Джоджия, а его призовой фонд составляет $25 тыс.

Как пояснили сотрудники Microsoft Чэйз Томас (Chase Thomas) и Роберт МакКанн (Robert McCann), исследователям потребуется создать более сложную модель, нежели простой алгоритм, оценивающий шансы заражения машин на базе Windows XP и Windows 10.

«Цель - предсказать вероятность заражения Windows-компьютера различными семействами вредоносного ПО на основании различных характеристик устройства. Не все компьютеры обладают одинаковым риском инфицирования, специалистам потребуется разработать модели для определения устройств с самой высокой вероятностью заражения, чтобы можно было принять упреждающие меры», - отметили Томас и МакКанн.

Для работы Microsoft предоставит исследователям 9,4 ГБ анонимизированных данных, собранных с 16,8 млн устройств с установленным антивирусом Windows Defender. Информация включает данные о местоположении компьютера, установленных и активных антивирусных решениях, модели центрального процессора, установленном по умолчанию браузере, номере сборки операционной системы, активированном режиме S Mode и пр.

Организованный Microsoft конкурс уже привлек внимание 80 команд исследователей. На разработку алгоритма специалистам предоставляется три месяца» ***(Microsoft задумалась о создании ИИ, способного прогнозировать риск заражения ПК // SecurityLab.ru (https://www.securitylab.ru/news/497020.php). 17.12.2018).***

***

«Сети SCADA в любом заводском или критически важном инфраструктурном приложении требуют защиты от все более изощренных и

хорошо финансируемых киберугроз… Эффективная киберзащита требует сквозного подхода к безопасности устройств, от базового оборудования до приложений верхнего уровня и обратно в цепочку поставок…» ***(Как обезопасить промышленные интернет-системы от взлома // Goodnews.ua (http://goodnews.ua/technologies/kak-obezopasit-promyshlennye-internet-sistemy-ot-vzloma/). 17.12.2018).***

***

«USBGuard будет предотвращать чтение или исполнение кода при подключенном USB-устройстве, если экран в это время заблокирован.

Операционная система Chrome OS обзаведется новой функцией безопасности под названием USBGuard, которая ограничит доступ к USB-порту при заблокированном экране. В настоящее время функционал доступен в сборках Chrome OS Canary и в ближайшее время появится в стабильной ветке ОС.

Новая опция позволит Google защитить пользователей от стороннего проникновения в файловую систему их персональных компьютеров. Предполагается, что USBGuard будет предотвращать чтение или исполнение кода при подключенном USB-устройстве, если экран в это время заблокирован.

Таким образом Google намерена обеспечить защиту от атак типа «Rubber Ducky» («Резиновая уточка»), предполагающих использование вредоносных «флешек» для имитации нажатий клавиш и выполнения вредоносных команд. За последние несколько лет появилось немало возможностей, например, BadUSB , PoisonTap, USBdriveby или USBHarpoon , с помощью которых любой может создать собственный инструмент для атаки и извлечь данные с компьютера жертвы или заразить его вредоносным ПО. Впрочем, большинство подобных атак можно предотвратить, отключив USB-порт…» ***(Chrome OS будет блокировать доступ к компьютеру через USB // (https://www.securitylab.ru/news/497180.php). 24.12.2018).***

***

«…Компания Microsoft готовит обновление Windows 10, которое получит ряд нововведений, в том числе касающихся безопасности операционной системы. В предварительных версиях обновления 19H1 разработчик усовершенствовал приложение «Безопасность Windows», добавив возможность устанавливать настройки Tamper Protection и Protection History.

…страница Protection History, которая помимо стандартных результатов Защитника Windows, будет отображать более подробную и понятную информацию об обнаруженных угрозах и действиях, которые пользователь сможет предпринять при выявлении вредоносного ПО.

…новая настройка Tamper Protection (доступ к ней можно получить в разделе Windows Security -> Virus & Threat Protection -> Virus & Threat Protection Settings). При активации данной функции будет задействована дополнительная защита от модификации ключевых настроек безопасности.

В настоящее время новые функции тестируются в рамках программы Windows Insider, а рядовые пользователи смогут опробовать нововведения весной 2019 года.» ***(Microsoft работает над новыми функциями безопасности в***

Windows 10 // SecurityLab.ru (https://www.securitylab.ru/news/497294.php). 29.12.2018).

***

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

Золотар О. О. Правові основи інформаційної безпеки людини : автореф. дис. ... д-ра юрид. наук : 12.00.07 / Золотар Ольга Олексіївна ; Нац. юрид. ун-т ім. Ярослава Мудрого. - Харків, 2018. - 36 с.

З'ясовано правову природу, сутнісні ознаки та особливості інформаційної безпеки людини. Проаналізовано етапи становлення українського законодавства в інформаційній сфері в цілому, та щодо інформаційної безпеки людини, зокрема. Запропоновано методологію правових досліджень інформаційної безпеки людини. Узагальнено сучасні наукові концепції щодо розуміння інформаційної безпеки людини та визначено її правову природу. Виявлено теоретико-правові та нормативно-правові підвалини формування інформаційно-правового статусу людини.

Шифр зберігання НБУВ: РА436691

***

Матеріали XVI Всеукраїнської наукової конференції «Теорія та практика сучасної юриспруденції», [25 травня 2018 року]. - Харків, 2018. - Т. 2. - 339 с.

Зі змісту:

- Голуб О.Р. Кібернатична атака як загроза національній безпеці України.

Шифр зберігання НБУВ: В357340/2.

***

Побудова інформаційного суспільства: ресурси і технології : матеріали XVII Міжнар. наук.-практ. конф., 27 верес. 2018 р. - Київ , 2018. - 170 с.

Зі змісту:

- Шахбазян К.С. Вимоги до обробки персональних даних в ЄС при їх використанні в цифровому просторі;
- Петренко А.І., Кириленко А.І. Інформаційна безпека: імплементація законів Євросоюзу в законодавство України.

Шифр зберігання НБУВ: ВА826073.

***

Права, свободи і безпека людини в інформаційній сфері : матеріали наук.-практ. конф., 10 трав. 2018 р. - Київ : КПІ ім. Ігоря Сікорського, 2018. - 174 с.

Зі змісту:

- Довгань О.Д. Права і безпека людини: правові норми;
- Мисливий В.А. Кримінально-правова охорона інформаційної безпеки як гарантія конституційних прав і свобод людини;
- Ожеван М.А. PER ASPERA – AD ASTRA: безпекові виклики становлення української системи e-HEALTH;
- Полевий В.І. Фейкові новини чи рейковий медіапростір: постановка проблеми;
- Сірик А.О. Досвід країн ЄС та НАТО щодо удосконалення нормативно-правової бази забезпечення інформаційної безпеки в умовах інформаційної експансії РФ;
- Камоцкий А.Б. Компьютерная преступность: правовые, психологические и технико-криминалистические аспекты.

Шифр зберігання НБУВ: ВА826103.

***

Прикладні науково-технічні дослідження = Applied scientific and technical research : матеріали II міжнар. наук.-практ. конф., (3-5 квіт. 2018 р.). - Івано-Франківськ : Симфонія форте, 2018. - 191 с.

Зі змісту:

- Толюпа С.В., Браіловський М.М., Толюпа Є.О. Забезпечення безпеки інформаційних систем від кібератак.

Шифр зберігання НБУВ: ВА825347.

***

Самойленко О. А. Інформаційний продукт як предмет посягання під час вчинення злочинів із використанням обстановки кіберпростору / О. А. Самойленко // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки. - 2018. - Т. 29(68), № 4. - С. 165-169.

Визначено зміст інформаційного продукту та його природу як предмет посягання під час вчинення злочинів із використанням обстановки кіберпростору. Деталізовано зміст інформації з обмеженим доступом та об’єктів авторського права або суміжних прав із позицій різновидів інформаційного продукту як предмету посягання.

Шифр зберігання НБУВ: Ж70795/юрид.н.

***

Теоретичні і практичні засади еволюції від інформаційного суспільства до «суспільства знань» і до smart-суспільства: виклики і можливості четвертої

промислової революції : матеріали Міжнар. наук.-практ. конф., 23-24 квіт. 2018 р. - Запоріжжя : ЗДІА, 2018. - 220 с.

Зі змісту:

- Пырч Д. Разновидности компьютерных вирусов и способы защиты от них;
- Шатц К. Дослідження методів захисту веб-додатків як головний тренд інформаційної безпеки.

Шифр зберігання НБУВ: ВА825621.

***

Фундаментальні проблеми кримінальної відповідальності : матеріали наук. полілогу, м. Харків, 7 верес. 2018 р. - Харків : Право, 2018. - 204 с.

Зі змісту:

- Стрельцов Л.С. Проблема розмежування кримінальної відповідальності за кіберзлочин (на прикладі ст. 361 КК).

Шифр зберігання НБУВ: ВА825615.

***

Шапочка С. В. Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж : автореф. дис. ... канд. юрид. наук : 12.00.08 / Шапочка Сергій Володимирович ; Донец. юрид. ін-т МВС України. - Кривий Ріг, 2018. - 20 с.

З’ясовано історичні та соціальні передумови виникненні шахрайства, що вчиняється з використанням комп'ютерних мереж. Здійснено кримінологічну характеристику шахрайства, що вчиняється з використанням комп'ютерних мереж. Автором створено власну класифікацію шахрайства, що вчиняється з використанням комп'ютерних мереж. Визначено загальні та спеціальні заходи запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж. Виокремлено основні проблеми запобігання такого виду злочину. Внесено пропозиції щодо шляхів удосконалення законодавства України у сфері запобігання шахрайству з використанням комп'ютерних мереж.

Шифр зберігання НБУВ: РА436305.

***

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.