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

№ 10 (жовтень)

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

«Центральна виборча комісія просить Верховну Раду дозволити витратити 49 мільйонів 660 тисяч гривень на забезпечення кібербезпеки майбутніх виборів.

Відповідну постанову ухвалено на засіданні ЦВК в середу…

Як пояснив заступник голови ЦВК Євген Радченко, цим рішення комісія просить парламент "перекинути" 49 млн 660 тисяч гривень з одних статей витрат комісії на інші, що стосуються кібербезпеки…» ***(ЦВК просить Раду подбати про її кібербезпеку // Українська правда (https://www.pravda.com.ua/news/2018/10/10/7194744/). 10.10.2018).***

***

«Україна вперше бере участь у міжнародній високотехнологічній виставці "Congress & Expo" у Гаазі (Нідерланди), що відбувається в рамках традиційного Місяця кібербезпеки Європи…

4 жовтня в рамках "Cyber Security Week" відкриється виставка "Congress & Expo", на якій Україна вперше представить національну панель, що була створена зусиллями Київської торгово-промислової палати. Українські учасники запропонують нові методи і рішення задач попередження кіберзагроз та представлять консолідовані можливості нашого бізнесу на європейській арені…» ***(Марія Куцина. Україна презентує у Гаазі свої методи попередження кіберзагроз // Трибуна (https://tribuna.pl.ua/news/ukrayina-prezentuye-u-gaazi-svoyi-metodi-poperedzhennya-kiberzagroz/). 06.10.2018).***

***

«…8 жовтня 2018 року, починаючи з 18:00, на зовнішню віртуальну адресу ІТС «Електронний кабінет» в мережі інтернет та 9 жовтня 2018 року, починаючи з 9:00, на зовнішню віртуальну адресу ІТС «Офіційний веб-портал ДФС України» була зафіксована велика кількість запитів, що спричинило збільшення навантаження на центральний процесор мережевого екрану (до 100%) та призвело до його нестабільної роботи», – повідомила прес-служба ДФС. У відомстві зазначили, що провайдер ідентифікував DOS-атаки та застосував механізм захисту…». ***(Державна фіскальна служба заявила про кібератаки на свої ресурси // "Українські медійні системи" (https://glavcom.ua/news/derzhavna-fiskalna-sluzhba-zayavila-pro-kiberataki-na-svoji-resursi-534976.html). 09.10.2018).***

***

«Страницу в Facebook первой вице-миссис «Земной шар 2018», обладательницы титулов «Первая вице-Миссис Украина Вселенная 2017» и «Миссис Украина Земной Шар 2017» Ирины Келлер взломали неизвестные хакеры и продвигали через её аккаунт рекламные кампании в «привязанном» к профилю сообществе. Теперь Facebook требует с девушки деньги за чужую рекламу.

Об этом Ирина Келлер написала на своей странице в Facebook…

Ирина Келлер оказалась «спонсором» рекламной кампании страницы Independent Store – онлайн магазина часов из Индонезии. Страница магазина была создана 21 сентября 2018 года.

На данный момент сообществом не проводится никаких рекламных акций, как следует из информации самой страницы…» ***(Владимир Кондрашов. Facebook требует от украинской модели деньги за чужую рекламу // Internetua (http://internetua.com/facebook-trebuet-ot-ukrainskoi-modeli-dengi-za-csujuua-reklamu). 11.10.2018).***

***

«Вход в административную панель портала Государственного учреждения «Институт охраны грунтов Украины» (iogu.gov.ua) до 11 утра вчера осуществлялся с помощью логина «admin» и простого пароля «748956». Более того, на web-ресурсе госучреждения в свободном доступе находился 12-страничный документ под названием «Инструкция для управления сайтом».

«Уязвимость» сайта Института охраны грунтов Украины (ГУ «Держґрунтохорона») обнаружил эксперт по кибербезопасности, ведущий разработчик компании ИТ Лаборатория Александр Галущенко…

Опубликованная на портале iogu.gov.ua «Инструкция для управления сайтом» – простой файл в формате .doc – начинается с пункта входа в административную панель – в нем прописаны логин и пароль для входа…

В Институте охраны грунтов Украины после обращения журналиста InternetUA изменили данные для входа в административную панель и удалили файл-инструкцию…» ***(Владимир Кондрашов. Институт охраны грунтов Украины подарил хакерам подробную инструкцию по доступу к своему сайту // Internetua (http://internetua.com/institut-ohrany-gruntov-ukrainy-podaril-hakeram-podrobnuua-instrukciua-po-dostupu-k-svoemu-saitu0. 10.10.2018).***

***

«На портале old.data.gov.ua был обнаружен находящийся в открытом доступе документ Microsoft Word с логином и паролем, которые, как выяснилось позже, дают доступ к сети wi-fi Министерства регионального развития, строительства и жилищно-коммунального хозяйства Украины.

Документ, индексируемый поисковыми системами, обнаружил эксперт по кибербезопасности, ведущий разработчик компании ИТ Лаборатория Александр Галущенко…

Сайт old.data.gov.ua – старая версия Единого государственного портала, на котором органы власти, местного самоуправления, госучреждения загружают наборы открытых данных…» ***(Владимир Кондрашов. Минрегион "засветил" данные о доступе к своей сети wi-fi // Internetua (http://internetua.com/minregion-zasvetil-dannye-o-dostupe-k-svoei-seti-wi-fi). 10.10.2018).***

***

«На одном из сайтов Главного территориального управления Юстиции Министерства юстиции Украины в открытом доступе находились десятки

файлов и программ, среди которых – весьма специфическое программное обеспечение, предназначенное для взлома Windows и использования нелицензионных копий операционной системы и других продуктов Microsoft.

«Уязвимость» сайта ГТУ Юстиции в Полтавской области обнаружил эксперт по кибербезопасности, ведущий разработчик компании ИТ Лаборатория Александр Галущенко…

Эксперт обнаружил незащищенное соединение на сайте www.just.gov.ua. На портале управления юстиции доступны директории и программы с десятками файлов и программ. Есть и запрещенное ПО – архивы программ AAct Network 1.1.4 Portable by Ratiborus и Windows Loader DAZ 2.2.2. Оба появились в директории /Program/ 4 сентября этого года…

Кроме «общераспространенного» ПО и драйверов к различным принтерам, на сайте можно найти и ряд более специфического программного обеспечения, используемого органами юстиции для своей работы. В том числе – и для работы с Государственным казначейством…» ***(Владимир Кондрашов. В Минюсте используют софт для взлома Windows // Internetua (http://internetua.com/v-minuaste-ispolzuuat-soft-dlya-vzloma-windows). 08.10.2018).***

***

«В Украине продолжают использоваться инструменты противодействия киберпреступлениям для влияния на свободу слова и наступления на права граждан.

Об этом говорили на Девятом форуме по управлению Интернетом IGF-UA…

Секция «Кибербезопасность» стала, пожалуй, самой многочисленной на форуме. В этом году заседание касалось, в первую очередь, попыток власти «зарегулировать» свободу слова через различные, направленные на борьбу с киберугрозами, законопроекты и указы…

Глава ОО «Украинская группа информационной безопасности» Константин Корсун говорил от имени комьюнити ИБ-специалистов о национальной системе обеспечения кибербезопасности…

Константин Корсун отметил, что деятельность основных субъектов обеспечения кибербезопасности в Украине никак не координируется…

Наиболее открытой к ИБ-комьюнити, говорит глава «УГИБ», является, как не странно, на сегодняшний день Служба безопасности Украины, готовая реагировать, прислушиваться и сотрудничать с компаниями, работающими на рынке обеспечения информационной безопасности. Больше все же претензий у ИБ-специалистов – к Минобороны и разведчикам: их вклад в построение национальной системы киберзащиты, по мнению Константина Корсуна, мягко говоря, незаметен…

В этом году показательно многие представители силовых структур открыто проигнорировали форум…

Чиновник Госспецсвязи сосредоточился на том, что ответственность за защиту объектов критической инфраструктуры в первую очередь должна лежать на собственнике ОКИ…

В ГССЗИ видят перспективными такие направления развития системы киберзащиты:

– нормативно-правовое регулирование вопросов кибербезопасности и киберзащиты;

– развитие организационно-технической модели киберзащиты;

– государственно-приватное партнерство;

– международное партнерство;

– киберзащита ОКИ;

– развитие киберпространства…

Представитель СНБОУ Михаил Гуцалюк… рассказал о подготовке Меморандума между основными субъектами национальной системы кибербезопасности и операторами, провайдерами телекоммуникаций по противодействию киберпреступности… документ позволит создать рабочую группу, «которая может разработать рекомендации, предоставить их правоохранителям, что позволило бы эффективней работать на результат» к примеру, выработать, наконец, пути и способы получения информации от операторов при расследовании киберпреступлений…» ***(Владимир Кондрашов. В Украине путают цензуру с кибербезопасностью // Internetua (http://internetua.com/v-ukraine-putauat-cenzuru-s-kiberbezopasnostua). 01.10.2018).***

***

«Секретар Ради нацбезпеки та оборони Олександр Турчинов доручив перевести у посилений режим кібербезпеки Єдиної інформаційно-аналітичної системи «Вибори» під час проведення чергових виборів президента та народних депутатів у 2019 році.

Про це він заявив під час засідання Національного координаційного центру кібербезпеки, повідомляє прес-служба РНБО…

За словами Турчинова, наразі є обґрунтовані підстави вважати, що Росія намагатиметься використати виборчий процес для реалізації планів гібридної агресії проти України…

За даними РНБО, будуть проведенні кібернавчання з відпрацювання спільних заходів з кіберзахисту та протидії зовнішнім втручанням у роботу інформаційних та інформаційно-телекомунікаційних систем ЦВК…

Також було вирішено провести підготовку персоналу ЦВК та забезпечити захист інтернет-сайтів комісії…» ***(Спецслужби – задля захисту від російських хакерів – переведено в посилений режим // Західна інформаційна корпорація (https://zik.ua/news/2018/10/18/spetssluzhby__zadlya_zahystu_vid_rosiyskyh_hakeriv__perevedeno_v_posylenyy_1429209). 18.10.2018).***

***

«В открытом доступе опять оказались документы НАЭК «Энергоатом». На этот раз - касающиеся работы Южно-Украинской АЭС.

Утечку данных обнаружил эксперт по кибербезопасности, ведущий разработчик компании «IT Лаборатория» Александр Галущенко…

Эксперт на своей странице в Facebook опубликовал скриншоты некоторых из обнаруженных им документов и попросил представителей Энергоатома связаться с ним…

На данный момент утечка закрыта…» ***(Владимир Кондрашов. Документы Энергоатома были доступны российским террористам // Internetua (http://internetua.com/dokumenty-energoatoma-byli-dostupny-rossiiskim-terroristam). 17.10.2018).***

***

«Науково-практична конференція «Конвергенція квантового майбутнього: електронна трансформація в епоху четвертої промислової революції», яка нещодавно відбулася в Києві, згуртувала навколо себе урядовців, освітян, науковців, співробітників вітчизняних і міжнародних установ, викладачів та студентську молодь університету…

Головною метою проведення науково-практичної конференції було:

1.Обговорити стратегію розвитку України в умовах геополітичних викликів епохи цифрової комунікації;

2.Визначити роль стратегічних комунікацій в забезпеченні національної безпеки України в умовах розвитку інформаційної сфери;

3.Визначити пріоритетні напрями запобігання і протидії кіберзлочинності та кібертероризму в XXI столітті;

4.Розглянути питання кібербезпеки, електронних сервісів в державі та особливості транскордонної взаємодії;

5.Розкрити сутність транскордонної взаємодії в транспортному сполученні з використанням електронних довірчих послуг…» ***(Петро Біленчук. В КУП НАНУ пройшла науково-практична конференція з глобальної цифрової комунікації і кібербезпеки // Київський університет права (http://kul.kiev.ua/novini/v-kup-nanu-proyshla-naukovo-praktichna-konferencija-z-globalnoji-cifrovoji-komunikaciji-i-kiberbezpeki.html). 17.10.2018).***

***

«Науково – дослідним інститутом інформатики і права Національної академії правових наук України спільно з Навчально-науковим центром інформаційного права та правових питань інформаційних технологій Національного технічного університету «Київський політехнічний інститут імені Ігоря Сікорського» проведено Першу науково-практичну конференцію «Інформаційне право: сучасні виклики і напрями розвитку»…

Науково-практична конференція пройшла в умовах фахового обговорення найбільш актуальних питань, які стосуються філософії інформаційного права, інформаційної і національної безпеки, інновацій у розвитку правової науки та освіти в інформаційній сфері, місії інформаційного права у забезпеченні інформаційної безпеки, кібербезпеки в умовах сучасного розвитку інформаційних технологій…» ***(Інформаційне право: сучасні виклики і напрями розвитку // «Українське право» (http://ukrainepravo.com/news/ukraine/informatsiyne-pravo-suchasni-vyklyky-i-napryamy-rozvytku-/). 19.10.2018).***

***

«Міністерство інформаційної політики продовжує роботу над проблемою кібербезпеки України у трьох напрямах – комунікаційному, освітньому й законодавчому.

Про це заявив заступник міністра інформаційної політики України Дмитро Золотухін…

Заступник міністра взяв участь у форумі з кібербезпеки HackIT 4.0 у Києві. Під час відкриття заходу він також зазначив, що нині вдосконалюється система кризових комунікацій, яка є визначальною для мінімізації наслідків під час різного роду кібератак.

Крім цього, МІП опікується питанням кіберграмотності, особливо в органах державної влади, "оскільки провідна більшість усіх вразливостей інформаційних систем ґрунтується саме на людському факторі", наголосив Дмитро Золотухін.

"Щодо законодавчого аспекту, за словами Золотухіна, значної уваги заслуговує модель розкриття вразливостей Responsible disclosure, зокрема в державному секторі, нормативне забезпечення якої дало б змогу підвищити рівень кібербезпеки на національному рівні", – йдеться у повідомленні…» ***(МІП працюватиме над посиленням кіберграмотності в Україні // UATV (https://uatv.ua/mip-pratsyuvatyme-nad-posylennyam-kibergramotnosti-v-ukrayini/). 16.10.2018).***

***

«Школу по подготовке специалистов в области кибербезопасности запустили на территории инновационного парка UNIT… Обучение стартует в декабре 2018 года и продлится 5 месяцев Первый набор составит 40 человек…

Для участия в программе кандидаты должны обладать базовыми техническими знаниями и навыками программирования. Организаторы будут выбирать учащихся на конкурсной основе. Отбор в школу включает в себя онлайн- и оффлайн тестирования, собеседование, а также экспресс-курс…

В рамках Cyber School учащиеся пройдут интенсивные курсы по безопасности сетей и приложений, систем эксплуатаций, обратного инжиниринга и др...» ***(В Украине открыли бесплатную школу «белых хакеров» // ChannelForIT (http://channel4it.com/publications/V-Ukraine-otkryli-besplatnuyu-shkolu-belyh-hakerov-32159.html#). 18.10.2018).***

***

«Міністр закордонних справ України Павло Клімкін повідомив, що підконтрольне йому відомство щотижня піддається мінімум одній кібератаці.

Про це він сказав, виступаючи на Варшавському форумі з безпеки в середу…

Очільник МЗС зазначив, що вимагає від профільних структур і відомств й України, й інших держав Європи, перебування в постійній готовності до кібератак…». ***(Павло Клімкін заявив про систематичні кібератаки на МЗС // Західна інформаційна корпорація***

(https://zik.ua/news/2018/10/24/pavlo_klimkin_zayavyv_pro_systematychni_kiberataky_na_mzs_1433363). 24.10.2018).

***

«Украинским бойцам, которые частично потеряли работоспособность, позволили восстановиться на военной службе. Министерство обороны определило перечень частей и должностей, где могут служить люди с инвалидностью.

Среди них — центры защиты информации и кибербезопасности, военная служба правопорядка, военкоматы, госпиталя и учебные заведения.

…Всего в перечне 62 должности для офицеров, рядового и сержантского состава…» ***(Руслан ГРИШКО. Люди с инвалидностью могут служить в кибервойсках // Gazeta.ua (https://gazeta.ua/ru/articles/ukraine-newspaper/_lyudi-s-invalidnostyu-mogut-sluzhit-v-kibervojskah/866133). 26.10.2018).***

***

«Украинские хактивисты снова обнаружили на ряде сайтов государственных организаций XSS и SQL-уязвимости…

Информацию об этом на своей странице в Facebook опубликовал спикер Украинского кибералъянса, известный в сети под ником Sean Townsend…

Согласно опубликованной информации, проблемы с безопасностью обнаружены на сайтах Физико-механического института им Г. В. Карпенко НАН Украины, Управления агропромышленного развития Черкасской ОГА, Малой академии наук, Департамента социальной защиты Закарпатской ОГА и Корецкой РГА (Ровенская область).

Сайты Малой академии наук и Департамента социальной защиты Закарпатской ОГА уже взломали хакеры из Ближнего Востока.

На сайте Корецкой РГА активисты обнаружили незапароленный вход в административную панель…» ***(Владимир Кондрашов. Украинские государственные сайты почему-то оставляют лазейки для хакеров // Internetua (http://internetua.com/ukrainskie-gosudarstvennye-saity-pochemu-to-ostavlyauat-lazeiki-dlya-hakerov-). 22.10.2018).***

***

«Флешмоб Украинского кибералъянса #fuckresponsibledisclousure, начатый около года назад, несмотря на официальное окончание, похоже, заканчиваться и не собирается. Причина тому – наплевательское отношение органов власти к собственной кибербезопасности.

…Публичная огласка уязвимостей, считают участники флешмоба, позволяет чаще добиваться желаемого результата: государственные органы реагируют на подобную информацию намного оперативней, устраняя бреши и проблемы на своих ресурсах.

Согласно опубликованной информации, на пяти государственных информационных ресурсах обнаружены XSS- и SQl-уязвимости. В список «жертв» флешмоба на этот раз попали сайты «Киевпастранса», Национальной академии

государственного управления при Президенте Украины, Фонда государственного имущества (дважды), Прилуцкого городского совета и Управления образования Днепровской районной в Киеве государственной администрации…

– Обнаруженные уязвимости на сайтах госструктур свидетельствуют о том, что любой профессиональный хакер пройдёт через всю государственную и критическую инфраструктуру, как нож сквозь масло… Вплоть до того, что пароли администраторов лежат в открытом доступе, или важная информация лежит онлайн, – говорит спикер УКА…

За время с начала акции, отмечает спикер УКА, в отношении государства к безопасности собственных Интернет-ресурсов существенно ничего не поменялось…» ***(Владимир Кондрашов. Информационный "стриптиз" государственных сайтов продолжается // Internetua (http://internetua.com/informacionnyi-striptiz-gosudarstvennyh-saitov-prodoljaetsya). 30.10.2018).***

***

«Державні підприємства, зокрема об'єкти критичної інфраструктури, абсолютно не готові до протистояння кіберзагрозам, кількість яких збільшується. 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, ситуація із кібербезпекою в органах державної влади України наразі складна, оскільки захист від кібератак потребує великих ресурсів і затрат часу. Крім того, за його словами, в країні не вистачає підготовлених спеціалістів, які могли б працювати в сфері захисту від кібератак.

При цьому він додав, що комерційні підприємства більш захищені від таких загроз, ніж державні, оскільки для захисту останніх не вистачає коштів…» ***(Марія Мамаєва. Об'єкти критичної інфраструктури в Україні абсолютно не готові до кібератак – експерт // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1759176-obyekti-kritichnoyi-infrastrukturi-v-ukrayini-absolyutno-ne-gotovi-do-kiberatak-ekspert). 24.10.2018).***

***

Національна система кібербезпеки

«…За словами Генерального секретаря Альянсу Йєнса Столтенберга, зараз НАТО допомагає Україні в створенні центру реагування на кіберінциденти. Це буде одним із способів допомогти нашій державі справитися з інцидентами або спробами втрутитися, вторгнутися або зламати наші кібермережі…» ***(Людмила Кліщук. NATO створює в Україні центр із захисту кіберпростору // Na chasi (https://nachasi.com/2018/10/04/nato-kiberprostir/). 04.10.2018).***

***

«Новий підрозділ увійде до складу Департаменту кіберполіції. Планується, що управління надаватиме підтримку не тільки поліцейським, а й іншим правоохоронним структурам. Про це йшлося сьогодні, 3 жовтня, під час зустрічі Голови Нацполіції Сергія Князєва та керівника кіберполіції Сергія Демедюка з Міністром Великої Британії з питань безпеки паном Беном Воллесом.

Під час зустрічі сторони обговорили співробітництво поліцейських двох країн у боротьбі із кіберзлочинністю…

Під час зустрічі українські поліцейські презентували британській стороні проект створення на базі Департаменту кіберполіції нового підрозділу…» ***(У Нацполіції буде створено управління для допомоги правоохоронним органам у розкриті злочинів із кіберелементом // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/u-naczpolicziji-bude-stvoreno-upravlinnya-dlya-dopomogi-pravooxoronnim-organam-u-rozkriti-zlochiniv-iz-kiberelementom/). 03.10.2018).***

***

«Для посилення кіберзахисту в нашій державі планують створити єдину інтерактивну базу даних про кіберінциденти. Вона працюватиме для потреб Міністерства оборони, Державної служби спеціального зв'язку та захисту інформації, Служби безпеки, Національної поліції, Національного банку України та розвідувальних органів.

Відповідне рішення ухвалили на засіданні Національного координаційного центру кібербезпеки за участю секретаря РНБО України Олександра Турчинова…

Також силові структури приділятимуть особливу увагу запобіганню кібератакам на інформаційні системи та державні електронні інформаційні ресурси ЦВК…». ***(В Україні планують створити базу даних кіберінцидентів // UA\|TV (https://uatv.ua/v-ukrayini-planuyut-stvoryty-bazu-danyh-kiberintsydentiv/). 18.10.2018).***

***

Правове забезпечення кібербезпеки в Україні

«Комитет Верховной Рады Украины по вопросам информатизации и связи рекомендовал отправить на доработку скандально известный законопроект № 8186, известный как законопроект «О борьбе со спамом», авторства нардепов Березы, Усова и Емца.

Проект закона …декларирует своей целью «внедрение механизма защиты абонента телекоммуникационных услуг от несанкционированных электронных, текстовых и/или мультимедийных сообщений, с последующим использованием их контактных данных и возможностью использования этой информации в мошеннических целях».

Однако, не смотря на декларируемую цель, документ оказался «сыроват», поэтому был отправлен на доработку – множественные замечания общественности, отрасли и регулятора документом не были учтены…

В частности, законопроект пытается регулировать то, что уже регулируется Правилами предоставления и получения телекоммуникационных услуг, утвержденными постановлением Кабинета Министров Украины в апреле 2012 года. При этом даже само определение «спама» не соответствует действующим Правилам. Фактически авторы законопроекта, вместо того, чтобы сосредоточиться на борьбе с новыми видами спама, предлагают регулировать уже регулируемое.

Претензии у специалистов и к целому ряду других новшеств законопроекта. В частности, законопроект, как неоднократно заявлялось, обяжет операторов нарушить тайну переписки и телефонных разговоров, и даже обязывает идти на преступление…» ***(Владимир Кондрашов. Законопроект о псевдо борьбе со спамом отправят на доработку // Internetua (http://internetua.com/zakonoproekt-o-psevdo-borbe-so-spamom-otpravyat-na-dorabotku). 03.10.2018).***

***

«Верховна Рада схвалила за основу проект закону 8496 про внесення змін до додатка №3 до Закону України "Про Державний бюджет України на 2018 рік" щодо посилення безпеки інформаційних ресурсів Центральної виборчої комісії…

Зокрема, цим законопроектом пропонується збільшити видатки 49,66 млн гривень шляхом перерозподілу з бюджетних статей на посилення безпеки інформаційних ресурсів Центральної виборчої комісії…» ***(Дмитро Кропивницький. Рада підтримала перерозподіл майже 50 млн грн на кібербезпеку ЦВК // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1758223-rada-pidtrimala-pererozpodil-mayzhe-50-mln-grn-na-kiberbezpeku-tsvk). 18.10.2018).***

***

Кібервійна проти України

«Україна, Молдова та Грузія повинні мати спільну стратегію кібербезпеки та захисту інформаційного простору від впливу Російської Федерації з огляду на вибори, що мають відбутися в усіх трьох країнах, наголошує голова Верховної Ради Андрій Парубій.

«Рік виборів в усіх трьох країнах. І вплив Росії на виборчий процес у наших країнах дуже високий. Його не можна недооцінювати. Тому потрібна спільна стратегія кібербезпеки, інформаційної безпеки, підтримка одне одного через спостерігачів - вважаю, це великий виклик, який стоїть перед нами», - сказав А.Парубій у Тбілісі, виступаючи на інавгураційному засіданні міжпарламентської асамблеї Грузії, України та Молдови». ***(Україні, Молдові та Грузії потрібна спільна стратегія кібербезпеки та інформбезпеки від РФ – Парубій // Інтерфакс-Україна (https://ua.interfax.com.ua/news/election2019/536202.html). 05.10.2018).***

***

«Тільки протягом 2018 року на виконання завдань російських спецслужб зловмисники здійснили тридцять п'ять кібератак на українські автоматизовані системи та бази даних об'єктів критичної інфраструктури у галузях енергетики, транспорту, зв'язку, банківської сфери тощо…

СБ України виявлено п'ять хакерських угрупувань та ідентифіковано дев'ять осіб, які були задіяні російськими спецслужбами для кібератак…

СБ України наголошує, що уряд та силові структури РФ прикривають своїх кіберзлочинців від відповідальності за вчинені злочини та фактично припинили дотримання своїх міжнародних зобов'язань…». (Анастасія Ткачук. Цього року російські спецслужби здійснили 35 хакерських атак на об'єкти критичної інфраструктури – СБУ // Інформаційне агентство «Українські Національні Новини» ***(https://www.unn.com.ua/uk/news/1756002-tsogo-roku-rosiyski-spetssluzhbi-zdiysnili-35-khakerskikh-atak-na-obyekti-kritichnoyi-infrastrukturi-sbu). 05.10.2018).***

***

«З'явилися результати розслідування злому пошти і аккаунту у соцмережах російського опозиційного журналіста Аркадія Бабченко.

У вересні його аккаунт в "Твіттері" був зламаний. Від імені журналіста хакери опублікували повідомлення про його нібито підготовлюване затримання, а також лист з каяттям. Розслідування, природно, призвело до "ДНР"…

В той же день, коли були зламані "Твіттер", "Живий журнал" та інші акаунти Бабченко, на одній з сторінок в соцмережі "ВКонтакте" з'явився відеозвіт про злом від імені хакерів "Киберберкут". Відразу після цього звіт хакерів переопубліковать в групі "Зведення від ополчення Новоросії" у Вконтакті…». ***(Кібератака на Бабченка: хакери по-тупому спалилися, слід веде до "ДНР" // znaj.ua (https://znaj.ua/politics/178273-kiberataka-na-babchenka-hakeri-po-tupomu-spalilisya-slid-vede-do-dnr). 04.10.2018).***

***

«Національний центр кібербезпеки Великої Британії надав інформацію, яка говорить про участь спеціалістів ГРУ РФ у кібератаці на підприємства транспортної інфраструктури у жовтні 2017 року, і не виключено, що це повториться. Про це заявив міністр інфраструктури Володимир Омелян під час наради з директором міжнародного аеропорту "Одеса" Павлом Прусаком та начальником "Київського метрополітену" Віктором Брагінським…

Так, Омелян провів нараду з "приводу наявної інформації щодо спроб проведення кібератак спецслужбами Російської Федерації для виведення цих підприємств з ладу"…

Міністр підкреслив, що аеропорт "Одеса" та "Київський метрополітен" уже впроваджують низку проектів цифрової трансформації…» ***(Юлія Шрамко. Лондон вказав на причетність ГРУ РФ до кібератак на метро та аеропорт в Україні // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1757158-london-vkazav-na-prichetnist-gru-rf-do-kiberatak-na-metro-ta-aeroport-v-ukrayini). 12.10.2018).***

***

«Служба безпеки України отримала чергові докази ведення агресивних дій російських спецслужб проти України в кіберпросторі з використанням підконтрольного хакерського угруповання відповідального за проведення протягом 2015-2017 років кібератак на об'єкти критичної інфраструктури України відомих як "BlackEnergy" та "NotPetya"…

Хакери використали нові зразки шкідливого програмного забезпечення, функціональні можливості якого передбачають віддалене адміністрування процесів операційної системи та копіювання файлів, стеження за діями користувачів, перехоплення паролів.

За результатами розслідування проведеного фахівцями СБУ у взаємодії з відомою антивірусною компанією встановлено, що ці комп'ютерні віруси є оновленими версіями бекдору "Industoyer". Вони мають низку схожих характерних ознак, зокрема використовують подібні фрагменти програмного коду, процедури розгортання, використання обчислювальних можливостей заражених систем тощо.

Крім того зафіксовано використання окремих інструментів, що належать цьому хакерському угрупованню, які були виявлені під час розслідування попередніх кібератак. Ситуаційним центром забезпечення кібербезпеки СБ України встановлені об'єкти вказаної кібератаки, надано допомогу в локалізації її наслідків та мінімізації кіберзагроз ІТ-інфраструктурам органів державної влади…». ***(Саша Картер. СБУ отримала чергові докази причетності Росії до кібератак проти України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1757089-sbu-otrimala-chergovi-dokazi-prichetnosti-rosiyi-do-kiberatak-proti-ukrayini). 11.10.2018).***

***

«…Петро Поршенко відзначає, що, на фоні зростаючої кіберзагрози з боку Російської Федерації, зробить усе можливе задля безпечного та демократичного проведення президентських виборів в Україні…

"Хочу наголосити, що я звернувся з відповідними пропозиціями до наших партнерів, як з Європейського Союзу - до Німеччини, до Франції, де попросив передати досвід, у тому числі законодавчий, щодо недопущення втручання у виборчі процеси, так і до наших партнерів зі США. Не приховуватиму, вони вже надіслали експертів, які працюють з нашими фахівцями в галузі кібербезпеки, у галузі забезпечення захисту від зовнішнього втручання, і ця робота буде продовжена", - говорить Петро Порошенко

Президент підкреслив, що в Національну Раду Реформ буде внесено законопроект, який забезпечить посилення відповідальності за порушення виборчого законодавства» ***(Україна спільно із США та Євросоюзом запобігатиме хакерським атакам на виборах // 5 канал (https://www.5.ua/polityka/ukraina-spilno-iz-ssha-ta-yevrosoiuzom-zapobihatyme-khakerskym-atakam-na-vyborakh-179530.html). 17.10.2018).***

***

«Хакеры могут использовать Украину как полигон, тестируя на нашей стране свой арсенал кибер-оружия перед тем, как применить его против других стран и всего мира. Об этом в интервью УНИАН заявил Роберт Липовски, старший исследователь угроз Лаборатории ESET…

В то же время, эксперт не согласен, что главной причиной хакерских атак является плохо налаженная безопасность и недостаточная киберграмотность пользователей… Нужно продолжать искать ответ на вопрос: «почему Украина – цель?». Но виновны в этом хакеры, это они выбирают жертву. А не украинские пользователи, правительство или компании", - отметил он». ***(Хакеры тестируют кибер-оружие в Украине перед тем, как применить его против всего мира - эксперт по кибербезопасности // UNIAN.NET (https://www.unian.net/science/10309572-newsweek-na-marse-mozhet-byt-dostatochno-kisloroda-dlya-nekotoryh-zhivotnyh.html)/. 24.10.2018).***

***

Боротьба з кіберзлочинністю в Україні

«Краматорський міський суд Донецької області розглянув справу щодо групи осіб, які з 2015 до 2018 рік мали доступ до реєстру дозволів для переміщення осіб в районі проведення АТО.

Згідно з судовим вироком, двоє осіб у серпні 2015 року незаконно отримали програмне забезпечення, яке дало їм доступ до реєстру (https://urp.ssu.gov.ua). З його допомогою вони могли вносити в нього зміни чи додавати інформацію. Згодом вони почали пропонувати в мережі за гроші оформлювати перепустки до зони АТО…

Слідству вдалося встановити особу одного з учасників групи. Згідно з вироком, ця особа була засуджена до трьох років позбавлення волі з іспитовим терміном в один рік. Розслідування щодо інших учасників групи, які не були встановлені, виділили в окреме провадження…». ***(Зловмисники отримали доступ до реєстру пропусків до зони АТО й вносили зміни за гроші // MediaSapiens (https://ms.detector.media/web/cybersecurity/zlovmisniki_otrimali_dostup_do_reestru_propuskiv_do_zoni_ato_y_vnosili_zmini_za_groshi/). 03.10.2018).***

***

«Полтавська поліція розслідує справу хакера, який намагався зламувати комп'ютери користувачів програми для спаму у ВКонтакті, на Одноклассниках та Instagram

…На думку слідчих, невідомий хакер інфікував вірусами та розповсюджував програму, яку використовують спамери…

За даними Єдиного реєстру судових рішень, поліція проводила моніторинг мережі інтернет, в ході якого виявила невідому особу з нікнеймом L******. Його заблокували на великій кількості хакерських форумів за «порушення їхніх правил, шахрайство, розповсюдження шкідливого програмного забезпечення, продаж крадених ігрових акаунтів»…

L****** стверджував, що в його архіві міститься програма з ліцензією на декілька років вперед. Користувачі, охочі безкоштовно користуватися програмою для спаму та накрутки лайків, могли попастися на вудочку хакера.

Які саме дані з інфікованих комп'ютерів збирав L****** та чи були взагалі постраждалі — такої інформації в оприлюднених матеріалах справи поки немає…» ***(Дарина СИНИЦЬКА. Поліція шукає полтавця, який розповсюджував віруси на хакерських форумах // Інтернет-видання «Полтавщина» (https://poltava.to/news/48498/). 08.10.2018).***

***

«Правоохранительные органы Французской республики попросили помощи украинских полицейских в расследовании дела об атаке вируса-вымогателя на две компании, занимающиеся научными исследованиями и производством продуктов питания…

Согласно материалам дела, в сентябре 2016 года две французские компании – Roquette SA, расположенная в пригороде Парижа, и компания Fermentalg SA в Либурне (Новая Аквитания, Франция) – стали жертвами взлома, после того, как каждая из них получила мошенническое электронное сообщение с вложением.

После открытия этого вложения программа-вымогатель распространилась в компьютерной системе этих компаний, вызывав шифрование всех файлов на компьютере. Зашифрованными оказались несколько тысяч важных для предприятий компьютерных файлов. Затем на экране зараженного компьютера появлялась страница, где требовали выкуп в размере 4 биткойнов для получения ключа дешифрования. Руководители этих компаний выплатили выкуп вымогателям…

Французские правоохранители обнаружили «настоящую организацию европейского масштаба со многими филиалами, сконцентрированными вокруг торговой платформы Биткойн под названием «Btc-e.com»». Её правоохранители определили как «занимающую центральное место передачи сумм, собранных от жертв»…

Btc-e.com также сообщила IP-адреса подключения к этому счету клиента. Анализ этих журналов событий французскими правоохранителями показал много соединений с IP-адресов, принадлежащих украинским интернет-провайдерам…» ***(Владимир Кондрашов. Прокуратура Парижа просит украинскую полицию найти хакеров // Internetua (http://internetua.com/prokuratura-parija-prosit-ukrainskuua-policiua-naiti-hakerov). 08.10.2018).***

***

«Киберворы с помощью нехитрых комбинаций и ксерокопий документов списывают с банковских счетов Ощадбанка суммы в десятки и даже сотни тысяч гривен. Мошенникам удается получить доступ к Web-банкингу жертвы, открыв на её имя ещё один счет в этом же банке.

…27 июля прошлого года к старшему контролеру-кассиру отделения Ощадбанка в Трускавце обратилось неустановленное следствием лицо с просьбой открыть карточный счет на якобы его имя. При себе мошенник имел копию

паспорта и идентификационного кода с соответствующими на первый взгляд данными. Позже выяснится, что мошенник, открывший счет, не похож на того, на чье имя, собственно, открывался счет. Более того, с реальным клиентом Ощадбанка не совпадает образец подписи «клиента», дата и место рождения и даже дата выдачи паспорта. Несмотря на это, имея только ксерокопии документов «на руках» (оригиналы мошенник якобы пообещал занести позже), кассир открыла карточный счет и выдала неизвестному платежную карточку MasterCard Debit Standart на имя другого клиента Ощадбанка.

Получив с помощью выданной карточки возможность пользоваться Web-банкингом от имени своей жертвы, злоумышленники перевели на новый счет деньги с другого счета пострадавшего, также открытого в этом банке, а позже, с помощью выданной кассиром карты, сняли в банкоматах 158 тысяч 110 гривен.

…аналогичную аферу мошенники провернули со счетом в Ощадбанке ещё одной жертвы…». ***(Владимир Кондрашов. Киберворы украли у клиентов Ощадбанка сотни тысяч гривен // Internetua (http://internetua.com/kibervory-ukrali-u-klientov-osxadbanka-sotni-tysyacs-griven). 05.10.2018).***

***

«Предприимчивый хакер зарабатывал на том, что через собственный сайт предоставлял услуги взлома страниц в запрещенной ныне в Украине соцсети «Вконтакте». Горе-бизнесмен поставил взлом «на конвейер» и в результате получил 3 года лишения свободы с испытательным сроком на один год…

Как стало известно, безработный мужчина в марте 2017 года создал сайт xakercki-poslygu.hol.es, через который принимал заказы на взлом страниц. Суд признал «предпринимателя» виновным во взломе более чем шести десятков страниц «Вконтакте». Кроме того, хакеру удалось взломать страницы пользователей Facebook и Instagram...

Кроме взлома страниц в соцсетях мужчина также распространил вредоносную программу «mt_stabile.apk» Android. С помощью этого же ПО ему удалось получить доступ к смартфону ещё одной жертвы…». ***(Владимир Кондрашов. Предприимчивый хакер организовал сервис по взлому страниц «Вконтакте» // Internetua (http://internetua.com/predpriimcsivyi-haker-organizoval-servis-po-vzlomu-stranic-vkontakte-). 03.10.2018).***

***

«Працівники Київського управління Департаменту кіберполіції Національної поліції України викрили діяльність трьох киян, які організували схему збуту інформації з обмеженим доступом та персональних даних громадян, за допомогою всесвітньої мережі Інтернет.

…Пропозиції щодо своїх послуг зловмисники розміщували на закритому Telegram-каналі, через який також відбувалося і отримання замовлень від клієнтів.

Інформацію стосовно громадян зловмисники отримували з баз даних однієї із кредитних спілок та бази Державної фіскальної служби України (ДФС). При цьому

доступ до цих баз надавали співробітники цих організацій, які входили до складу злочинної групи…

Кримінальне провадження розпочато за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України…». ***(Кіберполіція викрила злочинну групу у продажі персональних даних громадян // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-zlochinnu-grupu-u-prodazhi-personalnix-danix-gromadyan/). 16.10.2018).***

***

«Правоохранительные органы Федеративной Республики Германия направили запрос украинским полицейским об оказании международной правовой помощи по уголовному делу по факту компьютерного мошенничества.

…европейские правоохранители расследуют деятельность законспирированной группы компьютерных мошенников, которые в онлайн-магазинах покупали товары, используя ворованные данные кредитных карточек или взломанных аккаунтов PayPal, пересылали их в различные страны ЕС и там перепродавали…

Существенными признаками группы правоохранители называют её «международную направленность» и сокрытие каких-либо сведений, позволяющих идентифицировать отдельных членов группы, которые «часто знакомы друг с другом в сети только по прозвищам»…

В ходе расследования в совместной следственной группе, литовские следователи запросили информацию с «Webmoney» о том, с какого счета или на какой счет проводились платежи по одному из счетов в системе, который связывают с участником преступной группы. В результате следователи вышли на след владельца аккаунта Webmoney из Украины. При этом удалось получить некоторые личные данные владельца аккаунта…» ***(Владимир Кондрашов. Германия подозревает украинцев в масштабном компьютерном мошенничестве // Internetua (http://internetua.com/germaniya-podozrevaet-ukraincev-v-masshtabnom-kompuaternom-moshennicsestve). 19.10.2018).***

***

«Штрафом в 8,5 тысяч гривен и оплатой судебной экспертизы на 10 тысяч гривен отделался студент-программист одного из украинских вузов…

Согласно приговору, студент второго курса Харьковского национального университета радиоэлектроники в период марта-апреля этого года из корыстных побуждений с неустановленного в ходе досудебного расследования сайта умышленно загрузил в программе «Digger Money» данные своего почтового ящика и электронного кошелька. Программа автоматически сгенерировала данные обвиняемого в файлы «taskmer.exe» и «intel.exe», а парень вручную прикрепил эти файлы в файл «ID Software by Moody.V2.exe» и поместил их в архив «ID Software by Moody.V2.rar», создав, таким образом, вредоносную программу. В дальнейшем

студент загрузил созданное им ПО на один из форумов в сети, установив пароль «123».

– Согласно разработанного обвиняемым плана преступления, после запуска зараженного файла на компьютере пользователя создаются дополнительные файлы и процессы, содержащие исполняемый код со ссылкой на загрузку скрытого от пользователя запуска в операционной системе программы для использования вычислительных возможностей процессора его компьютера для осуществления алгоритмических расчетов с целью майнинга (добычи) криптовалюты «Monero» (XMR), то есть для «скрытого майнинга», – говорится в приговоре…» ***(Владимир Кондрашов. Украинского студента засудили за «интерес» к вирусу // Internetua (http://internetua.com/ukrainskogo-studenta-zasudili-za-interes-k-virusu). 16.10.2018).***

***

«…Працівники Київського управління Департаменту кіберполіції та слідчого відділу поліції Полтавщини, під процесуальним керівництвом прокуратури Полтавської області, встановили хакера який за допомогою модифікованого вірусу отриму вав несанкціонований доступ до інформації, яка зберігалася на комп'ютерах потерпілих.

Ним виявився 17-річний студент одного із техічних навчальних закладів Полтавщини. Молодик, модифікував шкідливе програмне забезпечення, після чого розповсюджував його у мережі Інтернет. Основною метою таких його дій було отримання доступу до операційних систем уражених комп'ютерів.

В подальшому, отримавши доступ до операційної системи зараженого комп'ютера, хакер мав можливість копіювати всю файлову систему, логіни та паролі в браузері, отримувати віддалений доступ до комп'ютера, здійснювати запис роботи робочого столу та вчиняти будь-які несанкціоновані дії з цього ПК…» ***(Кіберполіція викрила хакера та припинила поширення модифікованого ним вірусу // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-ta-prypynyla-poshyrennya-modyfikovanogo-nym-virusu-1257/). 19.10.2018).***

***

«…Працівниками Придніпровського управління Департаменту кіберполіції, спільно з працівниками управління інформаційних технологій та програмування у Південному регіоні та слідчого управління поліції Дніпропетровщини, під процесуальним керівництвом прокуратури Дніпропетровської області, встановили хакера, який на постійній основі створював шкідливі програмні засоби призначені для несанкціонованого втручання у роботу комп'ютерів.

Працівники кіберполіції встановили причетність до таких дій 35-річного мешканця Дніпра. Різноманітне шкідливе програмне забезпечення чоловік створював власноруч та для його розповсюдження використовував власноруч створений закритий хакерських форум та сайт, де продавав створені ним віруси. Кількість авторизованих користувачів цих ресурсів перевищувала 2,5 тисячі…

Працівниками кіберполіції вже встановлено більше пів сотні осіб, які стали жертвами злочинних дій хакера…». ***(Кіберполіція викрила хакера у розповсюдженні вірусів за допомогою власних закритих хакерських ресурсів // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakera-u-rozpovsyudzhenni-virusiv-za-dopomogoyu-vlasnix-zakritix-xakerskix-resursiv/). 26.10.2018).***

***

«Три года лишения свободы с испытательным сроком на год получил украинский хакер, взломавший сети «Интертелекома», хостинг-провайдера «СитиХост» и телеком-провайдера "Феникс ВТ". Мужчина взламывал "Интертелеком", чтобы получать безлимитный интернет.

…частный предприниматель в течение 2016-2017 годов разработал программные коды и исполняемые файлы, предназначенные для несанкционированного вмешательства в работу автоматизированных систем, компьютерных сетей ООО «Интертелеком» и других предприятий, учреждений и организаций.

…предприниматель с помощью разработанного ПО совершил несанкционированное вмешательство в работу компьютерных сетей и систем хостинг-провайдера ООО «СитиХост», что привело к утечке информации об учетных записях работников общества, о данных обмена сообщениями между работниками общества, данных о серверном оборудовании компании, данных, которые хранились на компьютерах, находящихся в локальной сети компании, логинов и паролей работников общества, логинов и паролей к учетным записям пользователей, логинов и паролей к компьютерам и серверам компании, биллинговых программ.

Кроме того, мужчина несколько раз совершил несанкционированное вмешательство в работу компьютерных сетей и систем ООО «Интертелеком», что привело к утечке информации вышеуказанного общества…

Еще один доказанный следствием эпизод – несанкционированное вмешательство в работу компьютерных сетей и систем провайдера «Феникс ВТ», что привело к утечке информации вышеуказанного предприятия, а именно – информации об обмене сообщениями почтового клиента между работниками общества, клиентами и заказчиками, а также информации о программном обеспечении 1С:Бухгалтерия с сохраненными данными учетных записей и данными компании, то есть файлов, которые хранились в отдельных базах данных ЧПФ «Феникс ВТ»…» ***(Владимир Кондрашов. Хакер получил условный срок за неоднократный взлом «Интертелекома» // Internetua (http://internetua.com/haker-poluchil-uslovnyi-srok-za-neodnokratnuy-vzlom-intertelecoma). 26.10.2018).***

***

«Украинские полицейские ищут распространителя вредоносного программного обеспечения, позволяющего несанкционированно вмешиваться

в работу мобильных Android-устройств для последующего списания денежных средств с банковских счетов и электронных кошельков пораженных смартфонов.

…ранее …два студента, 24-летний волынянин и 19-летний уроженец Херсонщины, получили условные сроки за разработку мобильного приложения, которое под видом приложения для знакомств «ДругВокруг» получало доступ к банковским счетам пользователей мобильного банкинга и передавало эти данные злоумышленникам.

Студенты разработали и распространяли вредоносное ПО «SexDrugWokrug.apk»…

Несмотря на то, что создатели приложения ещё в марте получили приговоры по 3 года лишения свободы с освобождением от отбывания наказания и испытательным сроком в 2 года и конфискацией орудий преступления… досудебным расследованием установлено, что в период с 9 августа этого года по настоящее время установленное следствием лицо, используя возможности всемирной сети Интернет и путем создания собственных сайтов, распространяет это вредоносное ПО.

Также удалось выяснить, что житель Житомирской области совместно с неустановленными лицами, «создает и распространяет вредоносное программное обеспечение, осуществляющее несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), и приводит к утечке и искажение процесса информации»…

Следствие на данный момент продолжается». ***(Владимир Кондрашов. Украинские хакеры украли банковские данные с помощью приложения для знакомств // Internetua (http://internetua.com/ukrainskie-hakery-ukrali-bankovskie-dannye-s-pomosxua-prilojeniya-dlya-znakomstv). 25.10.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Міністр закордонних справ України Павло Клімкін на конференції "Втручання у вибори в цифрову епоху" у Брюсселі закликав використовувати всесторонній підхід у боротьбі з кіберзагрозами…

Виступаючи в Брюсселі, Клімкін закликав підвищувати поінформованість населення щодо кіберзагроз, мати чітку та сміливу стратегію, а також вирішити проблему інформаційної безпеки всебічно…» ***(Саша Картер. Клімкін у Брюсселі взяв участь у конференції щодо кібервтручання у вибори // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1757780-klimkin-u-bryusseli-vzyav-uchast-u-konferentsiyi-schodo-kibervtruchannya-u-vibori). 16.10.2018).***

***

«Спільну програму системної взаємодії проти тероризму та кіберзлочинності домовились розробити міністр внутрішніх справ України

Арсен Аваков та міністр внутрішніх справ Австралії Пітер Даттон під час робочої поїздки української сторони до Австралії…

«Україна – перший полігон, де Росія випробовує свої гібридні технології, і ми маємо великий досвід, як від них відбиватися. У цьому конфлікті є і «шукачі пригод» із Австралії, які увійшли до складу незаконних збройних формувань. Такі люди, які отримали досвід участі у гібридних конфліктах, так само небезпечні і для вашого суспільства, адже є носіями специфічної інформації, яка може шкодити національній безпеці на користь агресивним діям РФ…», - зазначив Арсен Аваков…

Міністр внутрішніх справ Пітер Даттон зазначив, що Австралія вже входить в так звану організацію «П'яти очей» із США, Канадою, Новою Зеландією та Великою Британією, проте зацікавлена розширювати співробітництво…» ***(Арсен Аваков: МВС України та Австралії спільно протидіятимуть траснкордонним кіберзагрозам // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/arsen-avakov-mvs-ukrajini-ta-avstraliji-spilno-protidiyatimut-trasnkordonnim-kiberzagrozam/). 24.10.2018).***

***

«Міністр внутрішніх справ України Арсен Аваков і міністр внутрішніх справ Сінгапуру Касивисванатхан Шанмугам під час офіційної зустрічі 29 жовтня в Сінгапурі обговорили гібридні загрози в сучасному світі і домовилися про співпрацю підрозділів кіберполіції…

В ході зустрічі сторони підписали спільну заяву про поглиблену співпрацю в сфері безпеки і домовилися вивчити можливості подальшого розвитку взаємодії, співпраці та обміну досвідом в сфері забезпечення національної безпеки з метою боротьби з тероризмом, транснаціональною організованою злочинністю, кіберзлочинами, торгівлею людьми...» ***(Іра Огнєва. Україна і Сінгапур спільно протидіятимуть світовим кіберзагрозам // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1759905-ukrayina-i-singapur-spilno-protidiyatimut-svitovim-kiberzagrozam). 29.10.2018).***

***

Світові тенденції в галузі кібербезпеки

«Близько 55% керівників компаній у світі усвідомлюють, що рано чи пізно кіберзлочинці атакують їхній бізнес…

Такі результати дослідження KPMG, проведеного влітку цього року. В опитуванні взяли участь 1150 керівників бізнесу з усього світу.

У 2017 році у США кіберкрадіжки були визнані злочином, що набув найбільшого поширення. Економічні втрати за підсумками 2016 року оцінюють в 450 млрд доларів, а до 2021 року ця сума може вирости до 6 трлн доларів.

Майже половина усіх кібератак спрямована на малий та середній бізнес…

За прогнозами компанії Cybersecurity Ventures, до 2019 року компанії ставатимуть жертвами ransomware-атак кожні 14 секунд…

При цьому кіберзлочинці часто використовують давно відомі вразливості, для усунення яких існують патчі, або проникають в мережі компаній шляхами, для яких є елементарні форми захисту. Що казати, якщо 4% користувачів Інтернету досі відкривають мейли і вкладені файли від невідомих осіб…». ***(Андрій Слободяник. Кібератаки малого та середнього бізнесу: як вижити // Економічна правда (https://www.epravda.com.ua/columns/2018/10/5/641243/). 05.10.2018).***

***

«Cisco обнародовала результаты исследования по кибербезопасности среди компаний малого и среднего бизнеса в рамках Cisco 2018 Security Capabilities Benchmark, в котором приняли участие 1816 респондентов из 26 стран…

В ходе исследования 53% респондентов заявили, что их компании подвергались вторжениям, повлекшим существенные финансовые издержки. Например, кибератаки часто провоцируют простой рабочих систем, в результате чего снижаются продуктивность и прибыльность бизнеса…

30% средних компаний сообщили, что вторжения обошлись им менее чем в 100 тыс. долл., тогда как 20% назвали суммы от 1 млн до 2,5 долл. Компании СМБ получают от систем безопасности до 5 тыс. уведомлений в день, при этом средние компании расследуют 55,6% уведомлений…

На фоне всеобщей озабоченности программами-вымогателями эксперты Cisco полагают, что значимость этой угрозы уменьшается в связи с тем, что все больше злоумышленников переключаются на незаконную добычу криптовалют…

Борясь с угрозами, компании инвестируют в технологии и кадры. При наличии достаточных кадровых ресурсов, прежде всего, решались бы следующие задачи: самый частый ответ — модернизация защиты оконечных точек с применением решений AMP/EDR (Advanced Malware Protection/Endpoint Detection and Response) — 19%; внедрение более совершенных приложений для защиты от веб-атак — 18%; внедрение технологии предотвращения вторжений, которая по-прежнему рассматривается в числе необходимых для отражения сетевых атак и внедрения эксплойтов — 17%...

Небольшие компании также присматриваются к решениям, необходимым для защиты современной рабочей среды, которая характеризуется непрерывным ростом числа мобильных устройств в сетях предприятий и внедрением облачных сервисов. В последние годы средний бизнес наращивает использование облачных сервисов: если в 2014 г. часть своих сетей в облаке размещали 55% компаний, то в 2017 г. их доля выросла до 70%...» ***(Более половины предприятий СМБ подвергались кибератакам в этом году // «Компьютерное Обозрение» (https://ko.com.ua/bolee_poloviny_predpriyatij_smb_podvergalis_kiberatakam_v_jetom_godu_126448). 19.10.2018).***

***

«Мировые расходы на информационные технологии в 2018 году вырастут на 4,5% и приблизятся к 3,7 трлн долларов США. В 2019 году

ожидается прибавка еще на 3,2%, с учетом которой объем рынка в денежном исчислении превысит 3,8 трлн долларов. Об этом сообщается в свежем исследовании аналитической компании Gartner.

Самым быстрорастущим направлением в ИТ-отрасли специалисты называют корпоративное ПО. В 2018 году выручка от продажи программного обеспечения предприятиям поднимется на 9,9%, до 405 млрд долларов, а в 2019-м прогнозируется рост на 8,3%, до 439 млрд долларов.

Движущей силой внутри категории будут облачные SaaS-сервисы (Software as a service, ПО как услуга), в том числе решения для управления взаимодействием с клиентами (CRM). В целом сегмент облачного ПО в 2018 году вырастет на 22%...

Более выраженный подъем, чем по ИТ-рынку в целом, ожидается в сегменте ИТ-услуг. В 2018 году мировые затраты на этом направлении увеличатся на 5,9% до 987 млрд долларов, а в 2019-м преодолеют отметку в 1 трлн долларов (+4,7%)…» ***(Мировые ИТ-расходы в 2019 году превысят 3,8 трлн долларов // Goodnews.ua (http://goodnews.ua/technologies/mirovye-it-rasxody-v-2019-godu-prevysyat-38-trln-dollarov/). 22.10.2018).***

***

Сполучені Штати Америки та Канада

«В части материнских плат, произведенных в Китае для государственных и частных компаний США, обнаружили микрочипы для шпионажа…

По данным Bloomberg, продавать оборудование с чипами могла компания Super Micro Computer Inc. из Кремниевой долины, которая сотрудничает с китайскими поставщиками. К 2015 году, когда следы шпионажа были обнаружены впервые, у нее было более 900 клиентов в 100 странах…

Потайные чипы на материнских платах размещала специальная служба армии Китая... Разведчики использовали для этого взятки и угрозы, добиваясь от производителей изменений в оригинальной конструкции плат. Чипы размещались рядом с контроллером, что позволяло получить удаленный доступ к памяти компьютера» ***(Анна Полякова. Bloomberg: Китайские производители вставляли чипы-шпионы в материнские платы для компаний США // Rusbase (https://rb.ru/news/spy-microchips-for-usa/). 04.10.2018).***

***

«В министерстве внутренней безопасности США поддержали заявления Amazon, Apple, Super Micro Computer и других американских технологических компаний о том, что в материнских платах их серверов не было чипов, которые якобы использовались для шпионажа спецслужбами КНР.

…по данным сотрудников службы безопасности, заражение компьютерных систем, которое исходило от серверов, собранных Super Micro Computer в Сан-

Хосе, было обнаружено в ходе расследования ФБР. Министерство не участвует в таких расследованиях, пояснили источники агентства…» ***(Мария Салтыкова. Власти США отрицают попытки китайских спецслужб шпионить на серверах Apple и Amazon // Rusbase (https://rb.ru/news/US-denial-spies/). 07.10.2018).***

***

«…Сегодня New York City Economic Development Corporation (NYCEDC) объявила о запуске Cyber NYC, 30-миллионном стартапе, "стимулирующем" приток инвестиций, направленных на быстрое развитие экосистемы города и инфраструктуры для кибербезопасности…

По оценкам NYCEDC, в Нью-Йорке работают около 6000 специалистов по кибербезопасности. Посредством этих программ число может увеличиться еще на 10 000 человек…

Для достижения заявленных целей в области кибербезопасности NYCEDC сотрудничает с двумя венчурными фирмами, Jerusalem Venture Partners (JVP) и SOSA. JVP является постоянным инвестором, который должен помочь учредителям в Hub.NYC получить доступ к капиталу, а также отраслевой и предпринимательский опыт…

"Global Cyber Center станет основным центром для всей индустрии кибербезопасности, где эксперты из Нью-Йорка, Штатов, Израиля и других стран смогут встречаться, взаимодействовать и общаться", - прокомментировал генеральный директор SOSA Узи Схеффер…» ***(Ирина Фоменко. Нью-Йорк хочет создать киберармию // Internetua (http://internetua.com/nua-iork-hocset-sozdat-kiberarmiua). 03.10.2018).***

***

«Пентагон не поспішає захищати свої основні системи озброєнь від кібератак і регулярно виявляє в них критичні уразливості, якими можуть скористатися хакери. Про це йдеться в доповіді Рахункової палати США (U.S. Government Accountability Office, GAO)…

Крім цього, відомство відзначає, що Пентагон також виявляє “уразливості в системах озброєнь”, які знаходяться в стадії розробки.

При цьому в документі підкреслюється, що кіберзагрози стають все витонченішими, що загрожує Пентагону більш серйозними проблемами, оскільки сучасні види озброєнь стають все більше комп’ютеризовані…» ***(Самуїл Проскуряков. Рахункова палата США дорікнула Пентагону в слабкому захисті зброї від кібератак // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1756712-rakhunkova-palata-ssha-doriknula-pentagonu-v-slabkomu-zakhisti-zbroyi-vid-kiberatak). 10.10.2018).***

***

«…Представители некоммерческой организации «Фонд электронных рубежей» (Electronic Frontier Foundation, EFF) направили письмо в Офис Генерального прокурора штата Техас с требованием обратить внимание на

недобросовестную практику компании Epson, которая выводит из строя чернильные картриджи сторонних производителей с помощью кода, встроенного в обновления прошивки принтеров.

Своими действиями производитель вводит в заблуждение клиентов, сначала уверяя, что принтеры могут работать со сторонними картриджами, а затем саботируя последние спустя несколько месяцев во время обновления прошивки, считают специалисты. Данная практика не только наносит финансовый ущерб потребителям, которые вынуждены приобретать более дорогие картриджи Epson, но и представляет риск с точки зрения кибербезопасности, поскольку многие владельцы принтеров просто не устанавливают выпущенные производителем патчи из опасений, что они выведут картриджи из строя. Таким образом миллионы принтеров остаются уязвимыми к кибертакам, с помощью которых злоумышленники могут получить доступ к внутренним сетям организаций и похитить конфиденциальные сведения, например, секретную коммерческую информацию или персональные данные сотрудников.

Эксперты EFF назвали действия компании «вводящими в заблуждение, антиконкурентными и опасными» и призвали власти начать расследование по данному вопросу. Представители Epson пока никак не прокомментировали ситуацию». ***(Epson обвинили в саботаже чернильных картриджей сторонних компаний // SecurityLab.ru (https://www.securitylab.ru/news/495977.php). 17.10.2018).***

***

«Представитель Пентагона подполковник Джозеф Буччино рассказал о проводимом ведомством расследовании утечки личных данных сотрудников. Он сообщил Reuters, что данные были украдены в результате хакерской атаки на компанию, которая предоставляла Пентагону услуги.

Утечка была обнаружена 4 октября. Военный отметил, что речь идет о данных небольшого числа работников Министерства обороны США…». ***(Пентагон расследует утечку личных данных сотрудников // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3770847). 13.10.2018).***

***

«В течение прошлого года канадские частные компании потратили на кибербезопасность 14 млрд долларов.

Об этом говорится в новом опросе Статистического агентства Канады…

Из этой суммы 8 млрд долл. было потрачено на зарплаты экспертов и консультантов, 4 млрд было вложено в обновление соответствующего программного обеспечения и оборудования, а остальные 2 млрд ушли на другие методы защиты и восстановления после него.

При этом в прошлом году какой-либо кибератаке подверглась каждая пятая канадская компания. “Из тех компаний, которые подверглись нападению, 39% не могли определить его мотив, 38% заявили, что злоумышленники пытались похитить деньги или требовали выкуп. Четверть предприятий подверглись кибератаке, имевшей целью получение неавторизованного доступа, и еще у 23%

бизнесов воры пытались похитить личную или финансовую информацию", – отмечает Статистическое агентство…» ***(В Канаде за год потратили $14 млрд на кибербезопасность // Finance.ua (https://news.finance.ua/ru/news/-/436592/v-kanade-za-god-potratili-14-mlrd-na-kiberbezopasnost). 16.10.2018).***

***

«..После аудита генеральный инспектор Министерства внутренних дел обнаружил, что сеть Геологической службы США (USGS) в EROS Center в Южной Дакоте была заражена после того, как один из сотрудников посетил тысячи страниц с порно, где были вредоносные программы.

Исследователи выяснили, что многие из порноизображений "сотрудник сохранил на несанкционированное устройство USB и персональный мобильный телефон Android", который был подсоединен к правительственному компьютеру. Смартфон также оказался заражен вредоносным ПО. В Министерстве внутренних дел не сообщили о дальнейшей судьбе сотрудника.

"Мы идентифицировали две уязвимости в средствах обеспечения безопасности сети Геологической службы США: доступ к веб-сайтам и открытые порты USB", - говорится в отчете…». ***(Ирина Фоменко. Служащий из-за просмотра порно заразил госсеть вредоносным ПО // Internetua (http://internetua.com/slujasxii-iz-za-prosmotra-porno-zarazil-gosset-vredonosnym-po). 30.10.2018).***

***

Країни ЄС

«Саміт ЄС закликав до посилення боротьби з кіберзлочинністю і запобігання кібератакам шляхом запровадження обмежувальних заходів…

"Європейська рада закликає до заходів з протидії незаконній і зловмисній кіберактивності і побудови міцної системи кібербезпеки. Потрібна подальша робота над здатністю реагувати та запобігати кібератакам шляхом обмежувальних заходів ЄС" - йдеться у документі.

Лідери ЄС підкреслили, що всі пропозиції щодо посилення кібербезпеки мають бути підготовленні до завершення каденції Європарламенту.

Також саміт ЄС підкреслив необхідність захистити демократичні системи ЄС і протидіяти дезінформації у контексті виборів до Європарламенту навесні наступного року…» ***(Лідери ЄС закликали продовжити роботу над підготовкою санкцій за кібератаки // Європейська правда (https://www.eurointegration.com.ua/news/2018/10/18/7088345/). 18.10.2018).***

***

«Великобритания опубликовала кодекс безопасности для производителей домашних устройств, которые подключены к интернету. Он направлен на то, чтобы защитить устройства, которые используются для кибератак, и искоренить преступления, когда хакеры крадут данные пользователей.

Инициатива правительства в первую очередь направлена на производителей небольших умных гаджетов для дома, таких как дверные звонки, камеры, игрушки и охранные сигнализации…

Документ был разработан Департаментом по цифровым технологиям, культуре, СМИ и спорту и Национальным центром кибербезопасности. Он включает в себя 13 шагов, которые производители могут предпринять для изготовления более безопасных продуктов. Это зашифрованное хранение данных клиентов, регулярное обновление программного обеспечения, требование к пользователям выбирать более надежные пароли и еще несколько десятков пунктов…» ***(В Великобритании выпустили инструкцию для защиты устройств от взлома // Goodnews.ua (http://goodnews.ua/technologies/v-velikobritanii-vypustili-instrukciyu-dlya-zashhity-ustrojstv-ot-vzloma/). 17.10.2018).***

***

«Германский страховщик Munich Re реально оценивает перспективы роста глобальных кибер-рисков, предлагая своим клиентам не только страховые продукты и услуги, но и рекомендации относительно предотвращения кибернетических потерь.

…По оценкам, объем рынка киберстрахования к 2020 году составит около $8-9 млрд, что вдвое больше показателя 2017 года…

Наряду с страховой защитой, предложение Munich Re включает в себя услуги, связанные с техническим анализом, профилактическими мерами, постоянным пересмотром стандартов безопасности технического оборудования, экспертными расследованиями после потери и восстановлением данных. …для реализации этих задач Munich Re сотрудничает с рядом технологических компаний». ***(Munich Re о киберстраховании: это не только вызов, но и новые возможности // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/munich-re-o-kiberstrahovanii-eto-ne-tolko-vyizov-no-i-novyie-vozmozhnosti). 23.10.2018).***

***

Китай

«…1 ноября 2018 года в КНР вступит в силу закон, наделяющий правоохранительные органы широкими полномочиями на проведение проверок в компаниях, работающих в сфере информационных технологий, в том числе правом получать доступ и копировать данные, имеющие отношение к кибербезопасности.

Согласно новым правилам, полицейские органы, как местного, так и центрального уровня, смогут проводить физический досмотр офисных помещений и аппаратных компаний, предоставляющих интернет-услуги, проверять применение и функционирование защитных мер, а также получать удаленный доступ в корпоративные сети для анализа на предмет возможных уязвимостей. В

последнем случае полиция обязана заблаговременно уведомить компанию о предстоящей проверке, чтобы не нарушить работу сети…

Согласно документу, полицейские проверки будут касаться различных аспектов: хранения компаниями регистрационных данных пользователей и записей журналов, реализации мер защиты от вредоносного ПО и взломов, обеспечения мер предосторожности против распространения запрещенной информации, сотрудничества с правоохранительными органами в сфере обеспечения национальной безопасности, технического содействия в ходе расследования террористической деятельности и других преступлений и пр.

Закон распространяется на территории, офисы и помещения аппаратных поставщиков услуг в сети Интернет - от провайдеров информационных сервисов до интернет-кафе и центров обработки данных» ***(Китайская полиция получила право копировать данные интернет-компаний // SecurityLab.ru (https://www.securitylab.ru/news/495827.php). 09.10.2018).***

***

Російська Федерація та країни ЄАЕС

«…У Росії вирішили чіпувати військовослужбовців. Про це повідомив міністр оборони РФ Сергій Шойгу…

За словами російського міністра, армію РФ мають намір оснастити автоматизованою системою «Паспорт», основа якої — біометричні параметри людини. У відомстві стверджують, що такий підхід дозволить видавати військовим «персональні електронні карти із вбудованим чіпом замість військового квитка».

Разом із тим експерти вказують на вразливість персональних біометричних даних російських військових, зібраних в єдину базу. У разі щонайменшого просочування інформації дані всіх військовослужбовців РФ можуть виявитися уразливими для кібератак…» ***(У Росії вирішили зібрати біометричні дані всіх військовослужбовців // Громадсько-правовий портал «Ракурс» (http://racurs.ua/ua/n112421-u-rosiyi-vyrishyly-zibraty-biometrychni-dani-vsih-viyskovoslujbovciv). 10.10.2018).***

***

«Нове розслідування журналістів перетворилося в шпигунський скандал. …база ГРУ доступна будь-якому користувачеві має доступ до бази ГИБДД.

Там всі співробітники вказані з усіма паспортними даними та мобільними телефонами, місцем роботи. По суті це означає, що будь-яка людина з доступом до базі ГИБДД (а це одна з найбільш доступних баз даних) може отримати імена, паспортні дані та мобільні телефони кількох сотень співробітників ГРУ. Причому не простих співробітників, а службовців саме тій самій військовій частині, яку звинувачували в найскандальніших хакерських атак останніх років…». ***(300 і ще 5: Журналісти розкрили імена найбільш засекречених співробітників ГРУ //***

znaj.ua (https://znaj.ua/world/178659-300-i-shche-5-zhurnalisti-rozkrili-imena-naybilsh-zasekrechenih-spivrobitnikiv-gru). 06.10.2018).

***

«Вчора долар на Московській біржі здорожчав на 1 рубль 19 копійок, вперше за два тижні переваливши за позначку 67 рублів. За євро платять більш як 77 рублів.

Акції Сбербанку впали на 4,5%, а біржовий індекс РТС втратив майже 3%.

Облігації російського уряду встановили місячний рекорд дешевизни.

А причиною обвалу стало масове викриття керованих Кремлем російських хакерів та їхньої підготовки нових масових кібератак по світу…» ***(Шпигунський скандал обрушив рубль і акції російських компаній // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20181005-shpygunskyj-skandal-obrushyv-rubl-i-aktsiyi-rosijskyh-kompanij/). 05.10.2018).***

***

«В Group-IB считают, что всего одна успешная кибератака может привести как к ликвидации самой кредитно-финансовой организации, так и коллапсу финансовой системы государства.

Ежемесячно от кибератак теряют деньги один-два банка, ущерб от одного успешного хищения составляет в среднем 2 млн долл… Ущерб российской финансовой сферы от кибератак за 2017-й и 2018 год в Group-IB оценили в 2,96 млрд руб.

В отчете выделяются четыре преступные хакерские группы, представляющие реальную угрозу для финансового сектора — это группы Cobalt, MoneyTaker, Silence, а также северокорейская Lazarus. Как заявили в Group-IB, они способны не только проникнуть в сеть банка, добраться до изолированных финансовых систем, но и успешно вывести деньги через SWIFT, АРМ КБР, карточный процессинг и банкоматы…» ***(Российская финансовая сфера за два года потеряла из-за кибератак 3 миллиарда рублей // «Открытые системы» (https://www.computerworld.ru/news/Rossiyskaya-finansovaya-sfera-poteryala-iz-za-kiberatak-3-milliarda-rubley). 09.10.2018).***

***

«Глава Сбербанка Герман Греф считает целесообразным создать в России министерство по чрезвычайным ситуациям в цифровой сфере... Такое ведомство должно контролировать чрезвычайные ситуации в цифровой сфере, которая коснется всей инфраструктуры без исключения, пояснил он…» ***(Герман Греф предложил создать «МЧС» в цифровой сфере // «Открытые системы» (https://www.computerworld.ru/news/Glava-Sberbanka-predlozhil-sozdat-MChS-v-tsifrovoy-sfere). 04.10.2018).***

***

«Число целевых хакерских атак на российские финансово-кредитные организации за первый и второй кварталы текущего года выросло почти

вдвое — до 72 против 39 годом ранее. При этом количество успешных атак снизилось, говорится в отчете Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России (ФинЦЕРТ).

«За 8 месяцев 2017 года кредитные организации потеряли 1 078 762 345 руб., а за аналогичный период 2018 года — 76 495 882 рублей. Количество успешных атак составило 22 и 20 случаев соответственно»,— подсчитали в ФинЦЕРТ.

Снижение ущерба в Банке России объясняют как деятельностью групп по реагированию на чрезвычайные ситуации, так и повышением уровня кибербезопасности банков. «Значительная часть фишинговых писем отфильтровывается на почтовом шлюзе и иными компонентами систем защит, в результате чего вредоносное письмо не доходит до получателя»,— говорится в отчете.

Также, как отмечают специалисты, на снижение ущерба повлияло задержание в Испании в марте 2018 года одного из руководителей группы киберпреступников, известной как Cobalt Group. Однако эта группа продолжает деятельность, атаки с использованием программного обеспечения Cobalt Strike не прекратились.

Дополняется, что интерес преступников смещается от банков в сторону их клиентов — юридических лиц…» ***(ЦБ зафиксировал рост числа кибератак на российские банки // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3773470). 18.10.2018).***

***

«Концерн «Автоматика», принадлежащий Ростеху, запустил производство серверов «Эльбрус-804», построенных на базе восьмиядерных процессоров «Эльбрус-8С».

Пиковая вычислительная мощность сервера составляет 920 гигафлопс одинарной точности и 460 гигафлопс двойной точности…

Сервер работает на отечественной сертифицированной ОС «Эльбрус», которая, по заверениям производителя, гарантирует защиту от несанкционированного вмешательства…» ***(Алексей Дегтярев. Ростех заявил о начале производства устойчивых к кибератакам серверов // Деловая газета «Взгляд» (https://vz.ru/news/2018/10/16/946369.html). 16.10.2018).***

***

«В национальный проект «Цифровая экономика» внесена новая инициатива, согласно которой небольшие компании могут быть подключены к системе ГосСОПКА…

В случае присоединения к ГосСОПКА малые компании смогут обмениваться данными о современных киберугрозах в автоматизированном режиме. Также малому бизнесу, согласно плану, откроются смежные услуги и сервисы… Сам проект должен стартовать 1 ноября этого года…» ***(Олег Иванов. Небольшие компании могут подключить к ГосСОПКА // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2018-10-17-1447/27764). 17.10.2018).***

***

«…Директора по информационной безопасности в российских компаниях испытывают недостаток ресурсов для эффективного противостояния угрозам в киберпространстве. К такому выводу пришли специалисты «Лаборатории Касперского» по результатам опроса 250 директоров по ИБ по всему миру, проведенному в июле нынешнего года (40 из них были из РФ и Казахстана).

Только 5% директоров по ИБ в российских компаниях сообщили о своем участии в принятии ключевых решений относительно компании, в том числе в планировании бюджета. Остальные же 95% уверены в неизбежности инцидентов безопасности…

На вопрос о возможных изменениях бюджета на обеспечение кибербезопасности в ближайшем будущем директора по ИБ в российских компаниях склонны к пессимистическим прогнозам. 48% из них не ожидают никаких изменений в бюджете, а 15% даже готовятся к сокращению финансирования. Только 38% опрошенных ожидают увеличения бюджета на обеспечение кибербезопасности.

Специалисты объясняют это невозможностью гарантировать руководству компаний стопроцентной защиты от киберугроз…

Помимо финансирования, большую проблему представляет нехватка квалифицированных кадров. По словам 85% опрошенных, когда дело доходит до поиска сотрудников, найти подготовленного специалиста крайне тяжело» ***(Директора по ИБ в российских компаниях ожидают снижения финансирования кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/496201.php). 29.10.2018).***

***

Інші країни

«Сингапурская глобальная инвестиционная компания Temasek и израильская консалтинговая фирма Sygnia, занимающаяся вопросами кибербезопасности, объявили во вторник, что они заключили сделку. Израильский стартап был приобретен на сумму около 250 миллионов долларов.

…сделка подчеркивает «растущее значение кибербезопасности для инвесторов во всем мире», и что Израиль в этой отрасли занимает первое место.

Основанная в 2015 году, в Тель-Авиве, Sygnia в первую очередь уделяет внимание вопросам консультирования по кибербезопасности и реагированию на сложные ситуации…» ***(Сингапурская компания укрепила свою кибербезопасность, купив израильский стартап // ISRAland Online Ltd (http://www.isra.com/news/221442). 17.10.2018).***

***

«Викрито причетність російської військової розвідки до кампанії кібератак». З таким заголовком зранку 4 жовтня з'явилася заява на сайті Національного центру кібербезпеки Великої Британії. Британський міністр закордонних справ Джеремі Хант заявив — ідеться про причетність російського ГРУ до хакерських атак в Об'єднаному Королівстві, США, Малайзії, Швейцарії і Нідерландах…

Того ж дня Нідерланди, Сполучені Штати і Канада одна за одною назвали РФ винною в потужних кібератаках…

Окремої уваги заслуговує втручання російської розвідки в спортивні й антидопінгові організації, яке тривало від 2014 року.

США представили розширений список обвинувачених: до чотирьох названих раніше нідерландською стороною долучилися Іван Єрмаков, Артем Малишев і Дмитро Бадін. «Серед жертв, в які цілило ГРУ, були міжнародні антидопінгові агентства, спортивні федерації та їхні представники, інші пов'язані зі спортом організації, а також близько 250 атлетів з 30 країн світу», — зазначається в документі Окружного суду США Західного округу Пенсильванії.

Серед масштабних організацій, які зазнали нападу та викрадення даних — Антидопінгове агентство Сполучених Штатів, Світове антидопінгове агентство (САДА), Міжнародна асоціація федерацій легкої атлетики, Спортивний арбітражний суд і навіть Міжнародна федерація футбольних асоціацій (ФІФА).

У цих звинуваченнях до США долучилася та Канада. На її Канадський центр спортивної етики теж атакували. Пізніше й очільник Міжнародного олімпійського комітету (МОК) Томас Бох заявив, що організація впродовж останніх років була ціллю для численних кібератак…

Іще одна атака, ймовірно пов'язана з Україною — енергетична. Російські хакери зламали також і мережу компанії Westingshouse, яка постачала ядерне паливо, зокрема й Україні…

У США заявили: підозрюваний Іван Єрмаков, якого спецпрокурор Роберт Мюллер назвав причетним до втручання в американські президентські вибори 2016 року, зламав систему Westingshouse з метою дістатися до IP-адрес, доменів і мереж у період з 2014 року. У грудні 2014 хакери зареєстрували фейковий домен і сайт та розіслали листи «з гачком» щонайменше п'яти робітникам — через них і добралися до мережі компанії…

Це не всі звинувачення: росіянам закидають також викрадення персональних даних і паролів користувачів, а також відмивання коштів за допомогою криптовалют. Сполучені Штати оприлюднили докладну біографію кожного з обвинувачених і заявили, що мають докази їхньої причетності до ГРУ…». ***(Олена Куренкова. Кібератаки глобального масштабу: кого і чому атакували російські хакери // Громадське Телебачення (https://hromadske.ua/posts/koho-i-chomu-atakuvaly-rosiiski-khakery). 05.10.2018).***

***

«Британське військове командування готове відповісти кібератаками на можливу агресію РФ проти країн Заходу.

Як зазначається, якщо не брати до уваги використання ракет з ядерними боєголовками Trident, Британія не має достатнього потенціалу зброї для протистояння Росії. У зв'язку з цим уряд прийшов до висновку розвивати потенціал у кіберпросторі, щоб мати можливість «відключити світло у Кремлі».

Передбачається, що це дасть Лондону більше варіантів, якщо Росія вирішить захопити невеликі острови Естонії, щоб потестувати на міцність статтю 5 або вторгнеться в Лівію, щоб встановити контроль над нафтовими запасами і спровокувати нову міграційну кризу в Європі, або використає нерегулярні війська щоб вчинити атаку на британських військових чи пригрозить новому авіаносцю…» ***(Лондон готовий відповісти кібератаками на агресію Росії, – The Sunday Times // Західна інформаційна корпорація (https://zik.ua/news/2018/10/07/london_gotovyy_vidpovisty_kiberatakamy_na_agresiyu_rosii__the_sunday_times_1421843). 07.10.2018).***

***

«Нідерланди заявляють, що росіяни планували проникнути в мережу Організації із заборони хімічної зброї. Окрім того, вони мали намір отримати дані розслідування щодо збиття літака рейсу MH17.

Міністерка оборони Нідерландів Анк Бейлевельд у четвер, 4 жовтня, заявила про вислання чотирьох російських шпигунів у зв'язку із запланованою кібератакою. Йдеться про кібернапад на базовану в Гаазі Організацію із заборони хімічної зброї (ОЗХЗ), якому влада Нідерландів запобігла… Росіян вислали ще в квітні, зазначила Бейлевельд. Розвідка країни опублікувала фото та імена чотирьох осіб.

Вислані прибули до Нідерландів 10 квітня і неодноразово були помічені поблизу штаб-квартири ОЗХЗ. 13 квітня їх затримали, а в багажнику винайнятого ними автомобіля було виявлено пристрої, необхідні для здійснення хакерських атак.

Розслідування показало, що росіяни також планували кібератаку в Швейцарії на лабораторію ОЗХЗ. Окрім того, хакери мали намір отримати доступ до матеріалів розслідування щодо збиття у 2014 році над Донбасом літака рейсу MH17 "Малайзійських авіаліній"…» ***(Нідерланди вислали чотирьох росіян через підозру в плануванні кібератаки // Deutsche Welle (https://www.dw.com/uk/%D0%BD%D1%96%D0%B4%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D0%B8-%D0%B2%D0%B8%D1%81%D0%BB%D0%B0%D0%BB%D0%B8-%D1%87%D0%BE%D1%82%D0%B8%D1%80%D1%8C%D0%BE%D1%85-%D1%80%D0%BE%D1%81%D1%96%D1%8F%D0%BD-%D1%87%D0%B5%D1%80%D0%B5%D0%B7-%D0%BF%D1%96%D0%B4%D0%BE%D0%B7%D1%80%D1%83-%D0%B2-%D0%BF%D0%BB%D0%B0%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%96-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B8/a-45752331). 04.10.2018).***

***

«Спільна заява Президента Європейської Ради Дональда Туска, Президента Європейської Комісії Жан-Клода Юнкера та Високої представниці ЄС із закордонних справ і безпекової політики Федеріки Могеріні щодо російських кібератак

У квітні Головне розвідувальне управління Росії (ГРУ) провело ворожу кібероперацію проти офісів Організації із заборони хімічної зброї (ОЗХЗ) в Гаазі. Розвідка Нідерландів у співпраці із Об'єднаним Королівством стали на заваді цій операції.

Окрім того, сьогодні, 4 жовтня, уряд Великобританії повідомив, що він виявив таке: безліч кібер-суб'єктів, які, як відомо, вчиняють кібератаки по всьому світу, насправді є Головним розвідувальним управлінням Росії (ГРУ).

Ми серйозно стурбовані цією спробою підірвати репутацію Організації із заборони хімічної зброї (ОЗХЗ). Вона є шанованою міжнародною інституцією, що знаходиться у Нідерландах. Цей агресивний акт показав зневагу до важливої мети ОЗХЗ. Відповідно до мандату Організації Об'єднаних Націй, вона прагне викорінити зброю в усьому світі.

Ми засуджуємо такі дії. Вони підривають міжнародне право та міжнародні інституції. Євросоюз продовжить зміцнювати стійкість власних інституцій та інституцій своїх країн-членів, а також міжнародних партнерів та організацій у цифровій сфері». ***(Спільна заява лідерів ЄС щодо російських кібератак // Представництво Європейського Союзу в Україні (https://eeas.europa.eu/delegations/ukraine/51640/%D1%81%D0%BF%D1%96%D0%BB%D1%8C%D0%BD%D0%B0-%D0%B7%D0%B0%D1%8F%D0%B2%D0%B0-%D0%BB%D1%96%D0%B4%D0%B5%D1%80%D1%96%D0%B2-%D1%94%D1%81-%D1%89%D0%BE%D0%B4%D0%BE-%D1%80%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B8%D1%85-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_uk). 04.10.2018).***

***

«Головне розвідувальне управління РФ за останній рік провело кілька атак в кіберпросторі Латвії, в тому числі проти держустанов, пов'язаних з оборонним сектором та МЗС.

Про це заявило латвійське Бюро із захисту Конституції…

У латвійський кіберпростір вторгалася група російських хакерів, яка атакувала Організацію по забороні хімічної зброї, Міжнародне антидопінгове агентство і малайзійські органи, що займаються розслідування катастрофи MH17.

Кібератаки на Латвію проводилися з розвідувальною метою. Основною мішенню були державні органи, але під приціл потрапили і приватні підприємства та ЗМІ. Хакери намагалися проникнути в інформаційні системи, щоб потім завантажувати дані - в першу чергу листування і документи…» ***(У Латвії заявили***

про кібератаки російських спецслужб // Європейська правда (https://www.eurointegration.com.ua/news/2018/10/8/7087918/). 08.10.2018).

***

«Російські хакери, які намагалися вчинити кібератаку проти Організації з заборони хімічної зброї у Гаазі, атакували і Бельгію…

"Федеральна прокуратура Бельгії розслідує інциденти від 2014 року, коли хакери викрали конфіденційну доповідь МЗС Бельгії щодо України" - йдеться у повідомленні…». ***(Російські хакери викрали доповідь МЗС Бельгії щодо України, – ЗМІ // Espreso.tv (https://espreso.tv/news/2018/10/05/rosiyski_khakery_vykraly_dopovid_mzs_belgiyi_schodo_ukrayiny_zmi). 05.10.2018).***

***

«Міністр закордонних справ Росії Сергій Лавров за підсумками переговорів з главою МЗС Італії Енцо Моаверо-Міланезі повідомив, що "нічого таємного" у поїздці до Гааги звинувачених в шпигунстві росіян не було…

Як зазначив глава МЗС РФ, ніяких демаршів у зв'язку з цим інцидентом ні в Москві, ні в Гаазі у квітні не робилося». ***(Саша Картер. Підготовка кібератаки на ОЗХЗ: Лавров розповів про "поїздку російських фахівців" до Гааги // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1756390-pidgotovka-kiberataki-na-ozkhz-lavrov-rozpoviv-pro-poyizdku-rosiyskikh-fakhivtsiv-do-gaagi). 08.10.2018).***

***

«Росія намагається будь-яким чином дестабілізувати ситуацію в Європі та на Заході. І тому вдається й до кібер-атак…

Вчені з Університету Клемсона в Південній Каролініі вивчили приблизно 3 мільйони твітів, які опублікували 2848 акаунтів у Twitter. Всі ці акаунти мали зв'язок із російським "Агентством інтернет-досліджень", проти якого США ввели санкції…

Акаунти у соціальних мережах навмисно привертали увагу підлітків близькими для них темами. Вони позиціювали себе як прихильники Гаррі Поттера або використовували фото знаменитостей, таких як актриса Емма Вотсон, пише Times.

Тисячі молодих британців були також аудиторією YouTube-каналу, який фінансується Кремлем. На цьому каналі намагалися створити плутанину з приводу справи про отруєння в Солсбері…

Крім іншого, російська "фабрика тролів", що спонсорується Кремлем, намагалася посіяти паніку, повідомляючи фальшиві новини про харчові продукти та воду. У безлічі твітів, відправлених з Росії, йшлося про те, що генномодифіковані продукти (ГМО) дуже небезпечні.

Акаунти, контрольовані "фабрикою тролів", пов'язаної з Кремлем, висували необґрунтовані твердження про зв'язок між ГМО й аутизмом.

У дискусії про ГМО брали участь понад 100 тисяч акаунтів, але особливо активні були 10 акаунтів, які дослідники ідентифікували як ботів. Ці 10 за 60 днів виробили близько 7,5 відсотків твітів, пов'язаних з темою ГМО.

Сотні твітів про ГМО були створені "фабрикою тролів" з Санкт-Петербурга, яку вважають головною силою хакерських атак під час президентських виборів в США у 2016 році…

Twitter "робить все більш активні кроки в боротьбі з маніпуляціями" і все частіше запобігає їм ще до того, як вони з'являються, заявили в компанії.

Компанія Google, яка володіє YouTube, натомість заявила, що вважає будь-яке втручання за допомогою цієї платформи неприйнятним. Компанія Facebook, що володіє Instagram, заявила, що зіштовхнулася зі "складними супротивниками", серед іншого – з цілими державами…». ***(РФ атакує у Twitter: цього разу "дісталось" британським підліткам // Телеканал новин «24» (https://24tv.ua/rf_atakuye_u_twitter_tsogo_razu_distalos_britanskim_pidlitkam_n1043695?utm_source=rss). 08.10.2018).***

***

«У Брюсселі провели засідання міністри оборони НАТО з приводу звинувачень Росії в хакерських атаках і спроби підриву кібербезпеки демократичного світу. Зараз вони планують викривати кібератаки Росії і зміцнювати кібернетичну оборону і безпеку НАТО.

У держав НАТО викликали роздратування спроби ГРУ Росії втрутитися в роботу Організації за заборону хімічної зброї, в тому числі спроби викрасти документи про катастрофу літака рейсу МН17 і хакерські напади у всьому світі. У зв'язку з чим міністри оборони провели консультації в штаб-квартирі альянсу…» ***(Кібератаки Росії: Захід згуртувався у щоденній боротьбі // znaj.ua (https://znaj.ua/world/178854-kiberataki-rosiji-zahid-zgurtuvavsya-u-shchodenniy-borotbi). 07.10.2018).***

***

Хакери, які працювали на Головне управління Генштабу Збройних сил Росії (колишнє ГРУ), у липні 2015 року зламали комп'ютерні системи британського телеканалу для мусульман Islam Channel…

Прес-секретар Islam Channel уточнив, що, за даними МВС, за кібератакою стоїть не хакер-любитель, а злом був здійснений на державному рівні».

Зазначається, що в хакерів був повний доступ до всієї внутрішній інформації Islam Channel…

За його словами, щоб позбутися наслідків кібератаки, знадобилось кілька місяців…» ***(Російські хакери з ГРУ зламали телеканал Islam Channel у 2015 році // Телеканал новин «24» (https://24tv.ua/rosiyski_hakeri_z_gru_tri_roki_tomu_zlamali_telekanal_dlya_musulman__zmi_n1043263?utm_source=rss). 06.10.2018).***

***

«Слідом за Великобританією, Австралією, США та Нідерландами, Німеччина також звинуватила Росію в здійсненні низки масштабних кібератак в останні роки.

«Федеральний уряд також виходить з того, що з високою часткою ймовірності за кампанією APT28 стоїть російська військова розвідка ГРУ. Ця оцінка базується на дуже надійних власних факти і джерелах», — заявив у п'ятницю, 5 жовтня, речник німецького уряду Штеффен Зайберт…». ***(Німеччина звинуватила розвідку РФ у масштабних кібератак // Українська служба швидких новин (https://ternopil.ukraines.news/nimechchina-zvinuvatila-rozvidku-rf-u-masshtabnix-kiberatak/). 06.10.2018).***

***

«Хакерські атаки несуть серйозну загрозу безпеки суспільству, заявив генпрокурор США Джеф Сешнс. Сімох агентів російських спецслужб США звинуватили у проведенні неодноразових кібератак. США мають намір домогтися справедливого правосуддя у справах обвинувачених в кібератаках можливих співробітників головного управління Генштабу ЗС Росії. Про це генеральний прокурор США Джеф Сешнс заявив у четвер, 4 жовтня. Він вказав на серйозні загрози безпеці і суспільства, які представляють спонсоровані державою хакерські атаки і кампанії з дезінформації.

У свою чергу, директор Федерального бюро розслідувань Крістофер Рей високо оцінив роботу працівників свого відомства та її міжнародних партнерів, завдяки якій вдалося пред'явити звинувачення передбачуваних агентів російських спецслужб…» ***(США обіцяють справедливе правосуддя по справі хакерів з ГРУ // Українська служба швидких новин (https://ternopil.ukraines.news/ssha-obicyayut-spravedlive-pravosuddya-po-spravi-xakeriv-z-gru/). 05.10.2018).***

***

«…Міністр закордонних справ Нідерландів Стефан Блок намагається змусити всі країни ЄС підтримати каральні заходи, які також стосуватимуться нещодавно висланих з країни російських шпигунів…

Минулого тижня коаліційні партії виступили за впровадження санкцій проти чотирьох росіян, яких Нідерланди звинувачують у шпигунстві та підготовці кібератаки на комп'ютерну мережу Організації із заборони хімічної зброї (ОЗХЗ). Для осіб, що потраплять під санкції, подорожі до європейських країни стануть неможливими, а їхні іноземні активи будуть заморожені.

…проблема наразі полягає в тому, що кібератаки ще не підпадають під умови європейських санкцій.

У випадку з Росією, зазначається, що крім економічних санкцій через анексію Криму та агресію на Сході України, застосовуються також персональні заходи проти 155 осіб та 44 організацій. Якщо голландські зусилля будуть успішними, пише видання, держави-члени ЄС також можуть впровадити покарання проти кібершпигунів, позбавивши їх доступу до країни або замороження банківських рахунків.

Так, зазначається, що накладання санкцій вимагає одностайної згоди усіх 28 країн Європейського Союзу…» ***(Саша Картер. Нідерланди вимагають від партнерів з ЄС нових санкцій за російські кібератаки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1757007-niderlandi-vimagayut-vid-partneriv-z-yes-novikh-sanktsiy-za-rosiyski-kiberataki). 11.10.2018).***

***

«В Нидерландах заявили, что они находятся в состоянии кибервойны с Россией, а действия Кремля вроде попыток атаковать Организацию по запрещению химического оружия является "по-настоящему опасными"…

Министр обороны королевства Анк Бейлевельд Бейдевельд отметила, что принимаются дополнительные меры в сфере кибербезопасности, а спецслужбы европейских стран получают дополнительное финансирование.

"Королевство Нидерланды располагает специальным управлением по борьбе с угрозами в сфере кибербезопасности, которое является способным противостоять угрозам на международном уровне. При необходимости мы можем направить наших специалистов на поддержку НАТО, и активно ищем направления, где мы можем усилить противодействие угрозам. В то же время голландские специалисты в области информационных технологий могут действовать наступательно в случае необходимости", - добавила министр обороны». ***(Нидерланды заявили о кибервойне с Россией // Gazeta.ua (https://gazeta.ua/ru/articles/politics/_niderlandy-zayavili-o-kibervojne-s-rossiej/864190). 15.10.2018).***

***

«Директор нацразведки США Дэниел Коутс убежден, что Россия, Китай, Иран и Северная Корея используют свои возможности в кибернетической сфере в качестве инструмента государственной политики для продвижения собственных интересов. С соответствующим утверждением он выступил на конференции по кибербезопасности в Вашингтоне.

«У стран, на которые мы обращаем особое внимание с точки зрения представляемой ими угрозы — таких, как Россия, Китай, Иран и Северная Корея — есть продвинутые или быстро совершенствующиеся возможности в кибернетической сфере. Эти страны используют кибероперации как дешевый инструмент государственной политики, чтобы продвигать свои национальные интересы. Они могут делать относительно небольшие с точки зрения финансового или человеческого капитала инвестиции, а результат при этом значительно окупит все первоначальные затраты»,— сказал господин Коутс…» ***(Глава разведки США: Россия, КНР, Иран и КНДР используют кибератаки как инструмент политики // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3773712). 19.10.2018).***

***

«Масштабна кібератака була здійснена на міністерство закордонних справ Словаччини. Про це заявив прем'єр-міністр країни Петер Пеллегріні…

"Цю атаку виявила Військова розвідка (VS) через нестандартну поведінку комп'ютера. Після поглибленого аналізу вони підтвердили, що це не поширений комп'ютерний вірус, а складний шкідливий код, який дозволяє зловмисникам фільтрувати дані всередині організації при атаці на сервери з-за кордону", - сказав Пеллегріні…». ***(Саша Картер. МЗС Словаччини стало об'єктом масштабної кібератаки з-за кордону // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1758022-mzs-slovachchini-stalo-obyektom-masshtabnoyi-kiberataki-z-za-kordonu). 17.10.2018).***

***

«У Чехії затримали громадян РФ, яких звинувачують у хакерській атаці на комп'ютерну систему МЗС Чехії та втручанні в роботу системи видачі посвідок на постійне проживання…

За повідомленням прокуратури, 18 вересня було затримано вісьмох осіб, серед яких - громадяни Росії та В'єтнаму…

Того ж дня їм висунули обвинувачення в несанкціонованому доступі до комп'ютерних мереж та участі в організованій злочинній групі.

Чотирьом з них також висунули обвинувачення у відмиванні грошей.

Обвинувачені могли заробити на хакерських атаках сотні мільйонів чеських крон, йдеться в повідомленні празької прокуратури…» ***(Саша Картер. У Чехії затримали росіян за звинуваченням у кібератаці на МЗС // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1757926-u-chekhiyi-zatrimali-rosiyan-za-zvinuvachennyam-u-kiberatatsi-na-mzs). 17.10.2018).***

***

«Глава национального центра кибербезопасности Киран Мартин заявил, что в ближайшие годы Великобритания практически неизбежно подвергнется масштабной кибератаке…

«Не приходится сомневаться, что нас подвергнут проверке по максимуму – и как центр, и как страну – путем крупного инцидента, который произойдет в какой-то момент в ближайшие годы, того, что мы называем нападением первой категории», – считает Мартин.

Под нападением первой категории подразумевается атака, последствием которой становится чрезвычайная ситуация на национальном уровне: при ней возможен срыв предоставления основных услуг или ущерб национальной безопасности, в результате которого страна сталкивается с тяжелыми экономическими и социальными последствиями и даже гибелью людей.

По словам Мартина, с момента открытия центра кибербезопасности два года назад его сотрудникам пришлось столкнуться с 1 тыс. 167 инцидентами. По его мнению, к большинству происшествий причастны недружественные Великобритании страны…

(Анастасия Норина. Британия предрекла себе масштабную кибератаку // Деловая газета «Взгляд» (https://vz.ru/news/2018/10/16/946340.html). 16.10.2018).

***

«Напередодні європейських виборів особливо гостро стоїть питання забезпечення захисту від можливого втручання у них ззовні, в тому числі за допомогою кібератак.

Про це заявила в середу канцлер ФРН Ангела Меркель, яка бере участь у саміті ЄС, що проходить в Брюсселі…

«Наш нещодавній досвід показує, що демократичне волевиявлення виборців може легко бути сфальсифіковано шляхом цілеспрямованих кампаній з дезінформації, кібератак і зловживання даними», - зазначила вона…

«В майбутньому ми хочемо більше зосередитися на кібератаках та "гравцях", які стоять за ними... Таким чином ми хочемо запобігати цим атакам превентивно, попереджати один одного у разі, якщо атака сталася, і усвідомити уроки з отриманого досвіду», - сказала глава уряду ФРН.

За її словами, Німеччина підтримує сильний загальний підхід до проблеми, але скептично ставиться до оперативної діяльності установ типу запропонованого Єврокомісією в 2017 році Європейського агентства з мережевої та інформаційної безпеки. Вона вважає, що може дуже швидко статися так, що національні і європейські дії будуть просто погано узгоджені.

Німецька канцлер також вважає правильним розробити «керівні принципи» для роботи з партіями, що активно застосовують дезінформацію у своїх кампаніях. Боротися з цим вона пропонує за допомогою фінансових санкцій…». ***(Меркель закликає Європу захиститися від кібератак // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/181018-merkel-zaklykaye-yevropu-zahystytysya-vid-kiberatak). 18.10.2018).***

***

«Рим протистоїть пропозиціям низки інших членів ЄС щодо введення санкцій проти країн, які здійснюють кібератаки…

Дипломати заявили, що новий режим санкцій ЄС був би спрямований переважно на Росію, яка останніми місяцями була об'єктом звинувачень у втручанні у вибори за допомогою соціальних мереж у різних західних державах. Захід також звинуватив російську військову розвідку в управлінні глобальними кібератаками, спрямованими на установи від спортивних антидопінгових органів до АЕС та лабораторій з дослідження хімічної зброї.

У зв'язку з цим Велика Британія, Нідерланди, Литва, Румунія, Фінляндія та Естонія закликали ЄС розширити дію режиму санкцій на кібернапади.

Італія є єдиною країною-членом ЄС, яка відкрито виступила проти нового режиму санкцій за кібератаки, згідно з конфіденційним документом ЄС, який бачило агентство.

Опозиція Італії сприяла пом'якшенню формулювань остаточного спільного документу на вищому рівні, у останній версії проекту якого міститься згадка про те, що робота над захистом від кібератак "через обмежувальні заходи ЄС має бути продовжена"…». ***(Італія виступила проти нового режиму санкцій ЄС за кібератаки // Європейська правда (https://www.eurointegration.com.ua/news/2018/10/17/7088308/). 17.10.2018).***

***

«В Швейцарии задержали двух граждан РФ по подозрению в планировании хакерской атаки на лабораторию Всемирного антидопингового агентства (WADA) в Лозанне…

Министерство юстиции Швейцарии дало разрешение на дальнейшее расследование дела. Двое предполагаемых хакеров, в дополнение к лаборатории WADA, планировали хакерские атаки на ряд других учреждений.

Месяц назад исполнительный комитет WADA обновил в правах Российское антидопинговое агентство (РУСАДА), которое было лишено аккредитации с ноября 2015 года, когда появилась информация об употреблении допинга российскими легкоатлетами. Впрочем, восстановление сопровождалось жесткими условиями и указанием четких сроков, в которые WADA может получить доступ к лабораторным данным и образцам проб в московской лаборатории.

По мнению главы разведслужбы Швейцарии Жана-Филиппа Годена Годена, РФ выбрала Швейцарию мишенью своих шпионских действий из-за того, что здесь расположены офисы многих международных организаций и учреждений». ***(В Швейцарии задержали двух россиян, готовивших кибератаку на WADA // ХВИЛЯ (http://hvylya.net/news/digest/v-shveytsarii-zaderzhali-dvuh-rossiyan-gotovivshih-kiberataku-na-wada.html). 24.10.2018).***

***

«Россия по сравнению с Китаем по кибератакам против США — «младший игрок», заявил советник американского президента США по нацбезопасности Джон Болтон.

«Что касается, так сказать, массированных компьютерных атак, кибератак, я могу привести здесь слова вице-президента Пенса по поводу того, чем сейчас занимается Китай <...> было сказано, что по сравнению с тем, чем занимается Китай, Россию можно назвать просто младшим партнером или младшим игроком»,— сказал господин Болтон на пресс-конференции в «Интерфаксе»…». ***(Болтон назвал Россию «младшим игроком» по сравнению с Китаем в плане кибератак // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3779058). 23.10.2018).***

***

Створення та функціонування кібервійськ

«Новий військовий командний центр НАТО, здатний стримувати і проводити кібератаки, повинен бути повністю укомплектований і функціональний в 2023 році…

Про це було оголошено на щорічній кібер-конференції НАТО в бельгійському Монсі.

31 серпня було створено Агентство НАТО з комунікацій та інформації (NCIA) в штаб-квартирі в Брюсселі. В даний час в операційному центрі працює

робоча група з 1500 цивільних і 1000 військових “кібер-воїнів” з бюджетом в 1 млрд. євро на 2019 рік.

За даними НАТО, агентство призначене для надання допомоги в області повітряної і протиракетної оборони, освіти і навчання, оперативного аналізу та розвідки для забезпечення безпеки комп’ютерних мереж.

Новий центр кібероперацій (CYOC) в Монсі буде складатися з 70 експертів, які будуть почнуть отримувати військові розвіддані і інформацію в режимі реального часу до 2023 року…» ***(НАТО створить новий кіберкомандний центр // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/nato-stvorit-noviy-kiberkomandniy-tsentr.html). 18.10.2018).***

***

«В США стартовала киберкампания, направленная против российских агентов и призванная сдержать распространение дезинформации в преддверии ноябрьских промежуточных выборов… Насколько известно, это первая операция подобного рода для защиты американских выборов.

…Киберкомандование США рассылало личные сообщения лицам, подозреваемым в попытках повлиять на исход выборов, чтобы те не распространяли ложную информацию.

Хотя никаких непосредственных угроз эти сообщения не содержали, предполагается, что ранее введенные санкции и выдвинутые обвинения могут отпугнуть российских агентов, когда те поймут, что их идентифицировали.

…операция, в рамках которой в последние дни было проведено несколько акций, имела ограниченный масштаб, с тем, чтобы предотвратить эскалацию реакции со стороны Москвы и распространение атак на не связанные с выборами объекты, в том числе электросети… Киберкомандование также направило своих специалистов в Европу, чтобы помочь союзникам в борьбе с российским вмешательством.

…представители Пентагона пока не отвечают на запросы о комментариях…». ***(NYT: киберкомандование США проводит операцию против российского вмешательства в выборы // «Голос Америки» (https://www.golos-ameriki.ru/a/reuters-us-targets-russia-operatives/4625610.html). 23.10.2018).***

***

Захист персональних даних

«Ирландская комиссия по защите данных (IDPC) заявила о начале расследования в отношении Facebook после утечки данных, которая могла затронуть 50 млн аккаунтов.

Регулирующий орган ЕС проверит исполнение социальной сетью правил Общего регламента по защите данных (GDPR), вступившего в силу в мае 2018 года.

В ходе расследования комиссия изучит соблюдение Facebook своих обязательств по реализации технических и организационных мер для защиты обрабатываемых персональных данных.

Facebook продолжает внутреннее расследование и предпринимает меры по устранению потенциальных рисков для пользователей, сообщили регулятору в компании…». ***(Екатерина Симикян. Власти ЕС начали расследование в отношении Facebook после крупной утечки данных // Rusbase (https://rb.ru/news/eu-rassledovanie-facebook/). 04.10.2018).***

***

«…Компании Apple и Cisco направили в парламент Австралии свои заявления по поводу рассматриваемого в парламенте проекта закона о предоставлении правоохранительным органам доступа к зашифрованным каналам связи, необходимого, как говорится в проекте, для проведения расследований и сбора доказательств. Обе компании резко возражают против предлагаемых изменений.

Шифрование — это математическая процедура, подчеркивается в заявлении Apple. Невозможно предоставить кому-то одному доступ к зашифрованным данным, не ослабив одновременно защиту для всех пользователей. Кроме того, формулировки закона слишком расплывчаты и, теоретически, в соответствии с ними правительство могло бы даже потребовать от компаний и операторов связи, чтобы те не отправляли клиентам пакеты исправления ошибок, связанных с безопасностью.

В заявлении Cisco указывается, что создание средств доступа к данным (вместе с запретом для компании публично сообщать об их разработке) является созданием «черных ходов». Между тем, Cisco всегда четко заявляла, что не встраивает в свою продукцию подобных «черных ходов», а одна из статей закона запрещает применять его для того, чтобы заставлять компании вводить публику в заблуждение.

С аналогичными возражениями ранее выступила группа Digital Industry Group Inc., куда входят Amazon, Google, Facebook, Oath и Twitter». ***(Apple и Cisco считают, что новый австралийский закон угрожает кибербезопасности // «Открытые системы» (https://www.computerworld.ru/news/Apple-i-Cisco-schitayut-chto-novyy-avstraliyskiy-zakon-ugrozhaet-kiberbezopasnosti). 17.10.2018).***

***

«Из-за халатности разработчиков в первый же день работы приложения для знакомств сторонников Дональда Трампа Donald Daters персональные данные его пользователей стали общедоступными. Об этом в среду, 17 октября, сообщил интернет-портал TechCrunch.

Появление новой социальной сети знакомств широко освещалось консервативными массмедиа, в том числе телеканалом Fox News. Но как выяснил один из экспертов по компьютерной безопасности, приложение позволяет скачать всю базу данных с именами пользователей, фотографиями профиля, частными сообщениями и т. д. Происходило это потому, что информация была размещена в публичном и незащищенном хранилище данных Firebase, который был встроен в приложение.

Создатели приложения сообщили, что знают о проблеме и принимают меры для ее ликвидации…». ***(Из приложения знакомств сторонников Трампа произошла утечка персональных данных клиентов // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3772790). 17.10.2018).***

***

«…Американська інтернет-компанія Facebook в п'ятницю, 12 жовтня, заявила, що два тижні тому до рук хакерів потрапили особисті дані 29 мільйонів користувачів соціальної мережі…

Інформація 14 мільйонів користувачів, котру отримали кіберзлочинці, містила такі дані як дату народження, освіту, місце роботи, релігійні погляди, та інформацію щодо особистих стосунків, а також 10 останніх місць, які користувачі позначили як такі, що ними відвідані, або у яких їх позначили інші користувачі соцмережі.

Крім того, хакери отримали доступ до особистих даних ще 15 мільйонів користувачів, зокрема до їхніх імен та прізвищ, а також контактних даних, в тому числі номерів телефону чи адреси електронної пошти. Щодо цих користувачів, то обсяги отриманої зловмисниками інформації залежав від того, які саме дані публікувалися користувачами соцмережі.

Ще один мільйон Facebook-юзерів стали жертвами крадіжки цифрових ключів, але їхні дані не потрапили до рук хакерів, запевняють у компанії. У Facebook також наголосили, що технічну вразливість, котра призвела до витоку цих даних, вже усунули…». ***(Валерій Сааков. Facebook: хакери отримали дані 29 мільйонів користувачів // Deutsche Welle (https://www.dw.com/uk/facebook-%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D0%B8-%D0%BE%D1%82%D1%80%D0%B8%D0%BC%D0%B0%D0%BB%D0%B8-%D0%B4%D0%B0%D0%BD%D1%96-29-%D0%BC%D1%96%D0%BB%D1%8C%D0%B9%D0%BE%D0%BD%D1%96%D0%B2-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D1%96%D0%B2/a-45870657). 12.10.2018).***

***

«…Facebook ускоряет планы покупки «крупной» компании по кибербезопасности и уже начал переговоры с «нескольким» большими игроками на этом рынке.

Приобретение может помочь Facebook укрепить свою защиту и снизить вероятность ошибки в кодировании, которая может нанести ущерб миллионам пользователей.

…Цукерберг и команда, планируют купить программное обеспечение, способное интегрироваться в существующие сервисы социальной сети. Среди важных инструментов: ПО для сигнализации попыток взлома или обеспечения безопасности отдельных учетных записей.

Не известно, насколько скоро состоится сделка. Покупка может быть совершенна и к концу этого года…» ***(Facebook займется киберзащитой после***

утечки даннях // Goodnews.ua (http://goodnews.ua/technologies/facebook-zajmetsya-kiberzashhitoj-posle-utechki-dannyx/). 22. 10.2018).

***

«В Cathay Pacific Airways Ltd сообщили, что хакеры получили личную информацию 9,4 млн клиентов. Это крупнейшее в мире хищение данных авиакомпании..

Акции авиакомпании впервые так сильно упали за 2 года – на 3,8%, что привело к потере Cathay Pacific Airways Ltd 201 млн долларов рыночной стоимости. Причиной стало раскрытие гонконгским перевозчиком несанкционированного доступа к данным спустя семь месяцев после обнаружения нарушения.

В компании заявили, что безопасность полетов не была скомпрометирована, а каких-либо доказательств неправомерного использования украденных данных – нет…

Комиссар по конфиденциальности в Гонконге выразил серьезную обеспокоенность по поводу утечки данных и сообщил, что офис проведет юридическую экспертизу. Специальный веб-сайт infosecurity.cathaypacific.com предоставляет информацию об инциденте и плане действий для пострадавших пассажиров.

Некоторые местные законодатели раскритиковали Cathay Pacific за молчание о нарушении на протяжении семи месяцев…

В свою очередь, в Cathay Pacific "открыли расследование", привлекли фирму по кибербезопасности и улучшили системы сетевой безопасности…». ***(Ирина Фоменко. Миллионы пассажиров пострадали из-за хакерской атаки на авиакомпанию // Internetua (http://internetua.com/milliony-passajirov-postradali-iz-za-hakerskoi-ataki-na-aviakompaniua). 26.10.2018).***

***

Кіберзлочинність та кібертерроризм

«По данным недавнего исследования GoDaddy, 73,9% скомпрометированных сайтов были взломаны в целях SEO.

Усиление безопасности web-сайтов должно стать частью процесса поисковой оптимизации (SEO), считают эксперты. Киберпреступники могут взломать сайт, и его рейтинг начнет стремительно падать вниз. Даже если сам ресурс и не был взломан, постоянные атаки могут препятствовать нормальному доступу к нему GoogleBot, из-за чего замедлится трафик и перестанут отображаться страницы…

Несмотря на большие риски, только 50% владельцев сайтов осуществляют мониторинг на предмет потенциальных кибератак. Как показал анализ 65 тыс. ресурсов, в поисковых системах не отображается только 6,5 тыс. В выявлении кибератак нельзя полагаться лишь на уведомления Google о том, что ваш сайт был забанен – по данным GoDaddy, доступ запрещается лишь к 10% инфицированных сайтов. То есть, остальные 90% зараженных ресурсов продолжают

функционировать как ни чем не бывало, а их владельцы, вероятно, не получали от Google никаких уведомлений». ***(Исследование: Безопасность web-сайтов непосредственно связана с SEO // SecurityLab.ru (https://www.securitylab.ru/news/495764.php). 03.10.2018).***

***

«На прошлой неделе Национальное агентство кибербезопасности Израиля разослало гражданам страны предупреждение о новом методе угона аккаунтов в WhatsApp. Он основан на возможности верификации с помощью аудиосообщений. В зоне риска оказались пользователи, которые не сменили пароль по умолчанию от своей голосовой почты.

…Технику взлома еще год назад описал израильский веб-разработчик компании Oath Ран Бар-Зик (Ran Bar-Zik).

Лазейка для махинаций скрывается в способе привязке приложения к номеру телефона на новом устройстве. Как правило, войти в аккаунт может только его владелец, так как для получения SMS-сообщения с подтверждающим кодом необходим физический доступ к смартфону.

Но это ограничение можно обойти, поскольку пароль можно получить при помощи голосовой почты. Если владелец аккаунта несколько раз неверно введет комбинацию из SMS, то ему предложат прослушать код в ходе звонка…

Для защиты эксперты рекомендуют пользователям, в том числе и из других стран, поменять пароль от голосовой почты либо включить в WhatsApp двухфакторную аутентификацию…» ***(Dmitry Nazarov. В Израиле аккаунты WhatsApp угоняют через голосовую почту // Threatpost (https://threatpost.ru/whatsapp-accounts-are-hacked-through-voicemail-in-israel/28606/). 09.10.2018).***

***

«Киберпреступники все больше автоматизируют свои атаки, лишая жертв времени на защитные меры. К такому выводу пришли эксперты Alert Logic в своем докладе о технологиях обнаружения угроз.

Исследование охватывает период с апреля 2017 года по июль 2018-го. Аналитики изучили более 254 тыс. инцидентов ИБ и 7,2 млн связанных с ними событий. В результате они выяснили, что сегодня кибератака разворачивается в три этапа, в то время как традиционная модель предполагала последовательное прохождение семи ступеней.

Так, сначала злоумышленники проводили разведку — собирали учетные данные, выясняли внутреннюю структуру компании-жертвы. Эта информация позволяла им подобрать необходимые инструменты, комбинируя имеющиеся эксплойты с обнаруженными уязвимостями.

Далее преступники проникали в инфраструктуру, размещали в ней зловред и устанавливали удаленный контроль. Последним шагом было применение полезной нагрузки — шифрование данных, кража ценной информации, перехват денежных средств.

Эта схема предоставляла специалистам по ИБ множество возможностей для реагирования. Они могли обнаружить вредоносную активность на каждом из подготовительных этапов и заблокировать ее…

Теперь же преступники научились автоматизировать первые пять этапов кибератаки — от разведки до установки вредоносного ПО. В результате поиск жертв, определение уязвимых мест, проникновение и закрепление в IT-инфраструктуре происходит гораздо быстрее, а злоумышленники могут максимально расширить охват без увеличения затраченных ресурсов.

Эксперты назвали этот метод spray-and-pray («стреляй и молись»). По их словам, такой подход сегодня применяется в 88% вредоносных кампаний…

Исследователи заключают, что в нынешних условиях для организаций оказываются особенно важными «вопросы базовой гигиены». Это означает, что компания должна регулярно отслеживать и закрывать уязвимости в своей инфраструктуре, не оставляя преступникам шансов использовать их…» ***(Egor Nashilov. Аналитики предупреждают о растущей автоматизации кибератак // Threatpost (https://threatpost.ru/black-hats-automate-their-horrendous-wrongdoings/28496/). 02.10.2018).***

***

«…Согласно отчёту специализирующейся на кибербезопасности компании Group-IB, за 2017 год и первые 9 месяцев 2018 года хакеры взломали 14 криптовалютных бирж и нанесли ущерб на $882 млн. Пять из 14 торговых платформ (Yapizon, Coinis, YouBit, Bithumb, Coincheck) атаковали северокорейские хакеры из группы Lazarus.

Эксперты отметили, что чаще всего для атаки на криптобиржи и ICO-проекты злоумышленники используют целевой фишинг…

В случае со взломанными пятью криптобиржами после фишинга группа Lazarus проводила разведку локальной сети. Хакеры искали сервера, на которых велась работа с приватными кошельками площадок…

В отчете также отмечается, что в 2017 году кибермошенники завладели 10% всех привлеченных во время ICO инвестиций. Специалисты Group-IB добавили, что одна неназванная крупная группировка похищает около $1 млн инвестиций в месяц…

В 2018 году аналитики зафиксировали несколько случаев кражи информации об ICO-инвесторах с целью ее дальнейшей продажи или шантажа. Отмечается, что в последнее время среди мошенников обретает популярность похищение white paper чужого проекта.

Group-IB заявила, что в 2019 году криптобиржи станут новой целью для более «агрессивных хакерских групп», атакующих банки, а количество целенаправленных атак на площадки только увеличится…» ***(Криптовалютные биржи всё чаще взламывают // РосКомСвобода (https://roskomsvoboda.org/42439/). 17.10.2018).***

***

«Бюро з питань інтелектуальної власності Європейського Союзу вирішило дослідити твердження про те, що сайти з піратським контентом поширюють й шкідливі програми…

Для аналізу було обрано по п’ять найпопулярніших фільмів, телевізійних шоу, музичних треків та відеоігор (всього 20 назв). …для вибірки взяли 10 країн, вибраних випадковим чином. Також для аналізу були відібрані сайти, які пропонували користувачам піратський контент через стріми, торенти, лінки тощо…

Збір даних для дослідження відбувався у два етапи, під час яких дослідники збирали та аналізували небажані та шкідливі програми, отримані з піратських сайтів, які пропонували отримати доступ до фільмів, музики та ігор…

Дослідники порівняли дані служби VirusTotal та зібрані ними дані, аби перевірити який відсоток сайтів уже був позначений як потенційно небезпечний. Як виявилося, 8% сайтів у вибірці вже були марковані у VirusTotal. Більшість зібраних прикладів шкідливих програм були ідентифіковані як трояни…

Додатковий аналіз також виявив деякі програми, в яких були як заявлені корисні функції, так і приховані шкідливі, наприклад, клавіатурні шпигуни, сервіси для втручання в мережу і руткіти (програми або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі).

У своєму звіті Бюро з питань інтелектуальної власності Європейського Союзу наголосило, що такі сайти та потокові сервіси зазвичай не вважаються домінуючими джерелами шкідливого або небажаного програмного забезпечення. Однак, з огляду на зростаючу популярність стрімінгових сервісів, збільшену пропускну здатність широкосмугових мереж і впровадження мереж 4G, не можна виключати появу ризиків». ***(Чи дійсно через піратські сайти поширюють віруси — дослідження від бюро ЄС // Українська Антипіратська Асоціація (https://apo.kiev.ua/chy-dijsno-cherez-piratski-sajty-poshyryuyut-virusy-doslidzhennya-vid-byuro-yes/). 05.10.2018).***

***

Діяльність хакерів та хакерські угруповування

«У день парламентських виборів в Латвії проросійські хакери атакували місцеву соціальну мережу draugiem.l…

Варто відзначити, що хакерам вдалося розмістити там фото російських військових, президента РФ та його найгучніші висловлювання про "русский мир".

Так, 6 жовтня користувачі соціальної мережі при відкритті головної сторінки бачили всі ілюстрації "русского міра".

При відкритті сайту починав грати гімн Росії.

У свою чергу представники соціальної мережі підтвердили факт кібератаки, проте зараз соцмережа працює у штатному режимі…» ***(Санкцій замало? Російські хакери атакували ще одну країну напередодні виборів // znaj.ua (https://znaj.ua/world/178964-sankciy-zamalo-rosiyski-hakeri-atakuvali-shche-odnu-krajinu-naperedodni-viboriv). 07.10.2018).***

***

«Российские хакеры, атаковавшие Ticketmaster и British Airways, взломали рейтинговую компанию, связанную с тысячами сайтов, включая Google, Bing, Facebook и Twitter…

Анонимная организация киберпреступников Magecart взломала Shopper Approved, чтобы получить доступ к более чем 7 000 сайтов сразу.

Shopper Approved собирает отзывы от покупателей в области электронной коммерции, отправляя полученные результаты онлайн-продавцам и нескольким поисковым системам, таким как Google, Yahoo и Bing, а также социальным сетям - Facebook, YouTube и Twitter.

Хакеры установили вредоносный код в систему компании, пытаясь получить доступ к сайтам, которые с ней сотрудничают. Shopper Approved смог обнаружить его и защитить системы. Компания еще не подтвердила, были ли какие-либо данные скомпрометированы в ходе атаки…». ***(Ирина Фоменко. Российские хакеры атаковали рейтинговую компанию // Internetua (http://internetua.com/rossiiskie-hakery-atakovali-reitingovuua-kompaniua). 10.10.2018).***

***

«Группа преступников, работающих на северокорейское правительство, украла сотни миллионов долларов из банков за несколько грабежей…

Ранее неизвестная организация APT-38 потратила 2 года на планирование преступлений. Теперь компания по кибербезопасности FireEye обвиняет APT-38 в ограблении банков в 2016 и 2017 годах.

По мнению аналитиков, группа с 2014 года украла более 100 млн долларов (76 млн фунтов стерлингов) из банков в Юго-Восточной Азии и Южной Америке в "отчаянной" попытке уклониться от санкций.

"Нападения APT-38 на банки характеризуются длительным планированием, расширенными периодами доступа к уязвимым средам жертвы, любым попыткам украсть деньги и постоянными усилиями по пресечению расследований, в том числе уничтожением скомпрометированных машин", - говорится в отчете FireEye…

В одном из случаев хакеры внутри компьютерной сети жертвы пробыли в среднем 155 дней, изучая структуру, устанавливая бэкдоры и маскируя свою деятельность. Главной их целью было понять, как каждый пострадавший использовал Swift…

Как только хакеры были готовы, они отправляли сообщения Swift другим банкам, просив их перевести деньги жертвы на счета, контролируемые преступниками. Время было тщательно спланировано: в Бангладеше злоумышленники совершили кражу в отрезок времени с пятницы на субботу, а в США – с субботы на воскресенье.

После перевода краденные деньги перенаправляли в другое место – на новые счета или в игорные дома. После совершения преступления APT-38 уничтожала доказательства, стирая жесткие диски и отключая целые офисы.

…Согласно отчету, в целом APT-38 попыталась украсть не менее 1,1 млрд долларов…». ***(Ирина Фоменко. Северокорейские хакеры украли сотни миллионов долларов // Internetua (http://internetua.com/severokoreiskie-hakery-ukrali-sotni-millionov-dollarov). 05.10.2018).***

***

«Гакери інфікували вірусом три енергетичні й транспортні фірми в Польщі та в Україні. Можливо, що плануються чергові кібератаки, – про це повідомила словацька компанія ESET, не уточнюючи, однак, про які конкретно фірми йдеться…

Експерти компанії ESET, яка виробляє антивірусне програмне забезпечення, повідомили, що мова йде про діяльність гакерів, зафіксовану в період з 2015 року до середини 2018 року. Кібератаки приписують гакерській групі, яку Велика Британія звинувачувала у зв'язках з російською військовою розвідкою.

За інформацією ESET, гакери, відповідальні за серію попередніх кібератак, які проводилися з використанням шкідливого програмного забезпечення BlackEnergy і метою яких була українська енергетична система, згодом розробили та застосували нове програмне забезпечення, яке називається GrayEnergy.

Експерти ESET підтверджують, що гакери залишаються активними.

ESET допомагає розслідувати серію кібератак на український енергетичний сектор. За даними американської фірми FireEye, яка займається кібербезпекою, за кібератаками стоїть гакерське угрупування Sandworm. Британська спеціальна служба CGHQ повідомляла цього місяця про зв'язок BlackEnergy та Sandworm з російською військовою розвідкою ГРУ.

У фірмі ESET вважають, що найновіші гакерські атаки у Польщі та Україні – це «розвідувальний та шпигунський етап», що може призвести до кіберсаботажу.

Українська кіберполіція підтвердила, що гакерські атаки були здійснені на дві фірми в Україні, однак відмовила розкрити подробиці…». ***(Компанія ESET заявила, що гакери російського ГРУ атакували три компанії в Польщі та Україні // «Конфликты и законы» (http://k-z.com.ua/ynternet-konflykty/48365-kompaniya-eset-zayavila-shcho-gakeri-rosiyskogo-gru-atakuvali-tri-kompaniyi-v-polshchi-ta-ukrayini). 18.10.2018).***

***

«Специалисты компании McAfee раскрыли подробности новой кампании по кибершпионажу, направленной на организации в США, Канаде и Южной Корее. В операции применялось вредоносное ПО, основанное на исходном коде импланта в последний раз замеченного в 2010 году в атаках группировки APT1 (также известна как Comment Crew), предположительно связанной с китайской армией. В период с 2006 по 2010 годы в рамках операции Operation Seasalt группа осуществила кибератаки на более чем 141 американское предприятие…

Операция Oceansalt включала пять волн кибератак, адаптированных под конкретную цель. В рамках первой, второй и третьей волны киберпреступники в целях кибершпионажа распространяли фишинговые письма, содержащие

документы Microsoft Word и Excel на корейском языке, служащих в качестве загрузчиков ряда троянов, в том числе Trojan.Ecltys, Backdoor.Barkiofork и Trojan.Downbot. Судя по содержанию документов, злоумышленников интересовали финансовые организации и компании в сфере сельского хозяйства. Последние две волны атак были направлены на небольшое количество объектов в США и Канаде..» ***(Старое шпионское ПО китайских военных замечено в атаках на США, Канаду и Южную Корею // Goodnews.ua (http://goodnews.ua/technologies/staroe-shpionskoe-po-kitajskix-voennyx-zamecheno-v-atakax-na-ssha-kanadu-i-yuzhnuyu-koreyu/). 19.10.2018).***

***

«Компания ESET сообщает об обнаружении подробностей о преемнике APT-группы BlackEnergy. Группа злоумышленников, которая получила название GreyEnergy, нацелена на шпионаж и разведку и, вполне возможно, готовится к будущим атакам с целью киберсаботажа.

BlackEnergy атакует Украину в течение многих лет. В частности, в декабре 2015 г. она вызвала прекращение электроснабжения, оставив без электричества 230 тыс. человек во время первого в мире отключения электроэнергии в результате кибератаки. Примерно во время этого масштабного инцидента исследователи ESET начали выявлять еще одно семейство вредоносных программ, которое получило название GreyEnergy…

Атака на энергетическую инфраструктуру Украины в 2015 г. была последней известной операцией с использованием набора инструментов BlackEnergy. Через некоторое время исследователи ESET зафиксировали новую APT-подгруппу — TeleBots.

TeleBots стала известной благодаря глобальному распространению NotPetya — вредоносного программного обеспечения, которое нарушило глобальные бизнес-операции в 2017 г. и привело к убыткам в размере миллиардов долларов. Как недавно подтвердили исследователи ESET, TeleBots также связана с Industroyer, мощной современной вредоносной программой, нацеленной на промышленные системы управления, которая вызвала второе прекращение электроснабжения в Украине в 2016 г…

В соответствии с подробным анализом ESET, вредоносное программное обеспечение GreyEnergy тесно связано с вредоносными программами BlackEnergy и TeleBots. Оно имеет модульную структуру, поэтому его функционал зависит от конкретной комбинации модулей, которые оператор загружает в системы жертв.

Модули этого вредоносного программного обеспечения использовались для шпионажа и разведки. К функциональности модулей входят бэкдор, сбор файлов, осуществление снимков экрана, чтения нажатий клавиатуры, похищение паролей и учетных данных и другое…». ***(Группа GreyEnergy, возможно, готовится к разрушительным атакам на критическую інфраструктуру // «Компьютерное Обозрение»(https://ko.com.ua/gruppa_greyenergy_vozmozhno_gotovitsya_k_razrushitelnym_atakam_na_kriticheskuyu_infrastrukturu_126437). 18.10.2018).***

***

«Збиток від кібератаки з використанням вірусу WannaCry для Національної системи охорони здоров'я Великобританії (National Health Service, NHS) склав 92 млн фунтів стерлінгів (понад 120 млн доларів США). Про це сказано в доповіді британського міністерства охорони здоров'я та соціального захисту…

Згідно з даними, що містяться в доповіді, кібератака привела до порушення роботи "приблизно однієї третини фондів NHS і 8% клінік лікарів загальної практики". "Було скасовано 19 тис. записів на прийом до лікаря", — констатували автори доповіді.

…міністерство заявило про те, що в майбутні три роки витратить 150 млн фунтів стерлінгів (близько 200 млн доларів) на забезпечення кібербезпеки….». ***(Самуїл Проскуряков. WannaCry завдав британській системі охорони здоров'я збиток більш ніж на 120 млн доларів США // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1757104-wannacry-zavdav-britanskiy-sistemi-okhoroni-zdorovya-zbitok-bilsh-nizh-na-120-mln-dolariv-ssha). 12.10.2018).***

***

«Появился новый опасный вирус для гаджетов на операционной системе Android. Он использует значок, похожий на Google Apps. Ярлык маскируется под названием "Google Play Marketplace".

Эксперты по кибербезопасности назвали новый троян "GPlayed". Вирус имеет много встроенных возможностей…

Вирус позволяет удаленно управлять устройством - блокировать его, звонить, отправлять сообщения, пользоваться памятью устройства, в частности, похищать платежные данные». ***(Гаджетам грозит новый вирус // Gazeta.ua (https://gazeta.ua/ru/articles/science/_gadzhetam-grozit-novyj-virus/864208). 15.10.2018).***

***

«Фирма Palo Alto Networks, которая занимается кибербезопасностью, обнаружила в сети фальшивую версию Flash. Поддельный файл установки обманывает пользователей, и устанавливает скрытое ПО XMRig, который превращает ваш компьютер в крипто ферму.

Пользователи не могли этого заметить, ведь поддельная уставка на самом деле и обновляла Flash плеер. Во время своих поисков команда нашла 113 примеров вредоносного ПО. После проведенных тестов на Windows 7 с пакетом обновления 1 (SP1), обнаружилось, что система предупреждает о вредоносным ПО…». ***(В интернете появился Fake Flash, который устанавливает на ваш компьютер ПО майнинга // Qled (https://www.qled.com.ua/news/%d0%b8%d0%bd%d1%82%d0%b5%d1%80%d0%bd%d0%b5%d1%82%d0%b5-***

%d0%bf%d0%be%d1%8f%d0%b2%d0%b8%d0%bb%d1%81%d1%8f-fake-flash/). 22.10.2018).

***

«Опасный компьютерный вирус, предназначенный для разрушения систем безопасности на промышленных предприятиях, который остановил в 2017 году энергетический завод в Саудовской Аравии, мог быть разработан российским научно-исследовательским институтом, заявили в США.

Речь идет о вирусе Triton, который в 2017 году атаковал системы безопасности на саудовском энергетическом заводе. Американская компания FireEye, специализирующаяся на услугах кибербезопасности, …утверждает, что вирус был разработан Центральным НИИ химии и механики (ФГУП ЦНИИХМ) в Москве…

Директор отдела разведки FireEye Джон Хултквист заявил, что Россия «пересекла красную линию», перейдя от разведки на промышленных объектах к созданию вирусов, способных вызвать разрушения…». ***(Сергей Гурьянов. Россию заподозрили в разрушительной кибератаке на саудовский завод // Деловая газета «Взгляд» (https://vz.ru/news/2018/10/23/947487.html). 23.10.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«…окружной суд штата Кентукки вынес приговор автору программы LuminosityLink, которую покупатели использовали для захвата контроля над компьютерами. Житель Стэнфорда Колтон Граббс (Colton Ray Grubbs) наказан лишением свободы на срок 30 месяцев.

Коммерческий инструмент удаленного доступа LuminosityLink появился на рынке 3,5 года назад. Согласно материалам дела, до разгромной операции в Западной Европе его успели приобрести свыше 6 тыс. пользователей (британское Агентство по борьбе с преступностью дало более высокую оценку — 8,6 тыс.).

Граббс позиционировал свой продукт как легитимную программу для системных администраторов. Тем не менее, в числе ее достоинств продавец прежде всего указывал, что данный RAT-инструмент можно устанавливать удаленно и без предупреждения — то есть без ведома владельца компьютера. Продажа LuminosityLink производилась как со специализированного сайта (luminosity.link), так и через портал HackForums.net, где этот продукт числился в разделе Hacking Tools and Programs («Инструменты и программы для взлома»).

Текст заявления о признании вины, которое суд заслушал в июле, свидетельствует о том, что Граббс прекрасно знал, с какой целью большинство покупателей приобретает его продукт. Он также охотно и безвозмездно помогал пользователям советами, когда требовалось скрытно установить LuminosityLink на чужой компьютер. Более того, для оказания аналогичных услуг молодой человек набрал добровольцев из числа участников хакерских форумов.

…По итогам расследования Граббса обвинили по нескольким статьям: сговор с целью получения несанкционированного доступа к компьютерам, отмывание денег по предварительному сговору и препятствование правосудию посредством сокрытия улик…» ***(Maxim Zaitsev. За создание LuminosityLink дали 2,5 года // Threatpost (https://threatpost.ru/luminositylink-author-sentenced-to-30-months-in-prison/28778/). 17.10.2018).***

***

«Оперативники управления «К» МВД РФ при помощи службы безопасности «Почта-банка» и компании Group-IB раскрыли группу хакеров, участники которой взламывали личные кабинеты клиентов банков, интернет-магазинов и страховых компаний…

Получив доступ к аккаунтам, злоумышленники под видом специалистов по информационной безопасности требовали от организаций вознаграждения за якобы обнаруженные «уязвимости» в их системах. В качестве доказательства они предоставляли скомпрометированные ими учетные записи организаций-жертв. Размер «вознаграждения» составлял от 40 тыс. до 250 тыс. Кроме того, злоумышленники продавали полученные данные для доступа к аккаунтам на хакерских форумах.

Только по подтвержденным данным, жертвами группы стало не менее десяти компаний, среди которых крупный продуктовый ретейлер премиального класса, сайт, на котором приобретают авиа- и железнодорожные билеты, сайт крупного иностранного автоконцерна, одна из ведущих российских страховых компаний и т.п…» ***(Задержаны хакеры, маскировавшиеся под специалистов по кибербезопасности // «Открытые системы» (https://www.computerworld.ru/news/Zaderzhany-hakery-maskirovavshiesya-pod-spetsialistov-po-kiberbezopasnosti). 26.10.2018).***

***

«…22-річний житель Фанвуда (штат Нью-Джерсі) Парас Джа засуджений до виплати компенсації в розмірі 8,6 млн доларів і домашнього арешту строком на шість місяців за організацію кібератаки у відношенні до комп'ютерної мережі Ратгерського університету…

Джа раніше визнав свою провину в тому, що брав участь в кібератаці на комп'ютери навчального закладу. Хакер створив так званий ботнет — мережу, на яку потай від власника встановлюється шкідливе програмне забезпечення для подальших кібератак і розсилки небажаних повідомлень вже на інші адреси. Всього було заражено понад 100 тисяч комп'ютерів.

…Джа і ще двоє зловмисників використовували створений ними ботнет для здійснення фінансових махінацій, а також кібератак щодо Ратгерського університету і ряду мереж інтернет-компаній. Джа сам був студентом цього навчального закладу.

Два спільника Джа — 20-річний Джошуа Уайт і 21-річний Далтон Норман — в грудні минулого року також визнали провину в причетності до кібератаки…». ***(Олексій Супрун. Американського хакера засудили до виплати 8,6 млн доларів***

компенсації за кібератаку // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1759634-amerikanskogo-khakera-zasudili-do-viplati-8-6-mln-dolariv-kompensatsiyi-za-kiberataku). 27.10.2018).

***

Технічні аспекти кібербезпеки

«…В облачных сервисах хранится много ценной информации, что делает их привлекательной мишенью для киберпреступников…

В свою очередь, у специалистов в области безопасности облачных сервисов есть собственные методы усиления защиты учетных записей и противодействия кибератакам. На случай, если кому-то все-таки удастся прорвать защиту, безопасники оставляют специальные цифровые ловушки. Эти ловушки, так называемые ханитокены (honeytoken), срабатывают при проникновении постороннего и подают соответствующий сигнал.

В роли ханитокена зачастую выступают данные, оставленные ИБ-специалистами для привлечения киберпреступников…

Как сообщают эксперты Rhino Security Labs, киберпреступники научились обходить расставленные для них ловушки… они похищают данные в обход ханитокенов, используемых крупнейшим облачным провайдером Amazon Web Services (AWS).

Данная проблема имеет две составляющие. Первая – сервис CloudTrail, используемый AWS для управления токенами. CloudTrail не поддерживает целый пласт нишевых сервисов – на них не распространяются функции видимости и не создаются записи активности, а для киберпреступников отсутствие записей означает отсутствие следов.

Вторая составляющая проблемы – слишком информативные сообщения об ошибках. В частности, в них отображается Amazon Resource Name – название учетных данных, использовавшихся для отправки запроса. Amazon Resource Name также указывает, используется ли ханитокен. Атакующий может просто вызвать ошибку и увидеть, с каким пользователем имеет дело и есть ли ханитокены, а в CloudTrail не появится об этом ни единой записи.» ***(Киберпреступники научились обходить ловушки в облачных сервисах // SecurityLab.ru (https://www.securitylab.ru/news/495778.php). 04.10.2018).***

***

«…Компания Google обновила политику Chrome Web Store, добавив пять новых правил, призванных предотвратить размещение в интернет-каталоге вредоносных приложений, а также обеспечить защиту пользователей.

…отныне Chrome Web Store не будет принимать приложения с обфусцированным (запутанным) кодом… Техногигант предоставил разработчикам срок до 1 января 2019 года для приведения расширений в соответствие новым требованиям и удаления обфусцированного кода.

Компания также намерена добавить в Chrome Web Store дополнительную процедуру проверки новых расширений, требующих широкого ряда разрешений в браузере, а также приложений, чей код хранится на удаленных системах…

Третье изменение относится к новой функции в Chrome 70, запланированного к выпуску в текущем месяце. С релизом Chrome 70 пользователи получат возможность ограничивать расширения определенными сайтами, что позволит предотвратить исполнение вредоносных расширений на конфиденциальных страницах (интернет-банкинг, криптовалютные кошельки, почтовые ящики и пр.)…

Начиная с 2019 года, разработчики должны будут использовать механизмы двухфакторной аутентификации Google…

Наконец, пятое требование касается новой версии руководства по созданию манифестов для файлов .json, в которых содержатся инструкции по взаимодействию расширений с Chrome. Новый вариант руководства будет представлен только в 2019 году…» ***(Google запретит приложения с обфусцированым кодом в Chrome Web Store // SecurityLab.ru (https://www.securitylab.ru/news/495758.php). 02.10.2018).***

***

«С 2020 года все продающиеся в Калифорнии коммуникационные устройства должны будут иметь уникальный пароль или в обязательном порядке запрашивать у пользователя смену установленных по умолчанию учетных данных. Такое требование содержится в новом законе, подписанном губернатором штата. ИБ-специалисты положительно оценили инициативу властей, однако отметили ряд недостатков принятого правового акта.

Положения закона обязывают производителей снабдить все устройства, способные подключаться к Интернету, «разумными функциями безопасности», которые должны:

- Соответствовать характеру и функциям прибора
- Соответствовать тем данным, которые оборудование принимает, передает и хранит
- Защищать само устройство и находящуюся в нем информацию от несанкционированного доступа, модификации или раскрытия

Если реализация этих требований предполагает предустановку логина и пароля, то заданные производителем учетные данные должны быть уникальными для каждого устройства. Закон также предусматривает введение обязательного изменения аутентификационной информации пользователем при первом запуске оборудования.

К такому шагу власти Калифорнии побудил рост числа кибератак, направленных на устройства Интернета вещей…» ***(Dmitry Nazarov. В Калифорнии запретили одинаковые пароли на IoT-устройствах // Threatpost (https://threatpost.ru/california-law-bans-iot-devices-with-same-default-passwords/28608/). 08.10.2018).***

***

«Інкубатор технологій Jigsaw (Google Ideas) випустив новий додаток Intra. Він дозволить заходити на сайти, які заблоковані в певній країні…

Новий додаток буде створювати між сервером та смартфоном зашифроване з'єднання, яке не дозволятиме провайдеру визначати, які саме сайти відвідує користувач…

Окрім того, розробники наголосили, що за допомогою Intra користувачі отримають змогу відвідувати заборонені сайті і при цьому фактично не порушувати діюче законодавство…» ***(Google розробила додаток, який дозволить відвідувати заборонені сайти // Телеканал новин «24» (https://24tv.ua/techno/google_rozrobila_dodatok_yakiy_dozvolit_vidviduvati_zablokovani_sayti_n1043766). 08.10.2018).***

***

«Производители призвали отказаться от использования устаревших версий протокола TLS.

В первой половине 2020 года все основные браузеры (Safari, Chrome, Edge, Internet Explorer и Firefox) по умолчанию перестанут поддерживать стандарты TLS 1.0 и 1.1. Данные планы озвучили производители интернет-обозревателей, корпорации Apple , Google , Microsoft и Mozilla…

Google намерена приступить к отключению TLS 1.0 и 1.1 с выходом Chrome 72, полностью поддержка будет прекращена в начале 2020 года с релизом версии Chrome 81. Edge и Internet Explorer 11 прекратят поддерживать устаревший протокол в первой половине 2020 года, Firefox и Safari - в марте того же года.

Все вышеуказанные браузеры поддерживают версии TLS 1.2, в Chrome и Firefox уже имеется поддержка стандарта TLS 1.3. Apple и Microsoft пока работают над реализацией данной версии в своих браузерах…». ***(Apple, Google, Microsoft и Mozilla объявили о прекращении поддержки TLS 1.0 и 1.1 // SecurityLab.ru (https://www.securitylab.ru/news/495957.php). 16.10.2018).***

***

«…31 декабря нынешнего года официально прекращается выпуск обновлений безопасности для PHP 5.6.x, что ознаменует полное прекращение поддержки всех версий устаревшей ветки PHP 5.x.

В начале 2019 года из-за прекращения поддержки около 62% сайтов, до сих пор работающих на версиях PHP 5.x, перестанут получать обновления безопасности, а значит, сотни миллионов ресурсов окажутся под серьезной угрозой. Если после Нового года киберпреступники обнаружат в PHP уязвимость, огромное число сайтов и их пользователей подвергнутся большому риску…». ***(В конце года 62% всех сайтов в интернете лишатся обновлений безопасности // SecurityLab.ru (https://www.securitylab.ru/news/495935.php). 15.10.2018).***

***

«Експерт з кібербезпеки Дхірадж Мішра виявив, що десктопний додаток месенджера Telegram дозволяв викрити IP-адреси користувачів під час здійнення ними дзвінків.

Доступними були як публічні, так і приватні IP-адреси…

У той час, як користувачі мобільного додатка можуть зберігати конфіденційність своєї інформації, здійснюючи одноранговий дзвінок (peer-to-peer call, P2P), в десктопної версії Telegram такої змоги немає…

Компанія Telegram виправила вразливість як у версії 1.3.17 beta, так і у версії 1.4 Telegram, надавши можливість повністю вимкнути однорангові дзвінки або обмежити їх для деяких контактів. Засновник та гендиректор компанії Павло Дуров повідомив, що в десктопній версії здійснюється лише 0.01% всіх дзвінків…

Telegram нагородила Дхіраджа Мішру двома тисячами євро за відкриття цієї проблеми…» ***(Дослідник викрив можливість витоку IP-адрес у десктопній версії Telegram // MediaSapiens (https://ms.detector.media/web/cybersecurity/doslidnik_vikriv_mozhlivist_vitoku_ipadres_u_desktopniy_versii_telegram/). 02.10.2018).***

***

«Через год после выявления багов в алгоритме WPA2 некоторые модели устройств все еще уязвимы для KRACK-атак. К такому выводу пришел бельгийский ИБ-специалист Мэти Ванхуф (Mathy Vanhoef), который проверил патчи, выпущенные вендорами для закрытия брешей. В ходе исследования аналитик нашел несколько новых багов в стандарте Wi-Fi, а также сумел обойти методы защиты, предложенные Институтом инженеров электротехники и электроники (IEEE).

Ванхуф рассказал о KRACK в октябре 2017 года. Недостатки в механизме согласования ключей безопасности позволяли перехватывать отправляемый по беспроводному каналу трафик, а в ряде случаев внедрять в него сторонние пакеты. Как выяснил специалист, уязвимости касались всех устройств, работающих с Wi-Fi, поскольку присутствовали в самом протоколе передачи данных.

…ИБ-специалист выяснил, что более 100 моделей роутеров на чипсете MediaTek MT7620 по-прежнему принимают повторное сообщение в процессе так называемого четырехстороннего рукопожатия, являющегося основой регламента WPA2. Эксперт также усовершенствовал свой эксплойт для взлома этого алгоритма, существенно упростив условия атаки.

Еще одна находка исследователя касается возможности обхода методов защиты, разработанных консорциумом IEEE для противодействия KRACK-атакам. Ванхуф выяснил: несмотря на то что повторное использование ключей теперь затруднено, злоумышленник может использовать фрейм WNM-Sleep, чтобы объявить новый хэш, но согласовать вместо него старую секретную строку…

Несмотря на обнаруженные недостатки, ожидать всплеска KRACK-атак не стоит. Патчи для Android, устройств на чипсетах Rockwell и апдейты других

вендоров, выпущенные после выявления уязвимостей, надежно закрывают бреши, а Apple уже исправила механизмы работы с Wi-Fi в своих ОС» ***(Dmitry Nazarov. Ряд коммуникационных устройств все еще уязвим для KRACK-атак // Threatpost (https://threatpost.ru/some-wifi-devices-still-vulnerable-to-krack/28594/). 08.10.2018).***

***

«В домашніх роутерах популярною марки TP-Link знайдена небезпечна уразливість. Про це повідомили дослідники кібербезпеки компанії Tenable в блозі організації…

Пролом в моделі TL-WR841N дозволяє зловмисникам захопити пристрій і контролювати його. Хакери можуть використовувати проблеми в захисті пристрою, щоб управляти запитами і проходять трафіком…

Крім цього, фахівці виявили дві уразливості, які можуть призвести до збою в роботі маршрутизатора, викликавши відмову в обслуговуванні.

Експерти звернули увагу на те, що ці локальні уразливості не виправлені виробником…» ***(Популярний роутер краде ваші особисті дані // znaj.ua (https://znaj.ua/techno/178469-populyarniy-router-krade-vashi-osobisti-dani). 05.10.2018).***

***

«Новым источником глобальной угрозы информационной безопасности являются атаки по сторонним каналам (side-channel атаки) и уязвимости микропроцессоров, говорится в отчете международной компании Group-IB, специализирующейся на предотвращении кибератак…

По данным Group-IB, эти уязвимости невозможно быстро и эффективно закрыть при помощи программных обновлений. О самих атаках становится известно не благодаря исследованиям, а в результате утечек. Сегодня на рынке нет решений, которые могли бы эффективно выявить такие угрозы, отметили в компании. Хакеров, которые способны выполнять такие атаки, не так много, а разработка программ для борьбы с ними — процесс сложный и дорогой…

«Если устройство скомпрометировано таким образом, то переустановка операционной системы или даже выброс жесткого диска не решит проблему. Неважно, где вы находитесь, как только вы подключите устройство к интернету, преступник будет иметь над ним полный контроль»,— заключил он…» ***(Уязвимость микропроцессоров может стать главной угрозой для кибербезопасности // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3765240). 09.10.2018).***

***

«…Експерту з питань безпеки Маттео Пізані (Італія) вдалося виявити кілька недоліків в мобільному додатку Argenta на Android для мережі торгових автоматів…

В цьому мобільному додатку містилася база даних клієнтів, програміст без значних зусиль отримав до неї доступ.

Злом додатка відбувався у кілька хитромудрих етапів. Спочатку хакер здійснив декомпіляцію (тобто отримання програмного коду), далі увімкнув режим оцінювання. Після цього перевстановив додаток.

Коли Пізані отримав доступ до бази даних, він створив власний додаток для її редагування. Лише тоді, хакер попрямував до одного з автоматів, де розпочав отримувати "безлімітні" кошти та купувати за них товари. Система не розпізнала цих махінацій і видавала товар за товаром не отримуючи за це плату…» ***(Товари з автомату без обмежень: хакер зламував систему в один клік // «Znaj.ua» (https://znaj.ua/techno/181627-tovari-z-avtomatu-bez-obmezhen-haker-zlamuvav-sistemu-v-odin-klik). 19.10.2018).***

***

«Сотрудник организации Checkmarx Педро Умбелино заявил о том, что любое Android-устройство можно взломать при помощи NFC-чипа. Осуществить взлом возможно с большого расстояния. Детали он продемонстрировал на конференции Hack.lu 2018…

В видео показано, что для взлома использована технология NFC для передачи паролей. Взломать устройство можно даже в том случае, если на нем отключена передача данных.

Этот способ, по словам специалиста, можно использовать как для смартфонов, так и для ноутбуков.

В ролике показана атака, при которой на Android-устройстве изменяется режим работы NFC. Изначально на гаджете устанавливается вирусная программа, которая после начинает передавать пароли на другое устройство.

При этом расстояние между устройствами может составлять от пары метров и до 60 метров…» ***(Кражу паролей с Android-гаджета сняли на видео // NewsOboz (http://newsoboz.org/it_tehnologii/krazhu-paroley-s-android-gadzheta-snyali-na-video-22102018093600). 23.10.2018).***

***

«…Фахівці в області кібербезпеки організації Cymulate просять усіх користувачів утриматися від перегляду відео. Повідомляється, що через файли Microsoft Word можна підхопити на свій комп’ютер новий вірус, способу боротьби з яким поки немає.

Відомо, що кіберзлочинці розташовують в документі відеоролик, який може бути взятий з будь-якого інтернет-ресурсу і редагують файл document.xml, який і перенаправляє користувача на відео. Після цього в браузер Internet Explorer завантажується шкідливий код, за яким вірус потрапляє в пристрій. Фахівці розповіли, що відкриваючи такий документ, система не попереджає про небезпеку. Як можна боротися з такою проблемою – поки не відомо. Дослідники рекомендували користувачам блокувати текстові документи, що містять вбудоване відео…» ***(Нова уразливість загрожує документам Word // BCBITI (http://vsviti.com.ua/news/90172). 30.10.2018).***

***

«…В январе текущего года общественность всколыхнуло известие об уязвимостях класса Meltdown и Spectre, затрагивающих практически все современные процессоры производства Intel, AMD и ARM. Данные уязвимости позволяют получить доступ к конфиденциальной информации (например, к паролям и ключам шифрования), хранящейся в системной памяти…

Исследователи из лаборатории компьютерных наук и искусственного интеллекта (Computer Science and Artificial Intelligence Laboratory, CSAIL) Массачусетского технологического института (MIT) …разработали метод под названием DAWG (Dynamically Allocated Way Guard), предусматривающий так называемое «безопасное разделение данных», то есть секционирование памяти таким образом, чтобы информация не хранилась в одном месте.

DAWG разработана в качестве более безопасной альтернативы технологии Intel Cache Allocation Technology (CAT), представленной в 2016 году. По словам исследователей, DAWG работает по аналогии с CAT и не требует внесения большого числа изменений в оперативную систему.

Новая техника позволяет полностью изолировать данные в кеше, предотвращая утечки и обеспечивая защиту канала, использующегося для атак по времени…». ***(Эксперты MIT работают над новым методом предотвращения атак Meltdown/Spectre // SecurityLab.ru (https://www.securitylab.ru/news/496002.php). 18.10.2018).***

***

«…Тема приватности и защищенности электронной почты актуальна как никогда.

…Именно для этого Сринивас и создает Helm: персональный сервер, который управляет вашей почтой, календарем и контактами и никому эту информацию не отдает. Данные принадлежат вам, защищены Helm и хранятся прямо у вас дома…

Вот как все работает: Helm продает вам устройство, Helm-сервер, за 499 долларов. В цену включена годичная подписка; каждый следующий год стоит еще 99 долларов. С виду устройство похоже на забавный роутер; когда вы его подключите, нужно будет запустить приложение и пройти короткий процесс настройки: вы быстро настроите сервер на работу с доменным именем по вашему выбору. Затем останется лишь настроить способ доступа к вашим новым аккаунтам.

К сожалению, у Helm нет никакого веб-интерфейса, так что проверить почту и календарь из браузера, как с Gmail и Google Calendar, не получится. Своих приложений у Helm тоже нет. Вместо этого используются стандартные протоколы, так что вы сможете пользоваться вашими аккаунтами из любых почтовых или календарных приложений — только выберите те, которые работают локально, чтобы данные не синхронизировались с облаком какой-нибудь компании. На iPhone Helm после установки автоматически подключает Apple Mail…

Идея личного сервера сама по себе не нова. Крупные организации часто предпочитают держать сервисы у себя, чтобы лучше контролировать свою сеть. Частным лицам это тоже доступно — просто это трудно; во всяком случае, не настолько легко, чтобы любой мог их настроить…» ***(Helm — личный email-сервер, который не выдаст ваши данные // РосКомСвобода (https://roskomsvoboda.org/42489/). 19.10.2018).***

***

«Британская компания G4S, занимающаяся кибербезопасностью, предлагает криптовалютным инвесторам воспользоваться её системой защиты цифровых активов.

В заявлении компании отмечается, что в связи с растущей популярностью криптовалют увеличиваются риски кражи цифровых активов. Новый сервис позволит хранить монеты в безопасном автономном режиме, что защитит средства от хакеров…» ***(Британская компания предлагает «хранилище хранилищ» для цифровых актмвов // BIGFIN (https://bigfin.net/18/10/2018/britanskaja-kompanija-predlagaet-hranilishhe-hranilishh-dlja-cifrovyh-aktivov/). 18.10.2018).***

***

«…обезопасить киберпространство решилась крупная компания IBM, …разработав платформу IBM Security Connect…

«IBM Security Connect — это первая облачная платформа безопасности, основанная на открытых технологиях, управляемая ИИ»

Участники платформы смогут свободно использовать ИИ для своих целей. У них будет даже доступ к суперкомпьютеру IBM Watson. Искусственный интеллект платформы включает в себя нейронные сети и глубокое машинное обучение…

Одной из основных технологий, которая лежит в основе платформы, является проект STIX-Shifter (Structured Threat Information eXpression) — протокол, используемый для безопасного обмена информацией об угрозах. Он обеспечивает согласованность передачи данных во всех продуктах IBM Security Connect для глубокой аналитики. В сочетании с огромными массивами данных, которые предоставляют один общий API, программа может использовать информацию из любого источника…» ***(IBM будет использовать ИИ для решения проблем кибербезопасности // Український телекомунікаційний портал (https://portaltele.com.ua/news/companies/ibm-budet-ispolzovat-ii-dlya-resheniya-problem-kiberbezopasnosti.html). 17.10.2018).***

***

«Darktrace — ведущий британский стартап в области кибербезопасности…

Darktrace называет себя «ведущей мировой ИИ-компанией в области кибербезопасности». Ее решение для бизнеса — подключаемый к сети сервер, распознающий и реагирующий на скрытые угрозы. Darktrace утверждает, что система благодаря машинному обучению замечает вещи, которые игнорируют традиционные антивирусы и файрволлы. Среди ее клиентов — лондонский

аэропорт «Гэтвик», американская страховая компания AIG и лондонский Музей естественной истории.

В конце сентября в очередном раунде инвестиций компания привлекла $50 млн при оценке в $1,65 млрд…» ***(ИИ-антивирус защищает личные данные подобно иммунной системе организма // Goodnews.ua (http://goodnews.ua/technologies/ii-antivirus-zashhishhaet-lichnye-dannye-podobno-immunnoj-sisteme-organizma/). 15.10.2018).***

***

«Компания Zyxel Communications запустила облачный сервис SecuReporter, который позволяет получать детальные сведения о трафике и угрозах, а также оперативно реагировать на киберинциденты.

Решение, ориентированное на малый и средний бизнес, предназначено для мониторинга и анализа безопасности сети. Оно использует весь комплекс средств анализа и составления отчетов для обработки каждого пакета данных, который попадает в сеть компании.

На основе информации, которую предоставляет SecuReporter, ИТ-администраторы могут определять киберугрозы и в соответствии с этим оптимально настраивать политику защиты всей сети…

Сервисом можно пользоваться как на компьютере через веб-портал, так и при помощи мобильных устройств, на которые приходят оповещения, помогая системным администраторам отслеживать состояние сети, обнаруживать проблемы и кибератаки в реальном времени» ***(Zyxel запустила сервис мониторинга киберугроз // Goodnews.ua (http://goodnews.ua/technologies/zyxel-zapustila-servis-monitoringa-kiberugroz/). 21.10.2018).***

***

«Полицейская служба Европейского союза (Европол) выпустила бесплатный инструмент дешифрования вируса-вымогателя GandCrab, который позволит пользователям спасти зашифрованные файлы без выплаты выкупа злоумышленникам. В разработке принимали участие Европол, правоохранительные органы США и восьми европейских стран, включая Великобританию, а также компания в сфере кибербезопасности Bitdefender.

Как заверяет ведомство, инструмент дешифрования способен справиться практически со всеми существующими на данный момент версиями вируса GandCrab. При заражении компьютера пользователь должен перейти на сайт, загрузить защифрованные троянцем файлы, а также указать адреса, с которых хакеры прислали требование о выкупе. После этого инструмент определит тип вируса, который проник в устройство, и пришлет ссылку на утилиту для расшифровки…» ***(Выпущен инструмент дешифрования вируса GandCrab // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3780188). 25.10.2018).***

***

«…Google включила в OEM-соглашения условие, по которому …производители устройств на базе Android обязаны в течение как минимум

двух лет устанавливать обновления на популярные модели смартфонов или планшетов. Они обязаны предоставлять обновления безопасности «по меньшей мере четыре раза» в первый год выпуска гаджета, а также на протяжении второго года, хотя Google не указывает, с какой регулярностью…

Условия нового лицензионного соглашения Google распространяются на смартфоны и планшеты на базе Android, которые продаются на территории ЕС с предустановленными мобильными приложениями Google, включая Play Store. С февраля 2018 года новые правила применялись только к смартфонам и планшетам с тиражом от 100 тыс. единиц, выпущенным после 31 января 2018 года, в июле Google установила порог в 75% моделей, а с 31 января 2019 года обновления должны будут получать все новые устройства.

Производители обязаны исправлять все указанные Google уязвимости в рамках определенного периода времени. К концу каждого месяца в смартфонах и планшетах должны быть исправлены все уязвимости, выявленные за предшествующие 90 дней. Кроме того, все новые устройства должны быть обеспечены тем же уровнем защиты.

В случае несоблюдения требований Google оставляет за собой право приостановить сертификацию будущих устройств производителя, что может помешать их выпуску…» ***(Google заставит производителей Android-гаджетов выпускать обновления безопасности // SecurityLab.ru (https://www.securitylab.ru/news/496139.php). 25.09.2018).***

***

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

Бондаренко О. Аналіз загроз приватності особи крізь призму злочинності в інформаційній сфері / Олена Бондаренко, Олександр Малигін // Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Міжнародні відносини. - 2018. - № 1. - С. 45-53.

Проаналізовано сучасний стан розвитку ІКТ у світі. Всатановлено, що із зростанням розвитку ІКТ та мережевих технологій, зростає й рівень загроз від злочинності в інформаційній сфері. Досліджено види загроз приватності особи. Підтверджено факт, що крадіжки особистих даних є найбільш поширеним злочином проти приватності особи, а особиста інформація стала цінним товаром для кіберзлочинців. Розглянуто рівень збитків від злочинної діяльності в інформаційній сфері. Зроблено прогноз кількості компрометованих даних у світі на 2018 рік.

Шифр зберігання НБУВ: Ж69212.

***

Гапеєва О. Л. Міждержавне протиборство в інформаційній сфері на пострадянському просторі (1991-2017 рр.): історико-системне дослідження : монографія / Ольга Гапеєва. - Львів : Тріада плюс, 2017. - 423 с.

Особливу увагу приділено досліджено інформаційному протиборству. Виокремлено основні типи міждержавних суперечностей, які детермінують зміст й спрямованість міждержавної конфліктності в інформаційній сфері, а також концептуальні засади форми і методи інформаційного протиборства. Проаналізовано становлення національних систем забезпечення інформаційної безпеки у країнах пострадянського простору.

Шифр зберігання НБУВ: ВА823304.

***

Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. - Київ, 2018. - 81 с.

Проаналізовано теоретичні підходи до державно-приватного партнерства та їх особливості в питаннях кібербезпекової сфери. Досліджено світовий досвід (США, ЄС, Німеччини, Великої Британії, Польщі) із розбудови довіри між державним та приватним сектором з питань безпеки кіберпростору. Розглянуто нормативно-правові та організаційні основи державно-приватного партнерства в Україні, наведено ефективні приклади такого партнерства.

Шифр зберігання НБУВ: СО35905.

***

Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення : монографія / І. В. Діордіца. - Запоріжжя : Гельветика, 2017. - 547 с.

Досліджено теоретико-правові засади формування та розвитку кібербезпекової політики в Україні. Проаналізовано стан вітчизняних нормативно-правових актів, що регулюють інформаційні відносини у сфері кібербезпеки. Визначено основні ознаки кібербезпекової функції та політики. Охарактеризовано складові правовідносин, що виникають та складвються у сфері кібербезпеки. З’ясовано правову природу загроз у сфері кібербезпеки, напрями розбудови національної системи кібербезпеки.

Шифр зберігання НБУВ: ВА822390.

***

Злочинність у глобалізованому світі : матеріали XVI Всеукр. кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.). - Харків : Право , 2017. - 418 с.

Зі змісту:

- Власюк А.В. Кібербезпека військової сфери;
- Ільїн О.О. Кіберпіратство як кримінологічна проблема;
- Калашников І.О. До питання проблем протидії кіберзлочинності в Україні;
- Семко Н.В. Окремі питання міжнародно-правового співробітництва у сфері протидії кіберзлочинності;

- Склярова Р.В. Кіберполіція як засіб боротьби з кіберзлочинністю;
- Смалюк Д.І. Забезпечення кібербезпеки в Україні;
- Яременко А.В. Проблема розуміння категорії організованої кіберзлочинності та її ідентифікації в Україні.

Шифр зберігання НБУВ: ВА822401.

***

Сучасні виміри безпеки : зб. тез доп. та наук. повідомл. учасників Всеукр. студент. форуму (Харків, 18 трав. 2018 р.). - Харків : Право, 2018. - 206 с.

Зі змісту:

- Іващук П.С. Особливості забезпечення кібербезпеки України;
- Марущак О.В. Актуальні питання щодо створення національної системи кібербезпеки;
- Мотрій Є.О. Питання забезпечення кібернетичної безпеки;
- Сальніков Д.А. Кібертероризм як загроза національній безпеці.

Шифр зберігання НБУВ: ВА823041.

***

Матеріали третьої всеукраїнської студентської науково-практичної конференції «Реформування правової системи України під впливом євроінтеграційних процесів», 16-17 березня 2018 р.- Херсон : Гельветика, 2018. - 207 с.

Зі змісту:

- Кириченко В.Д. Характеристика кіберзлочинності.

Шифр зберігання НБУВ: ВА823640.

***

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.