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

№ 6 (червень)

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

«У Києві відкрився перший в Україні комерційний Центр управління кібербезпекою Security Operation Center. SOC, або Центр управління кібербезпекою, створений українською компанією «Октава Кіберзахист» на базі технологій компанії Cisco – провідного світового виробника рішень в області кібербезпеки.

Security Operation Center додатково забезпечуватиме: централізоване управління коштами кібербезпеки; автоматизоване виявлення і блокування кібератак в реальному часі; виявлення і розслідування інцидентів кібербезпеки; проактивний аналіз ризиків кібербезпеки, які можуть привести до виникнення інцидентів в майбутньому – Cyber Threat Intelligence.

Оснащення Центру компетенцій дозволяє змоделювати практично будь-яку конфігурацію рішень і сценаріїв, дає можливість оцінити їх переваги для бізнесу в будь-якій галузі і будь-якого розміру. У разі необхідності Security Operation Center готовий взаємодіяти з Державним центром кібербезпеки, профільними підрозділами СБУ, Держспецзв'язку та кіберполіції.» ***(У Києві відкрили Центр управління кібербезпекою // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/u-kiyevi-vidkrili-tsentr-upravlinnya-kiberbezpekoyu.html). 28.06.2018).***

***

«Відомий ІТ-бізнесмен, засновник Інком і Датагруп, Олександр Кардаков виплатив борги і запускає новий бізнес…

За інформацією ЗМІ, загальна сума позовів найбільших кредиторів компаній Кардакова - UniCredit, "Проінвестбанк" і "ВТБ" - досягла 700 млн грн. Повне погашення всіх боргів підприємець завершив в листопаді 2017 року.

Погашення кредитів не заважало Олександру Кардакову створювати і розвивати бізнеси, зокрема у сфері хмарних технологій і кібербезпеки…

Серед нових компаній Кардакова - перший в країні оператор послуг з кіберзахисту з власним Security Operation Center. Юридично вже створена компанія "Октава Кіберзахіст". Оператор орієнтований на середній бізнес, якому невигідно створювати і містити підрозділ з інформаційної безпеки. А також - на великі компанії, яким не вигідно утримувати цілодобову чергову зміну інженерів кібербезпеки…

У планах Олександра Кардакова зайняти нішу аутсорсингу в сфері кібербезпеки. За його оцінками, місткість ринку послуг кіберзахисту в Україні вже можна оцінити в сотні мільйонів гривень. У найближчі роки вона досягне мільярдів…» ***(Ольга Петрів. Відомий ІТ-бізнесмен Кардаков виплатив борги і запускає новий бізнес // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1734591-vidomiy-it-biznesmen-kardakov-viplativ-borgi-i-zapuskaye-noviy-biznes). 06.06.2018).***

***

«…Центральна виборча комісія потребує 36 млн грн, щоб гарантувати кібербезпеку виборів 2019 року. Про це заявив голова ЦВК Михайло Охендовський під час круглого столу «Кіберзагрози для виборчого процесу в Україні», організованого за підтримки Міжнародної фундації виборчих систем (IFES)…

Зокрема, Охендовський зазначив, що «ще не всі державні органи зрозуміли серйозність викликів, які стоятимуть і перед ЦВК, і перед Україною наступного року». За словами Охендовського, торік ЦВК «так і не вдалося переконати ані уряд, ані Верховну Раду в тому, що для успішної протидії сучасним кіберзагрозам Центральній виборчій комісії необхідно мати і сучасне обладнання».

«У результаті зараз, як і рік тому, потреба у коштах на закупівлю відповідного обладнання продовжує становити близько 36 млн грн. Без запровадження нового обладнання та нових підходів до захисту власних інформаційних ресурсів у 2019 році Центральній виборчій комісії буде складніше гарантувати той рівень кібербезпеки виборів, який ми змогли гарантувати у 2014-му. Діяти у цьому напрямку потрібно вже зараз – до осені цього року», – заявив Охендовський…» ***(ЦВК потребує 36 млн грн, щоб гарантувати кібербезпеку виборів 2019 року – Охендовський // «ДЕТЕКТОР МЕДІА» (http://detector.media/infospace/article/138355/2018-06-08-tsvk-potrebue-36-mln-grn-shchob-garantuvati-kiberbezpeku-viboriv-2019-roku-okhendovskii/). 08.06.2018),***

***

«19 червня 2018 року в ТПП України за ініціативи комітету електронних комунікацій при ТПП України відбувся форум «Кібербезпека − захисти свій бізнес». Одним із ключових елементів кібербезпеки є підвищення обізнаності суспільства про існуючі та потенційні загрози.

Форум став платформою для обговорення шляхів допомоги компаніям будь-якого масштабу в оцінці, розробці та зміцненні своїх програм кібербезпеки для захисту бізнесу, просвіти та обміну досвідом (технології, законодавство, рішення); виявлення кращих практик у сфері інформаційної безпеки; налагодження міжгалузевого діалогу «Суспільство – бізнес – держава»; надання дійсного поштовху в українському суспільстві щодо підвищення уваги до кібернетичних загроз і шляхів їх подолання.

Обговорення проблематики відбулося у трьох форматах: політичний – стратегія формування екосистеми безпеки держави; технологічний – прикладні технології з інформаційної безпеки для бізнесу; та освітній – проблеми і перспективи підготовки експертів із кібербезпеки…» ***(Президент ЛСОУ принял участие в форуме ТПП "Кибербезопасность - защити свой бизнес" // TRISTAR.com.ua - твой финансовый навигатор! (http://tristar.com.ua/1/news/prezident_lsou_prinial_uchastie_v_forume_tpp_kiberbezopasnost___zashiti_svoi_biznes_9932_9933.html). 20.06.2018).***

***

«Відкрита тендерна документація у сфері кібербезпеки в публічних закупівлях держпідприємств, зарахованих до об'єктів критичної

інфраструктури, становить загрозу для таких компаній, вважає перший заступник гендиректора ДП "Міжнародний аеропорт "Бориспіль" Євген Дихне.

"Необхідність повністю висвітлювати всі аспекти майбутніх завдань у галузі безпеки (у тендерній документації під час публічних закупівель у системі закупівель ProZorro - ІФ) є ризиком для підприємства. Компромісним рішенням міг би стати допуск лише визначених державних, ліцензованих компаній до участі в цьому тендері", - сказав він у коментарі агентству "Інтерфакс-Україна" в кулуарах форуму "Кібербезпека. Захисти свій бізнес" у Києві у вівторок.

Є.Дихне наголосив, що для об'єктів критичної інфраструктури мають бути особливі умови закупівлі послуг…

На думку Є.Дихне, ціна як визначальний чинник закупівлі є головним ворогом якості кіберзахисту…

Водночас, за словами першого заступника голови Державної служби спеціального зв'язку та захисту інформації Олександра Чаузова, законодавство передбачає в таких випадках можливість нецільової закупівлі, тобто закупівлі через посередника…

Окрім зазначеного, Є.Дихне відзначив необхідність винесення витрат на кібербезпеку за межі річного фінансового плану держкомпаній, оскільки такі питання потребують оперативнішого рішення…» ***(Відкрита тендерна документація у сфері кібербезпеки становить загрозу для держкомпаній критичної інфраструктури // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/513090.html). 19.06.2018).***

***

Національна система кібербезпеки

«Витрати Держспецзв'язку на заходи із забезпечення кібербезпеки торік становили 355 692 875 гривень. А в 2018-му використають 42 134 400 гривень. Про це повідомила Державна служба спеціального зв'язку та захисту інформації України… Цього року у складі Державного центру кіберзахисту та протидії кіберзагрозам ДССЗЗІ України створено Центр реагування на кіберзагрози. І вже понад 10 років – з 2007-го – працює CERT-UA – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку… Попри те, що Державна служба спеціального зв'язку та захисту інформації України отримує з бюджету значні кошти, Національна телекомунікаційна мережа в Україні досі – на етапі створення. Адміністрація Держспецзв'язку зараз лише розробляє нормативно-правові акти, що визначатимуть об'єкти, системи інформаційної безпеки яких підлягатимуть незалежному аудиту з кібербезпеки.» ***(Стало відомо, скільки бюджетних коштів Держспецзв'язку витрачає на кіберзахист // ТзОВ "Редакційні системи" (http://expres.ua/news/2018/06/08/297481-stalo-vidomo-skilky-byudzhetnyh-koshtiv-derzhspeczvyazku-vytrachaye). 08.06.2018).***

***

«Служба безопасности Украины провела для провайдеров-членов Интернет Ассоциации Украины презентацию Ситуационного центра кибербезопасности СБУ.

Презентация прошла в четверг, 14 июня. Члены ИнАУ ознакомились с работой Центра и узнали об основных задачах, которые выполняют его сотрудники.

На встрече, длившейся около двух часов, операторы и сотрудники спецслужбы обсудили особенности полномочий центров кибербезопасности СБУ и Госспецсвязи, обеспечения кибербезопасности объектов критической инфраструктуры и сотрудничества операторов и провайдеров в условиях атак со стороны «соседа»-агрессора…» ***(Владимир Кондрашов. СБУ показала провайдерам Ситуативный центр кибербезопасности // Internetua (http://internetua.com/cbu-pokazala-provaideram-situativni-centr-kiberbezopasnosti). 15.06.2018).***

***

Правове забезпечення кібербезпеки в Україні

«В Верховную Раду внесен в повестку дня законопроект №6688, который может позволить Службе безопасности Украины (СБУ) блокировать сайты, содержащие запрещенную к распространению в Украине информацию, без решения суда.

Так, 21 июня Верховная Рада включила в повестку дня законопроект, имеющий целью узаконить возможность временной блокировки доступа к сайтам и сервисам в интернете по решению не только суда, но и прокурора, следователя и Совета национальной безопасности и обороны Украины. Законопроект обнародован на сайте парламента…

В пояснительной записке к закону указано, что его целью является "разработка и внедрение механизмов направленных на формирование эффективной системы кибербезопасности".» ***(Верховная Рада хочет разрешить блокировать сайты без решения суда // Gazeta.ua (https://gazeta.ua/ru/articles/politics/_verhovnaya-rada-hochet-razreshit-blokirovat-sajty-bez-resheniya-suda/843779). 22.06.2018).***

***

«Интернет Ассоциация Украины направила замечания к проекту постановления Кабинета Министров Украины относительно киберзащиты объектов критической инфраструктуры…

Крупнейшее в Украине объединение операторов и провайдеров указывает, что в предложенном проекте постановления КМУ некоторые термины не соответствуют определению терминов законодательства в сфере кибербезопасности…

В ИнАУ считают, что это может привести к разным применениям Закона и этого НПА.

Операторы и провайдеры утверждают, что необходимо доработать определение термина «кризисная ситуация», поскольку предложенная в НПА редакция является нечеткой и, как следствие, непонятной и неоднозначной для использования в сфере законодательства о кибербезопасности. Кроме того, есть вопросы к определениям «элемент объекта критической инфраструктуры», «взаимосвязанные сферы» с элементом объекта критической инфраструктуры, «опасное событие», «штатный режим», «привлечение внешних сил и ресурсов»…

Также Интернет Ассоциация Украины обращает внимание разработчиков проекта постановления на 4 пункт Критериев: степень рисков касательно деятельности объекта критической инфраструктуры определяется Методикой оценки рисков на объектах критической инфраструктуры, которая утверждается Кабинетом Министров Украины. А положением пункта 7 проекта Критериев предлагается установить, что порядок отнесения к категориям критичности объектов критической инфраструктуры определяется Кабинетом Министров Украины. Однако, в то же время Законом не установлено полномочий Кабинета Министров Украины касательно разработки таких нормативно-правовых актов и, вообще, не указано на необходимость разработки ни Методики, ни Порядка отнесения к категориям критичности объектов критической инфраструктуры…

В замечаниях к разработанному документу ИнАУ, помимо прочего, указывает на несоответствие проекта Критериев Директиве ЕС от 8 декабря 2008 года об идентификации и определении европейских критических инфраструктур и оценивании необходимости их улучшения и защиты.

– В частности, в статье 3 указанной Директивы рекомендуется идентифицировать потенциальные европейские критические инфраструктуры, которые соответствуют как сквозным, так и секторальным критериям и определениям, предложенным в статье 2(a) и (b), – говорится в замечаниях. – При этом секторальные критерии должны учитывать особенности отдельных секторов ЕКИ...» ***(Владимир Кондрашов. Провайдеры предлагают доработать требования к киберзащите объектов критической инфраструктуры // Internetua (http://internetua.com/provaider-predlagauat-dorabotat-trebovaniya-k-kiberzasxite-ob-ektov-kriticseskoi-infrastruktur). 18.06.2018).***

***

«Новий законопроект про "кібератаки" розширює повноваження Служби Безпеки України. Тепер вона зможе назавжди поховати справи по ТОП-корупції.

У парламенті зареєстровано законопроект, який розширює перелік злочинів, що розслідує СБУ. Йдеться про злочини щодо так званих "об’єктів критичної інформаційної інфраструктури".

По суті мова йде про державні інфомаційні ресурси, до яких можна віднести, наприклад, державні реєстри. Депутатам пропонують прийняти закон, який надасть СБУ право розслідувати втручання в такі реєстри; порушення правил їх використання чи захисту інформації, що в них міститься; зміну, копіювання чи поширення здобутої у такий спосіб інформації. Необхідність прийняття такого

закону обгрунтовується, очікувано, "гібридною війною" та пов’язаним з нею зростанням кібератак. З першого погляду все ніби логічно і виправдано.

В еру цифрових технологій і електронного врядування, коли вдала хакерська атака може призвести не тільки до реальних матеріальних збитків, але й вирішити долю держави у війні, протидія кібератакам стає питанням національної безпеки.

… але насправді, важко навіть передбачити всі потенційні наслідки таких повноважень СБУ…» ***(Олександра Дрік. Кібербезпека: для чого насправді хочуть розширити повноваження СБУ // Телеканал новин «24» (https://24tv.ua/rozshirennya_povnovazhen_komu_naspravdi_sluzhit_sluzhba_bezpeki_ukrayini_n981905?utm_source=rss). 12.06.2018).***

***

Кібервійна проти України

«Хакери з Російської Федерації (РФ) заражають українські компанії шкідливими програмами, щоб створити так звані «backdoors» для масштабного скоординованого удару.

Про це сказав глава кіберполіції України Сергій Демедюк…

«Аналіз виявленого шкідливого програмного забезпечення і цілеспрямованість їх атак на Україну дають підставу припускати, що все це робиться під якийсь конкретний день», – сказав Демедюк…» ***(У кіберполіції заявили, що російські хакери готують масований удар по Україні // Західна інформаційна корпорація (https://zik.ua/news/2018/06/27/u_kiberpolitsii_zayavyly_shcho_rosiyski_hakery_gotuyut_masovanyy_udar_po_1354675). 27.06.2018).***

***

«Тема російської інформаційної агресії, а особливо серйозних кібератак активно обговорюється не лише в Україні, а й на міжнародній арені.

Найбільше акцентується увага на тому, що немає чіткого правового механізму, який би став регулятором безпеки в інформаційній сфері.

Тому, у зв’язку з тим, що рівень наслідків інформаційної війни з кожним днем збільшується, збільшується і необхідність правової протидії російській агресії в кіберпросторі.

Так, вчора, 26 червня, в інформаційному агентстві «Укрінформ» за участі експертів відбулась дискусія щодо нового законопроекту №6688…

Учасники дискусії практично одноголосно заявили про необхідність впровадження такого законопроекту в дію…» ***(Як захистити Україну в Інтернеті // hpib.life (http://hpib.life/yak-zaxistiti-ukra%d1%97nu-v-interneti/). 27.06.2018).***

***

«Спікер Верховної Ради України Андрій Парубій на зустрічі з помічником міністра оборони США Лорою Купер заявив, що Росія може втрутитися у проведення виборів в Україні через кібератаки…

Зазначається, що Парубій з Купер обговорили блок питань кібербезпеки та енергетичної безпеки…

Парубій також розповів про пріоритети регіональної безпеки у Центральній і Східній Європі…» ***(Парубій заявив, що Росія через кібератаки може втрутитися у вибори в Україні // Телеканал новин «24» (https://24tv.ua/parubiy_zaviv_shho_rosiya_cherez_kiberataki_mozhe_vtrutitisya_vibori_v_ukrayini_n990416?utm_source=rss). 27.06.2018).***

***

«Кібератаки, які відбувалися минулого року проти України, завдали великий удар нашій економіці, який обраховується "мільярдами". Про це сьогодні сказав секретар Ради національної безпеки й оборони України Олександр Турчинов на відкритті IX Національного Експертного Форуму у Києві…

За словами Турчинова, при РНБО створений Національний координаційний центр кібербезпеки.

"І за дуже стислий термін ми досягли дуже серйозних результатів. Фактично побудований захисний контур, який сьогодні достатньо надійно захищає інформаційні ресурси державних установ. Починаємо захищати системно об'єкти стратегічної інфраструктури", - сказав секретар РНБО.

За експертними оцінками, додав він, за дуже стислий термін вдалося досягнути здатності до кіберзахисту на рівні багатьох країн ЄС…» ***(Олександр Сивачук. Торішні кібератаки завдали економіці України мільярдні збитки – Турчинов // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1734753-torishni-kiberataki-zavdali-ekonomitsi-ukrayini-milyardni-zbitki-turchinov). 07.06.2018).***

***

«Заступник глави адміністрації президента України Дмитро Шимків заявляє, що більшість кібератак на українську економічну інфраструктуру відбувається з Росії

“Дуже часто в нашій інновації ми забуваємо, що є зловмисники, які б хотіли скористатися персональними даними громадян України, скористатися українськими державними або недержавними информресурсами і вивести з ладу ту або іншу економічну інфраструктуру. Ми повністю розуміємо, що більшість атак на українську інфраструктуру відбувається з Росії», — сказав Шимків в ході IX Національного експертного форуму…

Заступник глави АП зазначив, що окремим питанням є захист української критичної інфраструктури.» ***(Більшість кібератак на українську економічну інфраструктуру іде з Росії // Українська служба швидких новин (https://novosti.ternopil.ua/bilshist-kiberatak-na-ukra%d1%97nsku-ekonomichnu-infrastrukturu-ide-z-rosi%d1%97/). 03.06.2018).***

***

«Науковий співробітник Центру з питань трансатлантичних відносин при Університеті Джонса Хопкінса в США Микола Воробйов описав п’ять сценаріїв втручання Росії в українські вибори.

…Четвертий сценарій – масштабні кібератаки проти українських державних установ, банківської системи, Міністерства оборони, Ради національної безпеки і оборони та інших організацій.

«Виборча система і технології країни вразливі до вторгнення сторонніх осіб, і Кремль знає це. Ймовірно, ці слабкі місця будуть використовуватися для злому електронної пошти та виявлення персональних даних ключових кандидатів у президенти, особливо тих, хто серйозно загрожує Кремлю», — зазначає Воробйов…» ***(Названі п’ять сценаріїв, як Путін може втрутитися в українські вибори // Українська служба швидких новин (https://sumynews.online/nazvani-pyat-scenari%d1%97v-yak-putin-mozhe-vtrutitisya-v-ukra%d1%97nski-vibori/). 21.06.2018).***

***

Боротьба з кіберзлочинністю в Україні

«Співробітники кіберполіції в Донецькій області та слідчі Центрального відділу поліції викрили кіберзлочинця, який діяв з осені 2017 року.

32-річний маріуполець з метою отримання грошового заробітку… модифікував шкідливий файл та розмножив його у всесвітній мережі…

Після відкриття заражених файлів особами, які їх завантажили, хакер без дозволу користувачів отримав доступ до процесорів комп’ютерів . Кіберзлодій використовував отримані потужності для видобутку криптовалюти, яку він в подальшому через інтернет переводив у гривню та отримував кошти на свій банківський рахунок…

Дії зловмисника кваліфіковані за ст. 361 "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку" та ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального Кодексу України…» ***(Анастасія Ткачук. В Маріуполі поліцейські затримали хакера, який займався майнінгом криптовалюти // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1735039-v-mariupoli-politseyski-zatrimali-khakera-yakiy-zaymavsya-mayningom-kriptovalyuti). 08.06.2018).***

***

«Співробітники Служби безпеки України заблокували кібератаку на дипломатичне відомство однієї з країн-членів НАТО через несанкціоноване використання інформаційних ресурсів Міністерства охорони здоров'я України…

«Правоохоронці задокументували факт порушення правил захисту інформації та експлуатації автоматизованих систем посадовцями одного з державних підприємств Мінохорони здоров'я. Вказані порушення призвели до отримання зловмисниками незаконного доступу до інформаційно-телекомунікаційних систем держустанови. В подальшому хакери спробували скористатися вказаним зламом для проведення кібератак на іноземне представництво»…

За результатами перевірки керівництво МОЗ України прийняло рішення щодо звільнення генерального директора цього держпідприємства. Наразі йому оголошено про підозру в скоєнні злочину…» ***(Ірина Матюшенко. СБУ: хакери намагалися атакувати відомство країни НАТО через ресурси МОЗ України // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1734376-sbu-khakeri-namagalisya-atakuvati-vidomstvo-krayini-nato-cherez-resursi-moz-ukrayini). 05.06.2018).***

***

«На сьогоднішній день в Україні кожен третій клієнт банків стикається з шахрайськими операціями…

Про це в ексклюзивному коментарі Обозревателю заявив операційний директор компанії з кібербезпеки "10guards" Віталій Якушев, передають "Патріоти України".

За словами експерта, на сьогоднішній день існує два напрямки крадіжки грошей з банківських карток. "…Перший напрямок - це крадіжка за допомогою технічних інструментів. Це зчитувальні пристрої, це крадіжка грошей з картки, коли ви розраховуєтесь карткою на заправці, в ресторані і т.д…", - зазначив експерт…

За словами Якушева, є також ще один напрямок, в якому зараз працюють шахраї - це методи соціальної інженерії. "Це створення ситуації, коли жертва сама видає шахраям код від свого карти. Це смс-повідомлення про те, що карта буде заблокована, а щоб цього не сталося потрібно зателефонувати на такий-то номер…

"Абсолютно всі сайти з онлайн-оплати послуг - це зона ризику…", - заявив експерт.

"Якщо говорити про шанси повернути вкрадені гроші, то тут все залежить від реакції потерпілого. Чим швидше клієнт звернеться до банку, а потім до кіберполіції, тим вищі шанси знайти шахраїв і повернути викрадені гроші. По суті, є один основний спосіб захисту від шахраїв - це підключення смс-інформування. Крім того, потрібно назавжди вбити в голову, такі прості речі, як нікому не давати свою карту і нікому не називати код. Крім того, в банку можна отримати карту з чіпом і карту для онлайн-покупок. Причому на цю карту гроші краще покласти безпосередньо перед здійсненням покупки. У разі шахрайської операції ви втратите не всі гроші з вашої загальної карти а тільки суму покупки", - заявив експерт зазначивши, що масштаби проблеми досягають 40% всіх користувачів банківських карток…» ***(В Україні масово зламують банківські карти: Що треба знати, щоб захиститися // ВОЛЯ НАРОДУ громадсько-політичний портал (http://www.volianarodu.org.ua/uk/Gromadyanske-suspilstvo/V-Ukrajini-masovo-zlamuiut-bankivski-karty-Scho-treba-znaty-schob-zachystytysya). 09.06.2018).***

***

«Пресс-служба департамента киберполиции сообщила о том, что правоохранителями задержан житель Львовской области, который занимался взломом аккаунтов пользователей в социальных сетях и распространением вредоносного ПО…

«Полицейские установили, что житель Львовской области, обладая необходимыми навыками в области программирования, создал интернет-сайт xakercki-poslygu[.]hol.es. На этом сайте злоумышленник предлагал свои услуги по взлому учетных записей, электронных ящиков и тому подобное. Все переписки между ним и клиентами происходило посредством закрытого сообщества, которое администрировал злоумышленник в этой же социальной сети»…

В киберполиции отметили, что во время общения с клиентами он также посылал им ссылку на якобы форму обратной связи. Вместо этого — пользователи попадали на фишинговую страницу, с помощью которой происходила компрометация логинов и паролей пользователей социальной сети.

В дальнейшем, злоумышленник проверял полученные данные авторизации по всем социальным сетям и популярных веб-ресурсах. Получив доступ к учетным записям, блокировал владельцам доступ к ним, путем изменения пароля. При возврате доступа хакер требовал деньги. Суммы, которые он запрашивал, колебались в зависимости от платежеспособности жертвы.

Кроме этого, в этой же сообществу, под видом приложения для взлома социальных сетей, злоумышленник разместил для свободного скачивания вредоносное программное обеспечение. Оно предназначалось для несанкционированного вмешательства в работу мобильных телефонов с операционной системой «Android», в результате чего хакер мог просматривать телефонную книгу, фотографии и записи входящих и исходящих вызовов жертвы.

Отмечается, что подозреваемому уже объявлено о подозрении в совершении более двух десятков преступлений, а дело направлено в суд…» ***(На Львовщине задержали хакера, который взламывал аккаунты украинцев в соцсетях // «Факты и комментарии®» (http://fakty.ua/272392-na-lvovcshine-zaderzhali-hakera-kotoryj-vzlamyval-socseti-i-rasprostranyal-virus). 20.06.2018).***

***

«Чоловік… протягом останніх двох місяців за допомогою шкідливого програмного забезпечення несанкціоновано втручався в роботу комп'ютерних систем охорони приватних підприємств м. Запоріжжя та м. Маріуполь.

Працівники Придніпровського управління кіберполіції встановили, що до таких протиправних дій причетний 29-річний мешканець Маріуполя.

За допомогою шкідливого програмного забезпечення зловмисник здійснював цілеспрямований несанкціонований вплив (DDOS-атаку) на маршрутизатори підприємства…

Шляхом навантаження на роутер зловмисник блокував доступ обладнання підприємства до мережі Інтернет, унеможливлював моніторинг та не дозволяв

керувати віддаленим обладнанням близько трьох тисяч абонентів підприємства, розташованих у Запорізькій та Донецький областях.

Таким чином, інформація до центрального пульту охорони від обладнання абонентів у момент здійснення атаки не надходила. Внаслідок цього приватні підприємства втрачали своїх клієнтів, так як підприємство своєчасно не могло реагувати на надісланий сигнал про допомогу.

Працівники кіберполіції Запорізької та Донецької областей спільно зі слідчими поліції Запорізької області, за процесуального керівництва міжрайонної прокуратури №1 міста Запоріжжя, встановили: здійснення атак зловмисником відбувалося з квартири у місті Маріуполь, де тимчасово проживав зловмисник. Відтак, у цій квартирі правоохоронці провели санкціонований обшук…

Кримінальне провадження розпочато за ч.1 ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. Збитки підприємства, що виникли внаслідок злочину встановлюються. Слідство у справі триває.» ***(На Запоріжжі кіберполіція викрила чоловіка у здійсненні регулярних DDos-атак на приватні підприємства // Кіберполіція (https://cyberpolice.gov.ua/news/na-zaporizhzhi-kiberpolicziya-vykryla-cholovika-u-zdijsnenni-regulyarnyx-ddos-atak-na-pryvatni-pidpryyemstva-7519/). 12.06.2018).***

***

«Зловмисник за допомогою шкідливого програмного комплексу програмував банкомати на безконтрольну видачу готівки…

Працівники Причорноморського управління Департаменту кіберполіції Національної поліції України спільно з оперативниками управління карного розшуку Шевченківського відділу поліції Одещини викрили у протиправних діях 35-річного мешканця Луганщини.

Зловмисник протягом останніх кількох тижнів здійснив декілька спроб інфікування різних банкоматів на території Одещини. Для цього він використовував метод прямого діспенсу (встановлення і активація шкідливого програмного забезпечення, що призводить до видачі усіх грошей завантажених в касети банкомату).

У межах кримінального провадження розпочатого за ст. 361 КК України (незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж) поліцейські провели комплекс оперативних заходів. За їх результатом зловмисника було затримано одразу після вчинення злочину.

Під час огляду місця події правоохоронці вилучили у нього програмні та апаратні засоби для втручання в роботу банкоматів, а також банківські платіжні картки…» ***(У Одесі поліція затримала чоловіка за інфікування банкоматів шкідливим програмним забезпеченням // Кіберполіція (https://cyberpolice.gov.ua/news/u-odesi-policziya-zatrymala-cholovika-za-infikuvannya-bankomativ-shkidlyvym-programnym-zabezpechennyam-8080/). 08.06.2018).***

***

«…Правоохоронці задокументували злочинну діяльність 17-річного мешканця Львівщини, який починаючи з 2016 року займався поширенням шкідливого програмного забезпечення, що призначене для створення (побудови) вірусу-шифрувальника…

Працівники Київського управління кіберполіції спільно зі слідчими провели санкціоновані обшуки за місцем реєстрації та проживання хакера…

Правоохоронці наразі перевіряють молодика на причетність до міжнародного хакерського угрупування. Встановлюються і особи, які можуть бути причетними до цього міжнародного злочинного угрупування. Також спеціалісти з кіберполіції встановлюють кількість уражених вірусом комп'ютерів.

За даним фактом розпочато кримінальне провадження за декількома фактами: за ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ч. 2 ст. 28, ч. 1 ст. 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку), ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України.» ***(Кіберполіція викрила 17-річного хакера у створенні та розповсюдженні вірусу-шифрувальника // Кіберполіція (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla--richnogo-xakera-u-stvorenni-ta-rozpovsyudzhenni-virusu-shyfruvalnyka-2825/). 01.06.2018).***

***

«…Обвинувачений в поширенні вірусу Petya (Not.Petya) уродженець Росії не з'явився на суд…

Підготовче судове засідання було призначено на 15 червня. «Але на призначену дату обвинувачений не з'явився. На електронну адресу суду надійшло його заяву про неможливість прибути на судове засідання, в зв'язку з чим він просив суд перенести слухання на іншу дату. У справі оголошено перерву до 27 червня о 12:30», - повідомили в прес-службі суду.

Йому загрожує штраф від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправні роботи на термін до двох років, або позбавленням волі на той самий строк, з конфіскацією програмних або технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку, які є власністю винної особи…» ***(Обвинуваченому в поширенні вірусу Petya загрожує штраф // "Українські медійні системи" (https://glavcom.ua/news/obvinuvachenomu-v-poshirenni-virusu-petya-zagrozhuje-shtraf-506050.html). 18.06.2018).***

***

«ЄС та шість країн Східного партнерства - Вірменія, Азербайджан, Білорусь, Грузія, Республіка Молдова та Україна, домовилися активізувати співпрацю в цифровій економіці та прийняли дорожню карту щодо скорочення витрат на роумінг, усунення загрози кібербезпеки на скоординованій основі та розширення електронних послуг для створення більшої кількості робочих місць у цифровій промисловості…

Робочі сесії охоплювали секторне співробітництво в сфері цифрової економіки та іноземних справ.

На першому етапі були визначені три головні цілі:

1. Необхідність прийняття дорожньої карти щодо скорочення роумінгових сборів;

2. Координоване вирішення проблеми загроз кібербезпеки;

3. Використання потенціалу, який цифрові економіка та суспільство приносять зацікавленим сторонам бізнесу та громадянам…» ***(Саша Картер. Україна скоротить витрати на роумінг з державами ЄС // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1737701-ukrayina-skorotit-vitrati-na-rouming-z-derzhavami-yes). 23.06.2018).***

***

«29-30 червня у столиці Болгарії Софії відбудеться 82-а міжпарламентська зустріч у рамках Трансатлантичного діалогу законодавців ЄС та США.

Як поінформували у прес-службі парламенту Болгарії, законодавці обговорять питання співпраці із країнами Західних Балкан, кібербезпеки і торгово-економічних відносин, повідомляє Укрінформ…» ***(В Болгарії законодавці ЄС та США обговорюють кібербезпеку й торгівлю // UA\|TV (http://uatv.ua/v-bolgariyi-zakonodavtsi-yes-ta-ssha-obgovoryuyut-kiberbezpeku-j-torgivlyu/). 29.06.2018).***

***

«Україна і Угорщина обговорили можливості та перспективи подальшої співпраці у сферах безпеки та оборони… Зустріч Міністра оборони України Степана Полторака з угорським колегою Тібором Бенко відбулася у п’ятницю, 8 червня, у Брюсселі. Ми розглянули питання, пов’язані з військовою співпрацею між оборонними відомствами, – сказав очільник Міністерства оборони України. Україна розраховує на співпрацю з Угорщиною по лінії підготовки особового складу, кібербезпеки, дорадчої допомоги в питаннях реформи військової медицини…» ***(Україна та Угорщина співпрацюватимуть на рівні військових // 7dniv.info – інформаційно-аналітичне інтернет видання (http://7dniv.info/politics/102727-ukraiina-ta-ugorschina-spvpraciuvatimut-na-rvn-vyskovih.html). 09.06.2018).***

***

«Україна та Естонія посилять міжвідомчу взаємодію та обмін досвідом у сфері нейтралізації кібератак…

5 червня відбулися перші в історії українсько-естонських відносин двосторонні міжвідомчі консультації у цій сфері…

Під час заходу делегація Естонії ознайомила українську сторону з напрацюваннями в галузі моніторингу та нейтралізації проблем кібернетичного характеру, розбудови «цифрового суспільства», а також із стратегією естонської кібербезпеки.

Українська делегація повідомила естонських колег щодо окремих аспектів масштабних кібератак на електронні та урядові ресурси України з боку Росією у 2015-2018 роках. Українська сторона, згідно повідомлення відомства, відзначила, що кібератаки, підтримувані та фінансовані РФ, стали одним із головних елементів гібридної війни проти України.

Українська делегація також висловила зацікавленість інноваційним досвідом естонських фахівців у галузі забезпечення кібербезпеки під час проведення виборів місцевого та національного рівнів…» ***(Україна та Естонія посилять співпрацю з протидії кібератакам // MediaSapiens (http://ms.detector.media/web/cybersecurity/ukraina_ta_estoniya_posilyat_posilyat_spivpratsyu_z_protidii_kiberatakam/). 06.06.2018).***

***

«Україна і Німеччина домовилися активізувати співпрацю з кібербезпеки та у сфері електронного уряду. Про це посол України в Німеччині Андрій Мельник повідомив у своєму Twitter.

"З уповноваженим Федерального уряду з інформаційної техніки, держсекретарем МВС ФРН Клаусом Віттом домовилися пожвавити взаємодію у сфері кібербезпеки та e-government", - повідомив Мельник…» ***(Україна домовилася з Німеччиною про активізацію співпраці з кібербезпеки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/220618-ukrayina-domovylasya-z-nimechchynoyu-pro-aktyvizaciyu-spivpracyi-z-kiberbezpeky). 22.06.2018).***

***

Світові тенденції в галузі кібербезпеки

«…Международная ассоциация профессионалов в области конфиденциальности (IAPP) прогнозирует создание не менее 75 тысяч рабочих мест для обеспечения конфиденциальности, а компании Fortune Global 500 потратят около $8 млрд. для обеспечения их соответствия GDPR.

Положение о защите данных призвано создать единую систему регулирования данных в Европе и усилить контроль над хранением и использованием их персональных данных. Оно было принято в 2016 году и теперь вступает в силу…

GDPR предусматривает чрезвычайно высокие штрафы компаниям, которые не соблюдают установленные правила. Кроме того, его охват выходит далеко за пределы ЕС…

Формально деятельность правил распространяется лишь на страны ЕС, однако на практике он будет влиять и на другие государства. Прежде всего, это коснется тех, кто обрабатывает личные данные жителей ЕС за его пределами…

Блокчейн хранит некоторые личные данные, в том числе, истории транзакций. В таком случае он может попадать в сферу действия GDPR.

…блокчейн имеет много общих целей с GDPR. Они оба нацелены на децентрализацию контроля данных и смягчение неравенства между централизованными поставщиками услуг – отчасти, путем их подавления…

Одним из наиболее перспективных направлений исследований является сочетание надежного оборудования и блокчейна…

Сочетание надежных вычислений с общедоступными блокчейнами означает, что конфиденциальность данных может быть защищена от внешних угроз и храниться вне сети. В данном случае блокчейн выступает в роли «судьи» и решает, кто получит доступ к этим данным. После потери доверия к централизованным поставщикам услуг, правами на данные могут управлять исключительно с помощью блокчейна и надежного оборудования пользователями. Таким образом они возвращают контроль над своими данными и их конфиденциальность. В настоящее время ряд проектов реализуют эту идею, стараясь превратить блокчейн из кошмара GDPR в сказку…». ***(GDPR и блокчейн: регулирование защиты данных в ЕС // ИА «Jourtify» (https://jourtify.com/reviews/gdpr-i-blokchejn-regulirovanie-zashhity-dannyh-v-es/). 25.06.2018).***

***

«**Збиток від кібератак на фінансові інститути може в перспективі скласти від $100 млрд до $350 млрд у рік**, що буде підривати прибуток банків і може навіть загрожувати фінансовій стабільності в цілому, повідомив Міжнародний валютний фонд (МВФ)…

«Середні потенційні щорічні збитки від кібератак можуть бути більшими — близько до 9% чистої виручки банків в глобальному масштабі, тобто близько $100 млрд. На жорсткому сценарії, коли частота кібератак вдвічі вище, ніж у минулому, і вони поширюються легше, збитки можуть бути в 2,5-3,5 рази більше — $270-350 млрд (у рік)»,— заявила директор-розпорядник фонду Крістін Лагард…» ***(Павло Полтавченко. У МВФ підрахували, що збитки банків від кібератак може досягати $350 млрд — Олігарх // Українська служба швидких новин (https://sumynews.online/u-mvf-pidraxuvali-shho-zbitki-bankiv-vid-kiberatak-mozhe-dosyagati-350-mlrd-oligarx/). 23.06.2018).***

***

«…Информатика станет обязательным предметом для изучения в швейцарских школах…

Уже в ближайшие годы расписание швейцарских школьников пополнится ещё одним предметом – информатикой. В среду, 27 июня 2018 года, Министерство

экономики, образования и науки Швейцарии официально объявило о включении дисциплины в обязательную программу изучения во всех гимназиях Швейцарии.

Школьников познакомят с основами и концепциями информационных и коммуникационных технологий, а также научат основам языка программирования, расскажут о базовых принципах компьютерной сети и аспектах кибербезопасности…» ***(Информатика станет обязательной в швейцарских школах // Швейцария Деловая (https://business-swiss.ch/2018/06/informatika-objazatelnoj-shvejcarskih-shkolah/). 28.06.2018).***

***

«…в этом году исследователи Техасского университета A&M Абнер Мендоза (Abner Mendoza) и Гуофэй Гу (Guofei Gu) опубликовали результаты исследования, посвященного современным проблемам разработки мобильных приложений.

По словам исследователей, разработчики до сих пор включают бизнес-логику (проверку вводимых пользователем данных, авторизацию и аутентификации пользователей) в клиентскую, а не серверную часть кода. В результате пользователи мобильных приложений становятся уязвимыми к простым атакам с использованием инъекций параметров HTTP-запросов…

Мендоза и Гу создали систему WARDroid для массового анализа мобильных приложений. С ее помощью исследователи определили формат запросов, используемых приложениями, и проверили их на предмет уязвимости к инъекциям параметров HTTP-запросов.

С помощью WARDroid исследователи выявили порядка 4 тыс. приложений с проблемной логикой в API, и 1743 из них передавали данные в незашифрованном виде по http…» ***(Мобильные разработчики продолжают наступать на те же грабли // SecurityLabRu (https://www.securitylab.ru/news/493751.php). 05.06.2018).***

***

«Рівень кіберзлочинності зростає, однак лише п'ята частина компаній готова протистояти кібератаці.

Такого висновку дійшли Harvey Nash та KPMG, провівши опитування директорів з питань IT у 40 офісах країн Європи, Азії та США.

Кількість респондентів, які вважають вдосконалення систем кібербезпеки найвищим пріоритетом через пікове збільшення рівня загрози з боку кіберзлочинності, на 23% більше у порівнянні із 2017 роком.

Пріоритетність управління операційними ризиками та дотримання нормативних вимог збільшилася на 12%.

Компанії збільшують обсяг інвестицій у захист конфіденційності інформації та безпеки даних через впровадження Загального регламенту ЄС з питань захисту даних (GDPR). Понад третину організацій, що взяли участь в дослідженні, наразі не відповідають вимогам GDPR.

77% IT-експертів виразили глибоке занепокоєння через підвищення загроз з боку організованої кіберзлочинності (порівняно з 71% у минулому році). Лише 22% заявили про свою готовність протистояти кібернетичній атаці.

Разом з тим, більшість компаній визнають, що не мають сьогодні ефективної цифрової стратегії. 78% респондентів повідомили, що їх цифрова стратегія є лише помірно ефективною, а у деяких випадках не дає результату.

9% компаній взагалі не мають чіткого бачення чи стратегії у сфері IT, а 35% не можуть найняти необхідних їм працівників із необхідними навичками у сфері IT.

Серед навичок, на які зберігається найвищий попит з боку компаній, на думку 46% фахівців, — великі дані та аналітика. 65% повідомили, що дефіцит навичок не дає їм можливості встигати за змінами і реагувати на них.» ***(Рівень кіберзагроз досяг історичного максимуму – дослідження // Goodnews.ua (http://goodnews.ua/technologies/riven-kiberzagroz-dosyag-istorichnogo-maksimumu-doslidzhennya/). 09.06.2018).***

***

«…кибербезопасность должна рассматриваться как одна из основных проблем национальной и экономической безопасности, считает автор статьи «Политика сдерживания в киберпространстве» Крис Пэйнтер…

На происшествия в физическом мире правительства все еще реагируют гораздо быстрее, чем на кибератаки… Влияние событий в киберпространстве недооценивается, и у государственных органов нет официально принятых процедур борьбы с кибератаками.

Среди прочего автор считает нужным ускорить выявление групп и отдельных лиц, стоящих за кибератаками. Решение технических вопросов ускорить трудно, но бюрократические препятствия: взаимное рецензирование, координация между агентствами, нехватка политическая воля, должны быть устранены… Автор рекомендует налаживать гибкое сотрудничество между странами, улучшать обмен сообщениями по дипломатическим каналам и вырабатывать стратегии сдерживания противников в киберпространстве.» ***(Эксперты: Власти должны относиться к кибератакам так же, как к происшествиям в физическом мире // «Открытые системы» (https://www.computerworld.ru/news/Experty-Vlasti-dolzhny-otnositsya-k-kiberatakam-tak-zhe-kak-k-proisshestviyam-v-fizicheskom-mire). 04.06.2018).***

***

«Специалисты Positive Technologies проанализировали данные за первый квартал 2018 года и отметили рост числа киберинцидентов на 32% по сравнению с аналогичным периодом прошлого года, а также повышение спроса у хакеров на данные жертв и использование вредоносного ПО в большинстве атак.

…в I квартале текущего года существенно выросла (на 13% по сравнению со средним показателем за 2017 год) доля атак, нацеленных на получение данных: это преимущественно персональные данные, а также учетные записи и пароли…

Частные лица преимущественно становились жертвами вредоносного ПО, которое использовалось в пяти из каждых шести атак.

…в 63% атак использовалось вредоносное ПО, причем самым используемым типом ВПО стало шпионское: с его помощью злоумышленники получали не только

персональные данные пользователей или информацию, составляющую коммерческую тайну, но и учетные данные от различных сервисов и систем, что позволяло развивать атаку на внутреннюю инфраструктуру компаний. В 23% атак с применением ВПО злоумышленники распространяли майнеры криптовалюты (например, WannaMine или RubyMiner).

Продолжила расти доля киберинцидентов, нацеленных на госучреждения: в I квартале 2018 года она составила 16%. Большинство этих атак проводилось с использованием шпионского ВПО. В основном оно оказывалось в инфраструктуре государственных организаций при помощи фишинговых рассылок по электронной почте. Так, в марте 2018 года специалисты экспертного центра безопасности Positive Technologies (PT Expert Security Center) зафиксировали ряд целевых фишинговых атак на госсектор, в ходе которых использовался шпионский троян SANNY.

Традиционно наибольший ущерб продолжают наносить атаки на компании финансовой отрасли. В исследуемый период 64% кибератак на банки были совершены в целях получения финансовой выгоды, остальные 36% — для получения информации, например, сведений о личных счетах клиентов.

«По нашим оценкам, — подчеркивает аналитик Ольга Зиненко, — в течение года продолжится рост числа уникальных кибератак. Стоит ожидать появления новых видов вредоносного ПО, преимущественно шпионского. Также представляется высокой вероятность фишинговых атак во время проведения чемпионата мира по футболу». ***(Positive Technologies о первом квартале года: число киберинцидентов выросло на 32% // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/293069/). 18.06.2018).***

***

«В епоху інформаційних технологій усі компанії мають постійно вдосконалюватись, адже інакше неодмінно програють конкуренцію. І зараз до списку нових інструментів починає входити страхування від кібер-ризиків…

Кіберстрахування - це захист вашої IT-системи від будь-якої шкоди, заподіяної третіми особами. Сюди входять втрати інформаційних даних, поломки апаратури та ПО, а також різні кібератаки з вимаганнями. Забезпечується страхування відповідними полісами…

Кіберстрахування є обов'язковим для тих, кому треба захищатись від хакерських атак. Це не лише хостинг-центри, IT-провайдери, розробники програмного забезпечення, але й будь-які фірми з цінною інформацією клієнтів. Цікавий факт: 9 з 10-ти компаній, які гублять ці електронні дані, оголошують про банкрутство протягом наступного року…» ***(Що треба знати про кіберстрахування // BusinessUA.Com (http://businessua.com/news/44917szo-treba-znati-pro-kiberstrahuvannya.html#). 21.06.2018).***

***

«Випадки хакерських атак на комп'ютерні системи міських адміністрацій та різних організацій, що працюють у державному секторі, почастішали у США.

…у більшості випадків зловмисники заражають вірусами муніципальні комп'ютери, блокують їх і вимагають переказу грошових коштів для відновлення доступу. Зазвичай хакери просять розплатитися з ними у криптовалюті, зокрема, в біткоїнах, відзначає видання. Найчастіше мова йде про комп'ютерні системи у невеликих містах, так як ті захищені менш надійно.

… кількість кібератак на організації держсектора зростає в США значно швидше, ніж спроби зломів систем приватних компаній. У першу чергу це пов'язано з тим, що останні зазвичай роблять великі зусилля з метою захисту своїх електронних даних.

…хакери не зосереджують свої зусилля на системах якихось конкретних міст, а постійно шукають уразливості в комп'ютерах підприємств держсектора…». ***(Самуїл Проскуряков. У США почастішали випадки хакерських атак на комп'ютерні системи міської влади // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1737908-u-ssha-pochastishali-vipadki-khakerskikh-atak-na-kompyuterni-sistemi-miskoyi-vladi). 25.06.2018).***

***

«На скандально известного пионера кибербезопасности Джона Макафи (John McAfee) было совершено покушение. Как сообщил он сам в соцсети Twitter, неизвестные сумели отравить что-то, что Макафи принял внутрь. В результате разработчик два дня провел без сознания в медицинском центре «Видант» в Северной Каролине…» ***(На легендарного программиста Джона Макафи совершено покушение // IGate (http://igate.com.ua/lenta/22131-na-legendarnogo-programmista-dzhona-makafi-soversheno-pokushenie). 25.06.2018).***

***

«Сенат Конгресу США пропонує дозволити очільнику оборонного відомства США віддавати розпорядження про ведення стеження за межами Сполучених Штатів за особами та організаціями, які від імені Росії здійснюють різні зловмисні дії у кіберпросторі. Відповідне положення включено в законопроект про фінансування Пентагону на 2019 рік, прийнятий комітетом верхньої палати Конгресу у справах збройних сил…

Стеження також пропонується дозволити і щодо тих, хто від імені РФ розміщує в соціальних мережах різну інформацію і рекламу, "спрямовану на загострення соціальних і політичних конфліктів", а також безпосередньо залучених у кіберзлочини.

Крім того, в документі пропонується дати президенту і міністру оборони право віддавати вказівку голові кіберкомандування розпорядження про реалізацію

заходів у відповідь, якщо буде зафіксована достовірна інформація про "систематичні та триваючі" кібератаки із боку Росії проти США.

До теперішнього часу документ прийнятий тільки на рівні сенатського комітету і винесено на обговорення Сенату повного складу…» ***(Самуїл Проскуряков. Сенат США пропонує дозволити стеження за причетними до кібератак особами, пов'язаними із РФ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1734727-senat-ssha-proponuye-dozvoliti-stezhennya-za-prichetnimi-do-kiberatak-osobami-povyazanimi-iz-rf). 07.06.2018).***

***

«…В четверг, 31 мая, Госдепатамент США опубликовал рекомендации президенту Дональду Трампу по укреплению кибербезопасности. Как отмечается в сопроводительном заявлении госсекретаря Майка Помпео, рекомендации подчеркивают важность взаимодействия Госдепартамента и правительства США с иностранными партнерами для борьбы с угрозами в киберпространстве.

В документе выделяются пять основных направлений по обеспечению кибербезопасности, которые будут преследовать определенные цели. В частности, главными целями являются: укрепление стабильности в киберсфере; идентификация и противодействие кибератакам, а также поиск их организаторов; защита свободы интернета и прав его пользователей; развитие технических стандартов и защита интеллектуальной собственности.

Президенту также рекомендуется создать механизм, согласно которому организаторы и участники кибератак будут привлекаться к ответственности. Кроме того, предлагается разработать спектр «быстрых, чувствительных и прозрачных последствий ниже порога применения силы» для нарушителей. Планируется разработать механизмы внедрения подобных «последствий». Также президенту рекомендуют выстраивать сотрудничество с государствами-партнерами для обеспечения более эффективного реагирования на киберинциденты.» ***(Госдеп США опубликовал рекомендации Трампу по усилению кибербезопасности // SecurityLabRu (https://www.securitylab.ru/news/493695.php). 01.06.2018).***

***

«У результаті кібератак на комп'ютери підрядника Військово-морських сил США викрали плани розробки надзвукової ракети для підводних човнів

Підконтрольні владі китайські хакери викрали великий обсяг особливо секретної інформації про підводні човни США.

…Комп'ютерні злодії зламали систему одного з підрядників Науково-дослідного центру підводних бойових дій Військово-морських сил США в січні і лютому цього року.

У результаті кібератак викрали 614 гігабайтів інформації. Ці дані пов'язують із секретним проектом «Морський дракон», системами шифрування для радіозв'язку і засобами радіоелектронної боротьби.

Особливо важливою є інформація про плани із розробки надзвукової протикорабельної ракети, яка може надійти на озброєння американських підводних човнів до 2020 року.

Вкрасти дані хакерам вдалося через те, що вони перебували в несекретній мережі підрядника, а ВМС США погано контролювали підрядників, які займаються розробкою секретної зброї.

Нову кібератаку Китаю розслідує Федеральне бюро розслідувань. У ФБР інформацію не коментують, а в китайському уряді сказали, що не чули про подібні хакерські атаки…» ***(Китайські хакери викрали секретні дані ВМС США — ЗМІ // Racurs.ua (http://racurs.ua/ua/n106344-kytayski-hakery-vkraly-sekretni-dani-vms-ssha-zmi). 09.06.2018).***

***

«…США слід серйозно побоюватися кібератак, які можна порівняти за масштабами з нападом на Перл-Харбор або терактами 11 вересня 2001 року… При цьому зробити подібний напад, по суті, може будь-яка людина, що володіє достатніми навичками для застосування кіберзброї…

За даними каналу, такої думки, зокрема, дотримується аналітик в галузі інформаційної безпеки, професійний хакер і колишня глава відділу кібербезпеки компанії Symantec Тара Уілер…

По думці Уілер, висока ймовірність такого посягання обумовлена тим, що найважливіші елементи американської інфраструктури в області охорони здоров'я і транспорту занадто слабо захищені.

…у щорічній доповіді швейцарської НВО «Всесвітній економічний форум» про глобальні ризики за нинішній рік кібератаки називають другою за небезпеки загрозою на наступні п'ять років за оцінкою експертів форуму, вони будуть поступатися лише природним катаклізмам і екстремальних погодних явищ.

…американська компанія BluVector, що спеціалізується в галузі забезпечення кібербезпеки для штучного інтелекту, в лютому повідомляла, що хоча б однієї кібератаки протягом другої половини 2017 року піддалося майже 40% всіх промислових систем управління і ключових інфраструктурних об'єктів в США.

Як вважає Уілер, американські компанії та урядові установи не вживають належних заходів для захисту даних систем… Як підкреслює аналітик, в Америці досі є компанії, які використовують на найважливіших інфраструктурних об'єктах ОС Windows XP і інші системи, які більше не оновлюються, а значить — не перевіряються на предмет помилок і вразливостей. Іншим слабким місцем є також «інтернет речей», оскільки багато пристроїв, що працюють в ньому, в принципі не передбачають оновлення прошивки і усунення вразливостей, зазначає експерт…» ***(«Наступним 11 вересня» буде кібератака — CNBC // Українська служба швидких новин (https://novosti.ternopil.ua/nastupnim-11-veresnya-bude-kiberataka-cnbc/). 03.06.2018).***

***

«…Глава американской контрразведки рекомендовал американцам, отправляющимся в Россию на Чемпионат мира по футболу… не брать с собой

электронные устройства, объяснив это тем, что они с высокой долей вероятности будут взломаны преступниками или российскими властями.

Директор Национального центра контрразведки и безопасности США агент ФБР Уильям Эванина заявил Reuters во вторник, что болельщики могут стать жертвами хакеров…

«Корпоративные и правительственные чиновники подвергаются наибольшему риску, но не думайте, что вы слишком незначительны, чтобы стать объектом для атаки…».

Другой американский чиновник, выступая на условиях анонимности, сказал, что британские спецслужбы выступили с аналогичным предупреждением для британской публики и сборной Англии, которая участвует в Чемпионате мира…

НЦКБ, который является структурой Центра правительственной связи – британской службы радиоэлектронной разведки, также опубликовал предупреждение для общественности…» ***(США предупредили футбольных болельщиков о хакерских атаках в России // «Голос Америки» (https://www.golos-ameriki.ru/a/us-govt-warns-travelers-to-russia-of-hacking/4436623.html). 13.06.2018).***

***

«В понедельник пресс-служба корпуса морской пехоты США сообщила, что из Пентагона получен запрет на применение малых беспилотных летательных аппаратов в связи с возможной угрозой в области кибербезопасности.

Месяц назад американское министерство обороны запретило закупать и применять в войсках серийные коммерческие модели беспилотников. В меморандуме, выпущенном заместителем министра обороны США Патриком Шанаханом, говорится, что запрет вызван «уязвимостями беспилотных летательных аппаратов в области кибербезопасности»…

Командование корпуса морской пехоты направило запрос в министерство о том, чтобы из списка запрещенных были исключены восемь моделей беспилотных аппаратов, необходимых для реализации программы по повышению боевой мощи и эффективности морской пехоты США. Программа подразумевает оснащение каждого отделения пехотных дивизий небольшим квадрокоптером. В войска уже были поставлены 600 единиц из первых заказанных 800, но до тех пор, пока Пентагон не даст «зеленый свет», морпехи вынуждены отказаться от их использования. Под запрет в войсках также попали гражданские смартфоны и планшеты…» ***(Анастасия Норина. Морпехам США запрещено пользоваться беспилотниками из-за Китая // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/19/928547.html). 19.06.2018).***

***

«Компания Webroot совместно с социологическим центром Ponemon Institute провела исследование, посвященное привычкам американских пользователей, связанным с требованиями кибербезопасности.

Респонденты из всех 50 штатов ответили на множество вопросов…: используете ли вы антивирусные программы, оказывались ли ваши устройства

инфицированы вредоносным ПО, как часто вы создаете резервные копии данных и т.д.

Результаты показали, что самые сознательные пользователи проживают в северо-восточной части США. Наиболее безопасным оказался штат Нью-Гэмпшир, в число лидеров вошли также Массачусетс, Юта, Род-Айленд, Миннесота и Небраска. Большинство жителей этих штатов сообщили, что используют защитное ПО, причем отдают предпочтение платным (и более надежным) программам. У 43% опрошенных настроено автоматическое обновление операционных систем, 35% создают резервные копии ежедневно либо на постоянной основе, и 88% никому не сообщают свои пароли.

Худшим с точки зрения «кибергигиены» штатом оказалась Флорида. Впрочем, здесь никаких географических закономерностей нет: почти столь же беспечные пользователи проживают в Вайоминге, Монтане, Иллинойсе и Калифорнии. 28% респондентов из этих штатов признали, что за последний год их устройства оказывались инфицированными вредоносным ПО не менее 10 раз. Но даже этот печальный опыт, похоже, ничему их не учит: 47% опрошенных заявили, что никогда не создавали резервные копии данных, а 72% – что ни видят беды в том, чтобы поделиться своими паролями с кем-то из друзей или близких. В целом по стране ситуация с «кибергигиеной» также не выглядит слишком обнадеживающей. Например, лишь 50% американцев рассказали, что используют то или иное защитное ПО. При этом половина из них предпочитают бесплатные программы, а 20% не заботятся о том, чтобы регулярно обновлять защиту.» ***(Половина американцев не используют антивирусное ПО // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5504484-Polovina-amerikancev-ne-ispolzuyut.html). 07.06.2018).***

***

Країни ЄС

«…А.М., Банк Англии собирается провести киберстресс-тест банков, чтобы определить, насколько они в состоянии быстро восстановить работу ключевых сервисов после кибератаки. Целью стресс-теста является смягчение возможных негативных последствий кибератак для финансовой системы в целом… Банк Англии при проведении стресс-теста сотрудничает с Национальным центром кибербезопасности, в ходе тестирования банки должны будут продемонстрировать соответствие стандартам в «устойчивости к воздействиям». Тем банкам, которые не смогут пройти стресс-тест, нужно будет разработать меры по улучшению кибербезопасности. Первые проверки должны начаться в следующем году…» ***(Яна Рождественская. Банк Англии проверит банки страны на кибербезопасность // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3674281). 29.06.2018).***

***

«ЄС покращить свій кіберзахист, створивши на союзному рівні законодавчі рамки із сертифікації кібербезпеки продуктів, послуг і

технологічних процесів інформатики та засобів зв'язку, повідомила в п'ятницю прес-служба Ради ЄС.

"Промисловість зможе використовувати новий механізм для сертифікації таких продуктів, як пов'язані з мережами автомобілі та розумне медичне обладнання", - йдеться в комюніке, поширеному в Брюсселі. У документі зазначається, що Рада ЄС схвалила директиви, що стосуються такого законопроекту з кібербезпеки.

Передбачається, що цей законопроект посилить можливості нинішнього Європейського агентства з мережевої та інформаційної безпеки (ENISA), що допоможе перетворити його на постійний орган - Європейське агентство з кібербезпеки.

Схвалений у п'ятницю текст слугуватиме позицією Ради ЄС на майбутніх переговорах з Європейським парламентом. Після досягнутої між ними угоди остаточний варіант закону вступить у силу.» ***(ЄС створює сертифікацію кібербезпеки інформатики та зв'язку // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/510804.html). 08.06.2018).***

***

«Єврокомісія пропонує в період 2021-2027 років створити першу програму «Цифрова Європа», в яку буде інвестовано 9,2 млрд євро…

Очікується, що проект дозволить Європі стати світовим лідером в області цифрової інформації, поліпшить міжнародну конкурентоспроможність і зміцнить стратегічні цифрові можливості ЄС в таких передових областях, як суперкомп'ютери, штучний інтелект, кібербезпека і електронний уряд.

Пропозиція Комісії зосереджено на п'яти напрямках:

1. 2,7 млрд євро буде вкладено в розвиток і вдосконалення суперкомп'ютерів і обробку даних у багатьох секторах - від здоров'я і поновлюваних джерел до безпеки автомобілів і кібербезпеки. Це фінансування дозволить більш ефективно і ширше використовувати суперкомп'ютери в державному і приватному секторах.

2. 2,5 млрд будуть спрямовані на поширення штучного інтелекту в європейській економіці і суспільстві. Зокрема, Комісія пропонує розробити загальні алгоритми «європейських бібліотек», дозволяючи державному і приватному секторах виявляти і купувати «розумні» рішення, які найкращим чином відповідають їхнім потребам.

3. 2 млрд направляються захист цифрової економіки, суспільства і демократичних країн ЄС шляхом посилення кібербезпеки, фінансування передових технологій в цій галузі і розвитку необхідних навичок і знань.

4. 700 млн будуть надані для забезпечення можливості нинішньої і майбутньої робочої сили в ЄС більш легко купувати сучасні цифрові навички. У цьому допоможуть довгострокові і короткострокові навчальні програми і практичні заняття на робочому місці.

5. 1,3 млрд виділяються на розширення використання цифрових технологій у всіх секторах економіки і суспільства. Гроші будуть надані на забезпечення цифрового трансформації державного управління та громадських послуг. Нові «цифрові інноваційні вузли» будуть діяти як точки єдиного обслуговування для

малих і середніх підприємств і державних адміністрацій.» ***(Євросоюз інвестує понад дев'ять мільярдів в проект «Цифрова Європа» // Інформаційне агентство АСПІ (Агентство соціально-політичних ініціатив) (https://aspi.com.ua/ua/ekonomika/yevrosoiuz-investuie-ponad-deviat-miliardiv-v-proekt-tsyfrova-yevropa.html?view=item&id=13312:yevrosoiuz-investuie-ponad-deviat-miliardiv-v-proekt-tsyfrova-yevropa). 07.06.2018).***

***

«Нові гібридні загрози роблять життєво важливим посилення кіберзахисту ЄС зі швидкою командою кібер-реагування і більш тісне співробітництво з НАТО…

Резолюція кіберзахисту була підтримана 476 голосами "за" проти 151 голосу "проти". Ще 36 депутатів утримались від голосування.

В резолюції йдеться, що Росія, Китай і Північна Корея, а також недержавні суб'єкти, здійснюють зловмисні кібер-атаки на критичні інфраструктури ЄС, займаються кібер-шпигунством та масовим спостереженням за громадянами ЄС, проводять кампанії з дезінформації та створюють злочинні програми - наприклад, Wannacry, NonPetya.

Європейські депутати підкреслюють, що фрагментована стратегія та можливості оборони Європи зробили її вразливою для кібер-атак. Тому вони настійно закликають держави-члени ЄС посилити здатність своїх збройних сил працювати разом і зміцнювати кібер-співробітництво на рівні ЄС з НАТО та іншими партнерами…

Європейські депутати віддають перевагу двом кібер-проектам, що мають бути запущені в межах Постійної структурної співпраці (PESCO): платформи для обміну інформацією для кібер-інцидентів та групи швидкого реагування. Вони сподіваються, що це призведе до створення європейської групи швидкого реагування, яка б координувала, виявляла та протидіяла масовим кібер-загрозам…» ***(Саша Картер. Європарламентарі хочуть посилити зв'язки з НАТО щодо кіберзахисту // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1735917-yevroparlamentari-khochut-posiliti-zvyazki-z-nato-schodo-kiberzakhistu-yes). 13.06.2018).***

***

«В ходе голосования, прошедшего Страсбурге, Европарламент одобрил резолюцию, которая признает опасным использование в европейских учреждениях продукции "Лаборатории Касперского" и рекомендует от нее отказаться. Документ получил номер A8-0189/2018. Резолюция не имеет законодательной силы, она носит рекомендательный характер и в целом определяет совместную стратегию Евросоюза в сфере информационной защиты.

В пункте 76 резолюции ПО "Лаборатории Касперского" прямо названо "вредоносным".

Этот пункт призывает Евросоюз "провести всесторонний обзор ПО, ИТ, коммуникационного оборудования и инфраструктуры, используемых в институциях, с целью исключить потенциально опасные программы и устройства,

и запретить те, которые были подтверждены как вредоносные, такие как "Лаборатории Касперского"…

Тот пункт резолюции, в котором идет речь о "Лаборатории", в компании охарактеризовали как "не соответствующий действительности и основанный на ложных утверждениях". Несмотря на отсутствие у документа законодательной силы, "Лаборатория Касперского" объявила о решении временно прекратить совместные проекты в области кибербезопасности с европейскими партнерами, в том числе с Европолом. Проекты будут заморожены до получения официальных разъяснений от Европарламента, сообщает "Лаборатория".

В частности, компания приостанавливает проект NoMoreRansom, который развивала совместно с Европолом, полицией Нидерландов и компанией McAfee (бывшей Intel Security). Целью проекта является дешифровка файлов организаций и частных лиц, которые пострадали от атак вирусов-шифровальщиков. "Лаборатория" отмечает, что NoMoreRansom был признан примером успешного государственно-частного сотрудничество Исследовательской службой Европарламента (EPRS).

"Лаборатория" тоже акцентирует внимание на в формулировках, которые используются в пункте 76 резолюции. Компания и ее гендиректор Евгений Касперский считают, что "принятие резолюции с такой формулировкой про нашу компанию фактически стимулирует европейскую киберпреступность". Также в "Лаборатории" отмечают, что в апреле Еврокомиссия в официальном заявлении сообщила, что "не обнаружила никаких признаков опасности, связанных с антивирусом "Лаборатории Касперского"…» ***(Европарламент принял рекомендательную резолюцию по кибербезопасности, в которой назвал продукцию "Лаборатории Касперского" "вредоносной" и призвал отказаться от ее использования в европейских учреждениях // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123464). 14.06.2018).***

***

«Футболисты сборной Англии перед поездкой на чемпионат мира получили специальную защиту личных данных от кибератак в России.

Британские спецслужбы модифицируют телефоны сборной Англии с целью предотвращения российской кибератаки.

…на гаджеты команды добавлено специальное защитное программное обеспечение, которое будет удалено только по возвращению игроков на Родину.

Кроме этого игрокам было рекомендовано не получать доступ к своим онлайн-банковским счетам…» ***(Алина Чернявская. Спецслужбы вшили в смартфоны английских футболистов защиту от «русских хакеров» // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/13/927617.html). 13.06.2018).***

***

«…Согласно исследованию «Лаборатории Касперского», 17% российских пользователей не защищают свои мобильные устройства в принцип и 58% не ставят на них пароль. Наличие важных сведений не всегда побуждает людей озаботиться кибербезопасностью. Только 30% опрошенных создают резервные копии данных, 21% используют функцию «Антивор» и 11% шифруют файлы и папки.

При этом 71% респондентов регулярно выходят в сеть со смартфона, а 35% – с планшета. Поэтому кража этих устройств может оказаться довольно серьезной потерей, считают эксперты. 41% респондентов используют смартфоны для онлайн-банкинга. 57% регулярно заходят со смартфонов в свои аккаунты электронной почты, и 59% – в социальные сети…» ***(Половина россиян не использует пароль для мобильных устройств // «Открытые системы» (https://www.computerworld.ru/news/Polovina-rossiyan-ne-ispolzuet-parol-dlya-mobilnyh-ustroystv). 28.06.2018).***

***

«…Минюст зарегистрировал документ с новыми требованиями по кибербезопасности для банков… Он обязывает проводить аудит информационной безопасности, тесты на возможность проникновения и использовать сертифицированное программное оборудование…

Основная проблема в выполнении новых требований банки заключается в росте расходов бакнов… И для банков, и для их клиентов важны вопросом будет требование внедрить раздельные информационно-коммуникационные технологи при проведении платежей через Интернет или с использованием систем «банк—клиент». Предполагается, что один компьютер готовит платеж, другой отправляет.

Положение о раздельных технологиях вступает в силу 1 января 2020 года. Если требование выполнить невозможно, банк должен будет установить клиенту ограничения на максимальную сумму перевода, список возможных получателей перечень устройств, используемых для платежей…» ***(ЦБ вводит для банков новые правила безопасности // «Открытые системы» (https://www.computerworld.ru/news/TsB-vvodit-dlya-bankov-novye-pravila-bezopasnosti). 28.06.2018).***

***

…«Банки и операторы услуг платежной инфраструктуры с 1 июля 2018 года обязаны сообщать в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России о хакерских атаках и их технических параметрах», — сообщается на сайте Центробанка…

Подобный информационный обмен, действовавший на протяжении нескольких лет, оказался востребованным как финансовыми организациями, так и представителями правоохранительных органов, отмечается в сообщении

регулятора. Полученная информация будет использоваться для разработки рекомендаций финорганизациям по противодействию киберугрозам.

К числу киберугроз регулятор относит события, связанные с несанкционированными переводами денежных средств и нарушением бесперебойности оказания платежных слуг, в том числе несанкционированный доступ к устройству, эксплуатация уязвимости, вредоносный код, DDoS-атака, подбор паролей, фишинг и пр.

Для перевода денежных средств кредитные организации должны использовать только сертифицированное программное обеспечение и проводить его периодическое тестирование. Оценка соответствия уровня защиты будет проводиться организациями, имеющими лицензию Федеральной службы по техническому и экспортному контролю (ФСТЭК).

Кроме того, обязательной станет оценка выполнения требований к обеспечению защиты информации при переводах денежных средств сторонними организациями, указывается в сообщении ЦБ.» ***(ЦБ РФ обязал докладывать о хакерских атаках // РосКомСвобода (https://roskomsvoboda.org/39980/). 28.06.2018).***

***

«…Ассоциация банков России и компания Bi.Zone запустили пилотный проект по межбанковскому обмену информацией о киберугрозах…

На первом этапе работы платформы участники будут подключаться и настраивать обмен информацией, вырабатывать совместные подходы к обмену данными, создавая доверенную среду, в рамках которой банки смогут наполнять базу данных и пользоваться ей.

Решение позволит своевременно обрабатывать данные об актуальных для финансового сектора киберугрозах и автоматически применять эту информацию на средствах защиты.

Обширная база индикаторов компрометации и сопутствующей контекстной информации позволит сократить время реагирования на инциденты информационной безопасности, повысить качество их устранения и в итоге снизить ущерб от действий киберпреступников.

С помощью платформы можно использовать API-системы и повышать защищенность инфраструктуры, автоматически и в реальном времени применяя информацию об актуальных угрозах на средствах защиты…

Как пояснил глава комитета ассоциации по информационной безопасности, заместитель председателя правления Сбербанка Станислав Кузнецов, подключившиеся к платформе банки будут обмениваться информацией о вирусах, атаках и прочих угрозах за исключением персональных данных мошенников. Однако после принятия соответствующего законодательства платформа будет позволять участникам обмена идентифицировать преступников по лицу, голосу и другим признакам.

Как подчеркивается, при подключении к платформе на этапе пилотного проекта пользование ею будет бесплатным. В дальнейшем в Bi.Zone рассчитает стоимость пользования платформой, однако она не будет слишком высокой.»

(Ассоциация банков России запустила проект по обмену данными о киберугрозах // «Открытые системы» (https://www.computerworld.ru/news/Assotsiatsiya-bankov-Rossii-zapustila-proekt-po-obmenu-dannymi-o-kiberugrozah). 18.06.2018).

***

«За четыре месяца 2018 года госкорпорация Ростех отразила порядка 200 хакерских атак на свои предприятия, сообщил гендиректор корпорации Сергей Чемезов.

…Он подчеркнул, что в корпорации видят «тенденцию к росту противоправных действий злоумышленников в киберпространстве, в том числе заметно возросло число попыток получить доступ к конфиденциальной информации».

Потому одной из центральных тем предстоящей конференции «Цифровая индустрия промышленной России» (ЦИПР-2018) станет противодействие подобным угрозам.

…с той же целью в Ростехе в 2017 году был создан корпоративный центр по обнаружению, предупреждению и ликвидации последствий компьютерных атак на базе дочернего предприятия «РТ-Информ».

Центр «обладает очень мощной экспертизой в области ИТ-безопасности», способен оперативно реагировать на возникающие в Ростехе угрозы.

Также он взаимодействует с ФСБ и интегрирован в государственную систему обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА).

Ростех подписал с ФСБ соглашение, которое дает доступ к специализированным системам и средствам автоматизации в области киберзащиты. Соглашение также позволяет взаимодействовать с силовыми ведомствами по предотвращению кибератак». ***(Наталья Ануфриева. Чемезов рассказал об участившихся кибератаках на Ростех // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/5/926210.html). 05.06.2018).***

***

«Парламентариям необходимо разработать и утвердить соглашение, чтобы обеспечить защиту финансовой системы от кибератак, заявил председатель Комитета Госдумы по финансовому рынку Анатолий Аксаков.

Большинство участников круглого стола «Законодательное обеспечение развития мировой экономики в XXI веке» в рамках Международного форума «Развитие парламентаризма» готовы объединить усилия для борьбы с этой угрозой, подвёл он итоги заседания…

Участниками международного форума «Развитие парламентаризма» стали более 500 иностранных участников, парламентариев и экспертов из 96 стран мира. В работе форума приняли участие 58 официальных парламентских делегаций. Из них 19 делегаций возглавили главы парламентов, 15 — вице-спикеры.» ***(Светлана Заверняева. Аксаков предложил объединить усилия парламентариев для защиты финансовой системы от кибератак // «Парламентская газета»***

(https://www.pnp.ru/politics/aksakov-predlozhil-obedinit-usiliya-parlamentariev-dlya-zashhity-finansovoy-sistemy-ot-kiberatak.html). 05.06.2018).

***

«…Ни одна кредитная организация в России не соответствует нормам по кибербезопасности, установленным Центробанком РФ. Об этом сообщил исполняющий обязанности директора департамента информационной безопасности ЦБ Артем Сычев…

По словам чиновника, банки проходят серьезные проверки кибербезопасности и, хотя у регулятора есть замечания, они не носят критического характера…

Сычев также добавил, что две масштабные атаки с использованием программ-вымогателей, которые прошли в мире в последнее время, никак не затронули российскую банковскую систему, поскольку банковские средства защиты вовремя обнаружили угрозу и «не дали ей развиваться». Поэтому большой тревоги найденные недоработки у регулятора не вызывают.» ***(Ни один банк в РФ не соответствует требованиям по кибербезопасности в полной мере // SecurityLabRu (https://www.securitylab.ru/news/493849.php). 09.06.2018).***

***

«По мнению главы комитета ГД по инфополитике Леонида Левина, необходимо выработать международные правила по регулированию интернет-пространства, в том числе - борьбы с фейками, которые распространяются через мессенджеры и соцсети

Председатель Комитета ГД по информационной политике, информационным технологиям и связи Леонид Левин совместно с главным редактором European Post Марко Гомбаччи провел круглый стол «Законодательное обеспечение работы СМИ: безопасность и свобода слова». Мероприятие состоялось в рамках Международного форума «Развитие парламентаризма», проходящего в Москве…

Он напомнил о запрете распространять на территории российского сегмента интернета «порочащих сведений, не соответствующих действительности, а также призывы к беспорядкам, разжигание ненависти по социальному и религиозному принципу», и заверил: «Госдума сделает всё возможное, чтобы защитить россиян от другого зла во Всемирной паутине — от фейковых новостей».

Глава инфокомитета считает, что «мессенджеры и соцсети переключили внимание людей на новые медиа, и их открытость даёт простор распространению фейковых новостей и манипулированию общественным сознанием, что не может не привлекать внимания государства».

Отдельно Левин указал на необходимость совершенствования системы защиты персональных данных пользователей. Подводя итоги встречи, депутат отметил, что дискуссия высветила невозможность точного копирования норм какой-либо страны для их правового применения в другом государстве…» ***(В Госдуме предложили создать «Кибер ООН» // РосКомСвобода (https://roskomsvoboda.org/39429/). 05.06.2018).***

***

«…«Ростелеком» за 1,5 млрд руб. купил компанию Solar Security, занимающуюся целевым мониторингом и оперативным управлением информационной безопасностью. Оператор намерен создать экосистему из телеком-услуг и цифровых сервисов, в том числе сервисов информационной безопасности. На базе Solar Security будет сформирован единый центр компетенций по вопросам кибербезопасности, в рамках которого заработают три направления — сервисы, собственные продукты «Ростелекома» и комплексные решения по кибербезопасности.

В рамках первого направления планируется разработка сервисов, осуществляющих мониторинг, реагирование на инциденты и их расследование, эксплуатацию систем информационной безопасности, контроль защищенности, защиту внешних интернет-сервисов и др. В рамках второго — создание новых технологий и продвижение существующих по контролю за коммуникациями сотрудников (DLP), а также позволяющих автоматизировать контроль и управление правами доступа (IGA) и проверку защищенности исходного кода (SAST). В рамках третьего единый центр компетенций будет отвечать за центры управления информационной безопасностью (SOC), корпоративные и ведомственные центры ГосСОПКА, обеспечение безопасности критичной информационной инфраструктуры и АСУ ТП в соответствии с 187-ФЗ, а также построение и эксплуатацию комплексных систем защиты информации «под ключ»…

Некоторое время Solar Security будет сохранять свое название, затем оно изменится. Возможный вариант – «РТК-кибербезопасность». ***(Мелиса Савина. «Ростелеком» приобрел Solar Security для создания национального провайдера кибербезопасности // «Открытые системы» (https://www.computerworld.ru/articles/Rostelekom-priobrel-Solar-Security-dlya-sozdaniya-natsionalnogo-provaydera-kiberbezopasnosti). 04.06.2018).***

***

«Число инцидентов, связанных с кибератаками, в России выросло в первом квартале почти на треть. При этом увеличивается доля атак с целью получения информации, а не немедленного обогащения, в том числе с использованием методов социальной инженерии. Данные перепродают на черном рынке или используют для дальнейших атак.

Число киберинцидентов в России в первом квартале 2018 года выросло на 32% к аналогичному уровню прошлого года — до 312 случаев, говорится в отчете Positive Technologies (есть у “Ъ”). При этом злоумышленники стали чаще атаковать с целью получения данных: доля таких атак в первом квартале выросла до 36% по сравнению с 23% за 2017 год.

Данные можно продать на черном рынке или же использовать для продолжения атаки, объясняют аналитики: например, информацию о клиентах компании можно использовать для атаки уже на них самих. В основном мошенников интересуют персональные данные (33% случаев), учетные записи и

пароли для доступа (28%). Главным мотивом злоумышленников остается получение финансовой выгоды (53% случаев)…

Основные методы атак: вредоносное ПО (63%), в основном шпионское (30%), и майнеры — софт, использующий мощности зараженного компьютера для производства криптовалюты (23%).

Распространяют такой софт преимущественно по электронной почте (38%). Второй по популярности метод атак — социальная инженерия (например, фишинговые письма с требованием предоставить персональные данные; 29%), причем ее часто применяют одновременно с вредоносным ПО. Реже применялись хакинг (атаки, в ходе которых эксплуатируются уязвимости ПО, служб ОС, ошибки в механизмах защиты или другие недостатки систем; 20%), эксплуатация веб-уязвимостей (12%), подбор учетных данных (7%) и DDoS-атаки (3%).

Больше других от кибератак пострадали частные лица: на обычных людей были нацелены 28% атак за первый квартал. В этом случае, как правило, был использован вредоносный софт: шпионское ПО (34% случаев заражений), майнеры криптовалюты (27%) и софт для распространения рекламы (18%). Это может быть связано с отсутствием антивирусов и невнимательностью пользователей, полагают авторы отчета. Госучреждения атаковали в 16% случаев…

Организации в целом стали лучше защищать информацию, обойти эту защиту напрямую злоумышленникам становится более затратно, поэтому они и прибегают к методам социальной инженерии, поясняет руководитель отдела аналитики InfoWatch Сергей Хайрук. Для такой атаки мошенникам нужен минимум информации о жертве, например общий e-mail организации, имя и контактные данные сотрудника. Все это можно найти в интернете. Ценность информации растет, отмечает господин Хайрук, и государства уже начали на законодательном уровне устанавливать правила обработки данных, примером чего может служить новый европейский закон GDPR.» ***(Кристина Жукова. Имена дороже денег. Хакеры нацелились на персональные данные // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3661328?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 18.06.2018).***

***

«…CNews изучил план мероприятий программы "Цифровая экономика" по разделу "Информационная безопасность" и структуру соответствующих затрат. Документ был утвержден правительственной комиссией по использованию ИТ для улучшению жизни граждан и условий предпринимательской деятельности.

Всего за 2018-2020 гг. на описанные в плане мероприятия планируется потратить 34,04 млрд руб. Из них 22,33 млрд руб. будут взяты из федерального бюджета, 11,71 млрд руб. из внебюджетных источников…

Из задач, заложенных в плане мероприятий, наиболее дорогостоящей является "Обеспечение устойчивости и безопасности функционирования информационных систем и технологий". На эти цели будет направлено 16,91 млрд руб., в том числе 7,93 млрд руб. из федерального бюджета, 8,98 млрд руб. из внебюджетных источников…

Из конкретных мероприятий наиболее дорогостоящим является "Грантовая поддержка малых инновационных предприятий по разработке отечественного ПО". На эти средства будет выделено 5,3 млрд руб., из которых 4 млрд руб. будут взяты из федерального бюджета, 1,3 млрд руб. – из внебюджетных источников. Исполнителем мероприятия будет "Фонд содействия развитию малых форм предприятий в научно-технической сфере".

В целом весь комплекс мероприятий по поддержке отечественных разработчиков ПО обойдется в 17,96 млрд руб. Из этой суммы федеральный бюджет направит 6,86 млрд руб., а из внебюджетных источников будет взято 11,1 млрд руб…

В плане мероприятий говорится и об образовательной составляющей. На соответствующие мероприятия будет затрачено 4,52 млрд руб., большую часть данной суммы выделит федеральный бюджет…

1,59 млрд руб. федеральный бюджет потратит на реализацию мероприятий в рамках развертывания Государственной системы обнаружения предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Этим проектом занимается ФСБ…

Ряд мероприятий связан с созданием информационной системы (ИС) "Интернет", которая будет отвечать за критическую инфраструктуру российского сегмента глобальной сети. Общий размер затрат по этим мероприятиям составит 2,1 млрд руб, все они будут финансироваться из федерального бюджета…

800 млн руб. будет потрачено на организацию выдачи денежных премий (призов) за найденные уязвимости в программном и программно-аппаратном обеспечении. Из этой суммы федеральный бюджет выделит 500 млн руб., остальные 300 млн руб. будут взяты из внебюджетных источников…

Изначально проект плана мероприятий программы "Цифровая экономика" по разделу "Информационная безопасность" писался центром компетенций, созданным на базе Сбербанка. Документ предполагал общий объем затрат на уровне 116,85 млрд руб., из которых из федерального бюджета следовало бы выделить 100,17 млрд руб., а 16,68 млрд руб. из внебюджетных источников.

Затем отзыв на документ составила рабочая группа, которой руководила глава компании Infowatch Наталья Касперская. Эксперты высказали ряд отрицательных замечаний по ряду заложенных в документ мероприятий. Затем документ был отправлен в правительственную подкомиссию по цифровой экономики.

После этого заложенные в документе мероприятия и затраты по ним были значительно сокращены. Общий размер затрат будет в 3,5 раза меньше - 34,04 млрд руб. Из них 22,33 млрд руб. будут взяты из федерального бюджета (сокращение почти в пять раз), 11,71 млрд руб. из внебюджетных источников…» ***(Затраты на кибербезопасность в России урежут в 3,5 раза. Кто лишится денег // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123585). 21.06.2018).***

***

«Вооруженные силы РФ получат "сверзащищенный iCloud" — закрытое "облачное" хранилище для служебной и секретной информации. Минобороны

приступило к созданию сети территориально распределенных катастрофоустойчивых центров обработки данных (ТрКЦОД). Эту систему подключат к "военному интернету", не соединенному с обычным. Сегмент будущего комплекса уже функционирует в Южном военном округе. Стоимость всего проекта оценивается в 390 млн рублей.

Как рассказали "Известиям" в Минобороны, формирование ТрКЦОД будет завершено к 2020 году. За создание и развитие системы отвечает Главное управление развития информационных и телекоммуникационных технологий МО России. В нынешнем году будет выполнен основной объем работ, который обойдется государству в 245 млн рублей. Планируется, что полная стоимость системы составит 390 млн, пишут "Известия".» ***(Минобороны создает военное облачное хранилище // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123315). 05.06.2018).***

***

Інші країни

«Национальное собрание Вьетнама приняло во вторник закон о кибербезопасности, который вступит в силу 1 января 2019 года. Прежде всего, все местные и международные компании, собирающие и анализирующие данные своих пользователей, среди которых есть вьетнамские граждане, обязаны хранить эту информацию на серверах во Вьетнаме, а также иметь в стране офис. Те же компании должны будут проверять информацию о пользователях во время их регистрации и предоставлять данные о них по запросу отдела по кибербезопасности Министерства общественной безопасности Вьетнама.

Кроме того, закон запрещает использовать киберпространство для саботирования государственного строя и подрыва национального единства, оскорблять чувства верующих, распространять ложную информацию, которая спровоцирует социально-экономические потери, пропагандировать преступность, а также распространять порнографию. Все же незаконные с точки зрения государства материалы должны удаляться социальными сетями и прочими интернет-сервисами в течение суток после получения соответствующего запроса от Министерства информации и телекоммуникаций.» ***(Кирилл Сарханянц. Национальную безопасность Вьетнама оградили от вредных постов и комментариев // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3656805). 12.06.2018).***

***

«Одного из самых известных блогеров Японии закололи до смерти после его семинара о том, как разрешать личные споры в Интернете.

…Кеничиро Окамото, более известный как Хагекс, в воскресенье вечером был убит человеком, с которым он ругался в Интернете.

…Преступник сдался властям через три часа после нападения…» ***(Ирина Фоменко. Японского блогера закололи насмерть после его лекции // Internetua***

(http://internetua.com/yaponskogo-blogera-zakololi-nasmert-posle-ego-lektcii). 27.06.2018).

***

Протидія зовнішній кібернетичній агресії

«За ініціативою Литви країни Європейського союзу (ЄС) починають створювати сили швидкого кібернетичного реагування…

У понеділок протокол про наміри підписали в Люксембурзі міністри оборони Литви, Естонії, Хорватії, Нідерландів та Румунії.

«Франція, Іспанія, Польща і Фінляндія до ініціативи долучаться до кінця року», – заявив міністр оборони Литви Раймундас Каробліс.

Як повідомляється, країни ЄС передбачають створення кібернетичних команд з ротацією кожні шість місяців. Вони могли б прийти на допомогу державам-членам у разі великих кібернетичних інцидентів…». ***(За ініціативою Литви в ЄС створять сили швидкого кібернетичного реагування // Західна інформаційна корпорація (https://zik.ua/news/2018/06/25/za_initsiatyvoyu_lytvy_v_yes_stvoryat_syly_shvydkogo_kibernetychnogo_1353273). 25.06.2018).***

***

«Восемь из наиболее влиятельных компаний технологической индустрии, ожидая повторения ситуации с российским вмешательством в президентские выборы в 2016 году, встретились с разведслужбами США в прошлом месяце для обсуждения подготовки к промежуточным выборам…

На встрече, состоявшейся 23 мая в штаб-квартире Facebook в Менло-Парке, штат Калифорния, также присутствовали представители Amazon, Apple, Google, Microsoft, Oath, Snap и Twitter. Сотрудники компаний встретились с заместителем секретаря Министерства внутренней безопасности США Кристофером Кребсом и представителем ФБР.

Такие предприятия, как Facebook и Twitter, меняют методы своей работы для борьбы с дезинформацией, подрывавшей деятельность социальных сетей в 2016 году. Майская встреча стала первой важной дискуссией между группой технических компаний и разведслужбами в преддверии промежуточных выборов 2018 года…

…Как предполагают представители разведслужб, уже сегодня Россия и другие иностранные правительства вмешиваются в избирательную кампанию.

Facebook, в частности, сталкивается с серьезным давлением в борьбе с фейковыми новостями. Для компании информация о связях социальной сети с Россией стала сильным ударом: Facebook позволял российским агентам покупать рекламные объявления и управлять страницами социальной сети с целью повлиять на избирателей в Соединенных Штатах…» ***(Ирина Фоменко. Руководители крупнейших IT-компаний встречались с разведслужбами // Internetua***

(http://internetua.com/rukovoditeli-krupneishih-it-kompanii-vstrecsalis-s-razvedslujbami). 27.06.2018).

***

«Саммит Евросоюза (ЕС) дал поручение разработать предложения по реагированию организации на проблемы дезинформации и киберугрозы.

Как отмечается, план действий, включающий конкретные предложения по борьбе с дезинформацией и угрозами в сфере кибербезопасности должен быть представлен к декабрю этого года…» **(В ЕС решили разработать меры по противодействию дезинформации и киберугрозам // Goodnews.ua (http://goodnews.ua/technologies/v-es-reshili-razrabotat-mery-po-protivodejstviyu-dezinformacii-i-kiberugrozam/). 30.06.2018).**

***

«Одна из задач саммита G7 в канадском Квебеке – договориться о создании «информационного спецназа» для борьбы с российским влиянием…

Накануне встречи «группы семи» в Квебеке глава британского внешнеполитического ведомства Борис Джонсон анонсировал некий «план, пользующийся глобальной поддержкой». Его начальник – премьер Тереза Мэй – предложит G7 «учредить группу быстрого реагирования для выявления преступных действий России... кибератак или убийств»…

Запуск «европейского информационного спецназа» три года назад широко освещался в западных СМИ. Ключевой задачей контрпропагандистов называлась «коррекция и проверка фактов дезинформации и мифов»…» ***(Антон Крылов. Очередной «информационный спецназ» Запада постигнет судьба предыдущих // Деловая газета «Взгляд» (https://vz.ru/politics/2018/6/9/927167.html). 09.06.2018).***

***

«Британский парламент предупредил о якобы возможных кибератак со стороны российских спецслужб на компьютеры и другие девайсы болельщиков, которые приедут на ЧМ-2018 в Россию…

Возможность атаки ФСБ на девайсы не исключают в МИД Великобритании и в Центре национальной компьютерной безопасности страны.

Ранее сотрудникам британского парламента, которые намерены посетить в России матчи ЧМ-2018 по футболу, запретили брать с собой рабочие телефоны…» ***(Наталья Ануфриева. Британцев предупредили о возможной атаке ФСБ на девайсы во время ЧМ-2018 // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/9/927066.html). 09.06.2018).***

***

«Европейский союз и НАТО создали систему взаимных уведомлений в реальном времени о кибератаках, заявил генсек альянса Йенс Столтенберг…

В апреле Североатлантический альянс привлек более 1 тыс. специалистов из почти 30 стран для проведения масштабных международных учений в киберпространстве.

В ноябре 2017 года в НАТО заявили о мобилизации кибернетических возможностей стран-членов.» ***(Анна Инсарова. Евросоюз и НАТО решили оповещать друг друга о кибератаках // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/8/926923.html). 08.06.2018).***

***

«Північноатлантичний альянс (НАТО) та Європейського союзу (ЄС) запустили спільну систему повідомлень в режимі реального часу про погрози в кіберпросторі. Про це заявив генеральний секретар НАТО Йенс Столтенберг в Брюсселі, йдеться на сайті альянсу, передає "РБК-Україна".

Столтенберга повідомив, що між НАТО і ЄС були досягнуті угоди по 74 напрямках співробітництва, у тому числі з кібербезпеці і військового співробітництва…

Також Столтенберг зазначив, що сторони будуть проводити підготовку і навчання з протидії гібридним загрозам…» ***(ЄС та НАТО запустили систему повідомлень про кібератаки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/080618-yes-ta-nato-zapustyly-systemu-povidomlen-pro-kiberataky). 08.06.2018).***

***

«Пентагон розширив повноваження кіберкомандування збройних сил США, дозволивши представникам цього відомства здійснювати щоденні хакерські рейди на іноземні мережі для попередження кібератак…

«Нова стратегія передбачає постійну руйнівну діяльність на межі війни в зарубіжних комп'ютерних мережах», – йдеться у повідомленні.

Метою таких дій вважають «протистояння небезпечним діям противників, перш ніж ті зможуть завдати шкоди американським національним силам».

Зазначається, що це може збільшити ризик конфлікту США з іншими державами, які «спонсорують зловмисні хакерські групи». NYT вказує, що в цьому звинувачують, зокрема, Росію, Китай, Північну Корею та інші країни, що володіють ядерною зброєю…» ***(Пентагон дозволив армії США хакерські рейди на іноземні мережі, – ЗМІ // Західна інформаційна корпорація (https://zik.ua/news/2018/06/18/pentagon_dozvolyv_armii_ssha_hakerski_reydy_na_inozemni_merezhi__zmi_1348253). 18.06.2018).***

***

«В минувший четверг министерство внутренней безопасности США сообщило об активизации вредоносной киберактивности КНДР…

Центр исследования проблем нераспространения им. Джеймса Мартина (CNS), крупнейшая в США неправительственная организация, работающая в этой области, изучил работу северокорейской ИТ-индустрии, которая располагается не только на территории самой Северной Кореи, но и в ряде других стран Азиатско-Тихоокеанского региона. Сообщается, что главная задача северокорейской ИТ-индустрии — зарабатывать иностранную валюту, которая помогает стране возможность справляться с международными санкциями. Однако, как отмечают

авторы исследования, наибольшую обеспокоенность вызывает не факт обхода санкций, а то, что подставные северокорейские компании торгуют новейшими ИТ-технологиями в области кодирования данных и сканирования отпечатков пальцев и лица, а также технологиями искусственного интеллекта (ИИ)…

Эксперты CNS подчеркивают, что деятельность КНДР в ИТ-секторе представляет собой «угрозу кибербезопасности, масштабы которой серьезно недооцениваются»…

Министерство внутренней безопасности США в минувший четверг опубликовало очередное — уже одиннадцатое за последний год — предупреждение об активизации вредоносной киберактивности со стороны северокорейских властей. На тот момент прошло всего два дня с встречи Дональда Трампа и Ким Чен Ына в Сингапуре, но министерство совместно с ФБР сообщили о выявлении вредоносного ПО — в частности, 11 видов троянских программ — «для нанесения ущерба или выведения из строя компьютеров и компьютерных систем». «Этот тип вредоносного ПО известен как Typerframe»,— отмечает министерство, которое называет вредоносную киберактивность северокорейского правительства Hidden Cobra («затаившаяся кобра»).» ***(Алена Миклашевская. Северная Корея тайно приторговывает ИТ-технологиями и бесплатно рассылает компьютерные вирусы // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3661203?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 17.06.2018).***

***

«Глава німецького Федерального відомства з охорони конституції Ханс-Георг Масен звинуватив у нещодавній масштабній кібератаці на електромережі та енергетичні компанії Росію…

“Почерк злочинців — насправді лише один з індикаторів, що вказують на те, що атаку могли контролювати з Росії”, — зазначив він… Федеральне відомство з безпеки в сфері інформаційної техніки (BSI) повідомило про масштабну кібератаку “Berserk Bear” 13 червня.

За даними відомства, зловмисники намагалися вдертися в інтернет-мережі німецьких енергопостачальників. Хакерам, однак, вдалося зламати мережеву інфраструктуру лише в офісах декількох компаній…» ***(Олексій Супрун. Глава спецслужби ФРН звинуватив РФ у кібератаках на німецькі енергокомпанії // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1737242-glava-spetssluzhbi-frn-zvinuvativ-rf-u-kiberatakakh-na-nimetski-energokompaniyi). 21.06.2018).***

***

«Сполучені Штати Америки запровадили санкції проти п'яти російських компаній та трьох громадян за звинуваченнями у допомозі ФСБ у здійсненні кібератак…

Міністр фінансів США Стівен Мнучин (Steven Mnuchin) заявив, що нові санкції є кроком продидії зловмисникам, які працюють задля «розширення агресивних кіберзасобів Росії»…

Підприємствам та людям, проти яких запроваджені санкції, заборонені будь-які операції в межах американської фінансової системи. Також санкції забороняють американським компаніям та громадянам співпрацювати з компаніями та особами із санкційного списку.

Нові санкції також мають на меті обмежити діяльність Росії, пов'язану із підводними комунікаціями. У міністерстві фінансів США повідомили, що Росія веде активну діяльність, пов'язану із підводними кабельними комунікаціями, через які проходять світові телекомунікаційні дані.

До списку увійшли компанії Digital Security, ERPScan, Embedi, Kvant Scientific Research Institute (Kvant) та Divetechnoservices. Крім того, США наклали санкції на трьох керівників Divetechnoservices. Це Олександр Трібун (генеральний директор), Олег Чіріков (програмний директор) і Володимир Каганський (власник та колишній гендиректор). Вважається, що ця компанія спеціалізується на хакерських нападах на підводні комунікаційні системи…» ***(США запровадили нові санкції проти росіян через кібератаки // MediaSapiens (http://ms.detector.media/web/cybersecurity/ssha_zaprovadili_novi_sanktsii_proti_rosiyan_cherez_kiberataki/). 12.06.2018).***

***

«Німецька контррозвідка впевнена в тому, що як мінімум одну кібератаку на комп'ютерні мережі в ФРН здійснили спецслужби РФ. У Берліні планують приймати активні заходи. Коли офіційні представники німецької влади говорять про кібератаки з Росії на комп'ютерні мережі в Німеччині, то зазвичай додають, що їх вчиняють «імовірно», «ймовірно» або «скоріше всього» російські хакери, які перебувають на державній службі. В інтернеті, мовляв, неможливо зі стовідсотковою гарантією встановити національність і професійний статус кибершпиона.

Виступаючи на конференції з кібербезпеки, що проходить 21-22 червня в Потсдамі, керівник Федерального відомства по охороні конституції Ханс-Георг Ма (Hans-Georg Maßen) вперше заявив про свою впевненість у тому, що, принаймні, у випадку з кібератакою APT28 точно йдеться про операції російської спецслужби, а точніше — розвідки армії Росії. І він навіть знає, на якій вулиці в Москві працюють ці хакери в погонах…

Він упевнений, що великі операції в Мережі не під силу групами хакерів, а тим більше окремих «вільних художників», не пов'язаним з державними структурами. Тому в більшості випадків його відомство говорить про «ймовірності» або «високою часткою імовірності» того, яка спецслужба це була, орієнтуючись за непрямими даними: хто став жертвою кібератаки, які відомості цікавили зломщика і які цілі він переслідував…

Крім нарощування активності зарубіжних і, зокрема, російських хакерів у німецьких комп'ютерних мережах, Федеральне відомство з охорони конституції зазначає і деяка зміна в їх методикою.

…Ма, зокрема, заявив, що деякі, ймовірно російські атаки, ведуться дуже відкрито, їх і не намагаються приховувати, як це було у випадках з Sofacy і APT28…

Ще одне нововведення зарубіжних спецслужб у німецьких комп'ютерних мережах Ма бачить в тому, що багато кібератаки ведуться без конкретної мети, стріляють «наче з дробовика, навмання, авось куди-небудь потраплять і викачують все, що попадеться». Задум, за його словами, можливо, полягає в тому, щоб в разі ескалації політичної вже мати свої закладені в німецькі мережі міни, якими можна було б скористатися для проведення актів саботажу або демонстрації своєї сили і можливостей…

Про можливості, якими володіють спецслужби в країнах з автократичними режимами, розповідав на конференції у Потсдамі заступник директора Федеральної розвідувальної служби (BND) генерал-майор Вернер Чесні (Werner Sczesny).

В правовій державі — такому, як Німеччина — спецслужба працює в жорстко окреслених рамках чинного законодавства, перебуває під пильною парламентських наглядом і регулярно звітує перед депутатами. Тут деколи роками сперечаються про повноваження правоохоронних органів перш, ніж внести зміни до відповідного закону.

В автократичних ж державах, підкреслив Чесні, це робиться в два рахунки. «Там немає дискусій про те, що дозволено, а що не дозволено спецслужбі, — заявив він. — Лімітуючі фактори у деяких з таких країн — не закон і право, а тільки технічні можливості і ресурси», яких, за його словами, стає все більше…

Німецький уряд має намір нарощувати можливості бундесверу і спецслужб по захисту від кібератак та прийняття відповідних заходів.

Мова при цьому йде не тільки про постійної оптимізації пасивної безпеки, але і про активні заходи у відповідь у разі масивних кібернападів на цілі в Німеччині, розповів на конференції у Потсдамі держміністр у відомстві федерального канцлера Хендрік Хоппенштедт (Hendrik Hoppenstedt)…» ***(Чим відповість Берлін на кібератаки Росії? // Українська служба швидких новин (https://novosti.ternopil.ua/chim-vidpovist-berlin-na-kiberataki-rosi%d1%97/). 22.06.2018).***

***

«У США заявили, що китайські хакери здійснили масштабну кібератаку на оборонні, космічні та телекомунікаційні комплекси Штатів. Про це повідомляє ONLINE.UA з посиланням на агентство Reuters. За попередньою інформацією, влада КНР ініціювала атаку на державному рівні, щоб перехопити військовий і цивільний трафік…

Вказано, що першими можуть бути вражені пристрої Apple, DragonFly BSD Project, FreeBSD Project, ядро Linux, Microsoft, Red Hat, SUSE Linux, Ubuntu, VMware, Xen. Як повідомляв ONLINE.UA, раніше російські хакери в ніч на 20 квітня влаштували атаку на сервіс Google Maps для того, щоб змінити інформацію про Роскомнагляд.» ***(Це може вплинути на весь світ: хакери здійснили масштабну кібератаку на космічні комплекси США // ONLINE.UA***

(https://novyny.online.ua/798797/tse-mozhe-vplinuti-na-ves-svit-hakeri-zdiysnili-masshtabnu-kiberataku-na-kosmichni-kompleksi-ssha/). 22.06.2018).

***

Кіберзахист критичної інфраструктури

«…Министерство обороны РФ начало разработку технологий на базе блокчейна, предназначенных для защиты критически важной информационной инфраструктуры от кибератак. За внедрение технологии отвечает 8-е главное управление МО РФ, а работы проводятся в лаборатории в составе военного технополиса «ЭРА»…

Открытие комплекса запланировано на сентябрь нынешнего года, но исследования уже ведутся в дистанционном режиме…» ***(Минобороны России для защиты от кибератак применит blockchain // РосКомСвобода (https://roskomsvoboda.org/40014/). 29.06.2018).***

***

«Міністерство внутрішньої безпеки США продовжує досліджувати захисні заходи цивільного авіатранспорту, і результати поки невтішні. Такий висновок зробив ресурс Motherboard, вивчивши доповіді цього відомства…

З документів випливає, що лайнери слабо захищені від кібератак, і виробники приділяють цьому недостатньо уваги. Наприклад, в минулому році в рамках експерименту фахівці Міністерства внутрішньої безпеки віддалено отримали контроль над Boeing 737.

Ризик катастрофи великий, вважають фахівці: «Поява дірки в кіберзахисту лайнерів — лише питання часу». Додаткова проблема — Wi-Fi на борту деяких літаків Boeing і Airbus. Гіпотетично, через злом мережі зловмисники теж можуть захопити управління повітряним судном.

У той же час представник Boeing Підлогу Бергман зазначив, що авіавиробник серйозно ставиться до захисту своїх літаків від хакерських атак і використовує для цього ряд заходів.» ***(Хакери можуть легко зламати цивільні літаки – експерти // UkrMedia інтернет-газета (https://ukr.media/science/361020/). 07.06.2018).***

***

«Банки выстроили достаточно эффективные барьеры для защиты от внешних атак, однако не готовы противостоять нарушителям во внутренней сети. Преодолевая периметр с помощью социальной инженерии, уязвимостей веб-приложений или инсайдеров, злоумышленники оказываются в комфортной для себя среде, уровень безопасности которой не отличается от компаний из других сфер.

При наличии доступа к внутренней сети банка специалистам Positive Technologies удалось получить доступ к финансовым приложениям в 58% случаев. В 25% банков были скомпрометированы узлы, с которых осуществляется управление банкоматами…

В 17% банков недостаточно защищены системы карточного процессинга, что позволяет злоумышленникам манипулировать балансом на своих карточных счетах…

В отчете отмечается, что уровень защиты сетевого периметра в банках значительно выше, чем в других компаниях: за три года в рамках внешнего тестирования на проникновение доступ ко внутренней сети был получен в 58% систем, а для банков этот показатель составил лишь 22%. Однако и такой уровень весьма далек от идеала, учитывая высокую финансовую мотивацию атакующих и отсутствие во многих банках практики анализа защищенности кода онлайн-сервисов на этапах проектирования и разработки…

Большую опасность для банков представляют также интерфейсы удаленного доступа и управления… Среди наиболее распространенных — протоколы SSH и Telnet, которые встречаются на периметре сети свыше половины банков, а также протоколы доступа к файловым серверам (в 42% банков).

Но самое слабое звено — сотрудники банков. Злоумышленники легко обходят системы защиты сетевого периметра с помощью простого и эффективного метода — фишинга, который доставляет вредоносное ПО в корпоративную сеть… По оценкам Positive Technologies, в среднем в банках по фишинговой ссылке переходили около 8% пользователей и 2% запускали вложенный файл…

После того, как преступники получают доступ к локальной сети банка, им необходимо завладеть привилегиями локального администратора на компьютерах сотрудников и серверах — для дальнейшего развития атаки. Типовые векторы атак базируются на двух основных недостатках — слабой парольной политике и недостаточной защите от восстановления паролей из памяти ОС…

Внутри сети атакующие свободно перемещаются незамеченными с помощью известных уязвимостей и легитимного ПО, которое не вызывает подозрений у администраторов. Пользуясь недостатками защиты корпоративной сети, злоумышленники за короткое время получают полный контроль над всей инфраструктурой банка…». ***(Как хакеры грабят банки // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5504169-Kak-xakery-grabyat-banki.html). 06.06.2018).***

***

«Широко распространенная технология отслеживания кораблей может быть взломана злоумышленниками для подмены данных о размере и местоположении судов, что может потенциально привести к столкновению кораблей. Об этом сообщил исследователь безопасности Кен Мунро (Ken Munro) журналистам канала BBC.

Как полагает исследователь, эксплуатация уязвимости в данной технологии может привести к серьезным последствиям, вплоть до блокировки пролива Ла-Манш…

Уязвимость затрагивает электронно-картографическую навигационно-информационную систему (ЭКНИС), которая предоставляет экипажам альтернативу использованию бумажных карт…

В случае успешной атаки злоумышленники могут изменить местоположение корабля в пределах 300 метров, а также информацию о его размере.

Помимо этого, киберпреступники способны включать и отключать автоматическую идентификационную систему (AIS, Automatic Identification System) судна, что в свою очередь может создать экипажу множество проблем, в том числе привести к аварии.» ***(Обнаружен способ взлома навигационной системы морских судов // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123419). 09.06.2018).***

***

«Исследователь безопасности из компании IO Active Рубен Сантамарта (Ruben Santamarta) успешно взломал Wi-Fi сети и оборудование спутниковой связи находящегося в воздухе самолета с земли…

Эксперту удалось подключиться к бортовым сетям Wi-Fi, в том числе к устройствам пассажиров, а также получить доступ к важным спутниковым и коммуникационным устройствам в самолете.

Исследователь планирует продемонстрировать, как именно он получил доступ к самолетам и бортовым устройствам спутниковой связи на конференции Black Hat, которая будет проходить с 4 по 9 августа 2018 года в Лас-Вегасе (США). Сантамарта намерен рассказать, каким образом оборудование для спутниковой связи может быть превращено в оружие и в конечном итоге создать угрозу безопасности самолета.

По словам специалиста, он использовал аналогичные методы для поиска нескольких военных объектов НАТО в зонах конфликтов, а также смог получить доступ к сетям морских судов.

Ранее Сантамарта обнаружил уязвимость в мультимедийной системе Panasonic Avionics, используемой на борту самолетов 13 крупных авиакомпаний, в том числе Air France и American Airlines, позволяющую хакерам удаленно перехватить контроль над самолетом.» ***(Исследователь успешно взломал системы летящих самолетов с земли // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123366). 06.06.2018).***

***

Захист персональних даних

«…Криптовалютная биржа Bitkoex сообщила об утечке информации… Под угрозу были поставлены средства пользователей на сумму в 620 тыс. долл. Один из сотрудников опубликовал в групповом чате приложения Kakao информацию об инвестициях в токены Karma и указал электронную почту, кошельки и приватные ключи от них 19 клиентов…

В Bitkoex заявили, что инцидент произошел случайно, деньги сейчас находятся в полной безопасности. На данный момент неизвестно, что кто-то из клиентов пострадал.» ***(Bitkoex опубликовала приватные данные 19 клиентов // «Открытые системы» (https://www.computerworld.ru/news/Bitkoex-opublikovala-privatnye-dannye-19-klientov). 26.06.2018).***

***

«Персональная информация миллионов американцев оказалась в открытом доступе в незащищенной базе данных. Об этом сообщил ИБ-эксперт Винни Троя (Vinny Troia) после изучения выборки интернет-серверов под управлением движка ElasticSearch. Как сообщает исследователь, утечку конфиденциальных сведений допустила маркетинговая компания Exactis.

Аналитик использовал сервис Shodan для поиска открытых баз данных ElasticSearch. Проанализировав порядка 7000 таких хранилищ, Троя наткнулся на совершенно незащищенную подборку, которая содержала 340 млн записей.

В распоряжении специалиста оказались 2 терабайта данных, куда входили имена, домашние адреса и телефонные номера граждан США. Кроме того, выборка содержала информацию о миллионах американских предприятий и организаций…

Помимо анкетных данных, массив информации включал в себя широкий спектр дополнительных метрик, таких как отношение к курению, сведения о домашних животных, религиозные убеждения и интересы человека…

Исследователь сообщил о своей находке в ФБР и журналистам. Exactis пока никак не отреагировала на запросы прессы относительно утечки. В данный момент компания закрыла доступ к скомпрометированной базе данных…» ***(Dmitry Nazarov. Из базы данных Exactis могли уплыть 340 млн записей // Threatpost (https://threatpost.ru/exactis-database-exposed-340m-records/26933/). 29.06.2018).***

***

«Facebook Inc. оспаривает отчет New York Times о распространении компанией данных производителям устройств, от Apple и Amazon до Samsung…

The New York Times сообщил, что Facebook заключал сделки с производителями устройств, позволяющие им получать полный доступ к информации о пользователях и их друзьях…

В понедельник Андреа Елинек, отвечающий за соблюдение законодательства Европейского союза о конфиденциальности данных, заявил, что регулирующие органы намерены изучить отчеты. А регулятор конфиденциальности Гамбурга Йоханнес Каспар охарактеризовал их как "очень тревожные".

"Пришло время прекратить любые незаконные действия Facebook, особенно передачу пользовательских данных третьим лицам…", - утверждает Каспар…

The New York Times сообщил, что некоторые компании, среди прочего, могут получать информацию о статусе отношений людей, их религии и политических взглядах…» ***(Ирина Фоменко. Facebook "сливал" данные пользователей производителям телефонов // Internetua (http://internetua.com/facebook-slival-danne-polzovatelei-proizvoditelyam-telefonov). 05.06.2018).***

***

«Популярное приложение для футбольных болельщиков La Liga использует инструменты для тайной слежки за пользователями. Программа

записывает разговоры пользователей и отслеживает их местоположение для борьбы с пиратскими трансляциями матчей, сообщает издание El Pais.

При установке на Android-смартфоны приложение запрашивает разрешение на доступ к микрофону и определению местоположения. Авторы программы подтвердили факт записи разговоров и отслеживания геолокации.

По словам разработчиков La Liga, данная мера призвана помочь в борьбе с различными заведениями, транслирующими футбольные матчи без соответствующей лицензии. Нелегальные трансляции приводят к потерям испанской лигой порядка 150 млн евро ежегодно, добавили они.

Функция записи разговоров включается только в часы проведения матчей чемпионата испанской лиги.» ***(Приложение для футбольных болельщиков La Liga следит за пользователями // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123439). 13.06.2018).***

***

«**Facebook решила в конце недели прекратить действие партнерского соглашения с Huawei, открывающее китайской компании доступ к персональным данным пользователей.**

…Соответствующее соглашение с Huawei было заключено в 2010 г. Подобные договоренности у Facebook есть с другими китайскими компаниями, в том числе Lenovo, Oppo и TCL.

…соцсеть за последние 10 лет заключила такие контракты минимум с 60 крупнейшими производителями электронных устройств… все они ставят под сомнение соблюдение компанией Марка Цукерберга правил защиты данных пользователей и требований федеральной комиссии по торговле США…» ***(Facebook намерена закрыть Huawei доступ к личным данным пользователей // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123347). 06.06.2018).***

***

«**Эксперты компании Kenna Security выяснили, что более 31% организаций, использующих Google Groups и G Suite, рискуют в любой момент столкнуться с утечкой конфиденциальной информации из электронной почты.**

G Suite - это набор облачных приложений для организации совместной работы, прежде называвшийся Google Apps for Work и Google Apps for your Domain. В набор входят все популярные приложения Google, адаптированые для корпоративных сред, - Gmail, Hangouts, Calendar и Google+; Docs, Sheets, Slides, Forms, Sites и Jamboard; Google Drive для хранения данных, и, в зависимости от тарифного плана - администраторская панель и решение Vault для управления пользовательскими аккаунтами и службами.

Ещё в 2017 г. Kenna Security опубликовали бюллетень, в котором указывалось, что из G Suite возможны утечки, но на него тогда не обратили достаточного внимания.

Проблема, по данным экспертов Kenna Security, заключается в том, что в настройках Google Groups используется "слишком сложная терминология" и не

везде понятно, какие настройки в каких случаях требуются. В результате доступ к содержимому почтовых рассылок могут получать посторонние лица…

Индивидуальные настройки приватности Google Group могут выставляться на уровнях отдельного домена и отдельной группы. В организациях, где были отмечены проблемы, значение настроек доступности групп извне домена (пункт Group Visibility в консоли admin.google.com) выставлена в значение Public on the Internet", - говорится в публикации Kenna Security…

Представители Kenna Security пытались убедить Google сделать настройки (ещё более) очевидными и понятными, однако в Google не видят проблемы и не планируют ничего менять…

Единственный способ закрыть "уязвимость", указывают авторы исследования, это всегда выставлять значение Private в настройках приватности и - читать мануалы внимательнее…» ***(Секретная информация компаний утекает в Сеть через G Suite и Google Groups // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123329). 05.06.2018).***

***

Кіберзлочинність та кібертероризм

«…«Лаборатория Касперского», подсчитала, что количество интернет-пользователей по всему миру, ставших жертвами криптомайнеров, выросло с 1,9 миллиона в 2016-2017 годах до 2,7 миллиона в 2017-2018. Киберпреступники создают специальное ПО, способное к майнингу. Они получают меньшую прибыль, чем от программ-вымогателей, однако могут делать это незаметно и в течение более длительного времени.

В марте Check Point сообщила, что от майнинга уже пострадали 42% компаний во всем мире…» ***(«Лаборатория Касперского»: за год число атак криптомайнеров выросло на 44% // «Открытые системы» (https://www.computerworld.ru/news/Laboratoriya-Kasperskogo-za-god-chislo-atak-kriptomaynerov-vyroslo-na-44). 28.06.2018).***

***

«…Киберпреступники постепенно отказываются от массовых атак и применения готовых инструментов взлома, предпочитая более выгодный направленный шантаж, заключают специалисты компании Trend Micro в докладе о состоянии компьютерной безопасности в мире в 2017 году. Их целями являются самые ценные активы компании: деньги, данные и репутация. Число семейств вымогательских программ с 2016 годы выросло на 32%, число попыток взлома корпоративной почты увеличилось вдвое между первой и второй половиной 2017 года, а число выявленных заражений вирусами-майнерами криптовалют в октябре достигло 100 тыс.

В 2018 году, полагают специалисты, появится новый вид вымогательства. Преступники будут требовать от компаний выкупа за отказ от атаки, результатом которой может быть нарушение компанией директивы ЕС о защите данных

(GDPR)…» ***(Trend Micro: преступники готовятся шантажировать нарушением GDPR // «Открытые системы» (https://www.computerworld.ru/news/Trend-Micro-prestupniki-gotovyatsya-shantazhirovat-narusheniem-GDPR). 26.06.2018).***

***

«…Компания Fortinet предупредила о необходимости сохранять бдительность в связи с вероятным увеличением числа кибератак во время чемпионата мира по футболу 2018… Они предлагают пять рекомендаций по защите от киберугроз.

Во-первых, смотреть прямые трансляции и повторы следует только на проверенных сайтах, иначе можно столкнуться с фишинговыми атаками. Кроме того, злоумышленники могут создавать подставные веб-сайты и домены, замаскированные под официальные ресурсы, но на самом деле использующиеся для доставки вредоносного кода на устройства конечных пользователей. Во-вторых, стоит с осторожностью относиться к сообщениям о том, что адресат электронной почты выиграл билеты на финальный матч чемпионата мира. Щелкнув ссылку, можно попасть на веб-сайт с вредоносным кодом, предназначенным для хищения частной информации.

В-третьих, необходимо соблюдать осторожность при совершении сделок с интернет-магазинами, предлагающими билеты с большой скидкой или дешевую атрибутику. Важно убедиться, что магазин действительно ведет коммерческую деятельность. В-четвертых, желательно регулярно обновлять программное обеспечение. В целях предотвращения заражения известными угрозами рекомендуется настроить автоматическое обновление средств защиты и веб-браузера…» ***(Fortinet: во время чемпионата мира по футболу возможно увеличение числа кибератак // «Открытые системы» (https://www.computerworld.ru/news/Vo-vremya-chempionata-mira-po-futbolu-vozmozhno-uvelichenie-chisla-kiberatak). 27.06.2018).***

***

«Стоимость биткойна впервые с ноября прошлого года опустилась ниже уровня $6 тыс. Обновлению семимесячного минимума способствовали сообщения об успешных кибератаках на южнокорейские биржи. В таких условиях эксперты прогнозируют дальнейшее падение криптовалюты до $3 тыс…

Участников рынка смущает частота атак, а также то, что незащищенными оказываются даже крупные биржи…» ***(Виталий Гайдаев. Хакеры подкосили биткойн // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3668061?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 25.06.2018).***

***

«Исследователи по вопросам безопасности из Team Cymru недавно сообщили результаты исследования, предполагающего, что было взломано выше 300 000 домашних роутеров. Эти скомпрометированные устройства

представляют серьезную угрозу безопасности для всех, кто использует такое подключение к Интернету…

В докладе отмечается, что пострадали домашние роутеры ряда популярных производителей (D-Link, Micronet, Tenda и TP-Link)…

Хакеры изменили настройки адреса DNS-сервера, используемого устройствами для подключения к сети…

Данный конкретный взлом затронул только не обновленные роутеры…» ***(Взломаны тысячи домашних роутеров. Что вы можете сделать? // SecurityLabRu (https://www.securitylab.ru/blog/company/PandaSecurityRus/344214.php). 27.06.2018).***

***

«По словам эксперта израильской компании по кибербезопасности Check Point Software Technologies (CHKP), связанные с криптовалютами преступления превысят количество других кибератак в 2018 году…

Выступая на панельной дискуссии в ходе мероприятия «Blockchain, The New Digital Age» в Тель-Авивском университете, эксперт CHKP Лотем Финкельстин заявил, что незаконная деятельность на рынке ICO является основным препятствием на пути развития технологии blockchain…» ***(Назван вид киберугроз, который превзойдет все остальные в 2018 году // PAYSPACE MAGAZINE (https://psm7.com/news/nazvan-vid-kiberugroz-kotoryj-prevzojdet-vse-ostalnye-v-2018-godu.html). 23.06.2018).***

***

«З початку 2018 року зловмисники викрали понад 1,1 мільярда доларів в криптовалюте…

Зазначається, що найчастіше мова йде не про злочинні угруповання, а про простих користувачів.

У компанії Carbon Black, працюючої у сфері кібербезпеки, нарахували в дарквебе 12 тисяч майданчиків з 34 тисячами пропозицій, якими можуть скористатися для викрадення коштів навіть далекі від хакерства і технологій особи.

Ціна на шкідливе ПЗ може стартувати від 1 долара, а в середньому вона коштує 224 долара і має власну підтримку.

У цілому ринок у компанії оцінили в 6,7 млн доларів.

Відзначається, що розкраданнями найчастіше безробітні займаються інженери, які шукають будь-який заробіток, а також організовані угруповання.

Атак часто піддаються криптобиржи: на них припадало 27% активності зловмисників. 21% атак пов'язаний з атаками на компанії: часто зловмисники зламують внутрішні системи і вимагають криптовалюту в якості викупу.

При цьому биткоины воліють 10% хакерів, Ethereum – 11%, а Monero – 44%.

Найбільша кількість інцидентів зафіксовано в США, Китаї і Великобританії…» ***(Павло Полтавченко. З початку року хакери вкрали $1,1 млрд у криптовалюте — Олігарх // Українська служба швидких новин***

(https://novosti.ternopil.ua/z-pochatku-roku-xakeri-vkrali-11-mlrd-u-kriptovalyute-oligarx/). 08.06.2018).

***

«…Eset проанализировала киберриски, связанные с чемпионатом мира по футболу. В компании выяснили, какие схемы мошенники способны использовать для кражи данных банковских карт. Например, они могут прибегнуть к социальной инженерии, чтобы получить идентификационные данные. Или применят для этого вредоносные программы, встроенные в видеоплееры. Также злоумышленники воспользуются моментом для тайной добычи криптовалюты…

По прогнозу специалистов, классические схемы тоже будут широко эксплуатироваться. К ним относятся массовые спам-рассылки по электронной почте, соцсетям и мессенджерам, регистрация подозрительных доменов, и «официальные распродажи» билетов на матчи или турпакетов в российские города, «розыгрыши призов» от лица ФИФА, ссылки на «эксклюзивные новости» о чемпионате, ведущие на вредоносные сайты.

Eset советует игнорировать спам-рассылки и «розыгрыши», использовать проверенные новостные сайты и легитимные стриминговые сервисы, а также установить на устройства антивирусное ПО.» ***(Eset: мошенники поджидают гостей ЧМ-2018 на фишинговых сайтах // «Открытые системы» (https://www.computerworld.ru/news/Eset-moshenniki-ispolzuyut-fishingovye-sayty-i-primenyat-sotsialnuyu-inzheneriyu-vo-vremya-ChM-po-futbolu). 14.06.2018).***

***

«Злочинна група, що містить ознаки організованості, облаштувала всесвітню веб-мережу фейками, за допомогою яких ошукувала громадян, які бажали провести операції з криптовалютою…

Злочинна група складалася з чотирьох осіб. Зловмисники… створили власну CMS-систему керування контентом сайтів-обмінників. Створені веб-ресурси імітували легальну діяльність веб-обмінників з різнонаправленої конвертації криптовалют та отримували фіктивні позитивні рейтингові відгуки.

Потерпілі переводили гроші на електронні гаманці, зареєстровані на підроблені документи іноземних громадян. Після зарахування коштів зловмисники припиняли роботу веб-обмінника, натомість відкривали новий шахрайський веб-ресурс.

Отримавши оперативну інформацію про діяльність шахраїв поліцейські розпочали кримінальне провадження за ч. 3 ст. 190 (шахрайство) КК України. У його межах працівники кіберполіції провели комплекс оперативних заходів, за результатами яких встановили осіб, причетних до даного злочину. Ними виявилися мешканці міста Дніпра від 20 до 26 років…

Наразі трьом учасникам злочинної групи оголошено про підозру у вчиненні шести епізодів шахрайської діяльності. Вилучену техніку направлено на проведення усіх необхідних експертиз…» ***(Кіберполіція викрила онлайн-шахраїв, які створили мережу фейкових веб-обмінників з конвертації криптовалют // Кіберполіція (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-onlajn-***

shaxrayiv-yaki-stvoryly-merezhu-fejkovyx-veb-obminnykiv-z-konvertacziyi-kryptovalyut-6428/). 16.06.2018).

***

«Выявлена фишинговая кампания, связанная с началом Чемпионата мира по футболу 2018. Кибермошенники рассылают зараженный файл под видом расписания игр и турнирной таблицы.

Как сообщают эксперты Check Point Software Technologies, во вложении фишинговых писем скрывается вредоносное ПО под названием «DownloaderGuide», который известен как загрузчик потенциально нежелательных программ… Исследователи Check Point обнаружили, что фишинговая рассылка включает различные исполняемые файлы, все из которых были отправлены по электронной почте с использованием темы: «World_Cup_2018_Schedule_and_Scoresheet_V1. ## _ CB-DL-Manager»…

Специалисты Check Point Software Technologies ожидают новые всплески онлайн-мошенничеств и фишинг-атак во время Чемпионата мира по футболу…» ***(Поклонники футбола подверглись фишинговой атаке // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5506958-Poklonniki-futbola-podverglis-fishi.html). 19.06.2018).***

***

«Специалисты по информационной безопасности из компании Sucuri выяснили, как злоумышленникам удается повторно заражать сайты под управлением CMS Magento. Киберпреступники внедряют скрипт для кражи паролей и данных банковских карт в файл config.php, к которому Magento обращается при формировании каждой страницы. Таким образом, вредоносный код снова загружается на ресурс…

Сторонний скрипт очень трудно обнаружить при помощи обычных средств безопасности веб-ресурсов, поскольку благодаря обфускации алгоритм выглядит, как легитимная часть кода…

Под управлением Magento работает более 300 тыс. веб-ресурсов. CMS, ориентированная на интернет-торговлю, является желанной целью для злоумышленников…» ***(Dmitry Nazarov. Злоумышленники научились повторно заражать сайты на Magento // Threatpost (https://threatpost.ru/attackers-can-reinfect-magento-web-sites/26777/). 21.06.2018).***

***

«Как оказалось, ботоводы, использующие слабость паролей для распространения инфекции, иногда сами совершают ту же ошибку, что и жертвы заражения. Аналитик из NewSky Security Анкит Анубхав (Ankit Anubhav) недавно обнаружил в инфраструктуре двух IoT-ботнетов базы данных, доступ к которым защищен простейшей комбинацией root/root.

По словам эксперта, обе бот-сети построены на основе Owari — одной из многочисленных итераций Mirai, атакующих сетевые устройства перебором дефолтных учетных данных.

Слабость защиты серверов MySQL, используемых ботоводами, позволила исследователю получить доступ к базам данных (на порту 3306) и просмотреть информацию о заражениях, а также об операторах и арендаторах этих IoT-ботнетов.

Судя по найденных записям, сдаваемые в аренду ботнеты используются для проведения DDoS-атак… В комментарии для Bleeping Computer Анубхав отметил, что это обычная практика у операторов вредоносных сетей: они часто меняют IP-адреса своих центров управления, чтобы избежать блокировки…» ***(Maxim Zaitsev. Операторы IoT-ботнетов повторили ошибки своих жертв // Threatpost (https://threatpost.ru/iot-botmasters-making-same-mistake-as-their-victims/26449/). 06.06.2018).***

***

«После отключения серверов крупнейших торговых площадок даркнета AlphaBay и Hansa летом 2017 года киберпреступники переключились на использование альтернативных децентрализованных платформ, например каналов в мессенджере Telegram, следует из отчета экспертов по безопасности из компании Digital Shadows.

Согласно докладу, Telegram стремительно набирает популярность. За последние шесть месяцев исследователи обнаружили более 5 тыс. ссылок на Telegram-каналы на различных подпольных форумах, из которых 1 667 ссылок представляли собой приглашения в новые группы. Киберпреступники предлагали целый ряд услуг, включая обналичивание похищенных средств, кардинг и мошенничество с криптовалютами.

"Как правило, когда исчезает популярный рынок, появляется другой. Таким образом, последствия действий правоохранительных органов относительно недолговечны, а киберпреступники всегда на шаг впереди. Однако в данном случае этого не произошло и вместо этого злоумышленники ушли на альтернативные платформы", - отметили специалисты.

Помимо этого, некоторые киберпреступники начали использовать сервисы на основе блокчейна, полагая, что таким образом им удастся защититься от правоохранительных органов, заключили исследователи.» ***(После отключения двух крупнейших торговых площадок даркнета киберпреступники переключаются на каналы в чатах // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123406). 08.06.2018).***

***

«Как следует из опубликованного сенатором Роном Уайденом (Ron Wyden) письма, полученного им от Министерства внутренней безопасности (МВБ) США, для хищения данных преступники проэксплуатировали уязвимость в системе ОКС-7 и разместили аппаратуру, похожую на устройство для отслеживания мобильных телефонов Stingray. Данное оборудование маскируется под вышку сотовой связи и подключается к телефонам, позволяя собирать уникальные идентификационные номера и, потенциально, прослушивать переговоры…

"Известие о возможном иностранном Stingray возле Белого дома вызывает серьезную обеспокоенность, особенно после сообщений, что президент даже не использует безопасный телефон для защиты своих звонков", - заявил Уайден.

…Возобновление активности ботоводов VPNFilter, которыми предположительно являются участники APT-группы Sofacy, обнаружили эксперты JASK и GreyNoise Intelligence. Ссылаясь на их наблюдения, репортер Bleeping Computer пишет, что новые сканы замечены лишь на Украине и нацелены на выявление роутеров Mikrotik с открытым портом 2000.

Ботнет VPNFilter, составленный из 500 тыс. роутеров и NAS-устройств, привлек внимание ИБ-сообщества этой весной, когда сканирование с целью наращивания его потенциала стало очевидным…

Анализ показал, что зловред, на основе которого построен данный ботнет, состоит из трех компонентов, при этом сначала загружается модуль, от которого невозможно избавиться перезапуском. Два последующих плагина таким свойством не обладают, но могут быть повторно загружены. Третий компонент — самый опасный, так как он умеет стирать данные, эффективно выводя сетевое устройство из строя.

Попытка ликвидировать VPNFilter была предпринята в прошлом месяце. ФБР с разрешения суда захватило контроль над одним из C&C-доменов ботнета, что позволило запустить кампанию по выявлению зараженных устройств и очистке.

Судьба украинского центра управления бот-сетью неизвестна. По всей видимости, он продолжает функционировать, и злоумышленники решили использовать эту возможность для восстановления своих боевых порядков.» ***(Maxim Zaitsev. VPNFilter пытается вернуться // Threatpost (https://threatpost.ru/vpnfilter-attempting-to-return/26382/). 04.06.2018).***

***

Діяльність хакерів та хакерські угруповування

«…Хакеры стали использовать искусственный интеллект при кибератаках на банки, передает ТАСС заявление заместителя председателя правления Сбербанка Станислава Кузнецова.

По словам Кузнецова, атаки стали модифицироваться, опираясь на технологии искусственного интеллекта, чтобы можно было получать информацию о построении защиты, об архитектуре технологических и операционных систем банка, в том числе систем безопасности.

Он также отметил, что Сбербанк является для хакеров мишенью номер один среди кредитных организаций. В целом с начала года количество кибератак на банковский сектор увеличилось на 1,5-1,8 раза.

Сбербанк предложил организовать в России независимую роботизированную систему, с помощью которой банки смогут обмениваться информацией об актуальных угрозах, реагировать на инциденты и противодействовать фишинговым атакам. За основу предложено взять платформу по обмену данными об инцидентах, которая разработана и применяется в Сбербанке.

По словам Кузнецова, она агрегирует более 1 млн индикаторов в сутки и имеет актуальную информацию об угрозах в режиме онлайн. Нейронная сеть анализирует и оценивает шаблоны поведения клиентов, выявляет нетипичные для них действия и сообщает о них специалистам по безопасности.

Запуск платформы в промышленную эксплуатацию, предполагающую обмен информацией между Сбербанком и другими участниками финансового рынка, планируется 18 июня.» ***(Сбербанк: хакеры начали использовать искусственный интеллект // «Открытые системы» (https://www.computerworld.ru/news/Sberbank-hakery-nachali-ispolzovat-iskusstvennyy-intellekt). 09.06.2018).***

***

«Компания Symantec опубликовала во вторник отчет, согласно которому компании—операторы спутников, телекоммуникационные предприятия и подрядчики Министерства обороны США были атакованы группой хакеров с территории Китая. Хакерам удалось преодолеть защиту компьютеров, благодаря чему они якобы получили возможность даже менять траекторию полета космических спутников.

Компания Symantec, занимающаяся разработкой решений в области кибербезопасности, уже несколько лет следит за группой хакеров, называющих себя Thrip. Впервые в поле зрения корпорации они попали в 2013 году и с тех пор постоянно совершенствовали свои навыки взлома сетей. Недавно ими была совершена крупная атака на объекты США и стран Юго-Восточной Азии.

Среди взломанных объектов оказались оборонные предприятия, телекоммуникационные компании, а также компании, управляющие спутниками и занимающиеся составлением геопространственных карт. В отчете сообщается, что атака проводилась с территории Китая. Symantec уже передала данные о случившемся ФБР и Министерству обороны США…

Успешная атака Thrip означает, что злоумышленники могли перехватить и даже изменить данные, которые поступают от предприятий к их клиентам, говорится в отчете. «Препятствование работе спутников может привести к серьезным сбоям в работе гражданских и военных объектов»,— считает технический директор Symantec Викрам Тхакур.» ***(Кирилл Сарханянц. Американские спутники оказались в руках китайских хакеров. Symantec выявила крупномасштабную кибератаку из КНР // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3662913?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 20.06.2018).***

***

«Американская компания в области компьютерной безопасности FireEye заявила о кибератаках на южнокорейские интернет-ресурсы со стороны хакеров из России и Китая…

По сведениям FireEye, хакерская группировка Turla (предположительно базируется в России) заражала интернет-ресурсы с помощью вредоносного ПО на

языке JavaScript. Китайская группа TempTick распространяла файлы в формате Microsoft Word, в которых содержался вирус.

Сейчас FireEye оценивает ущерб от кибератаки. Какие конкретно сайты подверглись воздействию со стороны хакеров, компания не уточняет, однако отмечает, что среди них были правительственные ресурсы.» ***(Американская компания сообщила о российской кибератаке на Южную Корею // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3651056). 06.06.2018).***

***

«Хакеры из группировки Zacinlo открыли способ обойти защиту в Windows 10 и внедрить в ОС вирус…

Вирус может оставаться незамеченным годами при этом его функционал заключается в навязчивом показе рекламы, имитации кликов и скриншотах, который вредоносная программа отправляет по нужным взломщикам адресам.

Программа маскируется под бесплатный анонимный VPN-сервис s5Mark, а жертвами вируса уже стали жители США, Европы, Китая и Индии.

Исследователи отмечают: чтобы избавиться от вируса, необходимо запустить сканирование системных файлов в режиме восстановления…» ***(Дмитрий Зубарев. Хакеры обнаружили опасную уязвимость в ОС Windows 10 // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/19/928448.html). 19.06.2018).***

***

«Крупная южнокорейская криптовалютная биржа Bithumb подверглась хакерской атаке, в результате которой было похищено 35 млрд вон (около $31,5 млн)…

Атака была произведена с 19 на 20 июня 2018 г., в промежутке между поздним вечером и ранним утром по корейскому времени. …Bithumb заморозила операции по вводу-выводу средств и инициировала перевод уцелевших активов в холодные кошельки, которые в целях безопасности не подключены напрямую к интернету.

По данным аналитического сервиса CoinMarketCap, Bithumb занимает шестую позицию в рейтинге крупнейших криптовалютных бирж мира с суточным объемом торгов $396,51 млн. Самыми популярными криптовалютами на бирже являются EOS и TRON — около 33% и 22% от общего объема торгов соответственно. Далее идут Bitcoin (9,5%), Ethereum (8%) и другие криптовалюты.

Криптовалютных рынок отреагировал на новость падением курса биткоина более чем на 2% в первые полчаса, сообщает ресурс Bitcoinist.

За 10 дней до этого, в воскресенье, 10 июня, в Южной Корее хакерской атаке подверглась другая крупная криптовалютная биржа — Coinrail. Злоумышленникам удалось похитить криптовалюту на сумму более $40 млн. На момент ограбления биржа занимала в глобальном рейтинге CoinMarketCap 90-е место с суточным объемам торгов $2,6 млн.

Coinrail представляет собой популярный обменник токенов Pundi X на биткоины — на такие операции приходится до половины всех торгов. Pundi X и стал основной целью преступников, в результате чего биржа потеряла эти токены

на сумму $19,5 млн. Также хакеры украли токены Aston на сумму $13,8 млн, токены Dent стоимостью $5,8 млн и $1,1 млн в токенах Tron.

После атаки уцелело около 70% активов, которые Coinrail временно поместила в холодное хранилище…» ***(За 10 дней ограблены две крупнейшие криптовалютные биржи // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5507512-Za-10-dnej-ogrableny-dve-krupnejshi.html). 21.06.2018).***

***

«Експерти виявили нову кампанію по кібершпигунства з використанням як мінімум дев'яти проломів в платформі ActiveX, в числі яких zero-day. Імовірно за атаками стоїть угрупування Andariel - одна з дочірніх організацій Lazarus. Метою злочинців є розкрадання даних великих південнокорейських підприємств.

Як повідомляють дослідники безпеки, атаки почалися ще в минулому місяці. За прикладом батьківської угруповання учасники Andariel заражають легітимні сайти трояном, який потім передається відвідувачам. Зловмисникам залишається тільки чекати компрометації одного з пристроїв, які їх цікавлять організацій.

Кіберзлочинців з Lazarus, імовірно пов'язаних з керівництвом Північної Кореї, вже не вперше ловлять на експлуатації вразливостей в ActiveX. Як повідомляє представник південнокорейського агентства інтернет-безпеки (KISA), на цей раз в якості однієї з лазівок використовувалася уразливість нульового дня…

Andariel зв'язали з Lazarus південнокорейські дослідники з компанії AhnLab, причому це далеко не єдина дочірня організація кіберсіндіката, на рахунку якого - цілий ряд гучних інцидентів…» ***(Угруповання Andariel Group знайшло в ActiveX діру нульового дня // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2018/06/05/andariel-group-found-activex-0day-vulnerability.html). 05.06.2018).***

***

«В Міністерстві внутрішньої безпеки заявили, що хакери Північної Кореї продовжують здійснювати наймасштабніші кібератаки по всьому світу… «Мета цього сповіщення – дати розробникам антивірусів можливість виявити і зменшити небезпеку, яку несуть з собою заходи, здійснювані КНДР у кіберпросторі», – йдеться в заяві відомства. Працівники МВБ разом з колегами з ФБР виявили використовуваний офіційними органами КНДР комп’ютерний вірус, що атакує окремі комп’ютери і цілі мережі. Вірусу присвоєно найменування TYPEFRAME…» ***(МВБ США дізналося, хто організовує наймасштабніші кібератаки по всьому світу // ONLINE.UA (https://novyny.online.ua/798641/mvb-ssha-diznalosya-hto-organizovue-naymasshtabnishi-kiberataki-po-vsomu-svitu/). 15.06.2018).***

***

«Разработчик антивирусного программного обеспечения McAfee сообщил о резком росте вредоносных программ, которые скрытно устанавливаются на компьютеры и другие устройства для майнинга криптовалют. По итогам первого квартала объем зафиксированного компанией вредоносного программного обеспечения этого типа вырос более чем в шесть раз.

В июньском отчете McAfee Labs Threats Report исследователи проанализировали ситуацию с вирусами, вредоносными программами, вирусами-вымогателями и другими киберугрозами. Главной тенденцией компания считает взрывной рост криптоджекинга — скрытого использования компьютера или другого устройства для криптомайнинга в фоновом режиме. С начала года такие вредоносные программы, показав рост в 629%, стали популярнее предыдущего «лидера» — вирусов-вымогателей (ransomware)…

Исследователи отмечают, что помимо киберджекинга еще одной серьезной угрозой становится кража криптовалют при помощи хакерских атак…

McAfee также сообщает, что по итогам первого квартала наибольший рост кибератак (на 47%) отмечен в отношении компаний и организаций, работающих в сфере здравоохранения и медицины.

…На 40% выросли кибератаки против образовательных учреждений и компаний, работающих в этой области,— здесь также самым популярным видом атаки является вирус-вымогатель. На третьем месте по динамике роста кибератак оказались финансовые компании и учреждения — 39%. К ним исследователи также относят атаки на систему SWIFT. В McAfee отмечают, что атакам подвергались финансовые компании по всему миру, например, отмечается рост активности злоумышленников в России, Турции и ЮАР.» ***(Евгений Хвостик. Вредоносные майнеры растут быстрее биткойна // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3669919?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0). 27.06.2018).***

***

«Фахівці в галузі кібербезпеки з компанії RiskIQ заявили про те, що програма Advanced Battery Saver є шкідливим. Зокрема, воно краде особисті дані користувачів. Про це зазначено в блозі компанії.

Експерти відзначили, що програма має ряд прихованих механізмів, про яких користувачі і не підозрюють.

Зокрема, воно отримує доступ до всіх даних на пристрої, починаючи від геолокації і закінчуючи журналом дзвінків та SMS-повідомленнями. Також додаток сканує інтернет-трафік, демонструє власникові пристрою рекламу без його згоди, краде дані про моделі гаджета, марку виробника і навіть номер IMEI.

При цьому заявлені функції, серед яких моніторинг батареї і завершення енергоємних процесів, дана програма виконує.

Advanced Battery Saver було доступно для скачування на Google Play, проте в даний час воно видалено.» ***(Програму для збереження заряду викрили в крадіжці***

// Українська служба швидких новин (https://novosti.ternopil.ua/programu-dlya-zberezhennya-zaryadu-vikrili-v-kradizhci/). 23.06.2018).

***

«Фахівці компанії McAfee, яка спеціалізується на комп'ютерній безпеці, опублікували список додатків в Google Play, які крадуть гроші у власників смартфонів…

Повідомляється, що відповідальність за створення і розміщення шкідливих програм несе угруповання хакерів AsiaHitGroup. У 15 додатках, опублікованих в Google Play, був виявлений вірус SonvPay.C, який імітував фонове оповіщення про оновлення тієї чи іншої програми. Але на ділі замість апдейта користувачі отримували платну підписку на сторонні сервіси. Ще однією хитрістю вірусів стало використання WAP-білінгу замість SMS – власники пристроїв навіть не здогадувалися про те, що підписалися на сумнівну послугу.

За твердженням експертів McAfee, SonvPay.C з'явився в Google Play на початку цього року. За оцінками фахівців, троян приніс хакерам з AsiaHitGroup прибуток в сумі від 60 до 145 тисяч доларів. Найбільша кількість завантажень заражених програм для пошуку Wi-Fi мереж і створення рингтонів…

Щоб захиститися від подібних загроз, експерти порекомендували використовувати мобільні антивіруси і уважно вивчати відгуки про додатки перед установкою навіть з надійного джерела.» ***(В Google Play виявили вірус, який викрадає гроші в користувачів // Телеканал новин «24» (https://24tv.ua/v_google_play_viyavili_virus_yakiy_vikradaye_groshi_v_koristuvachiv_n991352). 29.06.2018).***

***

«…Аналітики Міністерства внутрішньої безпеки США спільно з Федеральним бюро розслідувань (ФБР) виявили використовуваний офіційними органами КНДР комп'ютерний вірус, що атакує окремі комп'ютери і цілі мережі. Вірус назвали TYPEFRAME й зарахували його до спектру підривних північнокорейських операцій у кіберпросторі, відомого у США як «Прихована кобра»…

Як повідомляє «Радіо Свобода», за минулий рік у США випустили в цілому 22 попередження про операції північнокорейських хакерів. Востаннє таке застереження про групу кіберпіратів, відому як Reaper, відомство оприлюдмило в лютому…» ***(Хакери з КНДР продовжують атакувати інші країни – США // MediaSapiens (http://ms.detector.media/web/cybersecurity/khakeri_z_kndr_prodovzhuyut_atakuvati_inshi_kraini_ssha/). 15.06.2018).***

***

«ESET открыла новый Android-троян HeroRat, который управляет зараженными устройствами и крадет данные с помощью бота в Telegram.

HeroRat – RAT-троян (Remote Administration Tool) для удаленного управления скомпрометированными устройствами. Авторы предлагают его в

аренду по модели Malware-as-a-Service (вредоносное ПО в качестве услуги)… Исходный код вредоносной программы продается за 650 долларов. Предусмотрен видеоканал техподдержки.

HeroRat ищет жертв через неофициальные магазины Android-приложений, социальные сети и мессенджеры. Атакующие маскируют троян под приложения, обещающие биткоины в подарок, бесплатный мобильный интернет или накрутку подписчиков в соцсетях. В Google Play данной угрозы не обнаружено. Большинство заражений зафиксировано в Иране…

Операторы HeroRat управляют зараженными устройствами через Telegram с помощью бота. Троян позволяет перехватывать и отправлять сообщения, красть контакты, совершать вызовы, записывать аудио, делать скриншоты, определять местоположение устройства и менять настройки…

Передача команд и кража данных с зараженных устройств реализована в рамках протокола Telegram – эта мера позволяет противодействовать обнаружению трояна.» ***(Троян управляет зараженными устройствами через Telegram // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5507595-Troyan-upravlyaet-zarazhennymi-ustr.html). 21.06.2018).***

***

«Криптомайнер Coinhive атаковал 22% организаций, по сравнению с апрелем (16%) количество атак увеличилось почти на 50%.

Пятый месяц подряд рейтинг топ-10 активных зловредов Check Point Global Threat Index возглавляет криптомайнер. В мае Coinhive по-прежнему сохраняет первенство среди самых распространенных вредоносных ПО. Еще один криптомайнер Cryptoloot расположился на втором месте (11%), на третьем — вредоносное рекламное ПО Roughted (8%).

Исследователи Check Point также отмечают, что киберпреступники продолжают эксплуатировать незакрытые серверные уязвимости Microsoft Windows Server 2003 (CVE-2017-7269) и Oracle Web Logic (CVE-2017-10271) для атак на корпоративные сети. В мировом масштабе 44% организаций подверглись атакам на уязвимости Microsoft Windows Server 2003, 40% — на Oracle Web Logic и 17% были подвержены влиянию внедрения SQL-кода…

Вредоносный криптомайнинг затронул почти 40% организаций в мае и продолжает быть самой распространенной киберугрозой…» ***(Криптомайнеры атаковали 40% организаций во всем мире // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5507199-Kriptomajnery-atakovali-40-organiza.html). 20.06.2018).***

***

«ESET обнаружила новую вредоносную программу, которая используется для кибершпионажа. InvisiMole открывает атакующим удаленный доступ к зараженному устройству, позволяет следить за действиями жертвы и перехватывать конфиденциальные данные.

По данным телеметрии ESET, кибергруппа, использующая InvisiMole, активна с 2013 года. Тем не менее, вредоносная программа не была изучена и не

детектировалась до момента обнаружения продуктами ESET на зараженных компьютерах в России и Украине. InvisiMole предположительно применялась только в целевых атаках на высокопоставленные объекты (несколько десятков устройств), что позволяло избегать обнаружения на протяжении пяти лет…

Вектор заражения InvisiMole пока не установлен. В настоящее время рассматриваются все варианты, включая установку вручную при наличии у злоумышленников физического доступа к компьютеру.» ***(В России и Украине обнаружено новое шпионское ПО // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5506621-V-Rossii-i-Ukraine-obnaruzheno-novo.html). 18.06.2018).***

***

«Эксперты по безопасности из компании Defiant описали вредоносную программу с характерным названием BabaYaga. «Баба-яга» используется для SEO-спама, однако, как выяснили исследователи, она способна удалять конкурирующий вредоносный софт и даже обновлять и переустанавливать CMS WordPress на заражённых ресурсах.

Основное назначение BabaYaga - это размещение на заражённых веб-сайтах «спамерских» ключевых слов и скрытых страниц, через которые пользователи перенаправляются на ресурсы, рекламируемые с помощью спама. Операторы BabaYaga получают комиссию от каждой продажи, сделанной на таких ресурсах. Вредонос состоит из двух модулей, один из которых отвечает как раз за инъекцию спам-контента в заражённые сайты, а другой представляет собой бэкдор, позволяющий злоумышленникам перехватывать контроль над сайтов в любое время.

Но самым интересным аспектом BabaYaga является его способность править, восстанавливать или переустанавливать систему управления контентом WordPress - автоматически.

Вредонос нуждается в том, чтобы сайт исправно работал, потому что в случае появления ошибок на нём, собственные скрипты BabaYaga также перестают исправно функционировать. Поэтому BabaYaga автоматически устанавливает все новейшие обновления на сайт под управлением WordPress, а в случае надобности - полностью обновляет CMS и даже создаёт и резервные копии на случай неудавшихся обновлений и удаляет их, когда надобность в таких файлах отпадает.

Интересно и то, что BabaYaga способна выполнять роль локального антивируса: если на заражённом сайте обнаруживается какое-то другое вредоносное ПО, BabaYaga его ликвидирует…» ***(Новый троян чинит зараженные сайты и «убивает» все другие вирусы // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5505214-Novyj-troyan-chinit-zarazhennye-saj.html). 09.06.2018).***

***

«Один из пользователей форума Reddit, использующий псевдоним TopWire, обратил внимание, что наряду с популярным Android-эмулятором Andy OS для Windows и macOS на компьютер скрыто устанавливается

вредоносная программа для добычи криптовалют за счет ресурсов графического процессора.

Согласно сообщению TopWire, майнер без ведома пользователей устанавливается в папку C:Program Files (x86)Updaterupdater.exe. TopWire неоднократно пытался связаться по этому вопросу с разработчиками Andy OS, однако все его обращения были проигнорированы. Пользователь опубликовал видео с демонстрацией процесса установки Andy OS.

На VirusTotal инсталлятор Andy OS детектируется как одна из версий InstallCore – известного установщика рекламного ПО. Подобные установщики позволяют разработчикам бесплатного программного обеспечения зарабатывать за счет показа рекламы.

Эксперт в области безопасности Лоуренс Абрамс (Lawrence Abrams) изучил текущую версию Andy OS и выяснил, что программа устанавливается на компьютер даже после отклонения всех рекламных предложений. Он протестировал эмулятор с помощью сервиса песочницы Any.Run. Как показал анализ, в процессе установки исполняется файл GoogleUpdate.exe, запускающий файл UpdaterSetup.exe, который, в свою очередь, устанавливает программу Updater.exe и настраивает ее на автоматический запуск при входе в Windows…

Специалист рекомендует пользователям воздержаться от установки эмулятора Andy OS, пока разработчики не прояснят ситуацию.» ***(Android-эмулятор Andy OS заподозрили в скрытом майнинге криптовалюты // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123546). 19.06.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«…Управление «К» МВД России при содействии Group-IB задержало двое киберпреступников, взламывавших и воровавших аккаунтов участников программ лояльности популярных интернет-магазинов, платежных систем и букмекерских компаний… Постарадали 700 тыс. учетных записей таких компаний, как «Юлмарт», «Биглион», «Купикупон», «PayPal», «Групон» и др. Как минимум 2 тыс. аккаунтов хакеры выставили на продажу от 5 долл. за каждый. Задержанные рассказали, что заработали не меньше 500 тыс. руб., однако реальную сумму еще предстоит выяснить.

Злоумышленники собирали на хакерских форумах скомпрометированные учетные данные от различных интернет-сервисов и с помощью специальных программ проводили автоматический поиск паролей к ним…

Расследование началось в 2015 году после того масштабной кибератаки на одном из сайтов…» ***(Group-IB помогла задержать укравших 700 тысяч аккаунтов хакеров // «Открытые системы» (https://www.computerworld.ru/news/Group-IB-pomogla-zaderzhat-ukravshih-700-tysyach-akkauntov-hakerov). 27.06.2018).***

***

«Адвокат Аркадий Бух сообщил, что россиянин Евгений Никулин, которого в Соединенных Штатах безосновательно обвиняют в причастности ко взлому социальных сетей, заявил в американском суде о своей невиновности.

…Никулина задержали 5 октября 2016 года в Праге чешские правоохранители совместно с представителями ФБР. Утверждалось, что россиянин якобы причастен к кибератакам на серверы Демократической партии, американской профессиональной соцсети LinkedIn, взлому серверов ЦРУ, а также попыткам заинтересованных лиц получить компромат на американского президента Дональда Трампа.

В марте россиянина экстрадировали из Чехии в США…» ***(Антон Никитин. Россиянин Никулин заявил о невиновности в американском суде // Деловая газета «Взгляд» (https://vz.ru/news/2018/6/27/929721.html). 27.06.2018).***

***

«Британский исследователь проблем безопасности, остановивший распространение вируса WannaCry в прошлом году, обвиняется в обмане Федерального бюро расследований (ФБР)…

Согласно четырем обвинениям, Хатчинс лгал ФБР при аресте. Кроме того, предполагается, что Маркус создал еще один компьютерный вирус под названием UPAS Kit, который был продан, а затем использован для атак на компьютеры в США. Также Хатчинса обвиняют в создании и распространении вредоносного ПО Kronos…

Хатчинс был арестован агентами ФБР 2 августа прошлого года в Международном аэропорту Маккаррана в Лас-Вегасе, после посещения конференции по кибербезопасности.

Согласно судебным документам, Хатчинс лгал ФБР, утверждая, что не знал, какой именно код использовался в банковском ПО Kronos. Вредоносная программа была впервые использована в 2014 году, а затем продана в даркнете. Так, Хатчинс фактически создал вирус и распространял его вместе с третьими лицами.

Более того, Маркус создал еще один вирус, UPAS Kit, в 2012 году, когда ему было 18 лет…» ***(Ирина Фоменко. Остановившему вирусную атаку WannaCry британцу ФБР предъявило обвинения // Internetua (http://internetua.com/ostanovivshemu-virusnuyu-ataku-wannacry-britancu-fbr-pred-yavilo-obvineniya). 08.06.2018).***

***

«Кіберполіція викрила 17-річного хакера у створенні та розповсюдженні комп'ютерного віруса-шифрувальника…

Правоохоронці задокументували злочинну діяльність 17-річного мешканця Львівщини, який починаючи з 2016 року займався поширенням шкідливого програмного забезпечення, що призначене для створення (побудови) вірусу-шифрувальника без наявності спеціальних знань у зловмисника.

Працівники Київського управління кіберполіції спільно зі слідчими провели обшуки за місцем реєстрації та проживання хакера…

Правоохоронці наразі перевіряють молодика на причетність до міжнародного хакерського угрупування. Встановлюються і особи, які можуть бути причетними до цього міжнародного злочинного угрупування. Також спеціалісти з кіберполіції встановлюють кількість уражених вірусом комп'ютерів.

За цим фактом розпочато кримінальне провадження за декількома фактами: за ч.2 ст.361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ч.2 ст.28, ч.1 ст.363-1 (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку), ч.1 ст.361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України…» ***(Євген Дем'янов. Юний хакер зі Львівщини створив і розповсюдив вірус-шифрувальник // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1733897-yuniy-khaker-zi-lvivschini-stvoriv-i-rozpovsyudiv-virus-shifruvalnik). 01.06.2018).***

***

«…Федеральное бюро расследований в понедельник объявило о 74 арестах в рамках международной правоохранительной операции, нацеленной на борьбу со схемой взлома электронной почты с целью похищения денежных переводов.

Как сообщили в ФБР, операция под кодовым названием WireWire проводилась в течение шести месяцев при участии многочисленных правоохранительных ведомств, в том числе Министерства внутренней безопасности, Министерства финансов и Службы почтовой инспекции. Из 74 арестов 42 были произведены на территории США.» ***(ФБР арестовало 74 человека в рамках операции против интернет-мошенничества // «Голос Америки» (https://www.golos-ameriki.ru/a/fbi-operation-cyber-fraud/4433986.html). 11.06.2018).***

***

«Суд признал виновными членов хакерской группировки, укравшей 12,5 млн рублей с 7 000 счетов российских банков

18 июня Савеловский районный суд Москвы вынес обвинительный приговор участникам хакерской группы, которую возглавляли братья-близнецы из Санкт-Петербурга Дмитрий и Евгений Попелыши. С марта 2013 по май 2015 года группа Попелышей получила доступ к более чем 7 000 счетов клиентов ведущих российских банков и похитила более 12,5 млн рублей…

Попелыши руководили группой, в которую входили «программисты», «трафферы» — люди, которые распространяли вредоносные программы, «крипторы» – специалисты, которые проводили своевременное обновление (изменение) кода вредоносных программ, «дропы» — люди, которые занимаются обналичкой украденных денег, «прозвонщики». Последние, в частности,

представляясь сотрудниками банка, сами звонили клиентам, оставившим номер карты и телефона на поддельном сайте и убеждали жертв назвать код подтверждения перевода. Такой вид мошенничества называется вишинг (англ. vishing, от voice phishing – голосовой фишинг) – тип фишинга, при котором для получения конфиденциальных данных используются голосовые коммуникации…

Попелышам и их подельникам были предъявлены обвинения создании и использовании вредоносных программ (ст 273 УК РФ), в неправомерном доступе к компьютерной информации и (ст 272 УК РФ) и мошенничестве (ст. 159 Ук РФ)…

В понедельник, 18 июня, Савеловский суд Москвы признал вину подсудимых – Евгений и Дмитрий Попелыши получили по 8 лет лишения свободы…» ***(Хакеры-близнецы Попелыши сели в тюрьму со второго раза // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5507028-Xakerybliznecy-Popelyshi-seli-v-tyu.html). 19.06.2018).***

***

«…Компания InfoWatch представляет дайджест судебных вердиктов в отношении киберкриминала.

В конце мая суд Сан-Франциско приговорил 23-летнего Карима Баратова, гражданина Казахстана и Канады, к пяти годам лишения свободы и штрафу в размере $250 тыс. за взлом почтовых аккаунтов Yahoo. В результате кибератаки, случившейся в 2014 году, эта компания потеряла данные более 500 млн человек. Американская прокуратура считает, что киберпреступник действовал в интересах российских спецслужб…

В то же самое время в Великобритании был осужден хакер Грант Уэст (Grant West). Он получил 10 лет и 8 месяцев тюремного заключения за взлом сетей десятков компаний, кражу данных и организацию фишинговых атак. С 2015 года киберпреступник торговал украденной информацией в даркнете. В одном только ноутбуке, изъятом следствием у девушки Уэста, содержалась финансовая информация более 100 тыс. человек. Сумма ущерба, который хакер нанес различным компаниям, исчисляется миллионами фунтов стерлингов.

Ранее гражданин России Владимир Дринкман осужден американским правосудием на 12 лет за участие в одной из крупнейших хакерских атак, в результате которой были украдены данные более 160 млн платежных карт. Вместе с сообщниками Дринкман наладил сбыт похищенной информации, получая от $10 до $50 за номер кредитной карты, в зависимости от страны эмитирования. Банки и крупные компании, пострадавшие от действий этой преступной группы, потеряли сотни миллионов долларов.

Обычно компьютерные преступления совершают довольно молодые люди, многие из которых выросли на цифровых технологиях. Хакерская романтика привлекает и многих подростков. В 2015 году 15-летний британец Кейн Гэмбл (Kane Gamble) взломал аккаунты директора ЦРУ Джона Бреннана и других высокопоставленных лиц США. После ареста тинейджер сознался в десяти эпизодах. По достижении 18 лет Гэмбл был осужден. Ближайшие два года он проведет в специальном исправительном изоляторе для юных преступников.

Хакерским ремеслом промышляет не только сильный пол. Суд Лос-Анджелеса недавно постановил на 57 месяцев отправить за решетку Пацар Бхаджан (Paytsar Bkhchadzhyan). Девушка признана виновной во взломе личных аккаунтов «светской львицы» Пэрис Хилтон (Paris Hilton). По данным следствия, Бхаджан украла со счетов знаменитости более $120 тыс. Также преступница похитила личные фотографии Хилтон, в том числе снимки интимного характера.» ***(Приговоры хакерам: каждому по заслугам // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5505779-Prigovory-xakeram-kazhdomu-po-zaslu.html). 13.06.2018).***

***

«Компания Tesla подала в суд на своего бывшего сотрудника Мартина Триппа (Martin Tripp), обвинив его в хищении большого объема конфиденциальных данных для дальнейшей передачи третьей стороне.

Как следует из материалов дела, житель штата Невада (США) Мартин Трипп работал на одном из заводов Tesla с октября 2017 года, однако плохо справлялся с рабочими обязанностями и в мае 2018 года был переведен на другую должность. Данная мера вызвала у мужчины недовольство, в отместку он "похитил конфиденциальную информацию, являющуюся коммерческой тайной, и раскрыл ее третьим сторонам".

По словам представителей Tesla, Трипп признался в заражении сетей компании вредоносным ПО, позволявшим пересылать данные компании сторонним лицам даже после того, как мужчина был уволен. В общей сложности Триппу удалось похитить несколько гигабайтов информации, в том числе фотографии и видеозаписи. Помимо этого, Трипп обвиняется в распространении заведомо ложных данных об использовании компанией бракованных аккумуляторов в автомобилях.

В настоящее время продолжается расследование по данному делу. Tesla требует от бывшего сотрудника компенсации, размер которой должен установить суд присяжных.» ***(Экс-сотрудник Tesla обвинен в хищении конфиденциальных данных компании // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123579). 21.06.2018).***

***

Технічні аспекти кібербезпеки

«Команда проекта OpenBSD откажется от поддержки технологии Intel Hyper-Threading (гиперпоточность) из-за рисков безопасности, связанных с уязвимостями Meltdown/Spectre и им подобных проблем.

Hyper-Threading представляет собой проприетарную реализацию Intel технологии Simultaneous Multithreading (SMT, одновременная многопоточность), которая появилась в начале 2000-х годов для процессоров Intel Pentium 4 и других. После активации HTT операционная система начинает "видеть" одно реальное физическое ядро процессора как два отдельных процессора. Благодаря этому при

определенных типах нагрузки процессор становится более продуктивным, поскольку используется на 100%. В процессорах Intel данная функция включена по умолчанию.

Как пояснил участник команды OpenBSD Марк Кеттенис (Mark Kettenis), отмена поддержки связана с тем, что HTT представляет возможность проведения атак по времени. К данному классу атак также относятся атаки с эксплуатацией уязвимостей Meltdown, Spectre и их многочисленных вариантов. По его словам, Intel HT упрощает осуществление атак по времени, что позволит более легкую эксплуатацию подобных Spectre уязвимостей.

Команда OpenBSD реализовала настройки (hw.smt sysctl) для отключения поддержки Intel HT, поскольку "многие современные машины больше не предоставляют возможность деактивировать гиперпоточность в настройках BIOS". Пока новая функция будет работать только для процессоров Intel, в будущем разработчики планируют расширить ее на CPU других производителей. Кеттенис считает, что изменение незначительно скажется на производительности, поскольку "в действительности SMT не настолько повышает производительность, как утверждают Intel и другие производители процессоров"…» ***(OpenBSD прекратит поддержку Intel HT из соображений безопасности // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123561). 20.06.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Сьогодні, 29 червня, експерти опублікували одну із наймасштабніших уразливостей Android-смартфонів за останні кілька років. Загрозу під назвою RAMpage виявила об'єднана група дослідників із трьох різних університетів. Повідомляється, що нею уражені мільйони користувачів по всьому світу, починаючи з 2012 року…

Згідно з результатами дослідження, уразливість RAMpage була знайдена в підсистемі ION – драйвер пам'яті, що використовується в Android, починаючи з версії 4.0 Ice Cream Sandwich. Але дослідники попереджають, що крім Android-смартфонів, вразливість теоретично може експлуатуватися і в пристроях під управлінням iOS.

Експлоїт змушує підсистему ION записувати і оновлювати дані в RAM: в деяких випадках ця дія дозволяє "залізти" в сусідні осередки пам'яті. Таким чином, шкідливе ПЗ може отримати доступ до даних іншої програми, права адміністратора і повний контроль над пристроєм. Як стверджується на спеціально створеному сайті, присвяченому RAMpage, самостійно виявити втручання в роботу пам'яті неможливо…» ***(Експерти виявили наймасштабнішу уразливість на Android-смартфонах // Телеканал новин «24» (https://24tv.ua/eksperti_viyavili_naymasshtabnishu_urazlivist_na_android_smartfonah_n991271). 29.06.2018).***

***

«Китайская корпорация, занимающаяся вопросами кибербезопасности, SlowMist, подтвердила, что недавняя уязвимость, связанная с двойными расходами в Tether (USDT), не присуща самой криптовалюте.

Вместо этого он активируется некоторыми базами данных криптобирж, не строго проверяя статус «действительного» параметра входящих транзакций USDT…» ***(Ольга Новикова. Ранее найденная уязвимость с двойными расходами не является проблемой в сети Tether // BIGFIN (https://bigfin.net/30/06/2018/ranee-najdennaja-ujazvimost-s-dvojnymi-rashodami-ne-javljaetsja-problemoj-v-seti-tether/). 30.06.2018).***

***

«…Немецкий электротехнический концерн Phoenix Contact опубликовал информацию о наличии четырех уязвимостей в промышленных коммутаторах серии FL SWITCH. Устройства используются для выполнения задач автоматизации на цифровых подстанциях, в нефтегазовой, морской и других отраслях.

Уязвимости были обнаружены экспертами Positive Technologies Вячеславом Москвиным, Семеном Соколовым, Евгением Дружининым, Ильей Карповым и Георгием Зайцевым.

Наибольшую опасность представляет уязвимость CVE-2018-10730 (оценка 9,1 по шкале CVSS). Она позволяет злоумышленнику выполнить произвольные команды на устройстве и, например, отключить от промышленной сети все устройства, нарушив технологический процесс промышленного объекта.

Вторая опасная уязвимость (CVE-2018-10731), получившая оценку 9,0, связана с угрозой переполнения буфера и может быть использована для получения несанкционированного доступа к файлам операционной системы устройства и выполнения произвольного кода. Также проблема переполнения буфера относится и к уязвимости CVE-2018-10728 (оценка 8,1). Нарушитель может использовать ее для атак на отказ в обслуживании, выполнения произвольного кода, отключения служб Web и Telnet.

Четвертая уязвимость CVE-2018-10729 (оценка 5,3) позволяет злоумышленнику, не прошедшему аутентификацию, прочитать содержимое конфигурационного файла устройства.

Недостатки выявлены в коммутаторах FL SWITCH 3xxx, 4xxx и 48xxx, функционирующих на программном обеспечении версий 1.0–1.33. Для устранения уязвимостей производитель рекомендует установить прошивку версии 1.34.

«Продолжается основной тренд минувшего года — мы видим все больше уведомлений о новых уязвимостях в промышленном сетевом оборудовании...» — считает руководитель отдела безопасности промышленных систем управления Positive Technologies Владимир Назаров…» ***(Новые уязвимости в коммутаторах Phoenix Contact представляют опасность для промышленных сетей // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/293446/). 19.06.2018).***

***

«Специалисты Positive Technologies подготовили статистику по уязвимостям, обнаруженным в ходе проведения работ по тестированию безопасности веб-приложений

По результатам анализа было установлено, что злоумышленники могут получить персональные данные в 44% систем, в которых осуществляется их обработка. Речь идет, среди прочего, о финансовых учреждениях, интернет-магазинах и телекоммуникационных компаниях. При этом доля приложений, для которых существует угроза утечки критически важной информации составляет 70%.

Атаки на пользователей веб-приложения могут быть совершены в 96% систем. Несанкционированный доступ к приложению может быть получен примерно в каждом втором случае (48%). При этом возможность получения полного контроля над приложением была выявлена примерно в каждом шестом случае (17%).

Уязвимости той или иной степени риска содержатся в каждом веб-приложении. При этом аналитики отметили позитивную тенденцию: доля веб-приложений, содержащих критически опасные уязвимости, снижается второй год подряд. В 2017 году в 52% приложений были выявлены уязвимости высокой степени риска. При этом наблюдается рост доли приложений, содержащих уязвимости низкой степени риска: в 2017 году они были обнаружены в 74% исследованных систем.

Самой распространенной уязвимостью по-прежнему является «Межсайтовое выполнение сценариев» (Cross-Site Scripting), она была выявлена в 74% систем. Также среди распространенных ошибок, позволяющих проводить атаки на пользователей, присутствуют «Подделка межсайтового запроса» (Cross-Site Request Forgery) и «Открытое перенаправление» (URL Redirector Abuse).

В каждом четвертом приложении эксперты смогли эксплуатировать уязвимость «Внедрение операторов SQL»; с ее помощью злоумышленник может получить чувствительную информацию из СУБД, включая учетные данные пользователей. В 9% приложений выявлялись такие опасные уязвимости, как «Выполнение произвольного кода» (OS Commanding), «Внедрение внешних сущностей XML» (XML External Entities), «Выход за пределы назначенного каталога» (Path Traversal).

Значительная доля обнаруженных ошибок (65%) были допущены при разработке приложений и содержатся в их программном коде, а некорректные параметры конфигурации веб-серверов составили около трети от общего числа недостатков безопасности…». ***(Positive Technologies: киберпреступники могут похитить персональные данные пользователей 44% веб-приложений // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/293050/). 15.06.2018).***

***

«Согласно отчету Positive Technologies, используя недостатки протокола Diameter, злоумышленник может лишить абонентов основных преимуществ

4G — высокой скорости и качества связи. Уязвимости протокола Diameter могут привести к блокировке работы банкоматов, POS-терминалов, приборов учета ЖКХ, автосигнализаций, а также систем видеонаблюдения. Если абонент является системой диагностики на магистральном газопроводе или GSM-контроллером утечки бытового газа, отсутствие связи может привести не только к прямому денежному ущербу, но и к опасным авариям…

Риску мошенничества в отношении оператора подвержена каждая третья сеть 4G. Киберпреступники могут пользоваться мобильной связью бесплатно и продавать подобные услуги третьим лицам. Под угрозой и приватность: все сети четвертого поколения позволяют отследить местоположение абонентов…

Большинство выявленных недостатков были связаны не только с некорректной настройкой или уязвимостями сетевого оборудования, но также с фундаментальными проблемами протокола Diameter, для решения которых требуются дополнительные средства защиты. Эксперты Positive Technologies подчеркивают необходимость комплексного подхода к безопасности.

В исследовании Positive Technologies участвовали операторы связи стран Европы и Азии. Большую часть (80%) составили крупные телекоммуникационные компании с объемом абонентской базы более 40 миллионов человек.» ***(Исследование Positive Technologies: отказ в обслуживании абонентов возможен в 100% сетей 4G // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/293021/). 13.06.2018).***

***

«Эксперт по информационной безопасности Брэннон Дорси (Brannon Dorsey) обнаружил, что IoT-устройствам Google, Roku и Sonos угрожает перепривязка DNS (DNS rebinding). Бреши в умных приборах позволяют взломщикам удаленно управлять ими и перехватывать пользовательские данные.

Атаки этого типа известны с 2007 года, когда их впервые описали специалисты Стэнфордского университета. Их суть такова: сетевое устройство привязывают к вредоносному DNS-серверу и превращают его в точку входа в инфраструктуру жертвы. Если атака проходит успешно, преступник может собирать информацию о состоянии и составе сети, отдавать команды ее различным компонентам — например, изменить настройки роутера и повысить свои привилегии.

Эксплуатация этой уязвимости требует как серьезной технической подготовки взломщиков, так и совпадения нескольких факторов на стороне пользователя. По этой причине производители зачастую не заботятся о защите своих продуктов от подобных атак. Однако в последние месяцы ИБ-сообщество часто говорит об угрозе перепривязки DNS, в частности, после того, как эти бреши обнаружились в клиентах Blizzard и uTorrent, а также в программе для добычи Ethereum.

Теперь под угрозой оказались IoT-устройства для умных домов. Как сообщил Дорси, интерактивная колонка Google Home позволяет злоумышленнику манипулировать ее настройками, сканировать WiFi-сети, запускать установленные приложения и воспроизводить мультимедийный контент. В дальнейшем взломщик

может получить доступ к местоположению пользователя…» ***(Egor Nashilov. IoT-устройствам угрожает брешь 11-летней давности // Threatpost (https://threatpost.ru/iot-devices-threatened-by-dns-rebinding/26773/). 21.06.2018).***

***

«Компания SAP выпустила очередной пакет ежемесячных исправлений, в котором закрыла десять уязвимостей своих продуктов. В их числе две критические бреши, четыре ошибки с высокой степенью опасности и четыре умеренные угрозы.

Два апдейта закрыли уязвимости с близкими к максимальным оценками по десятибалльной шкале CVSS. Они связаны с проблемой безопасности встроенного веб-браузера и возможностью инъекции для отправки операционной системе несанкционированных команд.

Бреши были обнаружены в продуктах SAP Business Client и SAP BASIS. Первый представляет собой пользовательский интерфейс для работы с ERP-решением, а второй служит интеграционным ядром для различных программных компонентов вендора.

Четыре уязвимости признаны особо серьезными. В бэкап-сервисе SAP Business One, ERP-системы для малого и среднего бизнеса, компания закрыла угрозу CVE-2018-2425 — возможность несанкционированного доступа к закрытой информации. В продукте для электронной коммерции SAP Internet Sales разработчики исправили баги CVE-2015-0899 и CVE-2014-0050, позволявшие удаленно отправлять команды и вызывать критические ошибки приложения.

Последняя серьезная проблема CVE-2018-2408 содержалась в аналитической системе SAP Business Objects — из-за некорректной обработки пользовательских сессий злоумышленник мог авторизоваться с применением устаревших паролей.

Остальные бреши получили умеренную оценку риска. В средствах веб-разработки SAPUI5 и UI5 Handler устранены угрозы возможности межсайтового скриптинга и раскрытия пользовательской информации — CVE-2018-2424 и CVE-2018-2428 соответственно. В аналитической системе SAP Crystal Reports разработчики закрыли возможность удаленного выполнения кода. В продукте SAP Identity Management, который обеспечивает хранение и распределение основных данных о пользователях, ликвидировали уязвимость CVE-2018-2416, скорректировав валидацию XML-документов…» ***(Dmitry Nazarov. SAP устранила десять проблем безопасности июньскими патчами // Threatpost (https://threatpost.ru/sap-patched-ten-vulnerabilities-in-june/26612/). 14.06.2018).***

***

«Китайский производитель IP-камер Foscam устранил три уязвимости в своих устройствах, которые позволяли злоумышленникам захватывать контроль над ними. Проблема затронула не только продукцию под собственным брендом вендора, но и другие торговые марки, закупающие у него камеры без лейбла.

Бреши обнаружили аналитики компании VDOO, которая специализируется на безопасности Интернета вещей…

Как пояснили эксперты, в основе этих уязвимостей лежит целая серия ошибок производителя: процессы протекают на корневом уровне, рядовые операции выполняются через отправку shell-команд вместо того, чтобы использовать для этого API и дополнительные библиотеки. Кроме того, камеры не проверяют безопасность поступающих данных, а прошивку несложно взломать и изучить.

Журналисты Bleeping Computer отмечают, что Foscam изменила политику работы с уязвимостями. В прошлом году производитель проигнорировал сообщение о 18 брешах в его камерах, которые позволяли перехватывать видеопоток, удаленно управлять устройствами, скачивать и загружать файлы на внутренний FTP-сервер. Сейчас же компания поблагодарила исследователей за информацию и оперативно устранила проблему.

Пользователям следует обновить прошивку по опубликованной на сайте Foscam инструкции…» ***(Dmitry Nazarov. Китайский производитель помешал появлению нового IoT-ботнета // Threatpost (https://threatpost.ru/foscam-prevented-botnet-emergence/26543/). 08.06.2018).***

***

«Исследовательская группа Snyk обнародовала детали уязвимости, затрагивающей тысячи программных продуктов и большие объемы пользовательских данных. Ошибка связана с распаковкой файловых архивов в библиотеках с открытым кодом, она позволяет обойти целевой каталог и в итоге выполнить на скомпрометированном устройстве небезопасную команду.

Проблема получила название Zip Slip, поскольку атака совершается с помощью файлов zip, rar, jar, 7z и других форматов. Ошибка не является уязвимостью конкретного архиватора, а связана с компонентами, которые осуществляют распаковку данных. Обычно за эту операцию отвечает одна из типовых подпрограмм, доступных в репозиториях или фреймворках.

Эксперты Snyk выяснили, что многие библиотеки с открытым кодом не проверяют корректность пути распаковки при обработке архива. Это значит, что злоумышленники способны разместить вредоносные файлы за пределами целевого каталога. Уязвимость позволяет киберпреступникам переписать данные операционной системы или, например, выполнить вредоносный код при перезапуске устройства…

Скомпрометированные библиотеки используются в тысячах программных продуктов. Исследователи обнаружили уязвимый код в компонентах .NET, Go, JavaScript, Groovy и других средств разработки. Хуже всего ситуация обстоит в Java, где отсутствует единый обработчик архивов и разные проекты реализуют функцию распаковки по-разному.

Как утверждают эксперты Snyk, речь идет о системном баге в реализации функции. Долгое время недостаток проникал в разные библиотеки, оставаясь незамеченным. Уязвимый код найден даже на специализированном сайте вопросов и ответов Stack Overflow, где программисты делятся своими разработками.

По информации аналитиков, ошибка присутствует в Google Cloud Platform, некоторых продуктах Amazon Web Services, Alibaba Group, HP, LinkedIn и ряде других сервисов…

Как утверждают эксперты, Zip Slip уже пропатчена в программах Oracle, Pivotal, HP, LinkedIn и Apache. Остальные разработчики пока не отчитались о выпуске заплаток…» ***(Dmitry Nazarov. Zip Slip угрожает тысячам сервисов удаленным выполнением кода // Threatpost (https://threatpost.ru/zip-slip-threaten-multiple-services-with-remote-code-execution/26468/). 06.06.2018).***

***

«Исследователи безопасности из компании SEC Consult обнаружили в радионяне Fredi Wi-Fi уязвимости, позволяющие удаленному неаутентифицированному злоумышленнику подключиться к устройству и использовать встроенную камеру.

По словам исследователей, устройство использует слабые методы обеспечения безопасности при подключении к Сети. Возможность online-подключения позволяет родителям следить за детьми через ноутбуки и мобильные устройства, однако также позволяет хакерами использовать встроенную в радионяню камеру для того, чтобы шпионить за людьми.

Исследователи обнаружили, что служба P2P подключается непосредственно к облачному сервису и к ней можно получить доступ указав 8-значный идентификатор устройства и заводской пароль…

Помимо этого, через незащищенные радионяни также можно подключиться к домашним сетям их владельцев для осуществления атак в будущем.» ***(Радионяню Fredi Wi-Fi можно использовать в качестве устройства слежения // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123615). 22.06.2018).***

***

«В устройствах Google Chromecast и Google Home обнаружена уязвимость, позволяющая любому web-сайту получить доступ к сервису геолокации Google и определить точное местоположение гаджетов с погрешностью до 1 м.

Как правило, web-сайты получают общие сведения о местонахождении пользователей по IP-адресам подключающихся к сайтам устройств. Однако такой метод не отличается высокой точностью и позволяет лишь примерно прикинуть географическое местоположение IP-адресов. Поэтому для установления местонахождения пользователей Google использует высокоточные геолокационные сервисы, определяющие местоположение устройств на основании их расположения по отношению к окружающим беспроводным сетям.

Как сообщает исследователь компании Tripwire Крейг Янг (Craig Young), уязвимость в Google Chromecast и Google Home позволяет web-сайтам определять ближайшие беспроводные подключения и с помощью перекрестных ссылок на базу данных Google устанавливать точное местоположение пользователей…» ***(Уязвимость в Google Chromecast и Google Home позволяет определить их***

точное местоположение // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123545). 19.06.2018).

***

«Промышленные системы управления могут быть уязвимы не только к атакам удаленных хакеров, но также к локальным и физическим атакам. В ходе прошедшей на прошлой неделе конференции BSides исследователи компании INSINIA продемонстрировали, как с помощью устройства, внедренного в системы предприятия, обнаруживать сети и вносить их в списки, а также управлять контроллерами для остановки производственных процессов.

На конференции специалисты представили свой доклад под названием "Hacking SCADA: How We Attacked a Company and Lost them 1.6M with Only 4 Lines of Code" ("Взлом SCADA: Как мы атаковали компанию и причинили ей ущерб на 1,6 млн фунтов с помощью лишь четырех строк кода").

Как пояснил глава компании Майк Годфри (Mike Godfrey) изданию The Register, долгое время автоматизированные системы управления создавались с учетом безопасности, продолжительности срока службы и надежности. Все системы были физически изолированными, поэтому при их проектировании ИБ не учитывалась.

С наступлением эпохи интернета все изменилось. Появился так называемый "Интернет вещей" (IoT), и системы управления стали подключаться к интернету. Тем не менее, SCADA-системы по-прежнему производятся без учета требований кибербезопасности, сообщают эксперты. В результате SCADA-системы изобилуют такими уязвимостями, как неизменяемые учетные данные и отсутствие шифрования.

Что еще хуже, большинство систем работают под управлением устаревших или неподдерживаемых версий Windows. Наиболее распространенной является Windows 7, однако до сих пор существуют системы, работающие на базе Windows 98. Терминалы под управлением Windows 98 уязвимы к одному из старейших хакерских инструментов Back Orifice из 1990-х годов.

Специалисты INSINIA разработали устройство, способное автоматически сканировать сети и отключать их компоненты. Устройство представляет собой вредоносный микроконтроллер Arduino и внешне не отличается от обычного ПЛК. Если его физически внедрить в атакуемую среду, оно быстро подсчитает число сетей и отправит команду "стоп". По словам Годфри, устройство способно "убить производственные процессы с помощью лишь четырех строк кода". В случае подобной атаки простой сброс настроек не поможет, и атакуемая среда будет отключаться снова и снова, отметил эксперт…» ***(С наступлением эпохи "Интернета вещей" SCADA-системы по-прежнему производятся без учета кибербезопасности // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123525). 19.06.2108).***

***

«Microsoft опубликовала документ "Security Servicing Commitments for Windows" ("Обязательства по обеспечению безопасности для Windows"), в

котором компания рассказала о своих обязательствах касательно исправления уязвимостей в операционной системе. В частности, в документе описано, какие именно проблемы программисты Microsoft будут исправлять, а какие останутся без внимания.

Документ призван дать экспертам по кибербезопасности более четкое понимание особенностей, ограничений и процессов в ОС Windows, а также пояснить обязательства по обслуживанию, которые берет на себя компания…

Как пояснили в Microsoft, при обнаружении очередной уязвимости действуют два критерия оценки:

- Угрожает ли найденая уязвимость особенностям операционной системы, которые Microsoft защищает?

- Достигает ли опасность уязвимости определенного уровня?

Утвердительный ответ на оба вопроса означает, что о проблемой займутся программисты Microsoft, а исправления для всех поддерживаемых продуктов будут выпущены в кратчайшие сроки.

Если ответ хотя бы на один из вопросов будет "нет", тогда компания отложит исправление уязвимости до выпуска новой версии ОС. В документе также описаны уровни опасности уязвимостей: "критический", "высокий", "средний", "низкий" и "нулевой". Компания будет исправлять только уязвимости уровня "критический" и "высокий".» ***(Microsoft описала, какие уязвимости не будет исправлять // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123479). 15.06.2018).***

***

«…Более половины уязвимостей в системах безопасности компаний мира не устраняются сразу после их обнаружения. Такими оказались данные опроса, проведенного аналитиками компании Outpost24 среди 155 ИТ-специалистов. В опубликованном исследовании уточняется, что 16% компаний исправляют уязвимости только раз в месяц, а 5% и вовсе делают это раз или два в год.

При этом, значительное число ИТ-специалистов (42%) оставляют уязвимые места без защиты, поскольку либо не знают, как их исправлять, либо не имеют времени для их устранения…

Аналитики отмечают, что 85% компаний даже не проводят тесты, связанные с качеством обеспечения безопасности. Из тех же, кто озаботился этим, 46% обнаружили критические недостатки, которые могли бы поставить под угрозу всю организацию. Тем не менее, каждый третий ИБ-специалист не считает, что, например, тесты на проникновение помогут выявить какие-то новые риски…

Вместе с тем, специалисты отмечают, что часто проблемой для бизнеса становится не игнорирование уязвимостей как таковое, а отсутствие квалифицированных кадров и нехватка бюджета на применение современных средств защиты информации…» ***(Исследование: половина специалистов по ИБ откладывают исправление критических уязвимостей // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123441). 13.06.2018).***

***

«…На единой электронной торговой площадке (ЕЭТП) начали применять технологии машинного обучения и нейронных сетей… применение машинного обучения при проведении электронных торгов уже дает первые результаты — с начала года предотвращено 73 вредоносные атаки. Этому предшествовала серьезная комплексная модернизация действующей системы информационной безопасности электронной площадки.

…необходимость использования искусственного интеллекта связана с киберугрозами, которым подвергаются финансовые организации.

Система информационной безопасности ЕЭТП в автоматическом режиме фиксирует все входящие и исходящие запросы. При этом искусственный интеллект отделяет запросы добросовестных пользователей от вредоносных атак и действий аукционных роботов, которые популярны среди мошенников…» ***(Правительство Москвы: искусственный интеллект защищает электронные аукционы от кибератак // «Открытые системы» (https://www.computerworld.ru/news/Pravitelstvo-Moskvy-iskusstvennyy-intellekt-zaschischaet-elektronnye-auktsiony-ot-kiberatak). 20.06.2018).***

***

«…Wi-Fi Alliance запустил WPA3, новый стандарт беспроводного Интернета, который лучше шифрует данные, что затрудняет перехват этой информации третьими лицами. Ввод пароля также обеспечит дополнительный уровень защиты.

Кроме того, программа, объявленная вместе с WPA3, упростит подключение домашних смарт-устройств к сети Wi-Fi. Easy Connect дает возможность использовать смартфон для настройки соединений.

Новый стандарт не будет автоматически отображаться на нынешних устройствах. Пользователю придется вручную устанавливать обновления, а некоторые старые девайсы могут не получить их вовсе.

В ближайшее время стандарт WPA2 останется без изменений. Два протокола, WPA2 и WPA3, совместимы, хотя WPA3 в будущем, предполагается, что к 2020 году, станет обязательным…» ***(Ирина Фоменко. Новая технология помешает хакерам взламывать Wi-Fi // Internetua (http://internetua.com/novaya-tehnologiya-pomeshaet-hakeram-vzlamvat-wi-fi). 27.06.2018).***

***

«…Twitter анонсировала новую возможность авторизации в соцсети с использованием физического U2F-ключа. Как полагают в компании, данная мера поможет усложнить взлом учетных записей пользователей сети микроблогов.

…Применение U2F-ключа также позволит защитить пользователей от фишинговых атак, поскольку новый метод будет работать только на настоящих страницах Twitter.

…для настройки физического ключа учетная запись пользователя должна быть связана с мобильным номером телефона (еще одно новое требование, которое будет действовать для всех новых аккаунтов в Twitter). Новый функционал будет запускаться поэтапно, начиная с 26 июня текущего года…» ***(Twitter защитит учетные записи физическим ключом // SecurityLabRu (https://www.securitylab.ru/news/494143.php). 27.06.2018).***

***

«Компания Check Point Software Technologies объявила о том, что решение SandBlast Agent для защиты конечных устройств признано лидером в области предотвращения атак вредоносного ПО, защиты данных, мобильной безопасности, внешней интеграции, технической поддержки, корпоративной стратегии и присутствия на рынке. По всем критериям решение получило наивысшие оценки в недавно опубликованном отчете независимого аналитического агентства Forrester Research – The Forrester Wave: Endpoint Security Suites, Q2 2018.

«Check Point предлагает полнофункциональную, традиционную комплексную защиту с современными обновлениями, – говорится в отчете…» ***(Forrester назвал Check Point в числе лидеров в области защиты конечных устройств // «Компьютерное Обозрение» (https://ko.com.ua/forrester_nazval_check_point_v_chisle_liderov_v_oblasti_zashhity_konechnyh_ustrojstv_125149). 27.06.2018).***

***

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

Актуальні шляхи удосконалення українського законодавства : зб. тез наук. доп. і повідомл. VI Всеукр. наук.-практ. конф. студентів, аспірантів, науковців та молодих вчених (Харків, 18 листоп. 2017 р.). - Харків : Право, 2017. - 439 с.

Зі змісту:

- Рогальська Н.В. Міжнародно-правове регулювання у сфері боротьби з кіберзлочинністю.

Шифр зберігання НБУВ: ВА819917.

***

Гуйван О.П. Засади інформаційної безпеки як способу захисту інформації / Гуйван О.П. // Актуальні проблеми вітчизняної юриспруденції. - 2017. - Вип. 6(1). - С. 46-50.

Досліджено сутність механізмів інформаційного захисту. Вивчено характер та спрямованість загроз правовідносинам у сфері інформаційного обороту.

Шифр зберігання НБУВ: Ж74269.

***

Діордіца І.В. Методологія дослідження кібербезпекової політики: кібернетичний підхід / Діордіца І.В. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2017. - Вип. 47(2). - С. 106-110.

Проаналізовано особливості кібернетичного підходу у дослідженні кібербезпекової політики. Розглянуто евристичні можливості кібернетичного підходу як методологічного інструменту дослідження кібербезпекової політики. Наведено алгоритм застосування кібернетичного підходу.

Шифр зберігання НБУВ: Ж68850/пр.

***

Діордіца І.В. Поняття та зміст кібернетичної деонтології / І.В.Діордіца // Прикарпатський юридичний вісник. - 2017. - Вип. 5. - С. 137-140.

Сформульовано визначення кібернетичної деонтології , а також визначено її мету, об’єкт, предмет і основні завдання. Охарактеризовано категорійно-понятійний апарат кібернетичної деонтології. Проаналізовано виявлені людиною фактори, що впливають на кібернетичної деонтології.

Шифр зберігання НБУВ: Ж74200.

***

Діордіца І. В. Репрезентація термінології кібербезпекової політики в текстах нормативно-правових актів України / І. В. Діордіца // Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. - 2017. - Вип. 29(1). - С. 64-67.

Проаналізовану процеси, що відбуваються у сфері кібернетичної безпеки. Використовуючи методи системного, порівняльного і контент-аналізу, встановлено тенденції термінотворення й застосування термінів, запропоновано фасетну класифікацію юридичної термінології в галузі кібербезпекової політики.

Шифр зберігання НБУВ: Ж74042/ю.

***

Інформаційне суспільство: проблеми та перспективи : матеріали II Всеукр. наук.-практ. конф., 12 трав. 2017 р., м. Одеса. - Одеса : Фенікс, 2017. - 123 с.

Зі змісту:

- Антар А. Основні пріоритети інформаційної безпеки України;

- Оніщук Д.Г. Деякі аспекти боротьби з кіберзлочинністю в Україні;
- Ращик К.В. Кібербезпека України в умовах євроінтеграції;
- Рішко П.П. Основні проблеми побудови системи кібернетичної безпеки України.

Шифр зберігання НБУВ: ВА820067.

***

ІТ-право. Теорія та практика : навч. посіб. / [Є. О. Харитонов та ін.]. - Одеса : Фенікс, 2017. - 467 с.

Викладено основи правового регулювання інформаційно-комунікаційних відносин та забезпечення інформаційної безпеки у сфері ІТ, охарактеризовано особливості суб'єктів та об'єктів відносин у цій сфері, віртуальну власність, електронну комерцію, технології блочейну і смарт-контактів, стартами і соціальні мережі у контексті проблем їх правового регулювання.

Шифр зберігання НБУВ: ВА820145.

***

ІТ-право та інформаційна безпека : монографія / [О. І. Харитонова та ін.]. - Одеса : Фенікс, 2017. - 174 с.

Розглянуто взаємозв'язки між категоріями «ІТ-право» та «інформаційна безпека». Проаналізавано теоретичне підґрунтя визначення взаємозв'язку інформаційної безпеки та ІТ-права.

Шифр зберігання НБУВ: ВА820049.

***

Кримінально-правове забезпечення сталого розвитку України в умовах глобалізації : матеріали міжнар. наук.-практ. конф., 12-13 жовт. 2017 р. - Харків : Право, 2017. - 557 с.

Зі змісту:

- Мисливий В.А. Кримінально-правова охорона кібернетичної безпеки в умовах глобалізації;
- Гоманюк О.О. Використання механізмів міжнародного співробітництва у кримінальних провадженнях, пов'язаних із кіберзлочинністю;
- Прудников Я.В. Щодо предмета і засобів злочинів, які вчиняються у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мережі електрозв'язку.

Шифр зберігання НБУВ: ВА819926.

***

Матеріали ІІІ Міжнародної науково-практичної конференції "Право, держава та громадянське суспільство в умовах системних реформ" (15-16 вересня 2017 року). - Одеса ; Херсон, 2017. - 111 с.

Зі змісту:

- Шумейко І.В. Проблеми нормативно-правового забезпечення інформаційної безпеки України.

Шифр зберігання НБУВ: ВА819908.

***

Матеріали V Міжнародної науково-практичної конференції «Перспективи розвитку сучасної науки» (29-30 вересня 2017 року, м. Київ). - Київ, 2017. - Ч. 2. - 151 с.

Зі змісту:

- Савінкін М.Ю. Забезпечення кібернетичної безпеки – нагальна потреба України:
- Ярмола В.Г. Проблемні аспекти визначення поняття «кібербезпека».

Шифр зберігання НБУВ: В357067/2.

***

Матеріали XX Ювілейної міжнародної звітної конференції юних юристів, студентів, аспірантів і молодих вчених, присвяченої 20-річчю Національного університету "Одеська юридична академія" та 170-річчю Одеської школи права, 12 травня 2017 року. - Одеса : Фенікс, 2017 . - Т. 1. - 470 с.

Зі змісту:

- Котляренко К.М. Стратегія кібербезпеки України;
- Полякова Е.С. Единый центр кибербезопасности Украины.

Шифр зберігання НБУВ: В357071/1.

***

Матеріали XX Ювілейної міжнародної звітної конференції юних юристів, студентів, аспірантів і молодих вчених, присвяченої 20-річчю Національного університету "Одеська юридична академія" та 170-річчю Одеської школи права, 12 травня 2017 року. - Одеса : Фенікс, 2017 . - Т. 2. - 467 с.

Зі змісту:

- Кос'яненко Є.В. «Комп'ютерні» злочини в сучасному кримінальному праві;
- Баранова А.І. Кіберпростір як фактор транснаціональної злочинності;
- Левкович В.М., Іоргачов Л.Л. Загальна характеристика деяких способів інтернет-шахрайства у сучасному суспільстві.

Шифр зберігання НБУВ: В357071/2.

***

Нізовцев Ю. Ю. Окремі питання упорядкування понятійно-термінологічного апарату у сфері кібербезпеки / Ю. Ю. Нізовцев // Вісник Харківського національного університету внутрішніх справ. - 2017. - Вип. 4. - С. 135-144.

Досліджено нормативні акти, що мають стосунок до кібербезпеки. Виявлено й проаналізовано неузгодженості та суперечності понятійно-термінологічного апарату кібербезпеки, запропоновано шляхи їх усунення.

Шифр зберігання НБУВ: Ж69872.

***

Професіоналізація у сфері публічного управління: стан, проблеми, перспективи вирішення : монографія / за заг. ред. С. К. Хаджирадєвої. - Київ, 2017. - 255 с.

Зі змісту:

- Алюшина Н.О. Кіберпрофесіоналізація фахівців публічної сфери.

Шифр зберігання НБУВ: ВА819475.

***

Самойленко Д. М. Спеціальні розділи математики у кібербезпеці : навч. посіб. для індивід. роботи студентів / Д. М. Самойленко. - Миколаїв : НУК, 2017. - 86 с.

Розглянуто основи вибраних розділів математики,що не входять до базового курсу вищої математики та є необхідними для професійної підготовки фахівців з кібербезпеки. Наведено приклади програмної реалізації окремих обчислювальних алгоритмів.

Шифр зберігання НБУВ: ВА820002.

***

Транскордонна співпраця: проблеми та шляхи їх вирішення : матеріали ІІ Регіон. круглого столу, 28-29 верес. 2017 р., м. Одеса. - Київ, 2017. - 261 с.

Зі змісту:

- Ковбан А. Засади права на безпеку у сфері інформаційної безпеки;
- Довгань О. Щодо тенденції кібербезпеки в 2017 році.

Шифр зберігання НБУВ: ВС63646.

***

Шуст Н.Б. Теоретико-правові питання кібербезпеки у сфері Інтернету та її стану в Україні, способи захисту від кіберзлочинців / Н.Б. Шуст, Т.С.Ярошенко, А.В.Яценко // Прикарпатський юридичний вісник. - 2017. - Вип. 5. - С. 110-113.

Досліджено загальну характеристику, розкрито суть кібербезпеки, її стан в Україні. Проаналізовано перспективи розвитку цієї сфери діяльності. Розглянуто такі поняття, як кібербезпека, кіберзлочин, кіберзахист, кібератака, кіберполіція.

Шифр зберігання НБУВ: Ж74200.

***

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.