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

№ 9 (вересень)

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.

© Науково-дослідний інститут інформатики і права Національної академії правових наук України,
© Національна бібліотека України імені В. І. Вернадського, 2018

ЗМІСТ

«ОБСЕ ищет международного эксперта по противодействию киберпреступности для обучения офицеров Департамента киберполиции Национальной полиции Украины.

Соответствующее объявление размещено на официальном сайте ОБСЕ и на странице OSCE Project Co-ordinator in Ukraine…

Вакансия открыта только для иностранцев…

Как объясняется в описании вакансии, в рамках своего мандата и в соответствии с целями Программы обеспечения безопасности Координатора проектов ОБСЕ в Украине, а также в соответствии с просьбой Министерства внутренних дел Украины, блок КПвУ ОБСЕ по борьбе с торговлей людьми оказывает содействие в повышении компетенции правоохранительных органов Украины в борьбе с киберпреступностью и торговлей людьми…

Эксперта планируют привлечь к разработке трехдневного учебного курса и его проведению 22-24 октября в Киеве.» ***(Владимир Кондрашов. ОБСЕ ищет "тренера" для украинской киберполиции // Internetua (http://internetua.com/obse-isxet-trenera-dlya-ukrainskoi-kiberpolicii). 10.09.2018).***

***

«Дыра», через которую ранее российские хакеры взломали сайт Донецкой областной военно-цивильной администрации, спустя несколько месяцев вновь оказалась на портале.

Об этом на своей странице в Facebook сообщил спикер Украинского киберальянса, известный в сети под ником Шон Таунсенд…

По словам хактивиста, уязвимость позволяет просмотреть любой файл на сервере, в том числе узнать root-пароль от MySQL…» ***(Владимир Кондрашов. Сайт Донецкой ОГА оставил лазейку для российских хакеров // Internetua (http://internetua.com/sait-doneckoi-oga-ostavil-lazeiku-dlya-rossiiskih-hakerov). 06.09.2018).***

***

«Не очень критическую, но неприятную» уязвимость обнаружил на сайте Генеральной прокуратуры Украины спикер Украинского Киберальянса, известный под ником Шон Таунсенд…

– А вот в Генеральной прокуратуре Украины сидят умники. Вместо того, чтобы правильно экранировать запросы, кто-то решил повыёживаться и проверить, не содержит ли запрос «недопустимые символы», но проверяет только первый. То, что вы видите на экране, называется XSS-уязвимость, не очень критичная, но неприятная. Передайте кто-нибудь прокурорским, чтобы починили, – написал спикер УКА…» ***(Владимир Кондрашов. На сайте Генпрокуратуры обнаружили XSS-уязвимость // Internetua (http://internetua.com/na-saite-genprokuratury-obnarujili-xss-uyazvimost). 06.09.2018).***

***

«Президент Украины Петр Порошенко одобрил решение Совета нацбезопасности и обороны (СНБО) о выделении в 2019 году более 5% ВВП на оборону и безопасность.

…часть средств будет потрачена на реализацию государственной политики в сфере кибербезопасности…» ***(Украина направит часть военного бюджета на кибербезопасность // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3743771). 15.09.2018).***

***

«Украинское телеком-сообщество всколыхнул пост Председателя Правления ГС «Национальная ассамблея Украины», основателя группы компаний «Адамант» Ивана Петухова о якобы строительстве в Киеве на Мельникова, 83Б под видом информационного депозитария идет строительство центра перехвата информации пользователей украинского сегмента всемирной паутины…

Как рассказал Иван Петухов… якобы под контролем Госспецсвязи происходит строительство и техническое оснащение некоего объекта для мониторинга

– Сообщили, что туда завезли очень мощное оборудование одного известного мирового бренда и что-то там строят. Говорят, что там строится якобы информационный депозитарий и, под видом информационного депозитария якобы хотят взять под контроль информационные потоки из Украины, и, скорее всего, это делается под президентские и парламентские выборы для того, чтобы изолировать доступ в Украину из внешних ресурсов и наоборот.

Петухов подчеркнул, что не уверен в правдивости полученной информации, однако за последнее время он получил похожие сведения из нескольких разных источников, что и подвигло его написать пост…

Пост Ивана Петухова одним из первых прокомментировал глава парламентского комитета по вопросам информатизации и связи Александр Данченко, который выразил свое мнение, что полученная информация «точно фейк»…» ***(Владимир Кондрашов. Инсайдер: Госспецсвязи строит центр перехвата информации в ранет // Internetua (http://internetua.com/insaider-gosspecsvyazi-stroit-centr-perehvata-informacii-v-uanet). 19.09.2018).***

***

«В рамках акции #fuckresponsibledisclosure Украинский кибералъянс обнаружил множественные уязвимости на порталах целого ряда высших учебных заведений и научных учреждений страны.

Сведения об уязвимостях двадцати одного портала опубликовал у себя на странице в Facebook спикер Украинского кибералъянса, известный под ником Шон Таунсенд…

Украинский кибералъянс обнаружил проблемы с безопасностью на порталах Запорожского национального университета, Украинского государственного университета железнодорожного транспорта, Национальной библиотеки имени Вернадского, Полтавского национального университета имени Короленко,

Полтавского национального технического университета имени Кондратюка, Учебно-научного института экологической безопасности Национального авиационного университета, Черноморского национального университета имени Петра Могилы, Киевского Университета имени Бориса Гринченко, Института информационных технологий Ивано-Франковского национального технического университета нефти и газа, Одесской юридической академии, Тернопольского национального педагогического университета имени Гнатюка, Национального института пищевых технологий, Военного института танковых войск ХПИ и Львовского национального университета имени Франко.

Кроме научных учреждений, в списке также сайт институций гражданского общества Винницкого горсовета, Свялявская РГА, Совет предпринимателей тернопольской области, Свято-Успенская Почаевская лавра, Николаевводоканал, Запорожское отделение Укргосфонда поддержки фермерских хозяйств и даже Киевский международный институт социологии. Если многие администраторы и руководители учреждений поблагодарили УКА за выявление брешей в защите, то в последнем случае КМИС отреагировали не совсем адекватно:

Как стало известно, в большинстве случаев на данных порталах обнаружены SQL и XSS-уязвимости. Некоторые сайты уже оказались взломаны иностранными хакерами, при чем – довольно давно.» ***(Владимир Кондрашов. Украинская наука не дружит с кибербезопасностью // Internetua (http://internetua.com/ukrainskaya-nauka-ne-drujit-s-kiberbezopasnostua).17.09.2018).***

***

«8-11 жовтня в КВЦ «Парковий» відбудеться щорічний форум з кібербезпеки HackIT. Цьогорічна тема — Exploit Blockchain. Захід об’єднає білих хакерів, фахівців з блокчейну та провідних cybersecurity-експертів

Організатором виступає міжнародна компанія Hacken, що спеціалізується на продуктах для кібербезпеки. У програмі заходу HackIT 4.0 — дводенна конференція, панельні дискусії, круглі столи, тренінги, виставкова зона та змагання для «білих» хакерів…

10–11 жовтня відбудеться дводенна конференція, що буде присвячена кібербезпеці. Контент умовно поділений на два блоки: «День нападу» та «День захисту». 10 жовтня спікери розкажуть про останні методики кібератак, а 11 — про актуальні інструменти захисту…

Загалом на конференції в рамках HackIT 4.0 виступатимуть понад 50 спікерів. Організатори готують 3 лекційні зали, 4 панельні дискусії, 2 000 кв. м. виставкової площі та декілька круглих столів.

Крім того, у дні конференції відбудеться CTF (capture the flag) — традиційна гра для білих хакерів. Гру буде проведено онлайн з 31 серпня по 2 вересня.

Ще одна активність для білих хакерів — bug bounty марафон Hacken Cup. 8 жовтня відбудеться фінал марафону в режимі onsite. Учасники отримають доступ до продуктів клієнтів і зможуть виявити вразливості в їхніх продуктах: сайтах, мобільних застосунках, платіжних системах. Переможці отримають фінансову винагороду та інші призи…» ***(Людмила Кліщук. У Києві відбудеться***

масштабний форум «білих» хакерів // Na chasi (https://nachasi.com/2018/09/25/u-kyyevi-vidbudetsya-masshtabnyj-forum-bilyh-hakeriv/). 25.09.2018).

***

«Глобальні корпорації вже друге десятиріччя проводять навчання своїх співробітників навичкам безпечної роботи з інформацією, розпізнавання та правильних дій під час інцидентів кібербезпеки…

Настав час, коли подібне навчання потрібно проводити не тільки для співробітників великих компаній, а й для всього населення…

Найпершим кроком має бути розробка структури програми, яка відповість на питання, які навички потрібні та які канали і методи навчання використовувати для різних "профілів" громадян.

Україна має вирішити, як рухатись у цьому напрямку – створити контент і платформи навчання самостійно чи зекономити час і купити готовий продукт…» ***(Олексій Янковський. Навчання населення з кібербезпеки: чому це важливо і як реалізувати // Українська правда (https://www.pravda.com.ua/columns/2018/09/15/7192149/). 15.09.2018).***

***

«З 2016 року проникнення неліцензійного програмного забезпечення в Україні знизилося на два процентних пункти. В Україні 80% програмного забезпечення (ПЗ), встановленого на комп'ютерах, не має необхідних ліцензій. Про це йдеться в тексті дослідження BSA Global Software Survey. Наголошується, що з 2016 року проникнення неліцензійного ПЗ в Україні знизилося на два процентних пункти. При цьому, у США цей показник використання піратського софту становить 15%. Всього проникнення піратського ПЗ в східній Європі становить 57%. Найнижчий рівень піратства спостерігається у країнах Північної Америки (16%) та Західної Європи (26%), що робить вплив на світову статистику: в цілому по світу використання «піратського» софту становить 37%. У дослідженні також наводяться відомості щодо обсягу та вартості неліцензійного ПЗ. В Україні, за результатами дослідження, вартість всього, встановленого без ліцензій ПЗ за 2017 рік, склала 108 млн доларів. В грошовому еквіваленті Україна на третьому місці після Росії (1,2 млрд доларів) і Чехії (149 млн доларів) в регіоні Центральна і Східна Європа. А по процентному співвідношенню - на шостому місці. Наголошується, що використання неліцензійного ПЗ сприяє зростанню кібератак і пов'язане з фінансовими втратами.» ***(В Україні 80% програмного забезпечення є неліцензійним - дослідження // "Українські медійні системи" (https://glavcom.ua/news/v-ukrajini-80-programnogo-zabezpechennya-je-nelicenziynim-doslidzhennya-529293.html). 20.09.2018).***

***

«Специалист в сфере имущественного страхования, компания Chubb провела опрос о кибербезопасности среди своих клиентов, ставя перед собой цель выяснить, насколько пользователи защищены от несанкционированного доступа к персональным данным.

Как сообщает УкрСтрахование, 86% респондентов заявили о своем беспокойстве ростом числа кибератак, но большинство из них недооценивают, либо не знают о кибер-угрозах, которые нацелены на личную информацию в социальных сетях и через подключенные к Интернету устройства: ноутбуки, смартфоны, смарт-холодильники и системы отопления.

Только 12% участников опроса знают о рисках использования общественного Wi-Fi и 4% респондентов обеспокоены уязвимостью смарт-устройств домашней автоматизации.

«В настоящее время любой человек может стать жертвой кибератаки», — сказал Фран О'Брайен, президент подразделения персональных рисков Chubb North America. В отчете приводятся данные, что только 40% из тех, кто осознает риск персональной кибер-угрозы, предпринимают меры для защиты.

«Хотя нет надежного способа защиты от любого риска, кибер-страхование действительно может помочь заполнить пробелы и снизить риск, связанный с кибербезопасностью», — прокомментировал Билл Стюарт, президент подразделения киберрисков Chubb.» ***(Персональные кибер-риски содержатся в общественном WiFi, соцсетях и смарт-устройствах: Chubb // TRISTAR.com.ua - твой финансовый навигатор! (http://tristar.com.ua/1/news/personalnye_kiber_riski_soderjatcia_v_obshestvennom_wifi_sotssetiah_i_smart_ustroistvah_chubb_10427.html). 27.09.2018).***

***

«В Вооруженных силах Украины (ВСУ) в качестве паролей доступа на сервера автоматизированной системы управления войсками «Днипро» были установлены пароли типа admin и 123456.

Об этом сообщил журналист Александр Дубинский…

По его словам, это "позволяло врагу сканировать информацию украинских военных вплоть до лета 2018 года" и стоило жизни бойцов на фронте.

Согласно документам, которые журналист имеет в своем распоряжении, 22 мая этого года во время настройки и проведения тестирования сетей Автоматизированной системы управления войсками «Днипро» специалист по базам данных Дмитрий Власюк выявил, что на многих серверах и коммутаторах с IP-адресами доступ происходит по стандартному логину и паролю…

"Про уязвимые места Власюк сообщил оперативному дежурному данной военной части А0334. При дальнейшей настройке оборудования было обнаружено что его обращение было проигнорировано и пароли не были изменены. После чего он обратился на горячую линию СБУ, и в тот же день представитель военной разведки встретился с ним на территории воинской части, где Власюк проходил службу", – сообщает Дубинский.

По данным журналиста, такая же ситуация была обнаружена 25 мая 2018 года на почтовых серверах ВСУ.

"Таким образом, без каких-либо специальных знаний можно свободно иметь доступ к свитчам, роутерам, АРМ, серверам, голосовым шлюзам, принтерам, сканерам и т.п. – то есть, иметь возможность анализировать огромный массив секретной информации Вооруженных сил", – подчеркивает журналист.

Он пишет, что учитывая такой объем утечки информации, противнику достаточно было всего нескольких дней чтобы просканировать всю сеть АСУ “Днипро” и создать топологию всех сетей по роду и виду войск, структурным подразделениям и использовать данную сеть для выяснения поставленных задач, учитывая то, что услуги связи предоставляются Укртелекомом.

“Поскольку обращение Власюка к руководству военной части было проигнорировано, он 25 мая 2018 года, рекомендованным письмом, обращается в СНБО и Службу внешней разведки, где излагает всю описанную ситуацию”, – сообщает журналист.

Дубинский приводит хронологию с письмом Власюка, сообщая, что спустя 10 дней, 5 июня 2018 года СНБО перенаправляет данное обращение Министерству обороны и СБУ, и подписано данное письмо – офшорным помощником президента Свинарчуком-Гладковским. Спустя еще 8 дней, 13 июня 2018 года Служба внешней разведки (СВР) сообщает Власюку, что проблема защищенной настройки АСУ «Днипро» не относится к компетенции Службы внешней разведки, поскольку Служба не использует данную систему в своей деятельности, и не имеет возможности влиять на информационные системы других госорганов, и кроме всего прочего – центр обеспечения кибербезопасности появился на базе департамента контрразведки СБУ, а центр киберзащиты ИТС на базе ГУ связи ВСУ…

Спустя месяц, 26 июня 2018 года, Минобороны (ВЧ0106), согласно письмк СНБО, предоставила ответ Власюку, в котором указала что Минобороны и ВСУ провели следующие мероприятия: запрет использования слабых паролей и периодическая проверка всех АРМ, сетевых приборов, серверного оборудования ИТС ВСУ на наличие слабых логинов и паролей.

Сообщили что ряд IP-адресов является элементом обучающим и не нуждается, по их мнению, в укреплении. Также, не предоставляет опасности один из серверов, который является тестовым, а еще один вообще не используется.

Также Власюк получил 05 июля 2018 года ответ от Департамента контрразведывательной защиты интересов государства в сфере информационной защиты СБУ, согласно которому, все нарушения доступа в сети АСУ «Днипро» устранены. Однако 12 июля 2018 года при очередном тестировании АСУ «Днипро» Власюк обнаружил что ряд оборудования с конкретными IP-адресами и далее используют стандартный пароль и логин, а в некоторых случаях – доступ в сеть с компьютеров и на компьютеры Минобороны, связанные в единую сетку, происходит без пароля.

Большая часть технических средств используется, при этом, в разных военных частях и закреплена за конкретными военнослужащими, которые за данные нарушения должны нести персональную ответственность.

“Власюк 13 июля 2018 года повторно обратился в СНБО, где указал на отсутствие реакции на его обращение. Одновременно он отправил дополнительно информацию в Аппарат ВР Украины, который в свою очередь 20 июля 2018 года ответил, что информация передана в Комитет ВР Украины по вопросам национальной безопасности и обороны”, – рассказывает журналист.

СНБО, на повторное обращение ответил, что направил обращение в СБУ и Минобороны для повторного рассмотрения. Подпись поставил все тот же Гладковский.

“Пошел четвертый месяц, а пароли доступа к техническим средствам, серверам и компьютерам Минобороны остаются теми же: 123654 и admin…”, – констатирует Дубинский.

“Что же касается Власюка, то после обращений в СНБО и СБУ его полностью отключили от сетей АСУ «Днипро», организовали проверку Генштаба и угрожают ему криминальным преследованием…”, – сообщает он, – “В качестве интересной детали этой истории, добавлю информацию о том, что в Украине работает восемь трастовых фондов НАТО по киберзащите, которые занимаются развитием оперативных способностей и содействие в трансформации ВСУ”.

В 2017 году НАТО выделило на эти цели порядка 40 млн евро. Ответственным за реализацию данного проекта является СБУ, напоминает журналист.» ***(“Admin” и “123456”: какими паролями защищали систему управления ВСУ // Goodnews.ua (http://goodnews.ua/technologies/admin-i-123456-kakimi-parolyami-zashhishhali-sistemu-upravleniya-vsu/). 26.09.2018).***

***

Національна система кібербезпеки

«Служба безпеки України посилює захист інформаційної безпеки на підприємства енергетичної галузі України. Про це повідомляє прес-центр СБУ…

“Для розбудови ефективної системи кібербезпеки держави СБУ підписала Меморандум з національною енергетичною компанією “Укренерго” та приватним акціонерним товариством “Укргідроенерго”, — йдеться у повідомленні.

Як зазначається, документ має забезпечити обмін інформацією з СБУ щодо кібернетичних загроз з використанням платформи MISP-UA зі стратегічно важливими підприємствами енергетичної галузі України. Обмін матеріалами, зокрема технологічною інформацією про реалізовані та потенційні кіберзагрози відбуватиметься в режимі реального часу. Така міжвідомча взаємодія сприятиме ефективному реагуванню з боку української спецслужби на кібернетичні атаки, насамперед високого ступеня складності.

“Будь-який представник великого, середнього та навіть малого бізнесу може звернутися до центру за консультаціями та допомогою”, — наголосив Голова СБУ Василь Грицак на відкритті ситуативного центру…» ***(Євген Дем’янов.СБУ посилить захист кібербезпеки в енергетиці // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1752184-sbu-posilit-zakhist-kiberbezpeki-v-energetitsi). 14.09.2018).***

***

«Вчера, 20 сентября, Комитет Верховной Рады Украины по вопросам информатизации и связи рассматривал проект Закона о Государственном

бюджете Украины на 2019 год. Как оказалось, в новом бюджете не хватает примерно 2 миллиарда гривен на кибербезопасность, лицензионный софт, строительство и поддержку уже действующих ИТ-систем.

Денег не додали Государственному агентству по вопросам электронного правительства, Госспецсвязи, Департаменту киберполиции, СБУ, НКРСИ, пограничникам и Укрпочте…

– Ситуация нам не очень нравиться. Проведение тендеров на 4G, 3G, рост платежей за радиочастоты во всем мире – это индустриальный сбор, который всегда возвращается обратно в отрасль для её развития. У нас же ситуации такая, что отрасль превысила на 3 миллиарда показатели поступления в бюджет и всё это забирается бюджетом, потому что там дырка, – прокомментировал нашему журналисту ситуацию глава Комитета Александр Данченко. – Поэтому мы будем пытаться получить дополнительное финансирование как минимум на поддержку программного обеспечения. В условиях войны кибербезопасность должна быть одним из приоритетных направлений. На сегодня же все деньги, которые у них (профильных органов, занимающихся вопросами кибербезопасности – Ред.) есть, они идут на повышение заработных плат, что уже неплохо, но всё съедается зарплатой и нет развития. Это очень плохо…

НКРСИ просит «всего» 8,5 миллионов…

По словам руководителя Госагентства по вопросам е-правительства Александра Рыженко, в рассматриваемом проекте бюджета на сферу электронного правительства и информатизации запланировано вцелом около 180,9 миллиона гривен. Дополнительно агентству нужно практически столько же: 148 миллионов гривен….

СБУ просит ещё почти полмиллиарда

Государственной пограничной службе нужно ещё 860 миллионов…

На заседании комитета оказалось, что правительство часто забывает дать денег на свои же инициативы…» ***(Владимир Кондрашов. В проекте Госбюджета не хватает 2 миллиарда на кибербезопасность // Internetua (http://internetua.com/v-proekte-gosbuadjeta-ne-hvataet-2-milliarda-na-kiberbezopasnost). 21.09.2018).***

***

«Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України та державне підприємство Міністерства інфраструктури "Галузевий центр цифровізації та кібербезпеки" підписали угоду про науково-технічне партнерство у сферах зв'язку, інформаційної та кібербезпеки…

У міністерстві зазначають, що наразі розпочалася розробка технічного проекту Security Operation Center (SOC) - Центру управління кібербезпекою на транспорті, забезпечення кіберзахисту апарату Мінінфраструктури та підключення стратегічних підприємств галузі до єдиної галузевої кібермережі.

Партнерство з Держспецзв'язку суттєво прискорить створення центру та забезпечить безшовну інтеграцію з системами національних центрів кіберзахисту та протидії кіберзагрозам, наголошують у міністерстві…» ***(Державний центр***

кіберзахисту та Галузевий центр цифровізації та кібербезпеки Мінінфраструктури домовилися про співпрацю // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/532666.html). 20.09.2018).

***

«…Согласно исследованию "Глобальный индекс кибербезопасности" (Global Cybersecurity Index), которое ежегодно проводится Международным союзом электросвязи (ITU), в 2017 году Украина заняла "почетное" 59 место в рейтинге из 193 возможных. При этом из стран постсоветского пространства — Латвия, Беларусь и Азербайджан существенно опередили нас в рейтинге. А Россия (10 место), Грузия (8 место), Эстония (5 место) и вовсе вошли в десятку мировых лидеров в данной области.

…Уровень кибербезопасности государств-респондентов оценивался по пяти основным показателям:

-Legal (законодательная база);

-Technical (технологическая база);

-Organization (методологическая база);

-Capacity Building (наращивание потенциала);

-Cooperation (развитие взаимодействия).

Из перечисленных показателей в Украине в "зелёной зоне" оказались только "Legal" и "Cooperation". Действительно, законодательные инициативы последних лет и создание государственных центров кибербезопасности должны были позитивно отразиться на результатах исследования… с практическим применением законодательных инициатив в области кибербезопасности в Украине дела обстоят не очень хорошо. Самые низкие показатели, повлиявшие на общий результат нашей страны в исследовании, лежат именно в практической плоскости. Это, в первую очередь, почти полное отсутствие R&D и инструментов стимулирования развития отрасли кибербезопасности.

…Минусом для Украины является также нехватка отраслевых центров управления кибербезопасностью, хотя за первое полугодие 2018 года в этом направлении наметился определенный прогресс.

Недостает нам и профильных, а самое главное — актуальных стандартов и методологий в области кибербезопасности. Вниз тянет повсеместно недостаточный уровень имплементации реальных мер киберзащиты в ИТ-инфраструктурах, слабо поставленный процесс обучения и повышения осведомлённости в вопросах кибербезопасности. Не спасает ситуацию ни наличие профильной государственной службы — Госспецсвязи, ни достаточно высокая степень вовлеченности Украины в международное сотрудничество по вопросам обеспечения кибербезопасности…» ***(Состояние кибербезопасности в Украине: независимая внешняя оценка // Goodnews.ua (http://goodnews.ua/technologies/sostoyanie-kiberbezopasnosti-v-ukraine-nezavisimaya-vneshnyaya-ocenka/). 15.09.2018).***

***

«Комітет з питань інформатизації та зв'язку розглянув на своєму засіданні проект Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері», № 6688…

У ході обговорення зазначалося, що Державне агентство з питань електронного урядування України повідомило про відсутність пропозицій та зауважень до законопроекту. Адміністрація Державної служби спеціального зв'язку та захисту інформації України надала зауваження та висловила позицію, що зазначений законопроект потребує суттєвого доопрацювання та активного залучення громадськості до розв'язання порушеної проблеми…

До Комітету звернулися профільні асоціації галузі інформаційно-телекомунікаційних технологій, які висловили категоричну незгоду з поданою редакцією законопроекту та наголосили на тому, що при підготовці законопроекту були повністю проігноровані пропозиції експертного середовища, законопроектом неможливо досягти задекларованих цілей, а його прийняття спричинить грубе порушення норм міжнародного права.

Комітет звертає увагу, що законопроектом пропонується внести зміни до Закону України «Про основи національної безпеки України», який втратив чинність на підставі Закону України «Про національну безпеку України», який набрав чинності 08.07.2018 р. у зв'язку з чим, законопроект не може бути прийнятий за основу.

Також, після реєстрації законопроекту № 6688 Верховною Радою України 05.10.2017 р. був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Таким чином, оскільки законопроект, № 6688, був розроблений до прийняття Закону України «Про національну безпеку України» та Закону України «Про основні засади забезпечення кібербезпеки України», та, відповідно, не враховує норм зазначених законів, він має бути узгоджений з ними.

Враховуючи зазначене, Комітет ухвалив рішення: 1. Рекомендувати Верховній Раді України повернути на доопрацювання суб'єкту права законодавчої ініціативи проект Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері», № 6688. 2. Звернутися до Голови Верховної Ради України Парубія А.В. відповідно до частини 4 статті 111 Закону України «Про Регламент Верховної Ради України» щодо надання виступу від Комітету при розгляді зазначеного питання на пленарному засіданні Верховної Ради України Голові Комітету Данченку О.І. 3. Направити висновок до Комітету Верховної Ради України з питань національної безпеки і оборони.» ***(Комітет з питань інформатизації та зв'язку рекомендує***

повернути на доопрацювання проект Закону про внесення змін до законодавства щодо протидії загрозам національній безпеці в інформаційній сфері // Народна Рада (http://narodnarada.info/news/komitet-pitan-informatizaciji-zvyazkukomitet-pitan-informatizaciji-zvyazku_105578-news-106355.html). 05.09.2018).

***

«Нацбанк предлагает для общественного обсуждения проект постановления по обеспечению киберзащиты и информационной безопасности в сфере перевода денег…

Соответствующий проект постановления Правления НБУ "Об утверждении Положения о киберзащита и информационной безопасности в платежных системах и системах расчетов" Нацбанк предлагает для общественного обсуждения", - говорится в сообщении.

Проектом постановления предусмотрено определить:

требования к субъектам платежного рынка по построению системы защиты информации и кибербезопасности;

порядок действий при обнаружении кибератак, которые снижают надежность функционирования платежных систем и систем расчетов;

требования к организационным и техническим мерам с целью обеспечения защиты информации и кибербезопасности субъектами платежного рынка и тому подобное.» ***(НБУ займется киберзащитой денежных переводов // Телеграф (https://telegraf.com.ua/biznes/finansyi/4532445-nbu-zaymetsya-kiberzashhitoy-denezhnyih-perevodov.html). 27.09.2018).***

***

Кібервійна проти України

«Про хакерські атаки і як з ними борються напередодні виборів, розповів в інтерв'ю UATV начальник Департаменту кіберполіції Сергій Демедюк.

"Кібератаки на нашу країну йдуть масово з усіх територій, це може означати, що їх використовують, щоб анонімізувати, хто саме робить атаку. Але найбільша кількість кібератак, яку ми фіксуємо, йде з РФ", – розповів Демедюк.

Кіберполіція України вже фіксує спроби скомпрометувати ресурси державних органів, підприємств та інших компаній, які стикаються з державним сектором.

"Ми постійно готуємося, щоб не допустити кібератак спільно з СБУ. Ми намагаємося працювати на випередження", – говорить експерт.

За його словами, види атак дуже різні, починаючи від простих DoS-атак. Він зазначив, що російські хакери готують так звані black door – потаємні ходи для непомітного доступу до техніки українців.

Демедюк підкреслив, що Україна для боротьби з хакерами, активно працює з міжнародними партнерами…

Демедюк наголосив, що кіберполіція фіксує всі спроби впливати на виборчий процес. "Ми підключаємо міжнародних партнерів, у яких для цього є хороша

технічна підтримка та інші ресурси, для недопуску втручання хакерів у вибори", – підсумував гість студії…» ***(Наталія МАРЧЕНКО. Україна готова протидіяти втручанню хакерів у вибори, – начальник кіберполіції // UATV (http://uatv.ua/ukrayina-gotova-protydiyaty-vtruchannyu-hakeriv-u-vybory-nachalnyk-kiberpolitsiyi/). 06.09.2018).***

***

«…З офісу Facebook (Фейсбук) на українських користувачів здійснюють кібератаки. Про це написав нардеп Ар'єв на власній сторінці у соцмережі.

За словами політика, від знайомих фахівців у сфері інформаційних технологій, він отримав листа про ймовірні атаки на українських користувачів з IP-адрес Facebook.

«Вони провели власне дослідження і з'ясували що в офісі Facebook у Дубліні не просто блокують українських користувачів чи слабко реагують на антиукраїнський контент. З IP-адрес цього офісу зафіксована кібератака на користувача, що є протизаконним», — йдеться в повідомленні.

За словами депутата, через цей лист адміністрація соцмережі повинна перевірити відділення, яке відповідає за контент з України…» ***(Нардеп заявив про ймовірні кібератаки на українців з офісу Facebook (ДОКУМЕНТ) // Громадсько-правовий портал «Ракурс» (http://racurs.ua/ua/n110388-nardep-zayavyv-pro-ymovirni-kiberataky-na-ukrayinciv-z-ofisu-facebook-dokument). 03.09.2018).***

***

«Упродовж останніх 5 років різновиди кібератак на інформаційні системи України еволюціонували. Про це сьогодні на відкритті Ситуаційного центру забезпечення кібербезпеки СБУ заявив глава відомства Василь Грицак…

"Протягом останніх п'яти років спостерігається еволюція різновидів кібератак на Україну, які все частіше набувають ознаки кібершпигунства та кібертероризму", — сказав Грицак.

За його словами, зафіксовано зростання активності спецслужб РФ щодо проведення цілеспрямованих кібератак, орієнтованих на отримання несанкціонованого доступу до інформаційних систем органів державної влади України. Здійснення акцій кібернетичного тероризму спрямовані, також, на порушення штатного функціонування комп'ютерних мереж та систем керування технологічними процесами об'єктів критичної інфраструктури.

За інформацією СБУ, використовуючи деструктивне програмне забезпечення "Black Energy" зловмисники неодноразово здійснювали кібератаки на комп'ютерні мережі об'єктів української енергетики…» ***(Євген Дем'янов. Грицак: за останні 5 років види кібератак на Україну еволюціонували // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1752188-gritsak-za-ostanni-5-rokiv-vidi-kiberatak-na-ukrayinu-evolyutsionuvali). 14.09.2018).***

***

«На сторінки і аккаунти, пов'язані з проектом "Книга добра", було здійснено кібератаки. Про це повідомив міністр закордонних справ Павло Клімкін на своїй сторінці у Facebook…

"Позавчора та вчора на сторінки та аккаунти, пов'язані з проектом "Книга Добра", було здійснено кібератаки", - повідомив П.Клімкін.

Зазначимо, "Книга добра" - це міжнародний соціальний проект, участь в якому за час реалізації взяли більше 300 дітей і дорослих. Усі охочі з усіх регіонів України писали реальні історії про добро, мудрі безкорисливі вчинки людей з добрим серцем і прагненнями. У "Книгу добра" увійшли 50 таких історій…» ***(Ірина Матюшенко. Клімкін повідомив про кібератаки на аккаунти проекту "Книга добра" // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1753752-klimkin-povidomiv-pro-kiberataki-na-akkaunti-proektu-kniga-dobra). 24.09.2018).***

***

«Останнім часом і на Фанар, і на Вселенський Патріархат, і на самих екзархів відбуваються масовані кібератаки. Про це повідомив міністр закордонних справ України Павло Клімкін після зустрічі з екзархами його Всесвятості Вселенського Патріарха…

"Останнім часом і на Фанар, і на Вселенський Патріархат, і на самих екзархів відбуваються масовані кібератаки", - написав Клімкін у Facebook…» ***(Тоня Туманова. На Вселенський Патріархат і на екзархів здійснюють масовані кібератаки – Клімкін // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1752653-na-vselenskiy-patriarkhat-i-na-ekzarkhiv-zdiysnyuyut-masovani-kiberataki-klimkin). 17.09.2018).***

***

«США та Україні необхідно докладати більше зусиль для протидії інформаційним війнам та кібератакам. Про це заявив Спеціальний представник Державного департаменту США з питань України Курт Волкер на 15-й Щорічній зустрічі Ялтинської Європейської Стратегії (YES)…

"Все починається з людської волі, в тому числі, коли ми говоримо про технології (інформаційних війн та кібератак) і їх застосування. Треба впливати на прийняття рішень, щоб уникнути небажаних подій, вчасно на них реагувати і робити це ефективно. Я хочу сказати, що в цьому питанні ми дуже мляво проявляємо свою волю. Ми маємо всі необхідні та дієві інструменти, зокрема, в порівнянні з нашим ворогом", — сказав він…» ***(Саша Картер. США та Україна дуже мляво проявляють свою волю в питанні кіберзахисту – Волкер // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1752249-ssha-ta-ukrayina-duzhe-mlyavo-proyavlyayut-svoyu-volyu-v-pitanni-kiberzakhistu-volker). 14.09.2018).***

***

«Секретар Ради національної безпеки і оборони України Олександр Турчинов та засновник і виконавчий директор компанії Jigsaw Джаред Коен

домовилися про співпрацю в питаннях забезпечення кіберзахисту та протидії інформаційній агресії, зокрема під час чергових українських виборів…

Окрім того, під час зустрічі сторони обговорили питання кібернетичної та інформаційної агресії РФ. Окрему увагу Турчинов та Коен приділили досвіду фахівців США та напрацюванням України, яка протистояла кільком найпотужнішим атакам з боку Російської Федерації.

За словами Турчинова, Україна за досить стислий термін значно посилила спроможності у питаннях кіберзахисту та, згідно з оцінками експертів, досягла в цьому напрямку рівня багатьох країн ЄС. Однак Турчинов додав, "що багато питань ще залишаються невирішеними, а тому необхідно ще багато зробити для забезпечення надійного кіберзахисту країни".

Коен у свою чергу зазначив, що інформаційні та кібератаки Росії спрямовані "в трьох напрямках", а саме на схід України, де тривають військові дії, на внутрішню дестабілізацію держави, руйнацію її політичної системи і компрометацію прозорих та чесних виборів, а також на дискредитацію репутації України у світі…» ***(Україна співпрацюватиме з Jigsaw у сфері кіберзахисту - РНБО // «Дзеркало тижня. Україна» (https://dt.ua/UKRAINE/ukrayina-spivpracyuvatime-z-jigsaw-u-sferi-kiberzahistu-rnbo-288499_.html). 14.09.2018).***

***

Боротьба з кіберзлочинністю в Україні

«Суд украинского города Никополь приговорил местного жителя к одному году лишения свободы условно за организацию массовой кибератаки на украинские компании с помощью вируса Petya, повлекшей большие убытки.

Украинский гражданин обвинялся по статье УК Украины «Создание с целью использования, распространения или сбыт вредных программных или технических средств, а также их распространение и сбыт». Обвиняемый полностью признал вину…» ***(Ольга Никитина. Слесарь на Украине осужден за вирус Petya // Деловая газета «Взгляд» (https://vz.ru/news/2018/9/6/940700.html). 06.09.2018).***

***

«На днях многие крупные украинские СМИ разразились заголовками о том, что Никопольский горрайонный суд осудил якобы распространителя вируса Petya. Интерес к этому делу разгорелся ещё в прошлом году, когда киберполиция сообщила, что задержала 51-летнего распространителя вируса…

Как оказалось, из приговора суда полностью исчезла вся информация, распространенная ранее киберполицией о компаниях, которые воспользовались услугами видеоблогера для «псевдоинфицирования» вирусом с целью сокрытия преступной деятельности и уклонения от уплаты штрафных санкций государству.

– Кроме того, был установлен перечень компаний, которые решили воспользоваться общегосударственной кибератакой и намеренно загружали себе

данный вирус для сокрытия преступной деятельности и уклонения от уплаты штрафных санкций государству. Меры по привлечению руководства этих компаний к ответственности уже ведутся, – говорилось в заявлении полицейских.

На данным момент в судебном реестре нам не удалось обнаружить ни одного решения, в котором бы говорилось о привлечении к ответственности компаний за такой способ сокрытия своей деятельности.

Также в приговоре вообще не упоминаются «около 400 инфицированных устройств», зараженных якобы по вине обвиняемого.

Интересно также, что в самом видео, созданном Департаментом Киберполиции, в отличии от опубликованного пресс-релиза, говорится о группе злоумышленников, а не об одном пользователе. Более того, в группе занимались не просто распространением, а и модификацией вируса…» ***(Владимир Кондрашов. Судили «распространителя вируса Petya.A» // Internetua (http://internetua.com/sudili-rasprostranitelya-virusa-petya-a). 13.09.20180.***

***

«Служба безопасности Украины объявила о разоблачении международной хакерской группировки, атакам которой подверглись более 20 государств…

В сообщении на сайте ведомства говорится, что с помощью специального программного обеспечения хакеры получали доступ к персональным данным юридических лиц банков из стран Евросоюза, Южной Азии и постсоветского пространства…

В Службе безопасности Украины заявили, что часть фирм-посредников, через которые проводились мошеннические операции, якобы была подконтрольна «российским спецслужбам».

Участники группировки проживали в Киеве, Черновцах, Одессе и Вознесенске… Организатором группировки на Украине назвали гражданина одной из стран Ближнего Востока, в настоящее время он задержан…» ***(Ольга Никитина. На Украине заявили о поимке международной хакерской группы // Деловая газета «Взгляд» (https://vz.ru/news/2018/9/7/940850.html). 07.09.2018).***

***

«Працівники кіберполіції у Сумській області викрили 19-річного мешканця міста Кривий Ріг (Дніпропетровська область) у створенні та розповсюдженні шкідливого програмного забезпечення…

Зловмисник створив шкідливе програмне забезпечення, яке потрапляючи в комп’ютер постраждалого, викрадало паролі та логіни інтернет-банкінгу та акаунтів в соціальних мережах. Крім того, розроблена хакером програма надавала доступ до веб-камери ураженого компютера, у результаті чого зловмисники могли стежити за власником техніки.

Працівники Слобожанського управління спільно з колегами з управління інформаційних технологій та програмування в східному регіоні Департаменту кіберполіції провели санкціонований обшук за місцем проживання зловмисника. Під час попереднього огляду комп’ютерної техніки спеціалісти з кіберполіції

знайшли підтвердження того, що молодик самостійно розробляв ШПЗ з метою збуту іншим особам. Оплату отримував на електронний гаманець російської платіжної системи, після чого переводив на особистий рахунок одного із українських банків…

Триває досудове розслідування у межах розпочатого кримінального провадження за 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 хакера, який створював віруси та поширював їх у мережі за гроші // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-yakyj-stvoryuvav-virusy-ta-poshyryuvav-yix-u-merezhi-za-groshi-4365/). 08.09.2018).***

***

«***Кіберполіція викрила групу зловмисників у викраденні облікових записів користувачів соціальної мережі…***

Основною метою зловмисників було отримання грошей від власників соціальних профілів за повернення доступу до сторінки. Її вартість вони оцінювали сумами від 15 до 30 тисяч гривень у криптовалюті. Наразі вже встановлено близько тисячі акаунтів соцмережі взламаних зловмисниками.

Працівники кіберполіції встановили, що за допомогою шкідливого програмного забезпечення зловмисники отримували незаконний доступ до електронних поштових скриньок, які були пов’язані з акаунтами жертв. Для цього, на електронні поштові скриньки власників акаунтів соцмережі «Instagram» здійснювалась розсилка листів, які були інфіковані цим шкідливим програмним забезпеченням. Усі ці листи були замасковані під нібито офіційні повідомлення служби підтримки соціальної мережі.

У подальшому, отримавши доступ, зловмисники вносили зміни до реєстраційних даних, чим блокували доступ справжнім власникам. За повернення доступу вони вимагали від 10 до 30 тисяч гривень у криптовалюті.

Зазвичай, у якості «жертви» обиралися сторінки, кількість підписників яких була більшою 15 тисяч користувачів (сторінки Інтернет-магазинів, відомих людей тощо)…

За даним фактом розпочато кримінальне провадження за двома статтями Кримінального кодексу України: ч.2 ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ч.3 ст.190 (Шахрайство). Зловмисникам загрожує до восьми років позбавлення волі…» ***(Кіберполіція викрила групу зловмисників у викраденні облікових записів користувачів соціальної мережі // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-zlovmysnykiv-u-vykradenni-oblikovyx-zapysiv-korystuvachiv-soczialnoyi-merezhi-6290/). 03.09.2018).***

***

«В конце августа Киберполиция накрыла в столице организаторов масштабной мошеннической онлайн финансовой биржи. По версии полицейских, злоумышленники специально создали веб-ресурсы «binex.ru»,

«binex.ua», «binex.kz» для привлечения потенциальных клиентов и создания впечатления участия в реальных онлайн финансовых торгах. Потом жертв, используя ряд методов психологического воздействия, заставляли максимально пополнить свой счет, и с помощью манипуляций лишали всех денег…

11 сентября в Киевский районный суд Харькова поступило ходатайство следователя о наложении ареста на имущество, изъятое днем ранее во время обысков.

Обыски проходили в рамках дела о мошенничестве в крупных размерах или путем незаконных операций с использованием электронно-вычислительной техники (ч. 3 ст.190 УКУ). В этом деле фигурируют пока двое пострадавших – один отдал злоумышленникам 500 долларов США, а второй - подарил целых 65 тысяч долларов.

Если в организации «работы» столичного офиса кибербполиция, по версии СМИ, подозревала гражданина Кипра, то в харьковском деле говорится о группе граждан Израиля – 6 граждан Израиля и гражданин Украины вступили в сговор с группой не менее чем из 10 человек, часть из которых следствием пока не установлены. Лидером преступной группировки следствие называет гражданку Израиля…» ***(Владимир Кондрашов. Киберполиция прекратила деятельность финансовых мошенников // Internetua (http://internetua.com/kiberpoliciya-prekratila-deyatelnost-finansovyh-moshennikov). 26.09.2018).***

***

«Суд вынес приговор в деле о хакере, который занимался модификацией и продажей вредоносного программного обеспечения для майнинга криптовалют. Как стало известно, осужденный занимался незаконной деятельностью как минимум с июля прошлого года и даже успел обмануть своих «коллег по цеху»…

Согласно материалов дела, в начале июля 2017-го безработный уроженец Рубежного скачал с неустановленного в ходе досудебного расследования сайта так называемый «конструктор», модифицировал его, путем внесения изменений в составляющие программного кода, при этом добавил сведения о своем логине на сайте «minergate.com», который был указан в пуле для «майнинга», и добавил команду для исполняющего файла для «осуществления процессором алгоритмических расчетов с целью извлечения с использованием алгоритма «cryptonight» криптовалюты», то есть – для майнинга Monero. Затем предприимчивый житель Луганщины собрал файлы в один с расширением «*.exe», который в дальнейшем скрыл в исполняемом файле, после чего поместил указанное вредоносное ПО в архив с паролем, а архив выложил на «хакерском форуме». В описании на форуме злоумышленник сообщил, что этот архив – конструктор для последующего создания и разработки вредоносного программного обеспечения, а не, собственно, самостоятельное вредоносное ПО…

13 июля между подозреваемым и прокурором было подписано соглашение о признании виновности. Исполняя условия соглашения, мужчина полностью признал свою вину, и согласился понести наказание.

Приговором суда безработного жителя Луганщины признали виновным в совершении уголовных преступлений, предусмотренных частью 1 и частью 2 статьи 361-1 УК Украины. Злоумышленнику дали 2 года лишения свободы и освободили от отбывания наказания с испытательным сроком 1 год . Кроме того, у мужчины конфисковали в пользу государства ноутбук. Также осужденный должен покрыть траты на экспертизы (без малого 20 тысяч гривен).» ***(Владимир Кондрашов. Украинский хакер обманывал «коллег» и получил 2 года лишения свободы // Internetua (http://internetua.com/ukrainskii-haker-obmanyval-kolleg-i-polucsil-2-goda-lisheniya-svobody). 21.09.2018).***

***

«Студент Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского» попался на продаже в сети скан-копий паспортов и ИНН украинцев…

Как стало известно, в начале февраля 2018 уроженец Киева «используя всемирную компьютерную сеть Интернет», загрузил на носитель информации, скан-копии официальных личных документов граждан Украины, а именно копии паспортов граждан Украины и копии карточек физических лиц – налогоплательщиков…

Студент заключил с прокурором соглашение о признании виновности. Суд утвердил соглашение, признав парня виновным в совершении уголовного преступления, предусмотренного ч.1 ст. 361-2 УК Украины (несанкционированные сбыт или распространение информации с ограниченным доступом, созданной и защищенной в соответствии с действующим законодательством). В наказание киевлянин заплатит штраф в размере 8500 гривен. Кроме того, приговорам суда у продавца персональных данных конфисковали 3 мобильных телефона, 2 системных блока и 3 флэшки.» ***(Владимир Кондрашов. Студент КПИ продавал персональные данные украинцев по 120 гривен // Internetua (http://internetua.com/student-kpi-prodaval-personalnye-dannye-ukraincev-po-120-griven). 20.09.2018).***

***

«Украинского «хакера» со средним образованием на днях приговорили к штрафу в 8,5 тысяч гривен и оплате экспертиз почти на 15 тысяч за создание вируса и его распространение под видом «чита» (программа для получения непредвиденного разработчиком преимущества над игроками в компьютерной игре) для Counter Strike 1.6. Идентифицировать злоумышленника удалось благодаря тому, что он выложил в Facebook видео, где продемонстрировал работу вируса на зараженных компьютерах и несколько раз «засветил» собственные страницы в ВК, Facebook и адрес в Skype…

Суд установил, что злоумышленник 13 июня прошлого года с помощью специальной программы создал вирус-троян под названием «123.exe», который замаскировал под специальную программу для получения непредвиденного разработчиком преимущества над игроками в компьютерной игре «Counter Strike

1.6». Парень разместил файл архива с вредоносным ПО на сайте файлообменника «rghost»…

Обвиняемый пошел на сделку со следствием, полностью признал свою вину и согласился на штраф в размере 500 необлагаемых минимумов доходов граждан, что составляет 8500 гривен. Суд также взыскал с осужденного в пользу государства 14872 грн. затрат на проведение экспертиз…» ***(Владимир Кондрашов. Хакер-неудачник заплатит 23 тысячи за распространение вируса // Internetua (http://internetua.com/haker-neudachnik-zaplatit-23-tysyacsi-za-rasprostranenie-virusa). 14.09.2018).***

***

«…Працівники Полтавського відділу Департаменту кіберполіції України спільно з детективами слідчого управління поліції у Полтавській області, під процесуальним керівництвом прокуратури Полтавської області, викрили 32-річного чоловіка у модифікації та розповсюдженні шкідливого програмного забезпечення.

Зловмисник модифікував шкідливе програмне забезпечення, яке призначалося для несанкціонованого втручання в роботу комп'ютерів. Отримавши доступ до враженого комп'ютера, зловмисник отримував усі відомості про збережені у баузері логіни, паролі, дані банківських карт, дані про гаманці криптовалют та файли з робочих столів. Загальна кількість інфікованих комп'ютерів становить понад 2,5 тисячі…

За даним фактом розпочато кримінальне провадження провадження за ст.361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України та ч.2 ст. 361 (Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж). Зловмисника затримано в порядку статті 208 КПК України. Вирішується питання щодо оголошення йому про підозру.» ***(Кіберполіція викрила хакера у модифікації вірусних програм // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-modyfikacziyi-virusnyx-program-2654/). 20.09.2018).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Украина и государство Катар будут сотрудничать в сфере кибербезопасности и обменяются опытом подготовки масштабных мероприятий, сообщает в понедельник департамент коммуникации украинского МВД.

…министр внутренних дел Украины Арсен Аваков встретился в понедельник с недавно назначенным послом Катара в Украине Гади Аль-Гаджри и обсудил украинско-катарское сотрудничество в сфере гражданской безопасности…

В МВД подчеркивают: "Посол Катара отметил, что его страна планирует воспользоваться опытом Украины в организации общественной безопасности во время проведения масштабных мероприятий вроде Лиги чемпионов, "Евро-2012" или "Евровидения"…» ***(Катар воспользуется опытом Украины в организации общественной безопасности во время масштабных мероприятий // Интерфакс-Украина (https://interfax.com.ua/news/general/533452.html). 24.09.2018).***

***

«Туск призвал ООН помочь в борьбе с вмешательством в выборы через кибератаки по всему миру.

Председатель Европейского совета Дональд Туск в четверг призвал ООН оказать ЕС и другим странам поддержку в противодействии распространению дезинформации и злонамеренным вмешательствам в выборы через киберпространство.

"Европа предприняла рад действий против распространения дезинформации и международной пропаганды, угрожающим демократическим выборам. Анонимность киберпространства используется злоумышленниками для незаконного вмешательства в политические процессы. И это не только проблема Европы. (...) ООН должна помочь бороться с этим феноменом", - заявил Д.Туск, выступая на Генассамблее ООН…» ***(Туск призывает ООН помочь миру в борьбе со вмешательствами в выборы // Телеграф (https://telegraf.com.ua/mir/europa/4533743-tusk-prizyivaet-oon-pomoch-miru-v-borbe-so-vmeshatelstvami-v-vyiboryi.html). 28.09.2018).***

***

Світові тенденції в галузі кібербезпеки

«На недавнем заседании Международного союза электросвязи (МСЭ), проходившем в южноафриканском Дурбане, было опубликовано «Руководство разработке стратегий национальной кибербезопасности» (National Cybersecurity Strategy Guide), которое представляет собой свод рекомендаций государствам по созданию и реализации стратегий национальной кибербезопасности, в том числе механизмов готовности и противостояния кибератакам…

Руководство разработано при содействии различных правительственных и международных организаций, а также представителей частного сектора, включая Содружество телекоммуникационных организаций, Женевский центр политики безопасности, Оксфордский университет, Microsoft, Объединенный центр передовых технологий кибероборонь НАТО и пр.

Документ предназначен для того, чтобы помочь политикам в разработке стратегий, учитывающих ситуацию, культуру и общественные ценности разных стран, для создания надёжных и устойчивых сообществ, которые во многом зависят от информационно-коммуникационных технологий. Старший вице-

президент и главный юрисконсульт Всемирного банка Сэнди Окоро (Sandie Okoro) подчеркнула необходимость разработки такой стратегии для защиты кибербезопасности…» ***(МСЭ рекомендует заняться национальной кибербезопасностью // РосКомСвобода (https://roskomsvoboda.org/41645/). 12.09.2018).***

***

«По оценкам Munich Re, рынок киберстрахования к 2020 году удвоится, обусловленный расширением использования подключенных устройств и связанными рисками. Такое мнение на ежегодной встрече перестраховщиков в Монте-Карло высказал член правления немецкого перестраховщика Торстен Джуворрек (Torsten Jeworrek).

…из выступления представителя Munich Re известно, что расходы на киберстрахование к 2020 году будут оцениваться в $8-9 млрд, что вдвое больше, чем в 2017 году ($3,4-4 млрд)…

Торстен Джуворрек также подчеркнул, что к 2030 году количество подключенных устройств по всему миру увеличится с 27 до 125 миллиардов единиц…» ***(Мировой сектор киберстрахования к 2020 году возрастет вдвое до $9 млрд: Munich Re // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/mirovoy-sektor-kiberstrahovaniya-k-2020-godu-vozrastet-vdvoe-do-9-mlrd-munich-re). 11.09.2018).***

***

Сполучені Штати Америки

«Адміністрація США планує посилити тиск на Китай і розглядає можливість введення санкцій відносно китайських компаній, викритих у крадіжці американської інтелектуальної власності шляхом хакерських атак.

…адміністрація президента США Дональда Трампа має намір скористатися виконавчим указом, підписаним екс-президентом країни Бараком Обамою. Згідно з ним, США мають право ввести серйозні обмежувальні заходи відносно підприємств і фізичних осіб, "залучених у ворожу кіберактивність" по відношенню до Сполучених Штатів…

В такому випадку США також зможуть вилучати або заморожувати активи, що знаходяться на території США або в американських банках, викритих у кібершпіонажі китайських компаній, пише агентство. Адміністрація США також зможе заборонити таким підприємствам Китаю вести бізнес із американськими компаніями…» ***(Самуїл Проскуряков. США планують вводити санкції проти китайських компаній, викритих на кібершпіонажі // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1751096-ssha-planuyut-vvoditi-sanktsiyi-proti-kitayskikh-kompaniy-vikritikh-na-kibershpionazhi). 08.08.2018).***

***

«Палата представителей Конгресса США приняла законопроект, который обязывает главу Белого дома вводить санкции в отношении лиц и организаций, замешанных в киберпреступной деятельности, заявил председатель Комитета по иностранным делам палаты Эд Ройс.

По мнению Ройса, этот законопроект позволит донести «до таких стран, как Иран, Северная Корея и Россия, что США готовы принимать жесткие меры в ответ на кибератаки…

Глава Белого дома может выбрать один или сразу несколько вариантов рестрикций, включая запрет на въезд в США, запрет на импорт и экспорт товаров, оказание финансовой помощи, заморозку финансовых активов.

Глава Комитета по иностранным делам Палата представителей отметил, что законопроект призывает главу Белого дома координировать введение санкций со странами-союзниками, чтобы максимизировать их эффект.

Законопроект также обязывает президента США публиковать список всех, кто попал под санкции в связи с киберпреступлениями, а также регулярно обновлять этот список…» ***(Антон Никитин. Конгресс собрался вводить санкции за киберпреступления // Деловая газета «Взгляд» (https://vz.ru/news/2018/9/5/940592.html). 05.09.2018).***

***

«…Агентство национальной безопасности США огласило результаты шестого ежегодного конкурса на лучшую исследовательскую работу в области кибербезопасности (6th Annual Best Scientific Cybersecurity Paper Competition). Победителем стал совместный доклад специалистов Университета Карнеги-Меллона и Калифорнийского университета в Санта-Барбаре. Работа под названием «How Shall We Play a Game? A Game-theoretical Model for Cyber-warfare Games» («Как нам играть в игру? Теоретическая игровая модель для кибервоенных игр») посвящена применению теории игр в кибервойнах.

Авторы исследования постарались определить «лучшую стратегию по использованию известной уязвимости нулевого дня в рамках кибервойны, где любое действие может раскрыть информацию противнику». Исследователи разработали теоретическую игровую модель и способы быстрого нахождения оптимальных решений проблемы. Данные стратегии помогают пользователям и компьютерным системам принимать решения при выявлении ранее неизвестных уязвимостей. Модель учитывает наступательные и оборонительные действия, а также описывает возможные меры, в том числе атаки с использованием данной уязвимости, устранение уязвимостей в системах, отсрочку решения проблемы или бездействие…» ***(АНБ выбрало лучшую исследовательскую работу по кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/495583.php). 13.09.2018).***

***

«…Пока Министерство внутренней безопасности США надеется на помощь дронов в обеспечении защиты американо-мексиканской границы,

сами данные, собранные беспилотниками, защищены недостаточно и могут быть похищены киберпреступниками или недобросовестными инсайдерами.

Как показала экспертная проверка, информационные системы, используемые Службой таможенного и пограничного контроля США для обмена данными с дронов, находятся под «большой угрозой компрометации со стороны доверенных инсайдеров или внешних источников».

Согласно отчету генерального инспектора Министерства внутренней безопасности, отсутствует непрерывный мониторинг систем, позволяющий эффективно реагировать, сообщать и устранять последствия инцидентов безопасности, а поддержка систем и надзор за подрядчиками осуществляется в недостаточной мере.

Причиной проведения проверки послужил запрос пограничников на использование для охраны границ более «продвинутых» дронов. По результатам аудита управление генерального инспектора пришло к выводу, что в недостаточном обеспечении кибербезопасности IT-систем повинно руководство или отсутствие такового. Соответствующий персонал, инструкции, обучение и экспертиза, необходимые для управления подобными системами, у таможенной службы отсутствуют, заключили эксперты.» ***(Данные мониторинга американо-мексиканской границы находятся под угрозой // SecurityLab.ru (https://www.securitylab.ru/news/495714.php). 27.09.2018)***

***

«В Калифорнии будут законодательно регулировать товары для умного дома

В том случае, если губернатором Калифорнии будет подписан документ, который уже одобрили законодатели штата, то производителям гаджетов для умного дома придется гарантировать максимальный уровень безопасности для всех, без исключения, устройств.

Главная причина — не дать возможность хакерам использовать ту или иную незащищенность в подключенной к интернету вещей системе вашего умного дома.

Жилье, наполненное гаджетами, подключенными к интернету, превращается в большую опасность для приватности. И власти Калифорнии хотят предупредить проблемы, которые могут быть вызваны IoT…» ***(В США примут закон о кибербезопасности умного дома // PaySpaceMagazine «доступно о платежах» (https://psm7.com/internet-veshhej/v-ssha-nachnut-zakonodatelno-regulirovat-tovary-dlya-umnogo-doma.html). 21.09.2018).***

***

«Соцсеть Facebook примет новые меры кибербезопасности в связи с выборами в США…

Согласно новой программе безопасности, кандидаты и их штабы будут помечаться как пользователи с высоким приоритетом. Это позволит быстрее реагировать в случае какой-либо подозрительной активности в соцсети, связанной с их аккаунтами.

До этого Facebook объявил, что заблокирует сотни фейковых профилей и страниц, которые демонстрировали подозрительную активность в течение избирательной кампании 2016 года…» ***(Facebook внедряет новую программу безопасности перед выборами в США // Информационное агентство ЦК, "Эксперт-Центр" (http://expert.org.ua/smi-i-tehnologii/2018/facebook-vnedryaet-novuyu-programmu-bezopasnosti-pered-vyborami-v-ssha). 19.09.2018).***

***

Країни ЄС

«Норвезька поліція почала розслідування у справі про зникнення Ар'єна Кампхьойса — фахівця з кібербезпеки і соратника засновника організації WikiLeaks Джуліана Ассанжа…

Представник поліції заявив, що правоохоронні органи не мають у своєму розпорядженні відомості про те, де може перебувати Кампхьойс.

За даними WikiLeaks, опублікованими в Twitter, 20 серпня чоловік покинув готель в місті Буді. 22 серпня він повинен був вилетіти з міста Тронхейм. "Поїзд між містами їде приблизно 10 годин, можливо, він міг зникнути протягом цього часу в Буді, в поїзді або Тронхеймі", — йдеться в повідомленні…» ***(Олексій Супрун. AFP: поліція Норвегії почала розслідування у справі про зникнення соратника Ассанжа // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1749988-afp-politsiya-norvegiyi-pochala-rozsliduvannya-u-spravi-pro-zniknennya-soratnika-assanzha). 03.09.2018).***

***

«Уряд Німеччини схвалив рішення про створення нової структури з кібербезпеки для посилення захисту країни – Агентства з питань інновацій у сфері кібербезпеки…

Нову організацію спільно очолюють міністри оборони та внутрішніх справ. Агентство отримає бюджет в розмірі 200 мільйонів євро у період між 2019 та 2022 роками. У новому агентстві працюватимуть близько 100 співробітників.

Німецький парламент обговорюватиме пропозицію щодо затвердження роботи агентства найближчим часом. Щойно фінансування буде схвалено, аналітики почнуть свою роботу з наступного року.

Однією з цілей нового агентства є прискорення циклу виробництва технологій кібербезпеки…

Очікується, що завдяки агентству урядові структури володітимуть продуктом для аналізу загроз та можливого віртуального удару у відповідь та не будуть змушені чекати його появи на ринку і купувати.

У створенні відомства Німеччина орієнтується на відповідні державні агенції США та Ізраїлю.» ***(Німеччина створює агентство з питань інновацій у сфері кібербезпеки // Західна інформаційна корпорація (https://zik.ua/news/2018/09/03/nimechchyna_stvoryuie_agentstvo_z_pytan_innovatsiy_u_sferi_kiberbezpeky_1398913). 03.09.2018).***

***

«…Меры предосторожности немецких банков, препринимаемые против хакерских нападений, с во многом нуждаются в улучшении и дополнении. Об этом заявил член правления Федерального банка Германии Йоахим Вуэрмелинг…

По его словам, финансовые институты располагают всеми возможными антихакерскими системами, однако, все в очень разной степени реализации…

Он также отметил, что опасность кибератак на финансовые учреждения высока и будет далее расти…» ***(Федеральный банк Германии заявил о необходимости улучшения системы безопасности банков // LLC "UBT" (https://www.rbc.ua/rus/news/federalnyy-bank-germanii-zayavil-neobhodimosti-1536561658.html). 10.09.2018).***

***

«Студенты Букингемского университета со следующего года получат возможность стать бакалаврами международного шпионажа… британский вуз собирается начать подготовку выпускников по специальности «безопасность, разведка и киберугрозы» в ответ на растущие и меняющиеся требования британских спецслужб к своим будущим сотрудникам.

…на протяжении многих лет обучение в британскую разведку проходило в Кембриджском университете, где к талантливым и родовитым студентам, изучавшим историю и международные отношения, в какой-то момент обращались люди с предложением служить короне. Однако как полагает автор новой университетской программы Джулиан Ричардс, «классическое» шпионское образование в гражданских университетах сегодня дает недостаточно навыков для успешной работы в МИ-6…

Студенты, выбравшие новую специальность, после окончания вуза получат знания не только в области истории дипломатии и нюансах международной политики. Им будут рассказывать о том, как устроена работа разведслужб, и как осуществляется обмен информацией между такими структурами из разных стран. Большое внимание также будет уделяться вопросам кибербезопасности, при чем не только технологическим, но и политическим аспектам проблемы хакеров и борьбы с ними.» ***(В британском университете появится программа подготовки разведчиков // Капитал (https://www.capital.ua/ru/news/119082-v-britanskom-universitete-poyavitsya-programma-podgotovki-razvedchikov). 27.09.2018).***

***

Китай

«В Пекине открылся второй интернет-суд на территории Китая…

Этот вид суда не предусматривает личного присутствия истца и ответчика. Все судебные процедуры, начиная с подачи иска и возбуждения дела, можно осуществить на сайте инстанции. Слушания и объявление приговора также будут проходить онлайн посредством видеотрансляции в режиме реального времени.

В суде будут рассматриваться дела, связанные с интернетом, например, случаями мошенничества в онлайн-торговле, спорах о заключенных онлайн долговых контрактах, нарушения авторских прав и т.д.…» ***(Второй на территории Китая интернет-суд заработал в Пекине // "Багнет" (http://www.bagnet.org/news/tech/375753/vtoroy-na-territorii-kitaya-internet-sud-zarabotal-v-pekine). 10.09.2018).***

***

«Влада КНР за три місяці заблокувала більше 4 тис. "шкідливих" веб-сайтів і акаунтів, заявили у Національному управлінні протидії нелегальним і порнографічним публікаціям…

Під блокування потрапили облікові записи та сайти, запідозрені в шахрайстві, поширенні порнографії, вербування в релігійні організації і навіть у "поширенні чуток". Компанія з виявлення "шкідливого контенту" стартувала в травні. За цей час було виявлено 120 порушень, приписи про їх усунення отримали 230 фірм. Зокрема, була закрита стрімінговая платформа, що налічувала понад 3 млн користувачів. Вона поширювала порнографію і базувалася на території Камбоджі.

В кінці серпні китайська влада запустили в національному сегменті інтернету платформу Ріуао для "спростування чуток". Вона контролюється 27 відомствами і відстежує підозрілу інформацію в соціальних мережах і месенджерах. Це сталося паралельно з початком розслідування щодо платформ на предмет порушення нового закону про кібербезпеку зокрема, розміщенні контенту, що містить "тероризм, фальшиві чутки і порнографію". Була також обмежена видача ліцензій на онлайн-ігри. Це призвело до втрати акціями найбільших соцмереж Китаю Momo, Weibo і YY від 11% до 17% вартості…» ***(Самуїл Проскуряков. У Китаї заблокували 4 тисячі "шкідливих" сайтів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1753646-u-kitayi-vlada-zablokuvala-4-tisyachi-shkidlivikh-saytiv). 23.09.2018).***

***

Російська Федерація та країни ЄАЕС

«…Проведя небольшой мониторинг Сети на предмет наказаний за нарушение ст.138.1, РосКомСвобода обнаружила только за этот месяц несколько подобных случаев, произошедших в самых разных регионах России.

В начале сентября текущего года стало известно, что Следственный комитет возбудил уголовное дело в отношении 57-летнего жителя поселка Озерновский Усть-Большерецкого района Камчатки.

«По версии следствия, в июне 2018 года подозреваемый посредством сети Интернет приобрел специальное техническое средство – авторучку-видеорегистратор китайского производства со встроенной фото-видео камерой и микрофоном, предназначенное для негласного получения информации», –

сообщила официальный представитель краевого управления СКР Елена Матафонова…

В середине сентября УФСБ России по Белгородской области сообщила о пресечении «незаконной поставки из Московского региона специальных технических средств, предназначенных для негласного получения информации»…

Молодой человек был задержан силовиками при продаже GPS-трекера, оснащённого функцией негласного контроля акустической информации. Экспертиза признала устройство специальным техническим средством, предназначенным для негласного получения информации.

Октябрьский районный суд Белгорода признал жителя области виновным по ст. 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации». Ему назначено наказание в виде лишения свободы на 2 года 3 месяца и штрафа в размере 30 тысяч рублей.

В Сочи за незаконную продажу прослушивающих устройств был оштрафован 35-летний житель Кубани. Как сообщает пресс-служба ПУ ФСБ России по Краснодарскому краю, мужчину задержали пограничники весной прошлого года в Сочи. Он решил заняться продажей подслушивающих устройств, несмотря на то, что оборот подобных технических средств в России запрещен.

Мужчина покупал устройство с портативным GPS-микрофоном на специализированном сайте в интернете, а затем перепродавал его с наценкой. Задержали его в ходе «проверочной закупки». Прослушивающее устройство изъяли. Экспертиза установила, что оно предназначено для негласного получения акустической информации и дистанционного слежения.

В отношении подозреваемого было возбуждено уголовное дело по ст. 138.1 УК РФ. Во время следствия мужчина, игнорируя подписку о невыезде, пытался скрыться от следственных органов. В Сочи суд признал его виновным и назначил штраф в размере 50 тысяч рублей. Приговор вступил в законную силу.

ГУ МВД по Красноярскому краю сообщило о задержании молодого человека, выложившего на сайте «Авито» объявление о продаже скрытой камеры наблюдения, находящейся в противопожарном датчике.

Отдел «К» вместе с УФСБ зафиксировали факт продажи камеры и задержали 22-летнего продавца — тот передал органам еще девять таких устройств.

Эксперты признали, что изъятая техника относится к категории специальных технических средств, предназначенных для негласного получения информации. Молодой человек рассказал стражам порядка, что он закупил камеры через интернет для дальнейшей перепродажи.

Возбуждено дело за незаконный оборот спецприборов, по ст. 138.1 УК РФ продавцу грозит до 4 лет лишения свободы.

На днях Советский районный суд города Махачкалы с участием прокуратуры Республики Дагестан (РД) вынес в отношении жителя дагестанской столицы приговор. Осужденный признан виновным за незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ)….

Как установили в судебном заседании, в прошлом году в сети «Интернет» злоумышленник оформил заказ на приобретение часов (наручных) с СИМ-картой с трекером, они относятся к категории специальных техсредств, предназначенных для негласного получения акустической информации а также негласного контроля за перемещением транспортных средств и других объектов. К свободному распространению на территории РФ такие спецсредства запрещены.

Мужчина получил указанное техническое средство, оплатив 3,5 тыс. неустановленному следствием продавцу. Приобретенный товар злоумышленник сбыл условному покупателю, после чего он был задержан сотрудниками правоохранительных органов. Осужденному назначили наказание в виде штрафа в размере 100 тыс. рублей.

Как уже говорилось выше, география вынесенных приговоров и возбуждаемых дел очень обширна. То же самое можно сказать и о суровости наказаний, которое варьируется от штрафов в десятки тысяч рублей до реальных тюремных сроков. А пресс-релизы составлены так, что пользователи могут отнести к запрещенным гаджетам слишком широкий спектр устройств…» ***(Россиян продолжают наказывать за «шпионские» гаджеты // РосКомСвобода (https://roskomsvoboda.org/41924/). 21.09.2018).***

***

«Под эгидой Национальной технологической инициативы ведется разработка абсолютно защищенных отечественных компьютеров и программного обеспечения…

Разработкой компьютеров и программного обеспечения займутся математики и инженеры бывших оборонных предприятий и институтов Москвы и Санкт-Петербурга…

Под эгидой НТИ решено создать так называемую доверенную вычислительную среду — линейку компьютеров, сетевое оборудование и программное обеспечение, — которой можно было бы полностью доверять с точки зрения всех видов защищенности.

…для достижения этой цели среда должна быть основана исключительно на отечественных разработках в области компьютерного оборудования и программного обеспечения. В частности, базовым процессором новой вычислительной системы станет отечественный «Эльбрус». ***(SafeNet обещает создать абсолютно защищенную вычислительную среду // «Открытые системы» (https://www.computerworld.ru/news/V-Rossii-sozdadut-absolyutno-zaschischennuyu-vychislitelnuyu-sredu). 24.09.2018).***

***

«ФСБ РФ создала Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который будет осуществлять противодействие кибератакам на критическую инфраструктуру…

Новая структура будет, в частности, заниматься координацией по вопросам обнаружения, предупреждения и ликвидации последствий кибератак. Также в её задачи входит обмен информацией между профильными ведомствами, а также с

зарубежными коллегами, анализ прошедших компьютерных атак и выработка методов противодействия им.

В документе указывается, что центр имеет право отказаться передать информацию органам международной организации или другого государства, если это угрожает безопасности России.

НКЦКИ возглавляет директор, который совмещает этот пост с должностью замглавы научно-технической службы — начальника Центра защиты информации и спецсвязи ФСБ.» ***(Алина Пятигорская. В России создали госорган по борьбе с кібератаками // «Парламентская газета» (https://www.pnp.ru/politics/v-rossii-sozdali-gosorgan-po-borbe-s-kiberatakami.html). 10.09.2018).***

***

«…Минкомсвязь предлагает законодательно обеспечить предустановку отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории РФ, начиная с 1 августа 2020 года, следует из внесенного в правительство паспорта нацпроекта «Цифровая экономика». Введение этой нормы следует обосновать «целью обеспечения национальной безопасности», говорится в отзыве Минэкономики, 11 сентября направленном в Минкомсвязь и аппарат правительства: это позволит обосновать отступление от принципов ВТО…» ***(Кристина Жукова, Владислав Новый, Денис Скоробогатько. Министерства подхватили антивирус. Власти обсуждают предустановку российского софта на все импортируемые компьютеры // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3745820). 20.09.2018).***

***

Інші країни

«МИД Северной Кореи отрицает обвинения США в организации кибератак. В КНДР заявили. что подобные инсинуации могут подорвать диалог между руководством обеих стран.

«Фарс с обвинениями со стороны США не является ничем иным кроме как злостной клеветой и очередной кампанией по дискредитации, полной лжи и фальсификаций, и направленной против КНДР»,— приводит «Интерфакс» слова представителя северокорейского МИДа.

Дипломаты КНДР добавили, что «США вводят в заблуждение общественное мнение, утверждая, что правительство КНДР стоит за преступлением, связывая несуществующего "преступника" и его так называемые "киберпреступления" с госорганами страны».

МИД Северной Кореи отметил, что власти КНДР «давно выбрали курс, направленный против всех видов кибератак, и за полное обеспечение кибербезопасности, и предпринимает все шаги для ее осуществления»…» ***(КНДР отрицает обвинения США в кібератаках // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3743562). 14.09.2018).***

***

«Критично важлива інфраструктура Великої Британії зазнала серії хакерських атак із боку Головного управління (колишнього Головного розвідувального управління, ГРУ) Генштабу Збройних сил РФ.

...цілями російської спецслужби нібито стали британські енергетичні мережі, телекомунікаційні системи та медійні організації. Так, глава Національного центру кібербезпеки (NCSC) Кіран Мартін у минулому році стверджував, що з моменту заснування цієї організації у 2016 році Росія нібито неодноразово здійснювала кібератаки на інфраструктуру Сполученого Королівства. В цілому співробітники NCSC протягом року (в період 2016-2017 років) відреагували на більш ніж 600 «серйозних інцидентів»...» ***(Самуїл Проскуряков. The Daily Telegraph: Британська влада запідозрила ГРУ в хакерських атаках на інфраструктуру країни // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1751189-the-daily-telegraph-britanska-vlada-zapidozrila-gru-v-khakerskikh-atakakh-na-infrastrukturu-krayini). 09.09.2018).***

***

«Палата представників конгресу США одноголосно прийняла законопроект "Про кіберстримування і реагування" на кіберзагрози, згідно з яким Вашингтон повинен буде вводити санкції щодо осіб, організацій та іноземних держав за кіберзлочини проти США…

Такий крок покликаний захистити американські вибори і найважливіші об'єкти інфраструктури країни від "спонсорованої іноземними державами умисної кіберактивності" і створить основу для стримування і реагування на майбутні кібератаки проти Сполучених Штатів.

Американське керівництво неодноразово заявляло, що Росія, Китай, Іран і Північна Корея є найбільшими кіберзагрозами для Сполучених Штатів.

У законопроекті йдеться про атаки вірусу WannaCry і шкідливого ПО NotPetya. Останню атаку, як зазначається в документі, "провела Росія". Вона, за оцінкою американських законодавців, стала найбільш руйнівною кібероперацією в історії і "завдала збитків на мільярди доларів Україні, Європі, Азії та Америці".

Законопроект у разі його повного прийняття вимагатиме від президента США визначати "Ризикованих виконавців кіберзагроз". Під це визначення може потрапити "будь-яка іноземна фізична особа або організація, відповідальні за спонсоровану іншою державою кіберактивність, яка представляє значну загрозу нацбезпеці, зовнішній політиці, економіці та фінансовій стабільності США".

Стосовно цих суб'єктів американського лідера законопроект також зобов'яже вводити певні санкції. Обмеження при цьому, згідно з документом, можуть залежати від скасування США надання якій-небудь країні гуманітарної допомоги і заборони на експорт та імпорт товарів і послуг до заборони видачі віз і в'їзду на територію США, а також обмежень при продовженні страхування кредитів.

Також ініціатива передбачає, що президент може відмовити у накладенні санкцій у кожному конкретному випадку на строк не більше одного року. Зовсім відмовитися від обмежень американський лідер зможе тільки коли надасть у відповідні комітети конгресу США письмові підтвердження про те, що рішення не вводити санкції у цьому випадку може мати важливе значення для економічних чи національних інтересів Сполучених Штатів, або ж така відмова стане "важливою гуманітарною метою".

Тепер прийнятий палатою представників законопроект буде переданий на затвердження Сенату. У разі затвердження його має підписати президент.» ***(У США схвалили законопроект про санкції за кіберзлочини // Espreso.tv (https://espreso.tv/news/2018/09/06/u_ssha_skhvalyly_zakonoproekt_pro_sankciyi_za_kiberzlochyny). 06.09.2018).***

***

«…Дональд Трамп нещодавно підписав Закон про національну оборону на 2019 рік (2019 National Defense Authorization Act), який передбачає видатки на військові потреби, а також повноваження осіб і організацій з управління обороною. Значна частина цього документа присвячена кібербезпеці. Для посилення безпеки США у "світовому павутинні" і формування стратегії поведінки Міноборони в цифровому світі вирішено створити Комісію з кіберпростору "Солярій" (Cyberspace Solarium Commission).

До комісії повинні увійти заступники голів національної розвідки, Міністерств оборони і внутрішньої безпеки, плюс ще десять людей, які обираються Конгресом. До повноважень комісії входить розгляд інцидентів, пов'язаних з кібератаками як на урядові установи, так і приватний бізнес. В якості потенційних супротивників у США розцінюють Китай, Росію, Іран, Північну Корею, а також різні злочинні і терористичні групи.

У даний час Конгрес доручив Комісії оцінити стратегії стримування та відбиття атак противника в кіберпросторі для захисту національної безпеки і економіки США, обсяг якої перевищує $ 19 трильйонів. Згідно з висновками, які містяться у нещодавньому дослідженні на замовлення Пентагону, Сполучені Штати "на роки відстають від своїх суперників в кіберпросторі", стратегія США "гальмує і обмежує сама себе", не маючи узгодженого підходу до стримування атак хакерів. Комісія "Солярій" саме і повинна запропонувати дієві шляхи просування вперед, щоб США перестали "пасти задніх".

У Вашингтоні не заперечують, що через розвиток технологій доведеться переглянути свої стратегії в галузі інформаційної безпеки, так само як зростання влучності ракет під час "холодної війни" призвела до переходу від стратегії контрнаступу до концепції протидії, від засипання "сліпими" бомбами населених пунктів - до ударів інтелектуальними ракетами по центрах військового управління.

У Міноборони США визнають, що на сьогодні держава не має монополії ані на знаряддя війни, ані на інструменти ведення кібервійни. Військові, які захищають Сполучені Штати і їхні інтереси в Мережі, перебувають у майже цілковитій залежності від приватних компаній - постачальників технологічних рішень у галузі оборони. Тобто державі необхідна тісна зв'язка з приватним сектором, інакше вона

ризикує відстати від прогресу.» ***(Воювати з хакерами і захищати кіберпростір США Трамп доручив Солярію - The National Interest // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/voyuvati-z-hakerami-i-zahischati-kiberprostir-ssha-tramp-doruchiv-solyariyu-the-national-interest-287329_.html). 03.09.2018).***

***

«…Американский президент Дональд Трамп подписал новую стратегию кибербезопасности, отменившую существовавшие при его предшественнике Бараке Обаме ограничения на действия наступательного характера. А в Великобритании в ближайшее время, как ожидается, объявят о создании специального киберподразделения: оно также будет заниматься не только отражением атак, в организации которых подозревают Россию, Иран, КНДР и Китай.…

Среди упомянутых в новой стратегии шагов — улучшение координации между ведомствами, повышение степени защиты информационных систем, поддержка технологий следующего поколения (Белый дом обещает сотрудничать с развивающими 5G компаниями и проанализировать возможности использования искусственного интеллекта и квантовых компьютеров), обучение специалистов в области кибербезопасности. Действия по уменьшению рисков будут предприниматься в первую очередь в семи ключевых сферах: национальная безопасность, энергетика, финансы, здравоохранение, коммуникации, информационные технологии и транспорт.

Новая стратегия… отменяет наложенные администрацией Барака Обамы в 2013 году ограничения на кибероперации наступательного характера…

В новой американской стратегии также описаны планы развития Инициативы по сдерживанию в киберпространстве, то есть создания коалиции союзников, которые будут совместно отвечать на киберугрозы и наказывать тех, от кого они исходят. Определенная координация есть уже сейчас. Например, одним из своих приоритетов кибербезопасность называет НАТО: на саммите летом этого года было объявлено о создании Центра кибероперацій альянса, который будет координировать действия национальных сил. Сотрудничество (в частности, в виде обмена разведданными) ведется и на двустороннем уровне.

В числе главных союзников США на этом направлении — Великобритания…». ***(Павел Тарасенко, Елена Черненко. Наступление по всем компам Политика США и их союзников в киберпространстве больше не связана никакими ограничениями // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3750423). 22.09.2018).***

***

«…Руководители американских разведывательных и оборонных ведомств предупреждают о растущей угрозе кибератак накануне ноябрьских промежуточных выборов в Конгресс США. При этом опасность исходит не только от России, но и еще от целого ряда стран и негосударственных групп…

«Киберугрозы для США не ограничиваются одной лишь сферой политических выборов. Многие часто забывают об этом», – сказал Дэн Коутс,

директор Национальной разведки США, выступая на конференции по вопросам безопасности, которая прошла в Вашингтоне 4 сентября. По его словам, разработка новых инструментов для проведения кибератак и тот факт, что хакеры могут довольно легко справиться с любыми защитными преградами в киберпространстве, способствуют росту риска новых нападений со «стратегическими последствиями».

Коутс добавил, что попытки «онлайн-воздействия» со стороны иностранных государств все чаще фиксируются спецслужбами по всему миру…

На конференции в Вашингтоне глава Национальной разведки США сказал, что он «крайне обеспокоен» угрозами, которые исходят от «нескольких стран» в отношении промежуточных выборов, выборов президента США в 2020 году и последующих кампаний. При этом глава разведывательного ведомства не уточнил, какие именно страны он имеет в виду.

…Представители силовых ведомств считают, что, помимо России, основные киберугрозы для США сейчас исходят от Китая, Ирана и Северной Кореи…

По словам Джона Руда, замминистра обороны США по вопросам политики, сейчас страна ежедневно подвергается подобным атакам. Руд обеспокоен возможностью того, что «кто-то попытается объединить кибероружие с более традиционными видами атак» для нападения на Соединенные Штаты…

Другие американские чиновники обеспокоены не столько перспективой крупномасштабных кибернападений, сколько ростом числа мелких инцидентов. Об этом во время конференции 4 сентября заявил Джордж Барнс, замдиректора Агентства национальной безопасности (АНБ) США.

По мнению Барнса, проблема в том, что власти «уделяют основное внимание крупным атакам, в то время как постоянно растет количество небольших инцидентов». Он уверен, что именно эти «мелкие проблемы» привели к росту воровства интеллектуальной собственности у американских бизнесменов.

Часть проблемы, по мнению Барнса и других чиновников – недостаточно тесное взаимодействие между властями и бизнесом в США в вопросах кибербезопасности. Это ведет к росту уязвимости как самого государства, так и отдельных компаний…». ***(Джефф Зельдин. Власти США обеспокоены растущей угрозой иностранных кибератак // «Голос Америки» (https://www.golos-ameriki.ru/a/cyberattacks-us-razvedka-ugroza-russkie-hakery/4558964.html). 05.09.2018).***

***

«Швейцарские прокуроры подозревают, что «российские шпионы», которые были арестованы весной в Гааге и высланы из страны, могли быть замешаны в кибератаках против Всемирного антидопингового агентства (WADA)…

Ранее швейцарская газета Tages Azeiger написала о том, что два российских шпиона пытались получить информацию о работе лаборатории Шпиц — Швейцарского института защиты от ядерных, биологических и химических угроз, подчиняющегося Министерству обороны Швейцарии. Отмечалось, что у агентов было «шпионское оборудование» для взлома компьютерной сети в лаборатории…» ***(Прокуратура Швейцарии подозревает «российских шпионов» в кибератаках***

на WADA // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3743761). 15.09.2018).

***

«Российское посольство в Швейцарии назвало «очередной сказкой» ранее появившиеся в газете NRC Handelsblad сообщения об атаке российских хакеров на Всемирное антидопинговое агентство (WADA). Дипломатическое ведомство указывает, что публикация появилась сразу после того, как комитет WADA рекомендовал восстановить в правах Российское антидопинговое агентство (РУСАДА).

Посольство также опровергло вызов посла России в МИД страны и вручение ему ноты протеста в связи с деятельностью предполагаемых «российских шпионов», о чем накануне сообщило информагентство ATS…» ***(Посольство России считает «сказкой» сообщения о причастности российских агентов к атакам на WADA // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3743797). 15.09.2018).***

***

«Генеральный секретарь НАТО Йенс Столтенберг заявил, что альянс может применить пятую статью устава в случае проведения кибератак со стороны России.

По словам Столтенберга, НАТО не намерено предупреждать заранее о применении пятой статьи, чтобы «не давать это преимущество никакому потенциальному противнику»…

По его словам, применение статьи 5 будет зависеть от характера кибератаки против НАТО и не будет автоматическим.

В то же время он сообщил, что в альянсе будут созданы наступательные киберсредства, которые якобы будут использоваться только в соответствии с международным правом.

Накануне НАТО запустило исследование методов разведки в интернете.» ***(Антон Никитин. НАТО пригрозило коллективным ответом в случае кибератак со стороны России // ООО «Деловая газета «Взгляд» (https://vz.ru/news/2018/9/17/942059.html). 17.09.2018).***

***

«Бельгийская разведка наняла сотрудника на должность главы рабочей группы, следящей за «российской киберугрозой».

Глава бельгийской разведки Клод ван де Ворде отметил, что речь не идет исключительно о деятельность Москвы – под наблюдением будет и активность Китая, передает Life со ссылкой на доклад, опубликованный на сайте парламента Бельгии.

Слушания по этому вопросу были проведены еще в июне, однако документ опубликовали только сейчас…» ***(Наталья Ануфриева. В Бельгии создали должность следящего за «российской киберугрозой» // ООО «Деловая газета «Взгляд» (https://vz.ru/news/2018/9/15/941898.html). 15.09.2018).***

***

«Минобороны и Центр правительственной связи Великобритании запланировали создать наступательное киберподразделение, деятельность которого будет направлена против России…

В него войдут 2 тыс. человек. Подразделение должно расширить британские возможности для ведения войны в киберпространстве. Ожидается, что британский наступательный потенциал в данной сфере вырастет в четыре раза…

Лондон намерен потратить на создание киберподразделения не менее 250 млн фунтов стерлингов (331 млн долларов)…» ***(Антон Антонов. Британия собралась создать наступательное киберподразделение против России // ООО «Деловая газета «Взгляд» (https://vz.ru/news/2018/9/21/942723.html). 21.09.2018).***

***

«…Продолжающиеся вокруг шифрования, конфиденциальности, приватности дебаты в плане использования современных технологий преступниками продолжились с новой силой после опубликования альянсом «Пять глаз» (разведывательный альянс, в который входят Австралия, Канада, Новая Зеландия, США и Великобритания) достаточно претенциозного постановления.

…страсти разыгрались снова из-за ультиматума, предъявленного альянсом «Пять глаз» (Five Eyes) технологическим компаниям, прозвучавшем фактически в такой формулировке: «Дайте нам доступ к зашифрованным данным и устройствам, в противном случае мы вас заставим».

На прошедшей встрече Five Country Ministerial (FCM) представители правительств стран-участниц альянса «Пять глаз» обсудили будущее кибербезопасности и нацбезопасности, а также растущую угрозу терроризма в киберпространстве. В ходе встречи был подготовлен ряд документов, в том числе касательно шифрования данных. Согласно заявлению «О принципах доступа к доказательствам и шифрованию», «конфиденциальность не является абсолютной», а ответственность за обеспечение доступа к «законно полученным данным» лежит как на правительственных организациях, так и на технологических компаниях.

…То есть, все, начиная от производителей электроники наподобие Apple и Samsung и заканчивая сервисами наподобие Facebook и WhatsApp, должны оказывать «помощь» спецслужбам.

«Если правительственным службам по-прежнему будут препятствовать в законном доступе к информации, необходимой для защиты граждан наших стран, мы можем применять технологические, принудительные, законодательные или

другие меры для получения законного доступа», – указано в постановлении.» ***(Разведальянс «Пять глаз» потребовал от IT-компаний отказаться от шифрования // РосКомСвобода (https://roskomsvoboda.org/41398/). 03.09.2018).***

***

«…Базу данных пользователей Veeam, насчитывающую порядка 445 млн записей и размером около 200 Гбайт нашел в сети специалист по компьютерной безопасности Боб Дьяченко. В базе содержалась маркетинговая информация о потенциальных клиентах, в том числе их имена и адреса электронной почты.

Veeam занимается средствами резервного копирования и восстановления данных. В компании утверждают, что как только о проблеме стало известно, доступ к базе данных быстро закрыли. Ведется расследование и принимаются меры, нацеленные на исключение повторения подобных случаев. Тем не менее, доступ к базе в течение какого-то времени действительно был открыт. Это произошло из-за ошибочных действий сотрудников компании, говорится в заявлении Veeam.» ***(В Veeam признали утечку данных о сотнях миллионах потенциальных клиентов // «Открытые системы» (https://www.computerworld.ru/news/V-Veeam-priznali-utechku-dannyh-o-sotnyah-millionah-potentsialnyh-klientov). 19.09.2018).***

***

«Европейский суд по правам человека постановил, что британская программа массовой киберслежки в ее нынешнем виде нарушает неприкосновенность частной жизни и свободу слова. ЕСПЧ не сомневается в необходимости существования данной системы, однако указывает, что она должна реализовываться при гарантиях того, что невинные люди не окажутся объектами наблюдения.

Суд признал, что британские разведслужбы добросовестно относятся к обязанностям и не злоупотребляют полномочиями. В то же время он обнаружил, что спецслужбы осуществляют свою деятельность без независимого надзора.

Подавляющим большинством голосов — шесть против одного — суд счел, что программа массового электронного слежения, проводившаяся британскими спецслужбами, нарушает ст. 8 конвенции, гарантирующую право на уважение частной жизни и переписки, и ст. 10, гарантирующую право на свободу слова.

Британские правозащитники, подавшие в суд на спецслужбы, не выдвигали требований по выплате каких-либо штрафов и компенсаций, кроме требования компенсации их судебных издержек, которое было удовлетворено.

Дело начало рассматриваться еще в 2013 году после того, как британские правозащитные организации подали в ЕСПЧ по результатам информации, обнародованной Эдвардом Сноуденом. Согласно полученным данным, британский Центр правительственной связи собирает сведения из перехватов телефонных разговоров и интернет-трафика, используя специальные компьютерные программы.» ***(ЕСПЧ: британский закон о массовой киберслежке посягает на права человека // РосКомСвобода (https://roskomsvoboda.org/41677/). 13.09.2018).***

***

«Експерти у сфері кібербезпеки нещодавно дізналися про зміни в політиці браузера Chrome, які погіршують приватність. Як виявилося, Google без гучного дебюту зробила так, що коли юзер входить в один з її сервісів, наприклад, Gmail, веб-переглядач Chrome автоматично починає входити в аккаунт користувача без його згоди.

…Як виявилося, при використанні Chrome і завантаженому акаунті Google збирати особисті дані та історію веб-серфінгу. Пошуковик впевнений, що це позбавить користувачів від необхідності вводити логін і пароль в сервісах Google. Проте, користувачі не хочуть використовувати всі сервіси Google.

Chrome шпигує за користувачами майже відразу після свого випуску. При цьому на Android цей браузер робить це в 50 разів частіше, ніж на iPhone. До речі, і в iPhone далеко не ідеальна система захисту персональної інформації користувачів. Саме з-за цього величезна кількість користувачів перейшли на браузер Firefox, який здатний навіть приховати місцезнаходження користувачів в мережі. В середньому у фоновому режимі Chrome за 24 години з'єднується з серверами Google 40 разів на годину. В активному режимі Chrome на Android пересилає до 4,4 МБ в день, що в 6 разів більше того, що відправляє iPhone до Google.

Аналітики повідомили, що Google збирає інформацію про користувачів в 10 разів більше, ніж Apple. Зазначимо, що яблучна компанія теж вплуталася в скандали зі стеженням за користувачами. Однак Apple повідомила, що це потрібно тільки для знищення спаму, який тільки набирає обертів…» ***(Chrome краде інформацію користувачів для Google // znaj.ua (https://znaj.ua/techno/175868-chrome-krade-informaciyu-koristuvachiv-dlya-google). 25.09.2018).***

***

«Uber тепер буде інформувати користувачів про можливий витік даних Компанія Uber виплатить США і федеральному округу Колумбія 148 млн доларів за те, що протягом року приховувала витік даних водіїв і клієнтів… Також Uber тепер буде інформувати користувачів про можливий витік даних. Крім того, компанія повинна прийняти заходи для захисту інформації… компанія повинна буде сформувати політику щодо забезпечення безпеки всіх даних, які збирає про своїх клієнтів. В документі повинні бути враховані потенційні ризики та запропоновані заходи захисту від кібератак.» ***(Uber заплатить рекордні $148 млн за витік даних користувачів Повний текст читайте // "Українські медійні системи" (тут: https://glavcom.ua/world/observe/uber-zaplatit-rekordni-148-mln-za-vitik-danih-koristuvachiv-531323.html). 27.09.2018).***

***

«Европейское агентство кибербезопасности и Управление защиты данных должны провести аудит компании Facebook.

Соответствующее положение предусмотрено в проекте резолюции Европарламента, которая касается незаконного использования данных пользователей…

Резолюцию разработал председатель комитета ЕП по гражданским свободам Клод Мораес в ответ на скандал с передачей персональных данных пользователей Facebook компании Cambridge Analytica…

Комитет намерен принять резолюцию 10 октября и передать ее на рассмотрение парламента в конце октября…

Еврокомиссия грозит Facebook санкциями в случае невыполнения до конца года условий предоставления услуг, которые могут ввести в заблуждение…» ***(В ЕС готовят аудит Facebook // Європейская правда (https://www.eurointegration.com.ua/rus/news/2018/09/27/7087473/). 27.09.2018)***

***

Кіберзлочинність та кібертероризм

«В Единый день голосования инфраструктура «Ростелекома» подверглась кибератакам, сообщил вице-президент компании Артемий Прокопенко в ЦИК России…

Как заявил вице-президент «Ростелекома», «это связано не только с тем, что масштабы намного меньше, но и по сравнению с президентскими выборами атаки не такие несерьезные».

Службы безопасности «Ростелекома», в частности, отразили попытки «анализа структуры портала»…» ***(Антон Антонов. Хакеры атаковали «Ростелеком» в день виборов // Деловая газета «Взгляд» (https://vz.ru/news/2018/9/9/941084.html). 09.09.2018).***

***

«Александр Петров и Руслан Боширов, которых британское правительство обвиняет в отравлении бывшего разведчика Сергея Скрипаля и его дочери Юлии в Солсбери, могли пересечь границу с помощью «российских киберэкспертов».

…предположительно, злоумышленники взломали систему безопасности аэропорта Хитроу, предоставив двум россиянам возможность пройти паспортный контроль и покинуть Великобританию.

…По мнению эксперта в области кибербезопасности Хэмиша де Бретгона Гордона (Hamish de Bretton Gordon), существует «высокая доля вероятности», что киберпреступники вмешались в работу систем Пограничной службы, чтобы отвести подозрения от россиян…» ***(«Российских киберэкспертов» заподозрили в помощи подозреваемым в отравлении Скрипалей // Goodnews.ua (http://goodnews.ua/technologies/rossijskix-kiberekspertov-zapodozrili-v-pomoshhi-podozrevaemym-v-otravlenii-skripalej/). 10.09.2018).***

***

«Ущерб мировой экономике от преступлений в сфере информационно-коммуникационных технологий (ИКТ) в 2019 году может составить $2 трлн, заявил директор департамента по вопросам новых вызовов и угроз МИД России

Илья Рогачев. Он выступил в Вене на семинаре G-77 (группа стран Латинской Америки и островных стран Карибского бассейна), посвященном предупреждению и борьбе с киберпреступностью…

По его словам, в результате ущерб от киберпреступности превысит «совокупный доход от интернета, что может привести к полному отказу пользователей от глобальной сети, которая прекратит существование в нынешнем виде»…» ***(МИД: хакеры в 2019 году могут нанести мировой экономике $2 трлн ущерба // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3738399). 11.09.2018).***

***

«Банкам и страховым компаниям в 2018 году удалось предотвратить 81% кибератак, что лучше прошлогоднего результата в 66%. Такие данные приводятся в исследовании Accenture, составленном на основе опроса более 800 профессионалов в области корпоративной ИТ-безопасности…

83% опрошенных считают новые технологии важными для обеспечения безопасности их компаний. В исследовании также говорится, что 69% кибератак на финансовый сектор обнаруживаются сами сотрудниками компаний.

Примерно половина (47%) угроз выявляется в течение одного-семи дней, а 11% — менее чем за сутки. 33% атак удается обнаруживать за одну-четыре недели, а 9% нападений хакеров вскрывается только спустя не меньше месяца…» Ф***инансовые компании стали лучше противостоять кібератакам // Goodnews.ua (http://goodnews.ua/technologies/finansovye-kompanii-stali-luchshe-protivostoyat-kiberatakam/). 26.09.2018).***

***

«Tesco Bank возможно заплатит штраф в £30 млн за то, что не смог предотвратить кибертатаки

В 2016 году тысячи клиентов британского розничного банка Tesco Bank пострадали от масштабной кибератаки. Мошенники украли деньги более чем с 40 000 счетов. В результате, система Tesco была недоступна два дня и клиенты не могли проводить финансовые операции…

Если FCA обнаружат в системе банка слабые места и недостатки, которые способствовали нарушениям, то Tesco Bank заплатит штраф в несколько раз больше, чем сумма возмещения пострадавшим клиентам…» ***(Британский банк заплатит штраф за нарушение кибербезопасности // PaySpaceMagazine «доступно о платежах» (https://psm7.com/bank/tesco-bank-zaplatit-shtraf-za-narushenie-kiberbezopasnosti.html). 25.09.2018).***

***

«Почти все правительственные сайты Индии оказались заражены вредоносными программами, использующими мощности компьютеров посетителей, чтобы добывать криптовалюту с помощью скрипта CoinHive…

Новое исследование аналитиков по кибербезопасности показывает, что правительственные сайты, доверие к которым весьма высоко, подверглись веб-

инжектам (внедрение кода), в частности одной из последних была заражена страница администрации штата Андхра-Прадеш.

Эксперты определили, что зараженные сайты являются одними из наиболее посещаемых ресурсов в стране. Правительство Индии подтвердило, что атака действительно произошла, однако пока устранить проблему не удалось. Объемы намайненных на правительственных сайтах токенов также пока не раскрываются…

Наряду с правительственными доменами CoinHive были заражены еще 119 индийских сайтов… особый интерес для хакеров представляют сайты незаконной потоковой трансляции видео, так как пока пользователь смотрит кино или сериал, скрипт имеет возможность по полной нагрузить процессор машины.

Скрытый майнинг приносит злоумышленникам заметную прибыль. Только месяц назад исследователи из RWTH Aachen University, Германия, подсчитали, что скрипт CoinHive, заразивший сайты по всему миру, майнит более $250 тыс. в месяц в Monero…

Хотя CoinHive и не единственное майнинг-расширение для браузера, было обнаружено, что оно имеет самую большую долю использования — более 75% использования в браузерах…» ***(Хакеры тайно майнят криптовалюту на правительственных сайтах // Goodnews.ua (http://goodnews.ua/technologies/xakery-tajno-majnyat-kriptovalyutu-na-pravitelstvennyx-sajtax/). 24.09.2018).***

***

Діяльність хакерів та хакерські угруповування

«Мережа авіаперевізника British Airways постраждала від хакерського злому. Аферисти здійснили атаку і протягом двох тижнів, з 21 серпня по 5 вересня 2018 року, викрадали дані про кредитні картки клієнтів компанії та іншу інформацію, яка зберігалася на серверах BA. Постраждавших від такого злому близько 380 тис. осіб. Перевізник повідомив цю інформацію в п'ятницю, 7 вересня, принісши вибачення клієнтам. Також в BA пообіцяли відшкодувати всі фінансові втрати в разі, якщо зловмисники викрадуть гроші з банківських карт пасажирів. У заяві авіакомпанії також говориться, що в результаті кібератаки не відбулося витоку паспортних даних пасажирів та інформації про їх маршрути. Повідомляється, що атака хакерів відображена, зараз сайт і додаток для мобільних телефонів працюють в звичайному режимі. Національний центр кібербезпеки Великобританії і Національне агентство з боротьби зі злочинністю почали розслідування цього інциденту.» ***(А ви літали з British Airways? Можливо, ваші дані в небезпеці! // 7dniv.info – інформаційно-аналітичне інтернет видання (http://7dniv.info/society/105537-a-vi-ltali-z-british-airways-mozhlivo-vash-dan-v-nebezpec.html). 09.09.2018).***

***

«Хакерській атаці піддалися представники як Республіканської, так і Демократичної партій США.

Іноземні хакери атакували особисті поштові акаунти сервісу Gmail ряду американських сенаторів.

Про це передає телеканал CNN з посиланням на представника компанії Google…

Скільки саме сенаторів постраждали від цієї хакерської атаки, не повідомляється. Проте наголошується, що атаці піддалися представники як Республіканської, так і Демократичної партій.

Представник Google не повідомив, чи виявилася розпочата хакерами спроба злому успішною чи ні…» ***(Хакери атакували Google-пошту сенаторів США // Західна інформаційна корпорація (https://zik.ua/news/2018/09/22/hakery_atakuvaly_googleposhtu_senatoriv_ssha_1411719). 22.09.2018).***

***

«Иранские хакеры похитили миллионы документов из нескольких британских университетов, в числе которых были Оксфорд и Кембридж…

Похищенные файлы включали конфиденциальные исследования в областях атомной энергетики и кибербезопасности… документы продаются на иранских сайтах всего за £2. Чтобы их купить, необходимо отправить запрос через мессенджеры WhatsApp и Telegram. Оплата осуществляется с помощью банковского перевода, после чего хакеры отправляют покупателям копию нужного документа по электронной почте…» ***(Telegraph: иранские хакеры украли миллионы документов из британских вузов // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3743853). 16.09.2018).***

***

«Невідомі хакери змогли зламати незасекречену поштову систему Держдепартаменту США і отримали доступ до особистої інформації невеликого числа співробітників відомства.

…недавно хакерська атака “торкнулася менше 1% поштових скриньок співробітників”. “Ми встановили, що особиста інформація окремих співробітників може бути розкрита, — йдеться в поширеному в Держдепартаменті оповіщенні. — Ми повідомили цих співробітників”…» ***(Олексій Супрун. Politico: невідомі хакери отримали доступ до даних співробітників Держдепартаменту // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1752662-politico-nevidomi-khakeri-otrimali-dostup-do-danikh-spivrobitnikiv-derzhdepartamentu). 18.09.2018)/***

***

Вірусне та інше шкідливе програмне забезпечення

«Приложение для проверки безопасности Adware Doctor в настоящее время занимает четвертое место в списке популярных приложений для Mac

App Store… исследователи безопасности Mac Патрик Уордл из Digita Security и Томас Рид из Malwarebytes проанализировали ее…

Исследователи обнаружили, что Adware Doctor собирает данные о своих пользователях, в частности историю просмотров и список других программ и процессов, запущенных на компьютере, сохраняет данные в заблокированном файле и периодически отправляет их на сервер, который, по-видимому, находится в Китае. Все эти действия нарушают правила App Store, но даже после уведомления Privacy 1st Apple о проблемах, приложение все еще находится в App Store…

Приложения Mac изолированы друг от друга и от операционной системы в контейнерах, так называемых "sandboxes", которые не позволяют программам получать доступ к другим. Adware Doctor использует разрешения, предоставленные ему для сбора данных, а затем находит способы обойти защиту изолированной среды. Так, программа пытается получить информацию о программном обеспечении, запущенном на компьютере пользователя.

Некоторые программы, например, антивирусы, используют эту возможность безопасно и законно, но приложения из App Store не должны иметь такой доступ. И хотя у macOS уже есть встроенная защита, Adware Doctor может собрать список запущенных программ и процессов через интерфейс прикладного программирования. Код, используемый Adware Doctor для составления списка запущенных процессов, взят из примеров, которые Apple публикует как часть своей документации…» ***(Ирина Фоменко. Популярнейшее приложение на Mac работает как шпионское ПО // Internetua (http://internetua.com/populyarneishee-prilojenie-na-mac-rabotaet-kak-shpionskoe-po). 10.09.2018).***

***

«…Один з творців антивіруса ESET, фахівець з кібербезпеки Лукас Стефанко, попередив всіх користувачів операційної системи Android про можливу небезпеку витоку даних…

Як виявилося, Лукас виявив фейковий Viber, створений з метою вкрасти фотографії та різного роду документи безпосередньо з ваших особистих чатів, в числі яких WhatsApp і WeChat…

Стефанко зазначив, що підробку практично неможливо відрізнити від оригіналу - інтерфейс шпигунської програми повністю відповідає оригіналу. Шахрайський Viber Лукас виявив на сайті, замаскованому під офіційний магазин Google Play. При цьому у програми стоїть значок «Вибір редакції» та показник в 500 мільйонів скачувань…

Під час установки на гаджет програма запитує розширений доступ до пам'яті пристрою, microSD-карті, отримавши який непомітно викрадає документи і медіа файли з месенджерів WhatsApp і WeChat.

Вірусний додаток Viber також записує телефонні розмови, які потім можуть бути використані злочинцями з метою шантажу…» ***(Фейковий Viber скачав 500 мільйонів користувачів. Додаток краде дані з метою шантажу // UkrMedia інтернет-газета (https://ukr.media/science/372356/). 05.09.2018).***

***

«В США експерти в галузі кібербезпеки виявили небезпечний вірус-шифрувальник, названий ім'ям колишнього американського лідера Барака Обами… Офіційно програма отримал назву "Вічний синій вірус-вимагач Барака Обами", тому що при зараженні пристрою на екрані виникає фото 44-го президента США. Вказано, що вірус блокує діяльність встановлених на комп'ютер антивірусів. Фахівці зафіксували його вплив на такі відомі продукти, як Kaspersky і McAfee…» ***(В США виявили небезпечний "вірус Обами" // ONLINE.UA (https://novyny.online.ua/800940/v-ssha-viyavili-nebezpechniy-virus-obami/). 04.09.2018).***

***

«Видання Wired опублікувало фрагмент книги «Sandworm» Енді Грінберга (Andy Greenberg), яка розповідає про вірус під назвою NotPetya…

Видання Wired дослідило роботу компанії Information Systems Security Partners (ISSP), що займалася кіберзахистом в Україні…» ***(Історія вірусу NotPetya: чи варто остерігатися подібних кібератак в майбутньому? // Goodnews.ua (http://goodnews.ua/technologies/istoriya-virusu-notpetya-chi-varto-osterigatisya-podibnix-kiberatak-v-majbutnomu/). 11.09.2018).***

***

«С мая по июль 2018 года количество кибернападений на маршрутизаторы и устройства Интернета вещей увеличилось более чем вдвое. Атаки связаны с распространением таких вредоносных программ, как Mirai, IoTroop/Reaper и VPNFilter, сообщили в компании Check Point Software, занимающейся разработкой программного обеспечения для информационной безопасности.

В июле 2018 года 45% организаций во всем мире подверглись атакам на эти уязвимости, в июне — атаки ощутили 35% компаний, в мае — 21%. Все эти уязвимости позволяют злоумышленникам выполнить вредоносный код и получить удаленный контроль над требуемыми устройствами.

По итогам второго летнего месяца 2018 года три уязвимости вошли в рейтинг 10 наиболее часто эксплуатируемых: удаленное выполнение кодов MVPower DVR маршрутизатора на 5-м месте; удаленное выполнение команд маршрутизатора D'Link DSL-2750B на 7-м месте; обход аутентификации маршрутизатора DANAN GPON A на 10 месте.

В число самых активных вредоносных программ для мобильных устройств вошли Lokibot (банковский троян для Android, который также может превратиться во вредоносную программу-вымогателя, блокирующую телефон в случае удаления прав администратора) и Triada (модульный бэкдор для Android, предоставляющий права суперпользователя загруженному вредоносному ПО, так как способствует его встраиванию в системные процессы).» ***(Кибератаки на Интернет вещей удвоились // Goodnews.ua (http://goodnews.ua/technologies/kiberataki-na-internet-veshhej-udvoilis/). 02.09.2018).***

***

«Эксперты констатируют, что пользователи по-прежнему переходят по подозрительным ссылкам, устанавливают ПО из неизвестных источников и дают приложениям любые разрешения.

«Лаборатория Касперского» зафиксировала масштабную кампанию по заражению мобильной банковской троянской программой Asacub. Количество пользователей, которые сталкиваются с этим зловредом, достигает 40 тыс. в день.

Asacub распространяется посредством фишинговых смс с предложением посмотреть фото или MMS по ссылке. На соответствующей веб-странице находится кнопка для скачивания, при нажатии на которую загружается файл вредоносной программы. Нередко фишинговые сообщения содержат обращение по имени, поскольку адресно рассылаются со смартфона предыдущей жертвы (в них используются имена, под которыми номера записаны в телефонной книге зараженного телефона).

Asacub попадает на устройство только в том случае, если владелец смартфона разрешил в настройках установку из неизвестных источников. Как правило, Asacub маскируется под приложения для работы с MMS или популярные сервисы бесплатных объявлений.

Asacub может красть деньги с привязанной к номеру телефона банковской карты, отправляя смс для перевода средств на другой счет по номеру карты или мобильного телефона. Пользователь не сможет проверить баланс через мобильный банк или изменить настройки, так как после получения специальной команды Asacub запрещает открытие на устройстве банковского приложения.

По данным «Лаборатории Касперского», 98% случаев заражения Asacub приходятся на Россию, также среди пострадавших стран — Украина, Турция, Германия, Белоруссия, Польша, Армения, Казахстан, США и другие.» ***(Троян Asacub атакует до 40 тысяч пользователей в день // «Открытые системы» (https://www.computerworld.ru/news/Asacub-atakuet-do-40-tysyach-polzovateley-v-den). 14.09.2018).***

***

«Хакери запустили новий вірус, який атакує користувачів Європи і краде банківські дані. За даними компанії ESET, прихований банківський троян DanaBot вперше був зафіксований раніше цьогоріч в Австралії та Польщі, а тепер поширюється і в інших країнах - Італії, Німеччині, Австрії і станом на вересень 2018 року в Україні…

"DanaBot є модульним банківським трояном, який вперше був проаналізований Proofpoint в травні 2018 року після виявлення кампаній по поширенню шкідливої програми через шкідливі електронні листи в Австралії. Написаний в Delphi, троян має багатоступеневу і багатокомпонентну архітектуру, більшість функцій якої реалізовані за допомогою плагінів. На момент виявлення шкідлива програма перебуває в стані активної розробки", - йдеться в повідомленні.

Через два тижні після широко відомого поширення в Австралії, DanaBot був виявлений в Польщі. Згідно з дослідженням спеціалістів ESET, спрямована на Польщу кібератака все ще триває, і є найбільшою і найактивнішою на сьогодні. Для зараження жертв зловмисники використовують електронні листи, замасковані під

рахунки різних компаній. А 8 вересня 2018 ESET виявила нову атаку DanaBot, спрямовану на українських користувачів.» ***(Банківським даним українців загрожує новий вірус – подробиці // 5 канал (https://www.5.ua/suspilstvo/bankivskym-danym-ukraintsiv-zahrozhuie-novyi-virus-178032.html). 22.09.2018).***

***

«Согласно последнему отчету McAfee Labs, количество майнинг-атак или случаев черного майнинга, когда компьютер пользователя используется для майнинга криптовалют, без разрешения владельца во втором квартале 2018 увеличилось на 86%.

В отчете, эксперты по кибербезопасности заявили, что во втором квартале было зарегистрировано более 2,5 миллионов случае черного майнинга. Для сравнения, количество подобных атак в четвертом квартале 2017 года составляло всего 400.000.

Авторы доклада приходят к выводу, что угроза со стороны черного майнинга остается одной из самых сильных в области кибербезопасности.

В частности, в докладе подчеркивается тот факт, что киберпреступники активно используют новые подходы к черному майнингу. И хотя, наиболее привлекательными целями по-прежнему служат мощные рабочие станции и игровые компьютеры и ноутбуки, растет число случаев майнинга на периферийных устройствах, таких как маршрутизаторы, видеокамеры и другие устройства являющиеся частью Интернета вещей.» ***(Новая киберугроза: черный майнинг растет потрясающими темпами // Goodnews.ua (http://goodnews.ua/technologies/novaya-kiberugroza-chernyj-majning-rastet-potryasayushhimi-tempami/). 28.09.2018).***

***

«В трояне Adwind, ранее использовавшемся в атаках на промышленные предприятия по всему миру, появился набор новых инструментов, предназначенных для обхода антивирусных программ…

Данный троян, также известный как AlienSpy, JSocket и jRat, содержит множество различных функций. Adwind способен собирать информацию о ПК и считывать нажатия клавиш, а также похищать учетные данные, записывать видео, звук и делать скриншоты.

В августе текущего года исследователи по кибербезопасности из компании Cisco Talos зафиксировали новую спам-кампанию, в ходе которой распространялся Adwind 3.0, один из последних обнаруженных вариантов трояна. Кампания нацелена на компьютеры под управлением ОС Windows, Linux и macOS с особым упором на жертв в Турции и Германии.

Особый интерес представляет новая функция внедрения кода Dynamic Data Exchange (DDE), целью которой является компрометация Microsoft Excel и обход антивирусных решений.

Злоумышленники отправляют вредоносные сообщения, содержащие вложения в формате .CSV или .XLT, которые открываются Excel по умолчанию.

По словам специалистов, новый метод был реализован в целях обфускации. В начале файла нет заголовка, который нужно проверить, что может, в свою очередь, запутать антивирусное программное обеспечение, которое ожидает, что символы ASCII будут присутствовать в формате CSV.

Вместо того, чтобы обнаруживать файл как вредонос, антивирусное программное обеспечение может просто рассматривать файл как поврежденный.

Затем вредонос создает скрипт Visual Basic, который использует bitasdmin. Инструмент bitasdmin, разработанный Microsoft, является средством командной строки для создания или загрузки заданий и контроля их выполнения. В конечном итоге bitasdmin загружает конечную вредоносную нагрузку, файл архива Java, который содержит программу Allatori Obfuscator, устанавливающую Adwind.» ***(Троян Adwind обходит антивирусы для заражения ПК // Goodnews.ua (http://goodnews.ua/technologies/troyan-adwind-obxodit-antivirusy-dlya-zarazheniya-pk/). 25.09.2018).***

***

«Эксперты в области кибербезопасности из Check Point обнаружили ботнет для Android-устройств, за разработкой которого стоит российская команда хакеров The Lucy Gang…

Исследователи назвали новый вирус Black Rose Lucy. По их словам, хакеры научились использовать Android accessibility service — службу, созданную для людей с ограниченными возможностями. С помощью нее злоумышленники обманом заставляют пользователей давать вредоносному коду права на установку других зараженных приложений.

Как только Black Rose Lucy попадает на телефон жертвы, он имитирует программу Monitor. Через минуту после ее инсталляции владельцы Android-устройства видят всплывающее окно с предупреждением, в котором говорится, что устройство находится под угрозой. Пользователя настоятельно просят включить службу Accessibility service для приложения «Безопасность системы».

После этого вирус получает права администратора на смартфоне и соединяется с сервером хакеров, чтобы установить на телефон жертвы остальные вредоносные программы. Кроме того, взломщики могут получить все пользовательские данные, которые хранятся на девайсе.» ***(Пользователей Android атаковали российские мошенники // Goodnews.ua (http://goodnews.ua/technologies/polzovatelej-android-atakovali-rossijskie-moshenniki/). 25.09.2018).***

***

«Компания Check Point опубликовала отчет Global Threat Index за август, в котором отмечает значительное увеличение числа атак с использованием банковского трояна Ramnit. За последние несколько месяцев Ramnit удвоил свою активность, чему способствовала широкомасштабная кампания, в ходе которой устройства жертв становились вредоносными прокси-серверами.

В августе Ramnit подскочил до 6-го места в рейтинге угроз Threat Index и стал самым распространенным банковским трояном в восходящем тренде банковских угроз…

В августе криптоминер Coinhive остался наиболее распространенным вредоносным ПО, атаковав 17% организации по всему миру. В топ-3 поднялся модульный бот Andromeda, который, как и Dorkbot, затронул 6% организаций по всему миру.

Самые активные зловреды в августе:

* Стрелки показывают изменение позиции по сравнению с предыдущим месяцем.

1. ↔ Coinhive — криптомайнер, предназначенный для онлайн-майнинга криптовалюты Monero без ведома пользователя, когда он посещает веб-страницу. Встроенный JavaScript использует большое количество вычислительных ресурсов компьютеров конечных пользователей для майнинга и может привести к сбою системы.

2. ↑ Dorkbot — IRC-червь, предназначенный для удаленного выполнения кода оператором, а также для загрузки дополнительного вредоносного ПО в зараженную систему. Это банковский троян, основной целью которого является кража конфиденциальной информации и запуск атак типа «отказ в обслуживании».

3. ↑ Andromeda — модульный бот, используемый главным образом как бэкдор для доставки дополнительных вредоносных программ на зараженные устройства, но может быть изменен для создания различных типов бот-сетей.

Больше всего в августе атакам подверглись Эфиопия, Сейшельские острова, Катар, Ангола и Ботсвана. Меньше всего атаковали Новую Зеландию, Норвегию и Лихтенштейн.

Lokibot, банковский троян и похититель данных с устройств на платформе Android, стал самой активной вредоносной программой для атак на мобильные устройства организаций. Следом за ним в рейтинге расположились Lotoor и Triada.

Самые активные мобильные зловреды в августе:

1. Lokibot — банковский троян для Android, который также может превратиться во вредоносную программу-вымогателя, блокирующую телефон в случае удаления прав администратора.

2. Lotoor — программа использует уязвимости в операционной системе Android, чтобы получить привилегированный root-доступ на взломанных мобильных устройствах.

3. Triada — Модульный троян для Android, который предоставляет привилегии суперпользователя для загружаемых вредоносных программ, а также помогает внедрить их в системные процессы.

Исследователи Check Point также проанализировали наиболее эксплуатируемые уязвимости. На первом месте уязвимость CVE-2017-7269, которая затронула 47% организаций по всему миру. На втором месте уязвимость OpenSSL TLS DTLS Heartbeat (41%), следом CVE-2017-5638 (36%).

Топ-3 самых эксплуатируемых уязвимостей:

1. ↔ Переполнение буфера Microsoft IIS WebDAV ScStoragePathFromUrl (CVE-2017-7269). Отправляя созданный запрос по сети на сервер Microsoft

Windows Server 2003 R2 через службы Microsoft Internet Information Services 6.0, удаленный злоумышленник может выполнить произвольный код или вызвать отказ условий обслуживания на целевом сервере. Главным образом это связано с уязвимостью переполнения буфера, вызванной ненадлежащей проверкой длинного заголовка в HTTP-запросе.

2. ↑ Heartbeat-уязвимость OpenSSL TLS DTLS (CVE-2014-0160; CVE-2014-0346). В пакете OpenSSL есть уязвимость, связанная с утечкой информации. Она возникает из-за ошибки при обработке heartbeat-пакетов TLS/DTLS. Злоумышленник может использовать эту уязвимость для раскрытия содержимого памяти подключенного клиента или сервера.

3. ↑ D-Link DSL-2750B Remote Command Execution — уязвимость удаленного выполнения кода в роутерах D-Link DSL-2750B. Успешная эксплуатация может привести к произвольному выполнению кода на уязвимом устройстве.» ***(Число атак банковских троянов выросло из-за крупномасштабной кампании Ramnit // «Компьютерное Обозрение» (https://ko.com.ua/chislo_atak_bankovskih_troyanov_vyroslo_iz-za_krupnomasshtabnoj_kampanii_ramnit_126078). 18.09.2018).***

***

«Компания ESET сообщила об обнаружении кибератаки с использованием UEFI руткита для заражения компьютеров жертв. Это вредоносное программное обеспечение, которое получило название Lojax, использовала известная группа Sednit для атаки на правительственные организации на Балканах, а также в Центральной и Восточной Европе…

UEFI руткиты являются невероятно опасными инструментами, которые могут быть использованы для получения доступа ко всему компьютеру. При этом это вредоносное программное обеспечение может оставаться в системе после повторной установки операционной системы или даже замены жесткого диска. Тогда как очищение системы от такой угрозы требует специальных знаний и не под силу обычному пользователю.

Выявление первого в реальной среде UEFI руткита должно стать тревожным сигналом для пользователей и организаций, которые часто игнорируют риски, связанные с модификациями встроенного программного обеспечения…» ***(Обнаружен первый UEFI руткит // «Компьютерное Обозрение» (https://ko.com.ua/obnaruzhen_pervyj_uefi_rutkit_126208). 28.09.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Міністерство фінансів США ввело санкції проти хакера Пак Чин Хьока з КНДР і північнокорейської компанії Chosun Expo Joint Venture, на яку він

працював у якості програміста, в зв'язку з кібератаками, проведеними за завданням Пхеньяна…

У повідомленні Мінфіну вказується, що Пак Чин Хьок несе відповідальність за кібератаку на Sony Pictures Entertainment у 2014 році, викрадення 81 млн доларів із Центробанку Бангладешу і кібератаку зі застосуванням вірусу-здирника WannaCry 2.0 у травні 2017 року…» ***(Самуїл Проскуряков. Мінфін США ввів санкції проти хакера з КНДР через вірус WannaCry // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1750871-minfin-ssha-vviv-sanktsiyi-proti-khakera-z-kndr-cherez-virus-wannacry). 07.09.2018).***

***

«Сполучені Штати екстрадували громадянина Росії Андрія Тюріна, якого звинувачують у кібератаках на американські компанії…

За інфомацією слідства, з 2012 року до середини 2015 росіянин Андрій Тюрин проводив хакерські атаки на американські компанії, зокрема викрав персональні дані понад 100 мільйонів людей.

Він входив до злочинної групи, ще три члени якої знаходилися в Ізраїлі. Двох арештували в Ізраїлі в 2015 році та екстрадували до США у 2016, третього арештували США у 2016.

Андрія Тюрина екстрадували з Грузії. Раніше влада Грузії арештувала Тюрина за запитом США.

Якщо Тюрина визнають винним, його можуть ув'язнити до 30 років…» ***(США екстрадували росіянина, якого звинувачують у кібератаках // громадське телебачення (https://hromadske.ua/posts/ssha-ekstraduvaly-rosiianyna-iakoho-zvynuvachuiut-u-kiberatakakh). 08.09.2018).***

***

«Власти Сингапура оштрафовали китайского исследователя безопасности на 5 тыс. сингапурских долларов ($3600) за взлом сети Wi-Fi в местном отеле без разрешения и публикацию в блоге информации, раскрывшей пароли гостиницы…

Инцидент произошел в конце августа текущего года, когда 23-летний Чжэн Дутао прилетел в Сингапур, чтобы посетить конференцию Hack In The Box, которая проходила в городе.

Чжэн взломать сеть Wi-Fi в филиале отеля Fragrance, где он остановился на время конференции. Исследователь, работающий на китайского интернет-гиганта Tencent, взломал интернет-шлюз отеля — устройство AntLabs IG3100, которое контролирует доступ к сети Wi-Fi для персонала и гостей.

Он обнаружил, что устройство использует пароль Telnet, установленный по умолчанию, который он ввел для доступа к защищенной оболочке устройства.

Далее он использовал различные скрипты и эксплойты для того, чтобы поднять свои привилегии и, в конечном счете, обнаружил пароль для базы данных MySQL, содержащий информацию о внутренней сети Wi-Fi отеля.

Исследователь не сообщил о проблемах безопасности представителям отеля, а вместо этого написал сообщение в блоге о своих выводах, которые он позже

опубликовал в Интернете. Чжен не нанес ущерб системам Wi-Fi, однако он также не принимал никаких мер предосторожности для сокрытия конфиденциальной информации в своем блоге, раскрыв пароли Telnet и MySQL отеля и другие данные, которые хакеры могли использовать в более серьезной атаке на сети.

Агентство кибербезопасности Сингапура (CSA) обнаружило блог Чжэна через несколько дней, предупредило гостиницу и взяло исследователя под стражу.» ***(Исследователь оштрафован за взлом Wi-Fi и публикацию паролей в Сети // Goodnews.ua (http://goodnews.ua/technologies/issledovatel-oshtrafovan-za-vzlom-wi-fi-i-publikaciyu-parolej-v-seti/). 27.09.2018).***

***

Технічні аспекти кібербезпеки

«11 октября произойдёт первая в истории интернета смена криптографических доменных ключей, которые служат защитой для DNS, и из-за их замены могут случиться сбои

Корпорация по управлению доменными именами и IP-адресами (ICANN) предупредила о возможных сбоях в работе интернета в октябре 2018 года. Причиной сбоев может стать «первая в истории смена криптографических ключей, которые служат защитой для системы доменных имен…

Переход на новые ключи (Key Signing Key, KSK) должен состояться 11 октября. Ожидается, что со сложностями при открытии сайтов столкнется «лишь небольшой процент интернет-пользователей»…» ***(ICANN: в октябре возможны сбои в работе интернета по всему миру // РосКомСвобода (https://roskomsvoboda.org/41505/). 06.09.2018).***

***

«…Компания решила поэкспериментировать Tesla Motors обновила условия программы вознаграждения за поиск уязвимостей, — говорится на сайте компании. Теперь одобренные участники программы могут взламывать автомобили Tesla без боязни юридических последствий или отзыва гарантии. Согласно новой политике, компания будет перепрошивать прошивку автомобилей, которая вышла из строя в процессе поиска уязвимостей.

…Как отмечается, исследования, проводимые в рамках программы bug bounty, не повлекут юридические последствия (обвинения в нарушении «Закона США о компьютерном мошенничестве», нарушении авторских прав и пр.), а гарантии на автомобили останутся действительными. Программа вознаграждения за найденные уязвимости Tesla действует с 2015 года. Размер вознаграждения варьируется от $100 до $10 тыс. Для того чтобы его получить, специалист должен предоставить подробности об обнаруженной уязвимости, а также код для эксплуатации проблемы. При этом нашедший уязвимость должен избегать нарушения конфиденциальности, не уничтожать и не модифицировать данные, а также не мешать работе сервисов.» ***(Tesla Motors предложила хакерам себя***

взломать // "Українські медійні системи" (https://glavcom.ua/ru/news/tesla-motors-predlozhila-hakeram-sebya-vzlomat-526770.html). 11.09.2018).

***

«Во втором квартале 2018 года объем продаж аппаратных средств компьютерной безопасности в мире достиг 3,6 млрд долл. Количество проданных устройств выросло на 25,3% до 921278 штук.

Сегмент систем унифицированного управления угрозами (UTM) вырос за год на 16,5% и достиг 1,9 млрд долл., занимая 52,9% всего рынка. На 7,8% вырос сегмент средств веб-безопасности, включая средства управления доступом к веб-ресурсам. Количество проданных устройств для обеспечения безопасности обмена сообщениями выросло на 9% по сравнению с прошлым годом, но по сравнению с предыдущим кварталом сократилось на 2,6%. Продажи снизились только в сегментах средств VPN с поддержкой IPSec и SSL.

Первое место по объемам продаж занимает Cisco (15,5% рынка). На втором месте Palo Alto Networks (14,4%), а третье делят Fortinet и Check Point (по 10,7%). Symantec принадлежит 4,3% рынка. Темп роста продаж у первой тройки производителей значительно опережает средний по рынку: 24,5%, 23,6% и 21,3% (у Fortinet), соответственно.» ***(IDC: мировой рынок устройств безопасности вырос за год на 17% // «Открытые системы» (https://www.computerworld.ru/news/IDC-mirovoy-rynok-ustroystv-bezopasnosti-vyros-za-god-na-17-protzentov). 24.09.2018).***

***

«С каждым кварталом дела в подразделении Cisco, специализирующемся на решениях для обеспечения информационной безопасности (ИБ), идут все лучше и лучше. Благодаря масштабам своего бизнеса, лидер рынка сетевого оборудования зарабатывает на ИБ-продукции больше, чем многие компании, занятые исключительно разработкой аппаратных и программных средств киберзащиты. Что впечатляет еще сильнее, выручка Cisco на этом направлении стабильно увеличивается.

На протяжении последних четырех кварталов оборот ИБ-бизнеса Cisco рос в годовом исчислении, а последние две четверти регистрируют двузначные темпы. По итогам трёхмесячного периода, который истек 28 июля 2018 года, продажи решений для обеспечения кибербезопасности принесли Cisco 627 миллионов долларов против 558 миллионов годом ранее.

С учетом 12-процентного подъема ИБ-бизнес стал самым быстрорастущим направлением деятельности Cisco в минувшем квартале, а в целом за прошлый фингод выручка этого подразделения достигла 2,35 миллиарда долларов, что на 9% больше предыдущего годового результата.

…являясь крупнейшим производителем сетевого оборудования, такого как маршрутизаторы и коммутаторы, американский вендор может встраивать средства защиты от сетевых угроз на аппаратном уровне, что дает ему огромное преимущество над конкурентами, которые специализируются только на разработке ИБ-решений.

Данные аналитиков это подтверждают: исследовательская компания IDC недавно сообщила, что Cisco продолжает лидировать на мировом рынке оборудования для обеспечения информационной безопасности, оборот которого во втором квартале 2018 года вырос на 17% в годовом исчислении и превысил 3,6 миллиарда долларов.

В апреле-июне Cisco заработала на продаже такой аппаратуры 560,5 миллиона долларов, с учетом чего она контролировала более 15% этого рынка. По сравнению с показателями годовой давности выручка Cisco от продажи аппаратных средств сетевой защиты увеличилась на 24,5%, а долевой показатель подрос почти на процент.

Ближайший конкурент – компания Palo Alto Networks – записала в свой актив свыше 520 миллионов долларов выручки (+23,6%), что соответствовало рыночной доле в 14,4% (+0,7%). В то же время уже упомянутая Check Point, которая долгое время шла в рейтинге следом за Cisco, прибавила в выручке лишь 1,8%, что привело к снижению доли с 12,3% до 10,7%. Из-за низких темпов роста Check Point пропустила вперед Fortinet, а замкнула пятерку ведущих поставщиков ИБ-аппаратуры компания Symantec.

Уверенная восходящая динамика Cisco доказывает эффективность ее стратегии “Security Everywhere”, которая предусматривает внедрение защитных технологий в ИТ-инфраструктуру всего предприятия, от центров обработки данных, мобильных и облачных сред до оконечных устройств…

По прогнозам исследовательской компании Grand View Research, спрос на системы многофакторной аутентификации в следующие семь лет будет ежегодно увеличиваться в среднем на 15%. Таким образом, Cisco обеспечила свое присутствие в еще одном быстрорастущем сегменте рынка ИБ-технологий, который поможет добиться дальнейшего увеличения выручки ИБ-бизнеса Cisco и компании в целом…

В долгосрочной перспективе кибербезопасность может стать мощным драйвером роста Cisco, ведь компания продолжает прилагать усилия для дальнейшего усиления позиций в данной сфере. Учитывая потенциал Cisco на этом и других направлениях, аналитики ожидают ускорение ее темпов роста до почти 9% в ближайшие пять лет. В предыдущую пятилетку компания ежегодно росла в среднем на 5,5%.» ***(Кибербезопасность: самый быстрорастущий бизнес Cisco // Український телекомунікаційний портал (https://portaltele.com.ua/news/companies/kiberbezopasnost-samyj-bystrorastushhij-biznes-cisco.html). 25.09.2018).***

***

«Миллионы британских домохозяйств могут оказаться уязвимыми перед неисправностью в веб-браузере Google Chrome, подвергающей сеть Wi-Fi новой форме взлома…

Уязвимость в исходном коде популярного браузера американского технологического гиганта означает, что хакеры могут проникнуть в чью-либо сеть Wi-Fi всего за одну минуту. По мнению исследователя компании по кибербезопасности SureCloud Эллиота Томпсона, 3 млн домов в Великобритании потенциально пострадали…

Хакеры используют уязвимость в системе, которая автоматически соединяет пользователей с Wi-Fi-сетями. Злоумышленники могут украсть пароли, данные с подключенных ПК, активировать веб-камеры на подключенных устройствах или устанавливать вредоносные программы и программы-шпионы. Доступ к Wi-Fi преступники могут получить, просто проезжая по улице в радиусе действия Wi-Fi-сети. Для того, чтобы атаковать всю сеть, требуется только одно устройство с Google Chrome.

Исследователи SureCloud заявили, что хакеры могут получить доступ к общим файлам, устройствам IoT, а также просмотреть, какие веб-сайты посещали. Есили они не зашифрованы, преступник может отслеживать конфиденциальную информацию, например, данные кредитной карты. Во время атаки жертва увидит всплывающее окно, которое выглядит как меню администратора Wifi-маршрутизатора…» ***(Ирина Фоменко. Дыра в Chrome позволяет хакерам контролировать ваш Wi-Fi // Internetua (http://internetua.com/dyra-v-chrome-pozvolyaet-hakeram-kontrolirovat-vash-wi-fi). 05.09.2018).***

***

«У найсвіжіший версії Android 9.0 виявили критичну уразливість, внаслідок чого тепер зловмисники мають можливість отримати доступ важливої інформації на Вашому мобільному пристрої.

Відповідні результати дослідження оприлюднила американська компанія Nightwatch Cybersecurity, що займається дослідженнями в галузі кібербезпеки.

Як з'ясували фахівці, завдяки такому пролому у захисті хакери можуть отримати детальний доступ, зокрема, до інформації про Wi-Fi, назву підключення, включно з IP-адресою, DNS-сервера, паролю та інших параметрів.

Таким чином, зловмисники отримали можливість відстежувати увесь вхідний і східний трафік, перехоплюючи особисті дані

Крім того, знаючи детальну інформацію про смартфон, за допомогою шкідливого ПО можна відстежити будь-який смартфон і навіть влаштувати атаку на бездротову мережу та інші підключені до неї пристрої…» ***(Нова вразливість у Android: хакери отримали повний доступ до будь-якого смартфону // BCBITI (http://vsviti.com.ua/news/87770). 06.09.2018).***

***

«ESET предупреждает о целевых атаках с использованием новой, пока не закрытой производителем уязвимости в Microsoft Windows. По данным телеметрии, атаки нацелены на пользователей в России, Украине, Польше, Германии, Великобритании, США, Индии, Чили и на Филиппинах.

Уязвимость представляет собой локальное повышение привилегий (Local Privilege Escalation), которое позволит выполнять вредоносный код с максимальными правами. Баг связан с работой Планировщика задач Windows и затрагивает версии операционной системы Microsoft Windows с 7 по 10.

Информация об уязвимости нулевого дня была раскрыта 27 августа. На момент публикации обновления безопасности отсутствовали.

Всего через два дня после публикации специалисты ESET обнаружили, что эксплойт к новой уязвимости используется в целевых атаках кибергруппы PowerPool. Хакеры несколько изменили опубликованный на GitHub код эксплойта и перекомпилировали его.

Атака начинается с рассылки вредоносных спам-писем с бэкдором первого этапа. Вредоносная программа предназначена для базовой разведки в системе — она выполняет команды атакующих и передает собранные данные на удаленный сервер.

Если компьютер заинтересовал хакеров, на нем будет установлен бэкдор второго этапа, обеспечивающий постоянный доступ к системе. Далее операторы PowerPool использует уязвимость нулевого дня для повышения привилегий. Для перемещения внутри скомпрометированной сети атакующие используют инструменты с открытым исходным кодом: PowerDump, PowerSploit, SMBExec, Quarks PwDump, FireMaster.

Атаки PowerPool нацелены на ограниченное число пользователей. Тем не менее, инцидент показывает, что злоумышленники отслеживают тренды и оперативно внедряют новые эксплойты. Раскрытие информации об уязвимостях до выхода обновлений безопасности может послужить причиной массовых кибератак.» ***(Хакеры PowerPool используют в целевых атаках уязвимость нулевого дня // «Компьютерное Обозрение» (https://ko.com.ua/hakery_powerpool_ispolzuyut_v_celevyh_atakah_uyazvimost_nulevogo_dnya_126007). 11.09.2018).***

***

«…Специалисты компании Tenable нашли в сетевом устройстве хранения данных и записи видео с камер наблюдения Nuuo NVRMini2 уязвимость, позволяющую просматривать и подменять записи. Уязвимость имеется в прошивках NVRMini2 версий старше 3.9.0, утверждают они. В компании Nuuo уже работают над исправлением ошибки и рекомендуют пользователям уязвимых устройств обратиться в компанию.

Программы и устройства Nuuo установлены более чем в 100 тыс. системах наблюдения по всему миру. Уязвимыми могут оказаться более 2500 различных моделей камер более чем ста марок. Уязвимость, которую в Tenable назвали Peekaboo, позволяет дистанционно получить доступ ко всей системе управления

видеонаблюдением и пароли доступа ко всем подключенным ко взломанному сетевому устройству NVRMini2 камерам. Злоумышленники могут отключить передачу видео или заменить его на свое. Пользователям советуют отключить устройства от Интернета и открывать доступ к ним через сеть только доверенным пользователям.» ***(В популярных камерах видеонаблюдения нашли очередную уязвимость // «Открытые системы» (https://www.computerworld.ru/news/V-populyarnyh-kamerah-videonablyudeniya-nashli-ocherednuyu-uyazvimost). 19.09.2018).***

***

«Специалисты Positive Technologies провели анализ защищенности приложений для трейдинга — торговых терминалов, которые позволяют покупать и продавать акции, облигации, фьючерсы, валюту и другие активы. Согласно исследованию, в 61% приложений возможно получение несанкционированного доступа к личным кабинетам, в 33% — проведение финансовых операций от имени других пользователей без доступа к личному кабинету, в 17% — подмена отображаемых котировок. Такие атаки могут вызывать изменение цен на рынке в пользу злоумышленника, спровоцировать панику на бирже и нанести значительный финансовый ущерб пользователям уязвимых приложений.

Эксперты изучили торговые платформы, которые популярны не только среди частных трейдеров, но и широко используются в банках, инвестиционных фондах и иных организациях, связанных с биржевой торговлей. Исследования проводились в отношении клиентских частей платформ. Были проанализированы десктопные торговые терминалы, а также мобильные (для Android и iOS) и веб-приложения для трейдинга.

В 61% приложений злоумышленник может получить контроль над личным кабинетом пользователя торгового терминала. Это позволит торговать активами пользователя, получить информацию о доступных средствах на балансе, подменить параметры автоматической торговли, просмотреть историю операций и запланированные операции. Перехват учетных данных в десктопных терминалах возможен при отсутствии шифрования трафика, а в мобильных приложениях этому способствуют root-права или jailbreak на устройстве. Доступ к личному кабинету можно получить и в некоторых веб-версиях приложений, перехватив сессию пользователя.

Уязвимости, обнаруженные экспертами Positive Technologies в каждом третьем приложении, позволяют посторонним лицам осуществлять сделки по продаже или покупке акций от имени пользователя и без доступа к личному кабинету. Злоумышленник может увеличить стоимость интересующих его ценных бумаг с помощью массовой покупки их на чужих аккаунтах или снизить стоимость акций, активно продавая их. Аналогичным образом можно манипулировать курсами валют — если атака затронет крупных игроков или большое количество пользователей. Покупка и продажа биржевых активов от чужого имени возможна как в десктопных, так и в мобильных и веб-терминалах.

Специалисты отмечают, что атаки на веб-версии торговых терминалов могут носить массовый характер…» ***(Positive Technologies исследовала приложения для трейдинга: хакеры могут обрушить котировки акций и курсы валют // SecurityLab.ru (https://www.securitylab.ru/news/495704.php). 26.09.2018).***

***

«Експерти з кібербезпеки групи Zero Day Initiative виявили дефект у продукті Microsoft… Як повідомили дослідники в своєму блозі, пролом був помічений ще в травні, але розробники не встигли його виправити за чотири місяці. І хоча компанії повідомили про уразливість, і не опублікували у відкритому доступі, щоб компанія встигла її виправити, через 4 місяці вразливість піддає небезпеки мільйони користувачів по всьому світу.

Фахівці дали компанії 120 днів на усунення уразливості в механізмі бази даних Microsoft JET Database Engine. Лазівка, яка криється в нульовому дні, дозволяє хакерам віддалено виконувати довільний код, а потім встановлювати на комп'ютер жертви віруси, які в підсумку можуть красти дані, включаючи особисту інформацію і дані з кредитних карт.

Щоб побачити цю уразливість, користувачеві досить відкрити заражений файл, у якому будуть міститися дані, що зберігаються у форматі JET. Цей файл є на кожному комп'ютері.

Небезпека злому була виявлена в Windows 7, проте експерти побоюються, що всі існуючі версії операційної системи, включаючи серверні, піддані атаці хакерів. В Zero Day Initiative сподіваються, що необхідний патч вийде в жовтневому оновлення. Залишається тільки чекати і не заходити на неперевірені сайти…» ***(Microsoft зливає дані користувачів хакерам // znaj.ua (https://znaj.ua/techno/175572-microsoft-zlivaye-dani-koristuvachiv-hakeram). 24.09.2018).***

***

«В сентябре 2017 года исследователи из компании Armis обнародавали информацию о восьми уязвимостях, получивших общее название Blueborne, затрагивающих реализации Bluetooth в устройствах на базе различных платформ — Android, Windows, Linux и iOS (до версии iOS 10). В худшем случае эксплуатация проблемы позволяла получить полный контроль над устройством и содержащимися на нем данными. По оценкам специалистов на тот момент, число уязвимых устройств превышало 5 млрд.

Как показал новый анализ, год спустя порядка 2 млрд устройств по-прежнему являются уязвимыми к данным атакам. По словам экспертов, причина заключается двух факторах: многие пользователи так и не применили выпущенные производителями патчи, а для некоторых устройств корректирующие обновления попросту недоступны, в частности, для устаревшего оборудования, поддержку которого вендоры намерены прекратить в скором времени.

По оценкам исследователей, незащищенными от данного типа атак остаются 768 млн устройств на базе Linux; 734 млн Android-гаджетов (под управлением версий Android 5.1 Lollipop и ниже); 261 млн устройств на базе Android 6

Marshmallow и более ранних; 200 млн устройств на базе уязвимых версий Windows; 50 млн гаджетов под управлением iOS 9.3.5 и ниже…» ***(Спустя год 2 млрд устройств все еще уязвимы к атакам Blueborne // Goodnews.ua (http://goodnews.ua/technologies/spustya-god-2-mlrd-ustrojstv-vse-eshhe-uyazvimy-k-atakam-blueborne/). 16.09.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Исследователи предложили «засевать» ПО поддельными безвредными уязвимостями и тем самым заставить хакеров тратить свое время впустую.

Как ни парадоксально это звучит, но чем больше уязвимостей в системе, тем надежнее она защищена. Если при разработке умышленно добавить в продукт поддельные, неэксплуатируемые уязвимости, хакерам придется потратить много времени и ресурсов в попытках осуществить атаку с их помощью. В итоге, так и не добившись успеха, злоумышленники оставят попытки еще до того, как найдут настоящую уязвимость.

Идея защиты ПО с помощью поддельных уязвимостей изложена в исследовании специалистов Политехнического института Нью-Йоркского университета (США). Изначально исследователи разработали технику для автоматического «засевания» программ поддельными багами в целях тестирования и улучшения работы систем по обнаружению уязвимостей. Однако потом специалисты решили также изучить другие возможные способы применения своего изобретения…» ***(Защитить ПО от хакеров помогут уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/494952.php). 08.09.2018).***

***

«Международная инициатива, курируемая токийским Технологическим центром Армии США (International Technology Center-Pacific, ITC-PAC), добилась существенного прогресса в разработке нового типа превентивной защиты от кибератак. Группа инженеров Армейской исследовательской лаборатории (ARL) в кооперации с учёными Кентерберийского университета (UC) Новой Зеландии и Научно-технического института Кванчжу (Южная Корея) впервые реализовала инновационную технику движущихся мишеней (Moving Target Defense, MTD) в программно-конфигурируемых сетях (SDN).

Идея MTD заключается в частом изменении IP-адреса компьютера: это вводит хакера в заблуждение, делая бесполезной собранную им предварительно информацию о потенциальной жертве, и приводит к снижению эффективности атак.

Реализация такого механизма превентивной защиты требует отвлечения дорогостоящих системных ресурсов на постоянное изменение «поверхности атаки». Исследователи предложили существенно снизить затраты, обратившись к

технологии SDN, которая делегирует задачи управления индивидуальными сетевыми устройствами централизованному контроллеру, что обеспечивает большую динамичность и программируемость сетевых операций в меняющейся обстановке.

Такой комбинированный подход, названный авторами Flexible Random Virtual IP Multiplexing (FRVM), позволяет серверам сохранять свои IP-адреса фиксированными, но маскировать их от остального Интернета виртуальными IP, непрерывно изменяемыми SDN-контроллером…» ***(Новый метод защиты позволит компьютерам «уклоняться» от атак // «Компьютерное Обозрение» (https://ko.com.ua/novyj_metod_zashhity_pozvolit_kompyuteram_uklonyatsya_ot_atak_125976). 10.09.2018).***

***

«Google собирается отказаться от классического адреса интернет-страниц в своем браузере… поскольку они являются слишком сложными и непонятными для пользователей.

Это часто играет на руку хакерам и мошенникам, которые создают фейковые страницы финансовых учреждений и прочие вредоносные сайты, распространяют ложную информацию или вирусное программное обеспечение.

Поэтому, программисты компании работают над такой системой, которая поможет упростить пользование веб-страницами в Chrome для каждого пользователя.

“Я еще не знаю как точно это будет выглядеть, потому что сейчас мы активно обсуждаем это в команде. Я знаю: что бы мы не предложили - это будет спорным”, - рассказала в интервью WIRED директор технологий в Chrome Париса Табриз. “Это один из самых главных вызовов в работе со старой, открытой и разваливающейся платформой. Изменения в любом случае будут спорными, независимо от того, что произойдет. Важно, что мы делаем это, поскольку все недовольны URL. Это вроде как отстойно”.

По сути, Google должен разработать новую систему, все участники которой смогут легко проверять и понимать с чем они имеют дело, заходят ли они на подлинный веб-сайт и легко различать страницы или сообщения, которым точно нельзя доверять.

Представители корпорации объясняют, что сейчас они сосредоточены на определении того, как люди используют URL-адреса, чтобы найти альтернативу с повышенными мерами безопасности и определением личности в интернете.

Очевидно, что Google пока не имеет определенного решения того, как будут функционировать веб-страницы без URL-адресов…» ***(Google хочет отменить URL-адреса веб-сайтов // AOinform (http://www.aoinform.com/news/google_khochet_otmenit_url_adresa_veb_sajtov/2018-09-06-25835). 06.09.2018).***

***

«…Опубликованный недавно новый стандарт в серии ISA/IEC 62443-4-2-2018 («Безопасность автоматизированных систем управления

технологическими процессами: Технические требования к безопасности компонентов АСУ ТП») описывает технические требования к кибербезопасности составляющих АСУ ТП, таких как встраиваемые устройства, сетевые компоненты, компоненты хоста и приложения. Стандарт описывает функции безопасности, позволяющие компонентам отражать угрозы на заданном уровне безопасности без использования компенсирующих контрмер.

«Стандартное определение возможностей безопасности для системных компонентов обеспечивает общий язык для поставщиков продуктов и всех других заинтересованных сторон. Это упрощает процессы закупок и интеграции компьютеров, приложений, сетевого оборудования и устройств, составляющих систему управления», - сообщил эксперт компании Honeywell Кевин Стаггс (Kevin Staggs), возглавивший рабочую группу по разработке ISA/IEC 62443-4-2-2018…» ***(Опубликован новый стандарт безопасности компонентов АСУ ТП // SecurityLab.ru (https://www.securitylab.ru/news/495698.php). 26.09.2018).***

***

«Програмні додатки, що використовують Azure Active Directory (AD) для автентифікації — в цю категорію, серед інших, входить Office 365 — незабаром можуть повністю припинити використання паролів…

Облікові записи AD Azure вже зараз можуть використовувати програму Microsoft Authenticator для двофакторної автентифікації, комбінуючи пароль із одноразовим кодом. Завдяки новій безпарольній підтримці, автентифікація буде повністю виконуватися програмним додатком; програма сама репрезентує «те, що у вас є», і це поєднується з біометричною автентифікацією або PIN-кодом…

Увімкнення двофакторної аутентифікації — лише один з засобів, який організації можуть впровадити для підвищення безпеки. З цією метою корпорація Microsoft розширила можливості Microsoft Security Score — інструменту, який використовується для оцінки організаційної політики та надання рекомендацій щодо заходів, які можуть бути застосовані для посилення захисту компанії проти нападу. Система Secure Score вже охоплює функції безпеки Office 365 та Windows; тепер Microsoft додав до них Azure AD, Azure Security Center і Enterprise Mobility + Security, щоб охопити ширший діапазон параметрів та опцій…

Коли відбувається кібератака, новий інструмент Microsoft Threat Protection забезпечує детекцію та налаштування широкого спектра систем захисту від загроз: від електронної пошти до ідентифікації та інфраструктури. Такі дії повинні полегшити виявлення підозрілої поведінки, такої як: незрозумілі спроби входу в систему, незвичні модифікації файлів, несподівані збої програм, атипова мережева активність та блокування облікових записів, ізоляція систем з мережі, а також будь-що інше, що може бути загрозою…» ***(Microsoft пропонує повністю безпарольну автентифікацію для інтернет-додатків // Blog Imena.UA (https://www.imena.ua/blog/passwordless-authentication-for-online-apps/). 27.09.2018).***

***

«Еще в конце прошлого года команда разработчиков браузера Firefox объявила о сотрудничестве с Тройем Хантом, австралийским специалистом по кибербезопасности и создателем сервиса проверки скомпрометированных учетных записей Have I Been Pwned («Взламывали ли меня?»). И вот вчера Mozilla официально запустила собственный сервис Firefox Monitor, который является точной копией Have I Been Pwned. Собственно, Firefox Monitor использует базу Have I Been Pwned, в которой на сегодняшний день содержатся данные более 5 млрд аккаунтов из 312 взломанных сервисов.

Как и Have I Been Pwned, Firefox Monitor позволяет проверить свою почту на причастность к какой-либо из известных утечек и подписаться на уведомления — если в будущей утечке аккаунт засветится, то вас предупредят.

…Благодаря сотрудничеству Mozilla и Have I Been Pwned еще больше пользователей узнают о существовании подобных инструментов, позволяющих быстро проверить безопасность своих личных данных…» ***(Владимир Скрипин. Сервис Firefox Monitor предупредит пользователей, если их личные данные окажутся под угрозой // ITC.ua (https://itc.ua/news/servis-firefox-monitor-predupredit-polzovateley-esli-ih-lichnyie-dannyie-okazhutsya-pod-ugrozoy/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 26.09.2018).***

***

«Национальное агентство кибербезопасности, иначе ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), открыло исходный код ClIP OS, сверхзащищенной операционной системы, разработанной его инженерами по заказу французского правительства.

В пресс-релизе ANSSI характеризует CLIP OS как базирующуюся на Linux ОС, которая имеет ряд механизмов безопасности, обеспечивающих ей очень высокую степень сопротивляемости вредоносным программам для защиты конфиденциальной информации.

В частности, сообщается, что в CLIP OS применён механизм разбиения, позволяющий распределить публичные и чувствительные данные по двум «абсолютно изолированным» программным средам.

ANSSI информировала, что эта ОС может устанавливаться не только а шлюзах безопасности, но и на обычных рабочих станциях. На данный момент не имеется готовой к употреблению версии CLIP OS для конечных пользователей, и нужную сборку им придётся компоновать самостоятельно.

Разработка CLIP OS продолжалась более десяти лет, а первыми подробностями о ней ANSSI поделилось три года назад на конференции по безопасности, проходившей в городе Ренн (Франция).

Код CLIP OS и сопроводительная документация выложены на сайте GitHub на условиях GNU Lesser General Public License v2.1. Там предоставлены две версии — CLIP OS 4 и 5. Версия 4 это стабильное ответвление CLIP OS, его документация доступна только на французском, что может создать трудности для иностранцев. CLIP OS 5 находится на стадии альфа-релиза и обеспечена англоязычной

документацией, то есть идеальна для быстрого включения в работу над проектом внешних контрибьюторов.

Разработчики ANSSI также подготовили и выложили 14 модулей CLIP OS 4, которые могут быть повторно использованы в проекте. Среди них — подключаемый модуль аутентификации (PAM), программа-демон для обслуживания пользовательских административных задач, облегчённый инструмент TPM (Trusted Platform Module) с интерфейсом командной строки и различные библиотеки, связанные с криптографией и шифрованием.

Инструкции по доступу к открытому коду CLIP OS и к участию в проекте можно найти на официальном веб-сайте clip-os.org.» ***(Франция открыла исходники защищённого от взлома клона Linux — CLIP OS // «Компьютерное Обозрение» (https://ko.com.ua/franciya_otkryla_ishodniki_zashhishhyonnogo_ot_vzloma_klona_linux_clip_os_126137). 21.09.2018).***

***

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

Буяджи С. А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект : автореф. дис. ... канд. юрид. наук : 12.00.01 / Буяджи Сергій Анатолійович ; Приват. ВНЗ Ун-т Короля Данила. - Івано-Франківськ, 2018. - 16 с.

Системно та ґрунтовно проаналізовано особливості теоретико-правового регулювання боротьби із кіберзлочинністю. Досліджено національне та міжнародно-правове регулювання боротьби із кіберзлочинністю. Визначено перспективи та тенденції розвитку правового регулювання боротьби із кіберзлочинністю в Україні. Розкрито специфіку правового регулювання боротьби із кіберзлочинністю у зарубіжних країнах.

Шифр зберігання НБУВ: РА435167

***

Довгань О. Д. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія / О. Д. Довгань, І. М. Доронін. - Київ, 2018. - 106 с.

Запропоновано вирішення проблемних питань у сфері кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібридних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України.

Шифр зберігання НБУВ: ВА821513.

***

Інституційне середовище становлення та розвитку правової економіки в Україні: матеріали міжрегіон. наук.-практ. конф. молодих учених (Харків, 28 листоп. 2017 р.). - Харків : Право, 2017. - 187с.

Зі змісту:

- Кругла М.В. Економічна кіберзлочинність; ризики та шляхи їх нейтралізації.

Шифр зберігання НБУВ: ВА821570

***

Інформаційне суспільство: проблеми та перспективи : матеріали Всеукр. наук.-практ. конф., 28 трав. 2016 р., м. Одеса. - Одеса : Фенікс, 2016. - 73 с.

Зі змісту:

- Дробожур Р.Р., Малишев М.А. Аналіз недоліків українського законодавства у сфері кібербезпеки;
- Логінова Н.І. Аналіз співвідношення інформаційної та кібернетичної безпеки.

Шифр зберігання НБУВ: СО35801.

***

Матеріали міжнародної науково-практичної конференції «Реформування національного та міжнародного права: перспективи та пріоритети» (8-9 грудня 2017 року. - Дніпро, 2017. - Ч. 1. - 151 с.

Зі змісту:

- Діхтярь А.В. Кбірнетичний тероризм як форма терористичної діяльності: міжнародний аспект;
- Бордюг Т.О. Авторське право у кіберпросторі: монетизувати, а не обмежувати.

Шифр зберігання НБУВ: В357211/1.

***

Правове життя: сучасний стан та перспективи розвитку : зб. тез наук. доп. XIV Міжнар. наук.-практ. конф. молодих учених (29-30 берез. 2018 р.). - Луцьк : Вежа-Друк, 2018. - 179 с.

Зі змісту:

- Мельничук К.Д. Незаконне втручання в роботу персональних комп’ютерів та комп’ютерних мереж, що заподіяло істотну шкоду.

Шифр зберігання НБУВ: ВА822067.

***

Прийняття державно-управлінських рішень в індетермінованих умовах: проблеми, сучасні методи, технології забезпечення ефективності : матеріали наук.-методол. семінару молодих учених Нац. акад. держ. упр. при Президентові України. - Миколаїв : Ємельянова Т. В., 2018. - 265 с.

Зі змісту:

- Сіренко Г.Г. Проблема професійного відбору персоналу підрозділів кіберзахисту органів публічної влади.

Шифр зберігання НБУВ: ВА822293.

***

Протидія терористичній діяльності: міжнародний досвід і його актуальність для України : матеріали II Міжнар. наук.-практ. конф., 15 груд. 2017 р. - Київ, 2018. - 429 с.

Зі змісту:

- Бугайчук К., Шороха Г. Забезпечення кібербезпеки як умова протидії терористичній діяльності: нормативно-правові аспекти;
- Карачевцев О., Осіпов Я. Інформаційна безпека: проблема боротьби з кібертероризмом;
- Куліков Д., Грищенко Д. Проблемні аспекти протидії кіберзлочинності в Україні;
- Присяжна Є., Бараненко Р. Кібератаки загрожують Україні: уроки від Petya A;
- Соколова-Височина Я. Терористичні організації та кіберзлочини в інформаційному просторі;
- Циб І. Кберзлочинність як одна із проблем інформаційного суспільства;
- Черновол В. Щодо окремих аспектів протидії кібертероризму в умовах глобалізації.

Шифр зберігання НБУВ: ВС64071

***

Стан та перспективи реформування сектору безпеки і оборони України : матеріали міжнар. наук.-практ. конф., 24 листоп. 2017 р. - Київ, 2017. - Т. 1. - 2017. - 474 с.

Зі змісту:

- Маковоз О.С., Передерій Т.С. Кібербезпека використання технології Краудфандінг в Україні;
- Мякухин Ю.В., Наконечный В.С., Оксиюк А.Г., Толюпа С.В. Определение уровня стойкости фуцнкционирования объектов критически важной инфраструктуры от киберугроз;
- Оксіюк О.Г., Даков С.Ю. Кібербезпека як один із приріоритетів держави;
- Пучков О.О., Конюшок С.М. Підготовка фахівців у сфері кібербзпеки для потреб органів сектору безпеки і оборони України: досвід ІСЗЗІ НТУУ «КПІ імені Ігоря Сікорського».

Шифр зберігання НБУВ: В357163/1.

***

Стан та перспективи реформування сектору безпеки і оборони України : матеріали міжнар. наук.-практ. конф., 24 листоп. 2017 р. - Київ, 2017. - Т. 2. - 161 с.

Зі змісту:

- Бараненко Р.В., Поточняк М.І. До питання протидії кіберзлочинності в контексті забезпечення національної безпеки держави;
- Кондратюк М.В. Комп’ютерна безпека України в системі національної безпеки.

Шифр зберігання НБУВ: В357163/2.

***

Сучасні правові системи світу: тенденції та фактори розвитку : матеріали міжнар. наук.-практ. конф. (25 трав. 2017 р., м. Київ). - Київ, 2017. - 309 с.

Зі змісту:

- Грицун О.О. Концептуальний підхід до розуміння кіберзагроз.

Шифр зберігання НБУВ: ВА822942.

***

Яцишин М.Ю. міжнародно-правовий захист прав людини у кіберпросторі / М.Ю. Яцишин // Вісник Маріупольського державного університету. Серія : Право. - 2017. - Вип. 14. - С. 166-174.

Проаналізовано концептуальні підходи до розуміння кіберпростору. Досліджено основні міжнародні ініціативи в рамках міжнародних міжурядових організацій щодо захисту прав людини в кіберпросторі.

Шифр зберігання НБУВ: Ж73529/пр.

***

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.