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 2017

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В. І. Вернадського у 2017р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С. Дорогих. Дизайн обкладинки С.Дорогих.

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань ; упоряд. О. Довгань, Л. Литвинова, С. Дорогих ; Науково-дослідний інститут інформатики і права НАПрН України ; Національна бібліотека України ім. В.І. Вернадського. – К.: Видавничий дім «АртЕк», 2017. – № 9 (вересень) . – 66 с.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

ЗМІСТ

Правове забезпечення кібербезпеки

«Подписанный на прошлой неделе Президентом Петром Порошенко Указ об усилении кибербезопасности развяжет руки проверяющим органам и поможет блокировать любой неугодный веб-ресурс…

Предлагается создать некий единый государственный центр управления сетями связи, который будет контролировать все в стране.

Между тем, нет сомнений, что его имплементация повлияет на отношение госструктур к информации, и подстегнет самих операторов к внедрению комплексной системы защиты информации (КСЗИ), утвержденной Госспецсвязью.

Кабмин должен разобраться в ситуации, согласно Указу Президента, в трехмесячный срок, и отрегулировать вопрос с закупкой услуг доступа к сети интернет посредством КСЗИ. Все это выльется в удорожание услуг интернет-провайдеров по доступу к сети через КСЗИ…» ***(Украинские власти смогут отключать любой неугодный сайт – эксперты // Файненс.ЮА (http://news.finance.ua/ru/news/-/409774/ukrainskie-vlasti-smogut-otklyuchat-lyuboj- neugodnyj-sajt-eksperty).- 04.09.2017).***

***

«…В пятницу, 7 сентября, парламент так и не рассмотрел законопроект о кибербезопасности, который депутаты подготовили к повторному второму чтению… Законопроект, напомним, определяет основные термины в сфере кибербезопасности и полномочия органов власти в сфере контроля за ней. Основную политику формирует и реализует Кабмин, но немалая роль отводится также президенту, СНБО, СБУ, разведке, военным, НБУ и правоохранителям. А вот у генпрокурора ко второму чтению функцию контроля в сфере кибербезопасности отобрали.

Исчезли и другие спорные пункты: например, согласно прошлой версии закона, Украина могла преследовать на своей территории лиц, причастных к киберпреступлениям, в том числе когда они планировались или были совершены за пределами Украины, но наносят ущерб нашему государству. Очевидно, пункт был недостаточно согласован с международными договорами…

Закон, несмотря на опасения, не предусматривает контроля за личными переписками, блогами и частными веб-ресурсами. Кроме того, государство обещает не трогать и информацию, циркулирующую в локальных сетях, не подключенных к интернету. Также закон запрещает сужение прав одних людей в сравнении с другими (например, право на тайну переписки). Это прямо прописано в документе. Правда, там же указано, что поводом для исключений может стать информация, которая должна быть защищена согласно закону…

…в силе остается поправка депутата от «Народного фронта» Руслана Лукъянчука, которая смущает украинских медийщиков. В частности, она вводит понятие «технологическая информация». Согласно документу это документированные сведения о составе, количественные и качественные показатели, особенности технологических процессов предприятий в различных отраслях хозяйства, данные автоматизированных систем на таких объектах…
По сути, несмотря на логичность поправки с точки зрения безопасности, она ограничивает возможности сбора и распространения информации о производстве, состоянии инфраструктуры — от дорог и объектов ЖКХ до функционирования транспорта и ситуации в АТО…

Еще один момент, за который эксперты критикуют закон, — отсутствие единого ответственного органа за все процессы по киберзащите. Хотя и предполагается создать специальную комиссию Кабмина в сфере кибербезопасности, в списке тех, кто контролирует процессы, — президент (через СНБО с Национальным координационным центром кибербезопасности), Кабмин, центральные и местные органы власти, правоохранители, разведка и контрразведка, СБУ, НБУ и команда реагирования на компьютерные чрезвычайные события CERT- UA...

Весь этот широкий перечень оставляет страну без единого ответственного органа, который будет оперативно командовать отражением глобальной кибератаки (все помнят вирус "Петя" и волну кибератак в Украине в декабре 2016 г.), поэтому вопрос глобальной кибербезопасности остается открытым…
Кположительным моментам закона стоит отнести логичный запрет на привлечение к мероприятиям по информбезопасности любые объекты под контролем страны-агрессора или лиц, в отношении которых государством введены санкции. Также закон ограничивает использование услуг таких лиц для усиления кибербезопасности госсайтов и других объектов. Минобороны и Генштабу тем временем будет поручено подготовиться к отражению военной агрессии в киберпространстве и работать в этом направлении вместе с НАТО. Также они должны будут разработать механизмы функционирования информсистем в условиях военного положения.

Очевидно, что при всех поправках закон нуждается в доработке, хотя и не создает возможностей для тюремных сроков за блог или репост в соцсети, как это происходит в России. Тем не менее возможности для засекречивания информации объектов инфраструктуры, прописанные недостаточно четко, могут позволить власти скрыть коррупционные схемы, некачественную работу и аварии…» ***(Александра ЗАХАРОВА. Совершенно секретно. За что критикуют законопроект о кибербезопасности// DsNews (http://www.dsnews.ua/society/kiberzakon-sbu-tayno-proverit-zavody-a-vlast-zasekretit- 11092017220000).- 12.09.2017).***

***

«Аналіз проекту постанови Кабінету Міністрів України «Про

реалізацію і моніторинг ефективності персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» (далі - ППКМУ).

…метою державного регулювання ППКМУ є визначення механізму блокування (обмеження) операторами, провайдерами телекомунікацій доступу споживачів телекомунікаційних послуг до інформаційних ресурсів (інформаційних сервісів) та способу моніторингу такого блокування (обмеження)…

Визначення ППКМУ завдань й повноважень органам влади та додаткових обов'язків суб'єктам господарювання не відповідає вимогам Конституції та Законам України.

ППКМУ не створює законної системи державного регулювання зазначеного питання та не відповідає вимогам державної регуляторної політики у сфері господарської діяльності, яка повинна бути спрямована на вдосконалення правового регулювання господарських відносин, а також адміністративних відносин між регуляторними органами або іншими органами державної влади та суб'єктами господарювання, недопущення прийняття економічно недоцільних та неефективних регуляторних актів, зменшення втручання держави у діяльність суб'єктів господарювання та усунення перешкод для розвитку господарської діяльності, що здійснюється в межах, у порядку та у спосіб, що встановлені Конституцією та законами України…

Висновок:

-новації ППКМУ не відповідають нормам та положенням Конституції та законодавства України, Конвенції про захист прав людини і основоположних свобод, рішенням Європейського суду з прав людини, Угоді про Асоціацію та європейському вибору України тощо;

-є черговою спробою посилити адміністративний тиск на український бізнес;

-несуть в собі потенційні загрози правової невизначеності та зловживань;

-повторюють аналогічні норми «диктаторського закону» від 16-го січня 2014 року, прийнятих злочинною владою та скасованих завдяки Революції Гідності стосовно блокування ресурсів без рішення суду та безперешкодного доступу до будь-якої інформації через ТЗ, що передбачається придбати» ***(Іван Пєтухов. Аналіз проекту постанови КМУ щодо санкцій до провайдерів, котрі проти цензури // Конфликты и законы (http://k- z.com.ua/ukrayna/43932-analiz-proektu-postanovi-kmu-shchodo-sankciy-do- provayderiv-kotri-proti-cenzuri).- 15.09.2017).***

***

«Президент Петр Порошенко подписал указ № 278/2017 «О решении Совета национальной безопасности и обороны Украины от 13 сентября 2017 года «О предложениях к проекту закона Украины «О Государственном бюджете Украины на 2018 год» по статьям, связанным с обеспечением национальной безопасности и обороны Украины»…

Глава государства ввел в действие соответствующее решение СНБО.

Контроль за его выполнением возложен на секретаря Совета национальной безопасности и обороны Украины Александра Турчинова.

В 2018 году должны быть приняты меры по обеспечению первоочередного финансирования деятельности субъектов сектора безопасности и обороны Украины по следующим приоритетным направлениям: усиление системы противовоздушной обороны государства и возможностей авиации Воздушных сил Вооруженных сил Украины; реализация государственной политики в сфере кибербезопасности, выполнение мероприятий по развитию и модернизации специальной связи и защиты информации; выполнение Национальной разведывательной программы на 2016– 2020 годы; усиление контрразведывательной защиты, борьбы с терроризмом и диверсионной деятельностью; проведение интенсивной боевой подготовки частей и подразделений ВСУ и других образованных соответственно законам Украины военных формирований; обустройство государственной границы Украины; реализация социальных гарантий военнослужащих, прежде всего увеличение в структуре денежного обеспечения военнослужащих удельного веса должностных окладов, окладов по воинским званиям.

Правительству поручено подготовить в десятидневный срок после вступления в силу законом Украины «О Государственном бюджете Украины на 2018 год» проект основных показателей государственного оборонного заказа на 2018–2020 годы и представить на рассмотрение Совету национальной безопасности и обороны Украины…» ***(Порошенко ввел в действие решение СНБО относительно предложений к госбюджету по обеспечению нацбезопасности // Капитал (http://www.capital.ua/ru/news/98552-poroshenko-vvel-v-deystvie-reshenie-snbo-otnositelno-predlozheniy-k-gosbyudzhetu-po-obespecheniyu- natsbezopasnosti#ixzz4t7sJQ0No).- 15.09.2017).***

***

«У новому політичному сезоні Верховна Рада має намір зайнятися питаннями кібербезпеки.

Влітку народні депутати зареєстрували два законопроекти, майже ідентичні, щодо протидії загрозам національній безпеці в інформаційній сфері…

Депутати ініціювали впровадження принципу тимчасового блокування сайтів терміном до двох діб (за ініціативою прокурора чи слідчого), або ж на два місяці (за рішенням суду). Законопроект № 6688 передбачає тимчасове блокування без обмежувального строку в два місяці.

Втім громадські організації виступили проти їх ухвалення, оскільки це може становити загрозу вільному інтернету. У липні 2017-го низка медійних громадських організацій висловила протест проти законопроектів 6676 і 6688, вимагаючи їх відкликати як такі, що ставлять під загрозу вільний розвиток інтернету…

У Києві, 15 вересня, відбулася дискусія навколо вищезгаданих законопроектів, у якій взяли участь представники громадських організацій, проте народні депутати не змогли бути присутніми. Фахівці обговорили ризики, які несе ухвалення цих законопроектів...» ***(Чи узаконить Рада загрозу інтернет-свободі // Pingvin.Pro (https://pingvin.pro/gadgets/news-gadgets/chy-uzakonyt-rada-zagrozu-internet- svobodi.html).- 19.09.2017).***

***

«…Государственная служба специальной связи и защиты информации (Госспецсвязи) разработала изменения в ряд законов, которыми предусматривается обязательная регистрация абонентов мобильной связи, их номеров и SIM-карт, а также регистрация телефонов, планшетов, смартфонов и других подобных устройств по их международному классификатору, так называемому IMEI-коду. Проще говоря, по номеру абонента и коду устройства мобильной связи можно будет установить его владельца, поскольку SIM-карта и устройство будут регистрироваться по паспорту или иному документу, удостоверяющему личность…

Законопроект о внесении изменений в законы «О телекоммуникациях» и «О радиочастотном ресурсе» разработан во исполнение протокольного поручения некоего «комитета по кибербезопасности СНБО». Непонятно, что это за «комитет» такой, и насколько серьезно следует относиться к его «ценным указаниям».

Профильный регулятор в лице Национальной комиссии регулирования в сфере связи и информатизации (НКРСЗИ) поддержал инициативу по введению идентификации всех абонентов мобильной связи…

В качестве причины этой новации называют, естественно, борьбу с агрессором, преступностью и терроризмом. Инициаторы законопроекта утверждают, что введение предлагаемых мер резко повысит эффективность борьбы с киберпреступлениями, экономическими преступлениями в банковской сфере и с террористическими угрозами. По мнению авторов документа, принятие норматива приведет к сокращению «мобильного мошенничества» и преступлений в банковской сфере, а также будет способствовать ведению бизнеса в условиях «цифровой экономики». Чиновники утверждают, что регистрация по паспортам мобильных средств связи и SIM-карт увеличит уровень национальной безопасности и обороны страны, позволит предотвращать киберугрозы, в том числе кибератаки на критически важные объекты и системы. Кроме того, по мнению авторов норматива, регистрация телефонов, смартфонов и прочих подобных устройств сократит количество их краж.

Зарегистрироваться должны будут не только новые, но и уже действующие абоненты. Правда, в нормативе ничего не говорится о последствиях, которые наступят в случае, если действующий абонент не

зарегистрируется…

Предлагаемые новации вызывают резкое неприятие у операторов мобильной связи. Главным камнем преткновения являются, прежде всего, сроки перерегистрации абонентов pre-paid.

Например, в пресс-службе мобильного оператора Vodafone, который имеет почти 21 млн абонентов, утверждают, что для перерегистрации потребуется минимум один год, а реально два года. Примерно то же говорят в компании Киевстар, обслуживающей более 23 млн абонентов. В обеих компаниях подчеркивают: возникает огромный риск того, что значительная часть абонентов не успеют зарегистрироваться, и они останутся без связи…

Как и любой запрет, регистрация мобилок и SIM-карт открывает широкие возможности для злоупотреблений и коррупции.

Прежде всего, будет однозначно спровоцирована регистрация аппаратов и SIM-карт на подставных лиц по аналогии с регистрацией фирм на подставных учредителей и директоров….

Возникает и масса проблем к связи с сохранностью баз данных, особенно с учетом военного времени…

Что же касается предотвращения воровства, то едва ли в случае кражи мобилок, полиция в нынешних условиях будет гоняться за ворами…

Вместе с тем, если телефон украли, и с этого телефона совершены противоправные деяния, то у официального владельца, на которого он зарегистрирован, могут возникнуть большие проблемы, если он вовремя не заявил о пропаже или заявил, но операторы-регистраторы не совершили необходимых действий, например, не заблокировали трубку…» ***(Александр Карпец. Мобилка по справке от венеролога? // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/188434-mobilka_po_spravke_ot_venerologa).- 01.09.2017).***

***

Організаційне забезпечення захисту інформації

«Стремительное распространение Интернета вещей приводит к возрастанию рисков, связанных с безопасностью… рассмотрим три утверждения о безопасности IoT…

Безопасность должна быть предусмотрена на уровне проектирования дизайна новых устройств, решений и технологий. Если создавать решения на изначально безопасной платформе – мы сможем избавиться от целого ряда классических проблем и уязвимостей…

Необходимо внедрять SDL для всех этапов разработки новых технологий, а также регулярно проводить исследования безопасности продуктов и технологий с привлечением сторонних команд по аудиту. Безопасность должна быть в основе всего, что только появляется, планируется или модернизируется.

В существующих сетях со smart- и IoT-решениями необходимо

разграничивать и отделять непроверенные и непротестированные решения от продуктовых сетей. Например, не стоит включать умную кофеварку в общую сеть на промышленном предприятии…

Безопасность должна быть частью жизненного цикла разработки любого продукта. Серьезные решения и технологии уже имеют внедренные циклы безопасной разработки. Но большинство новых современных решений и технологий появляются как стартапы, где основная идея заключается далеко не в безопасности.

…мы должны видеть шаги со стороны государства по вопросам регулирования безопасности в IoT. С другой – внутреннюю ответственность производителя перед потребителем. Нельзя допускать глупых ошибок, которые приводят к возникновению критичных уязвимостей в устройствах, собирающих информацию об активности в Интернете.

Решением будет слаженное взаимодействие и диалог регуляторов и производителей IoT/Smart-устройств и технологий…» ***(Что следует знать о кибербезопасности и Интернете вещей // SecurityLab.ru (http://www.securitylab.ru/news/488259.php).- 06.09.2017).***

***

«Согласно последнему исследованию CSFI Insurance Banana Skins 2017, основными рисками, стоящими перед страховыми компаниями, стали технологические изменения и кибербезопасность…

Вместе с беспокойством (как по поводу атак на самих страховщиков, так и по поводу стоимости страхования киберпреступлений) нарастает необходимость работать с киберугрозами. Еще одной важной проблемой является внутренняя технологическая оснащенность страховщиков для конкуренции в секторе InsurTech.

Анализ компании GlobalData показал, что безопасность должна быть обязательным и постоянным элементом в управлении страховым бизнесом. Предусмотрительные страховщики уже разворачиваются в сторону комплексной модели кибербезопасности, которая не только укрепляет их текущее положение, но и предусматривает возможность направить изменения на стратегическую составляющую.

Кибербезопасность требует переустановки кадров, процессов и технологий на выявление, предсказание и предотвращение угроз. Инвестирование исключительно в технологии не может защитить от всех кибернарушений, с которыми сталкиватюся страховые компании.

Вплане поддержки много могут предложить вендоры. Поставщики услуг и те, кто может похвастать локальным центром операций по обеспечению безопасности (Security Operation Center, SOC) для глобальных игроков, находятся в особенно хорошем положении.

Комплексная модель кибербезопасности должна опираться на эти ключевые области:

· Соответствие инвестиций в безопасность и бизнес-модели: Имеется в виду не только учет и регистрация каждого отдельного инвестиционного решения по стратегическим бизнес-целям страховщика, но и отслеживание частоты и значительности инцидентов для создания паттернов, которые могут быть предвосхищены в будущем.
· Создание одинакового уровня прочности защиты по всей системе обмена данными страховой компании: Строгая политика безопасности может распределить
иснизить риски.
·Постоянное и эффективное распределение финансирования: Не понимая диапазон решений, уже доступных для противостояния сетевым угрозам, страховщики не могут инвестировать разумно.

Вендоры могут консолидировать и направлять усилия страховщиков, представляя им решения для аутентификации личности и биометрии, сегментации сети, когнитивной сетевой аналитики, а также комплексные услуги по безопасности…

Согласно исследованию брокера FWD, несмотря на атаку вируса WannaCry, резкого подъема интереса к киберстрахованию не возникло. Недавний опрос 250 страховых брокерских фирм Великобритании, проведенный после атаки, выяснил, что было совсем небольшое увеличение спроса на страховку, покрывающую киберугрозы…» ***(Почему кибербезопасность должна быть в приоритете у страховщиков // Rusbase (https://rb.ru/story/cybersecurity-in-insurance/).- 07.09.2017).***

***

«Половина промышленных предприятий в мире испытывает не достаток в квалифицированных специалистах, способных обеспечить киберзащиту их производственных инфраструктур и автоматизированных систем управления технологическими процессами (АСУ ТП)…

Эти выводы были получены в результате исследования «Лаборатории Касперского», в котором приняли участие более 350 представителей индустриальных организаций по всему миру, включая Россию.

Недостаток кадров ощущается не только внутри, но и вне компаний. 48% участников исследования подтвердили, что найти надежного партнера, который сможет построить эффективную систему защиты АСУ ТП, не так-то просто. И более трети респондентов (39%) отметили, что владельцы и операторы промышленного оборудования также недостаточно хорошо осведомлены о киберугрозах и связанных с ними рисках для индустриальных предприятий.

Пытаясь решить существующую кадровую проблему, компании с готовностью инвестируют в образование своих сотрудников, партнеров и подрядчиков, стремясь повысить их уровень знаний об информационных угрозах. Подобная практика входит в пятерку наиболее популярных и эффективных мер обеспечения информационной безопасности

производственных инфраструктур…

Вместе с тем исследование показало, что предприятия рассматривают процесс создания системы информационной безопасности как комплекс различных мер. Среди них в приоритете большинства компаний (67%) – использование специализированных защитных решений для устройств, являющихся частью промышленной инфраструктуры. Помимо этого, многие предприятия подчеркивают необходимость внедрения технологии для мониторинга сети и анализа событий (62%) и контроля подключаемых устройств (61%). Поиску и закрытию уязвимостей, атакже предотвращению вторжений уделяют внимание меньше компаний – 46% и 45% соответственно…» ***(На индустриальных предприятиях не хватает ИБ-специалистов // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5435923-Na- industrialnyx-predpriyatiyax.html#ixzz4s4fczyNr).- 08.09.2017).***

***

«23 сентября во Дворце студентов (ул. Пушкинская, 88) стартовал форум по кибербезопасности HackIT-2017.

В нем принимали участие разработчики, системные администраторы, а также другие специалисты в сфере IT. Всего мероприятие посетило около 1000 человек.

В рамках форума харьковчане могли послушать более 20 докладов (hacking, бизнес, финансы), протестировать новые сайты, принять участие в викторине, а также взломать программное обеспечение с разрешения их создателей…

Организатор форума Никита Кныш рассказал о главной цели HackIT-2017, а также о том, какие компании чаще всего подвержены хакерским атакам.

«Чаще всего кибератакам подвержен финансовый сектор. Чтобы защититься от них, следует обратиться в нашу компанию или нанять фрилансеров, которые специализируются в этой области», - отметил Никита Кныш.

Также он напомнил, что "черные" хакеры взламывают софт ради собственной выгоды, а "белые" хакеры действуют в интересах компании, передавая ей данные об уязвимостях системы…

Также мероприятие посетили специалисты из Америки и Швейцарии, которые поделились своим практическим опытом с харьковчанами.

«С "черными" хакерами очень сложно сотрудничать, но сейчас мы привлекаем их к работе в наших организациях. В этой сфере работает много украинцев…», - сказал американский бизнесмен, основатель проекта Cryptoseal Райан Лэки…

Он рассказал, что американские правительственные организации нанимают специалистов, которые взламывают систему, чтобы оценить насколько она уязвима.

Кроме того он подчеркнул, что основная проблема Украины заключается

в том, что наши специалисты не получают достаточной финансовой мотивации.

Еще один специалист Алекс Бреннен, который приехал из Швейцарии, рассказал о том, как в их стране борются с кибератаками.

«В первую очередь перекрываются потоки денег. Затем применяется обратный инжиниринг (исследование программы, цель которого - понять принцип ее работы). Благодаря этому можно узнать, каким образом человек получает деньги и куда они передаются дальше", - сообщил Алекс Бреннен…

Алекс Бреннен посоветовал будущим украинским специалистам в области кибербезопасности изучать программирование и операционную систему Linux. Также очень полезным для них станет изучение программ с открытым исходным кодом.

Одним из ярких событий HackIT-2017 стала презентация криптовалюты Hacken. 1 хакен равняется 1 доллару, а в дальнейшем монета будет расти. Каждый расчет будет делать валюту более дорогой.

Хакены созданы не только для хакеров, но и для тех, кто пользуется услугами в сфере кибербезопасности.

Hacken - инструмент, который позволит хакерам зарабатывать…» ***(На выходных харьковчане тестировали новые сайты и взламывали программы // 057.ua - Сайт города Харькова (https://www.057.ua/news/1804908).- 24.09.2017).***

***

«21 вересня 2017 року у приміщенні Торгово-промислової палати України відбулось друге засідання Антикризового центру кібернетичного захисту бізнесу при ТПП України.

Учасники заслухали інформацію голови Центру Володимира Коляденка про проведені заходи з організації роботи Центру, розглянули проект плану заходів на 2017-2018 рр., стан нормативно-правового забезпечення з питань кібербезпеки в Україні та правові аспекти запобігання і недопущення наслідків кібератак.

Серед плану заходів Центру – налагодження взаємодії з державними інституціями щодо питань інформаційної та кібербезпеки; проведення консультацій, освітніх, наукових і виставкових програм, конференцій, форумів та симпозіумів; проведення аудиту існуючих стандартів і технічних регламентів з питань кібербезпеки; підготовка базових рекомендацій щодо кібербезпеки; надання консультацій з питань інформаційної безпеки; аналіз інцидентів у галузі кібербезпеки та інші…» ***(На заседании Антикризисного центра по киберзащите бизнеса обговорили план действий по предупреждению кибератак // TRISTAR.com.ua - твой финансовый навигатор! (http://tristar.com.ua/1/news/na_zasedanii_antikrizisnogo_tsentra_po_kiberzashite_biznesa_obgovorili_plan_deistvii_po_preduprejdeniu_kiberatak_8010.html).- 25.09.2017).***

***

«Эксперты из компании Armis выявили ряд уязвимостей более чем в 8 миллиардах устройств, имеющих поддержку Bluetooth. Исследователи назвали этот комплекс уязвимостей BlueBorne…

Уязвимости присутствуют в реализациях Bluetooth в операционных системах Android, iOS, Linux и Windows…

Три уязвимости BlueBorne охарактеризованы экспертами как критические. С их помощью киберпреступники могут захватить контроль над устройством, запустить вредоносный код и провести атаку типа man-in-the-middle. Как утверждают эксперты, ранее уязвимости в Bluetooth фиксировались, прежде всего, на разных уровнях протокола связи, но BlueBorne присутствует в реализации протокола и дает возможность захватывать полный контроль над устройством, обходя различные процедуры аутентификации…» ***(Свыше 8 миллиардов устройств с поддержкой Bluetooth являются уязвимыми // SecureNews (https://securenews.ru/blueborne/).- 13.09.2017).***

***

«…Компания Fortinet была ранним усыновителем искусственного интеллекта (ИИ), используя его для классификации вредоносного ПО, обучения машин для анализа продвинутых атак и создания более умных защитных механизмов для повышения защиты. С ростом спектра угроз компания Fortinet предоставляет инструменты организациям любого размера, чтобы идти в ногу с киберпреступниками…

…Fortinet продолжает внедрять новые усовершенствованные инструменты, помогающие обнаруживать, смягчать и предотвращать быстрые угрозы. Например, их Anti-Exploit Engine (AEE) фокусируется только на образцах, которые на самом деле преуспевают в использовании уязвимости, тем самым уменьшая количество «ложных срабатываний», которые могут замедлить традиционные системы безопасности. Чтобы ускорить этот процесс, разработали метод, известный как AutoCPRL (Content Recognition Language), который предназначен для семейств вредоносных программ, иногда более 200 000 вариантов, с одной сигнатурой CPRL, снижая требования к хранилищу и сверхзарядную пропускную способность.

Именно этим Fortinet отличается от других поставщиков безопасности. Используя свои собственные кластеры ANN (искусственная нейронная сеть) для глубокой проверки и обнаружения, запатентованные системы когнитивного искусственного интеллекта для анализа, машинного обучения для создания динамических алгоритмов и, в конечном счете, защиты от машин для защиты от передовых постоянных угроз (ATP) и усовершенствованные методы уклонения (AET), Fortinet строит и обеспечивает глубокую защиту мирового

класса…

Это всего лишь несколько нововведений, которые теперь защищают более 255 000 клиентов по всему миру» ***(Интеграция искусственного интеллекта в кибербезопасность // СОВИТ (http://www.sovit.net/news1/is_news/integraciya_iskusstvennogo_intellekta_v_kiber bezo pasnost/).- 04.09. 2017).***

***

«Врамках форума New Mobility World / IAA 2017 во Франкфурте «Лаборатория Касперскогоinfo-icon» и компания AVL представили прототип модуля безопасного соединения (Secure Communication Unit – SCU) для современных умных автомобилей. Это совместное решение обеспечит защиту всех коммуникаций между различными компонентами, а также самим автомобилем и внешней инфраструктурой, что позволит продумывать кибербезопасность транспорта еще на стадии проектирования…

В основе решения лежит безопасная операционная система KasperskyOS, запрещающая любую незапланированную активность. Другими словами, даже если вредоносный код каким-то образом попадет внутрь SCU-модуля, он просто не сможет быть выполнен, поскольку его функциональность не предусмотрена в системе. В свою очередь, все коммуникации и сценарии взаимодействия различных автомобильных компонентов между собой и внешней средой регулируются с помощью системы Kaspersky Security Systeminfo-icon. Она же обеспечивает защиту всех соединений благодаря алгоритмам шифрования и аппаратным возможностям…

Также для автопроизводителей могут быть созданы уникальные SCU-модули, исходя из конкретных аппаратных и программных компонентов и требований…» ***(ЛК и AVL представили модуль для киберзащиты автомобилей // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-09-18-3/24100).- 18.09.2017).***

***

«Управление перспективных исследовательских проектов (DARPA) Минобороны США разработает эксплойты, которые отыщут вирусы в публичных сетях и получат доступ к заражённым компьютерам.

Согласно документам DARPA, занимающегося проектом борьбы с вредоносным ПО по заданию Пентагона, его специалисты планируют получить доступ к зараженным компьютерам через написанную специально для этого программу-эксплойт, которую эксперты по кибербезопасности назвали «противоботнетный вирус». Проверке подвергнутся 80% всех мировых открытых IP-адресов на наличие вредоносного программного обеспечения.

По плану американских властей, программа будет обнаруживать зараженные компьютеры, проникать на них и удалять вредоносное ПО. Проект расчитан на четыре года...» ***(Пентагон проверит 80% всех мировых IP на наличие***

вредоносных программ // РосКомСвобода (https://rublacklist.net/31632/).- 01.09.2017).

***

«Системы отопления, вентиляции и кондиционирования (ОВК или HVAC) могут использоваться хакерами в качестве моста, соединяющего физически изолированные компьютеры с внешним миром. С помощью систем ОВК злоумышленники могут отправлять команды вредоносному ПО, заранее внедренному в изолированную сеть.

Ученые из университета имени Бен-Гуриона в Негеве (Израиль) представили атаку HVACKer и разработали PoC-код вредоноса для ее осуществления. Вредоносная программа способна взаимодействовать с датчиками температуры компьютера и с их помощью улавливать температурные колебания, которые затем переводятся в двоичный код. Заранее внедренный в изолированную от интернета сеть код фиксирует изменения температуры, спровоцированные системами ОВК, и конвертирует их в команды для выполнения…

Для осуществления атаки злоумышленнику прежде всего нужно найти систему ОВК, либо подключенную к интернету, либо находящуюся в подключенной к интернету внутренней сети. Обнаружив подходящую систему ОВК, атакующий должен ее взломать (например, проэксплуатировав известные уязвимости).

Следующий этап атаки предполагает создание кастомизированного вредоносного ПО, способного улавливать провоцируемые взломанной системой ОВК температурные колебания. Программа должна быть установлена в физически изолированную сеть… Установив ПО, атакующий может изменять температуру с помощью подконтрольной ему системы ОВК и отправлять вредоносу нужные команды.

Атака HVACKer подходит лишь для отправки команд вредоносному ПО внутри изолированной сети, но не для похищения данных. Датчики компьютеров способны улавливать температурные изменения, но датчики систем ОВК недостаточно чувствительны для того, чтобы получать данные путем измерения колебаний тепла компьютеров. Лучшее время для осуществления атаки – ночь, поскольку отсутствие людей позволит ей пройти незамеченной» ***(Системы отопления, вентиляции и кондиционирования могут использоваться в атаках на изолированные системы // "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=118780).- 21.09.2017).***

***

«Информационные сети Пентагона.

…Оборонная информационная сеть США DISN (Defense Information Systems Network) разрабатывалась с начала 1990-х гг. Назначение этой

глобальной сети – предоставлять услуги передачи различных видов информации (речь, данные, видео, мультимедиа) для эффективного и защищенного управления войсками, связью, разведкой и радиоэлектронной борьбой (РЭБ).

В1996 г. был утвержден план стратегического развития военных ведомств США на 15-летний период Joint Vision 2010. В ходе выполнения этого плана вскрылось множество недостатков DISN, прежде всего – низкий уровень интеграции входящих в нее многих сотен сетей, который существенно ограничивал взаимодействие в рамках единой сети и препятствовал эффективному управлению всеми ее ресурсами…

Кроме того, используемые сетевые технологии не были достаточно масштабируемыми и не могли в должной мере предоставлять пропускную способность по требованию. Из-за отсутствия общей архитектуры и стандартов затруднялась передача данных в интересах разведки и РЭБ. Несовместимость оборудования усложняла применение различных средств засекречивания и криптозащиты. В целом базовая архитектура DISN была недостаточно гибкой и масштабируемой, особенно для мобильных сил, оперативно развертываемых в различных точках мира.

Возник принципиальный вопрос: на базе какой технологии строить DISN далее?

…В условиях технологической неопределенности было решено строить военные сети связи США с использованием «открытой архитектуры» и программно- аппаратных средств коммерческого назначения (Commercial-Off-the-Shelf). Выбор пал на «старые» разработки Bell Labs, точнее, на протокол телефонной сигнализации SS7 и на интеллектуальную сеть (Advanced Intelligent Network, AIN)…

Сигнализация SS7 (Signaling System № 7, или ОКС-7, общий канал сигнализации № 7) является, образно говоря, нервной системой сети связи. Это набор сигнальных телефонных протоколов, используемых для установления телефонных соединений по всему миру… Основная особенность SS7 состоит в том, что передача сообщений о требованиях по установлению телефонных соединений вынесена в отдельный сигнальный канал…

В 2011 г. компания Tekelec проводила тестирование сети SS7 в составе DISN. Соединения на этой оборонной сети устанавливаются при помощи сигнализации SS7, т.е. в «сердцевине» сети находится сеть SS7 в полном объеме, а на периферии используются различные устройства любого типа. В основном это IP-оборудование (телефоны для четырехпроводных каналов, VoIP или ISDN BRI, устройства видеоконференцсвязи и т.д.), которое может подключаться по любым протоколам, включая нестандартные (proprietary).

Отсюда делаем важный вывод: наличие сети SS7 не препятствует переходу на IP-протокол, а скорее наоборот – облегчает переход на пакетную коммутацию, делает его постепенным…

Переход на IP-протокол означает замену системы сигнализации SS7

протоколом SIP (Session Initiation Protocol)…

SIP-протокол описывает способ установления и завершения интернет-сеанса, включающего обмен мультимедийным контентом (видео- и аудиоконференции, мгновенные сообщения, онлайн-игры)…

Главные недостатки протокола SIP – трудности обеспечения секретности (в условиях кибервойны) и обслуживания приоритетных вызовов, что важно для военных применений и экстренных служб. Поэтому по заказу Минобороны США был разработан защищенный протокол AS-SIP. Он получился очень громоздким: если «обыкновенный» SIP использует 11 стандартов RFC, то в AS-SIP задействовано почти 200 стандартов RFC…

Переход от сети коммутации каналов, где господствует протокол SS7, к коммутации пакетов и протоколу SIP (точнее, к AS-SIP) требует установки программных коммутаторов SoftSwitch, которые будут выполнять две важные функции: управлять согласованием протоколов сигнализации SIP и SS7 (посредством шлюза SGW) и преобразованием IP-пакетов в TDM-посылки (посредством шлюза MGW). В Министерстве обороны США разработаны детальные методические материалы по внедрению AS-SIP. Однако когда именно сеть DISN окончательно перейдет на протокол AS-SIP, предсказать трудно» ***(Манфред ШНЕПС-ШНЕППЕ. Информационные сети Пентагона: готовясь к кибервойне // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/articles/5434120- Informacionnye-seti-Pentagona-gotov.html).- 05.09.2017).***

***

Національна система кібербезпеки

«Кабмин в трехмесячный срок должен урегулировать вопрос о запрете госорганам, предприятиям, учреждениям и организациям государственной формы собственности закупать услуги (заключать договора) по доступу к сети Интернет у операторов (провайдеров) телекоммуникаций, у которых отсутствуют документы о подтверждении соответствия системы защиты информации установленным требованиям в сфере защиты информации.

Также перед Правительством стоит задача ввести в установленном порядке в рамках развития государственно-частного партнерства механизм привлечения физических и юридических лиц на условиях аутсорсинга к выполнению задач киберзащиты государственных электронных информационных ресурсов.

Правительство вместе с СБУ должно подготовить и представить на рассмотрение Парламента законопроект о разграничении уголовной ответственности за преступления в сфере использования компьютеров, систем и компьютерных сетей и сетей электросвязи, совершенные в отношении государственных и других информационных ресурсов, в отношении объектов

критической информационной инфраструктуры и других объектов, а также соответствующего разграничения подследственности…

НБУ с участием Администрации Госспецсвязи и СБУ рекомендуется безотлагательно принять меры, направленные на совершенствование киберзащиты системно важных банков Украины.

СНБО также поручил Кабмину проработать вопрос относительно определения Госспецсвязи органом, ответственным за сохранение резервных копий информации и сведений государственных электронных информресурсов, а также по установлению порядка передачи, хранения и доступа к этим копиям. Соответствующее решение СНБО об усилении мер по кибербезопасности государства введено в действие Указом Президента № 254/2017» ***(Введено в действие решение СНБО по защите от кибератак // Інформаційне агентство "ЛІГА:ЗАКОН"(http://jurliga.ligazakon.ua/news/2017/8/31/163845.htm).- 31.08.2017).***

***

«Секретарь СНБО Александр Турчинов назвал приоритетные направления в оборонной сфере, которым будет уделено особое внимание…

«По решению СНБО, объем финансирования бюджета обороны и безопасности в следующем году будет на уровне 163 млрд 268 млн грн, из них 156 млрд 893 млн грн - из общего фонда, и 6 млрд 375 млн грн - из специального», - сказал Турчинов…

«Кроме того, учитывая ситуацию с безопасностью, приоритетами будут реализация государственной политики в сфере кибербезопасности, выполнение мероприятий по развитию и модернизации специальной связи и защиты информации; выполнения Национальной разведывательной программы на 2016- 2020 годы; усиление контрразведывательной защиты и борьбы с терроризмом и диверсионной деятельностью», - отметил Турчинов…» ***(СНБО определил объем финансирования сферы обороны на 2018 г. // Информационное агентство ЛІГАБізнесІнформ (http://news.liga.net/news/politics/14819771-snbo_opredelil_obem_finansirovaniya_sfery_oborony_na_2018_g.htm).- 13.09.2017).***

***

«Киберполиция формирует единую систему экстренного информирования в условиях ЧС…

Мобильный оператор lifecell разработал собственную систему экстренного информирования в условиях чрезвычайных ситуаций Emergency Notification System (ENS) и передал ее киберполиции.

Оператор утверждает, что система хорошо проявила себя во время

кибератаки Petya.A. После этого компания решила поделиться наработками с украинским государством. Новая система уже начала функционировать на базе киберполиции…

Планируется, что система оповещения будет объединять сотни государственных и даже частных компаний, которые имеют стратегическое значение…

В случае если одна из компаний сообщает о заражении своих систем неизвестным вирусом (или полиция получает данные о потенциальных кибератаках от правоохранителей других стран), информация за несколько минут передается всем лицам, которые отвечают за кибербезопасность в этих компаниях…

Система также позволяет контролировать, прослушан ли звонок, и регистрировать ответ от получателя. После рассылки сервис способен формировать отчет: сколько человек прочло или прослушало сообщение и какая была обратная связь…

Как сообщили в пресс-службах Киевстар и Vodafone, у них также есть похожие решения по киберзащите, которые работают внутри их компаний. Но о том, что они выведут их на рынок и будут конкурировать с lifecell, ничего пока не говорят…» ***(Кіберщит: как полиция создает общую систему экстренных оповіщений//Информационно-аналитическийцентр"ЛІГА" (http://biz.liga.net/all/telekom/stati/3710808-kibershchit-kak-politsiya-sozdaet-obshchuyu-sistemu-ekstrennykh-opoveshcheniy.htm).- 27.09.2017).***

***

«…Киберполиция сообщила о заражении одного из обновлений популярной программы «CCleaner», созданной для планового технического обслуживания своих систем.

О вирусе в программе киберполиция узнала 18 сентября от подразделения компании «Cisco Talos».

…версия программы «CCleaner» с вредной полезной загрузкой (5.33) была выпущена в период с 15 августа по 12 сентября 2017 года. Эта версия подписана с использованием действительного цифрового сертификата, который был выпущен компанией - разработчиком «Symantec Piriform Ltd». Поэтому пользователи при загрузке обновлений были уверены в надежности источника…

Согласно имеющейся информации Украину указанная атака миновала.

Сейчас специалисты киберполиции временно не рекомендуют использовать программное обеспечение «CCleaner» украинским пользователям, а советуют искать аналогичные продукты…» ***(Киберполиция предупреждает о заражении программы «CCleaner» // Інформаційнеагентство"ЛІГА:ЗАКОН"(http://jurliga.ligazakon.ua/news/2017/9/19/164536.htm).- 19.09.2017).***

***

Світові тенденції в галузі кібербезпеки

«Тенденции кибербезопасности в 2017 году: общая картина

…в этом году зафиксировано 301 известное нарушение, в результате которых были скомпрометированы и опубликованы 5 338 608 критичных записей. Из этих нарушений 166 были связаны с взломом и вредоносными программами…

Глядя на общую картину, видно, что ИТ-специалисты, профессионалы в сфере безопасности и бизнеса сталкиваются со следующими проблемами:

·К тому времени, когда они получают достаточный бюджет, чтобы приобрести технологию сетевой безопасности, которую они хотели (и нуждались) пять лет назад, она может быть как актуальной, так и уже не актуальной;

·Они тратят огромные средства на программное обеспечение, которое потом не внедряется и не используется;

·Чувствуют ли они себя комфортно, позволяя своим консультантам по вопросам безопасности и аудиторам получать доступ к их сетям или приложениям, чтобы полностью проверить системы на наличие уязвимостей и дыр;

·Какие изменения они вносят в свою документацию по безопасности, о которой никто не знает и не заботится.

Во многих ситуациях нет реального руководства в области безопасности, а это означает, что решения не принимаются…

Что касается оставшейся части 2017 года, скорее всего, ситуация останется прежней: вредоносные программы, потерянные или обнародованные записи и, возможно, еще одна крупная атака типа «отказ в обслуживании» (DDoS). История будет повторяться еще не один год…» ***(Главные тенденции кибербезопасности первого полугодия 2017 года // Security-News.Today (https://www.security-news.today/glavnye-tendentsii- kiberbezopasnosti-pervogo-polugodiya-2017-goda/).- 14.09.2017).***

***

«Краткий обзор главных событий в мире ИБ за период с 28 августа по 3 сентября 2017 года.

Большой резонанс на прошлой неделе вызвал взлом Instagram. Поначалу считалось, что инцидент затронул только знаменитостей, однако, как оказалось позже, неизвестные хакеры могли похитить учетные данные 6 млн пользователей соцсети. По данным «Лаборатории Касперского», причиной утечки стала уязвимость в мобильном приложении Instagram...

Производитель новых смартфонов Essential по ошибке допустил утечку данных своих клиентов. 29 августа на форуме Reddit появилось обсуждение

подозрительного письма, отправленного с серверов компании некоторым покупателям. В письме сотрудники Essential просили подтвердить заказ на телефоны и предоставить удостоверение личности – паспорт или водительские права. 30 августа основатель Essential Энди Рубин подтвердил наличие проблем с системой поддержки клиентов и принес свои извинения.

На сайте Pastebin был обнаружен список из более 33 тыс. полностью рабочих учетных записей для доступа по протоколу Telnet к устройствам «Интернета вещей» (IoT). Данные могут использоваться для создания ботнетов и осуществления масштабных DDoS-атак…

Особенно остро проблема безопасности IoT-устройств встала после обнаружения опасных уязвимостей в кардиостимуляторах производства компании Abbott. С их помощью находящиеся неподалеку от пациента злоумышленники могут «посадить» аккумулятор устройства или ускорить сердцебиение и нанести непоправимый вред здоровью жертвы. Управление по контролю за качеством пищевых продуктов и лекарств США объявило об отзыве 500 тыс. проблемных кардиостимуляторов. Пациенты с уже установленными устройствами должны обратиться к лечащему врачу для установки патча.

На прошлой неделе после временного затишья снова напомнила о себе APT- группировка Turla, связываемая с российским правительством. О возобновлении активности Turla сообщили сразу две ИБ-компании. Эксперты ESET обнатужили новый бэкдор Gazer, применяемый в шпионских кампаниях против посольств и консульств по всему миру…

Благодаря публикации на сайте WikiLeaks новой порции документов ЦРУ, стало известно об инструменте Wolfcreek, применяемом спецслужбой для взлома Windows XP и Windows 7.

Примечательно, на прошлой неделе жертвой хакеров стал сам сайт WikiLeaks. Киберпреступная группировка OurMine заявила об успешной кибератаке на ресурс, хотя на деле «взлом» оказался не более чем дефейсом…» ***(Обзор инцидентов безопасности за прошлую неделю // SecurityLab.ru (http://www.securitylab.ru/news/488214.php).- 04.09.2017).***

***

«Краткий обзор главных событий в мире ИБ за период с 11 по 17 сентября…

Начало прошлой недели ознаменовалось сообщением о восьми уязвимостях в реализациях Bluetooth для Android, iOS, Windows и Linux. Проблема, получившая название BlueBorne, затрагивает практически все Bluetooth-устройства (более 8 млрд) и позволяет злоумышленнику получить полный контроль над атакуемым гаджетом. Для эксплуатации BlueBorne не требуется ни участие пользователя, ни сопряжение с устройством. Единственное условие – включенный Bluetooth.

Во вторник, 12 сентября, компания Microsoft выпустила ежемесячные

обновления безопасности для своих продуктов, исправляющие 82 уязвимости, в том числе одну уязвимость нулевого дня. CVE-2017-8759 затрагивает программную платформу .NET Framework и уже используется хакерами в атаках. По данным экспертов FireEye, с ее помощью злоумышленники распространяют шпионское ПО FINSPY, также известное как FinFisher.

В ходе плановой проверки специалисты Kromtech Security Center обнаружили на серверах ElasticSearch вредоносное ПО для PoS-терминалов.

Как сообщают исследователи, более 4 тыс. серверов оказались заражены вредоносами AlinaPOS и JackPOS…

Исследователи безопасности из Sophos сообщили о новом Windows-трояне для удаленного доступа Kedi. Вредонос может скрывать свое присутствие от антивирусов, связываться с C&C-сервером через Gmail и похищать данные пользователей. Троян распространяется через фишинговые письма, содержащие вредоносную полезную нагрузку, маскирующуюся под утилиту Citrix.

В свою очередь, исследователи из Check Point сообщили о новом вредоносном ПО для Android, получившем название ExpensiveWall. Вредонос способен без ведома пользователя отправлять SMS-сообщения и снимать деньги со счета для оплаты доступа к премиум-сервисам на мошеннических сайтах. ExpensiveWall распространялся через Android-приложения, загруженные порядка 4,2 млн раз…

Специалисты компании Malwarebytes рассказали о недавних атаках, в ходе которых злоумышленники использовали действительные учетные записи LinkedIn для рассылки фишинговых ссылок через личные сообщения и электронную почту. Отличительной чертой данной кампании является использование хакерами взломанных доверенных учетных записей с хорошей репутацией. Среди прочих, злоумышленники также использовали скомпрометированные премиум-аккаунты, позволяющие общаться с другими пользователями LinkedIn (даже если они не были добавлены в список контактов) по электронной почте при помощи функции InMail…

Не обошлось на прошлой неделе без сообщений об утечках данных. Известная хакерская группировка OurMine, ранее специализировавшаяся только на взломах учетных записей в соцсетях, теперь решила сыграть «по-крупному». Киберпреступники взломали музыкальный видеохостинг Vevo и опубликовали 3,12 ТБ внутренних документов компании.

Из-за некорректной конфигурации сервера CouchDB в открытом доступе оказались данные более полумиллиона американцев. База данных является частью более крупной БД, содержащей информацию свыше 191 млн зарегистрированных избирателей. БД принадлежит консалтинговой фирме TargetSmart, которая использует ее в политических кампаниях для сбора средств, исследований и пр.» ***(Обзор инцидентов безопасности за прошлую неделю // SecurityLab.ru (http://www.securitylab.ru/news/488535.php).-18.09.2017).***

***

«Краткий обзор главных событий в мире ИБ за период с 18 по 24 сентября 2017 года.

…эксперты компании FireEye раскрыли подробности о деятельности иранской кибершпионской группировки APT 33. Жертвами хакеров стали авиакомпании в США и Саудовской Аравии, а также один из южнокорейских конгломератов. Основными целями хакеров являлись предприятия аэрокосмической промышленности, энергетического сектора и военные объекты. С помощью фишинга и инструментов DropShot злоумышленники распространяли усовершенствованную версию червя Shamoon – ShapeShift.

Специалисты ESET обнаружили кампанию по распространению новой версии вредоносного ПО FinFisher, также известного как FinSpy. Жертвами вредоноса стали пользователи в семи странах...

Исследователи Trend Micro зафиксировали новую массовую спам-рассылку с вымогательским ПО Locky. Количество вредоносных писем уже преодолело отметку в несколько миллионов. По данным экспертов, основными целями атак злоумышленников стали пользователи в Чили, Японии, Индии и США. На долю России в среднем пришлось 6% от общего количества атак.

Среди вредоносных кампаний, раскрытых на прошлой неделе, также стоит упомянуть атаки на пользователей Mac. С помощью заранее полученных учетных данных жертвы злоумышленники авторизуются в ее учетной записи iCloud, удаленно блокируют компьютер, используя функцию Find My iPhone, и требуют выкуп за восстановление доступа.

После выхода 14 сентября инновационного инструмента Coinhive, позволяющего монетизировать сайты за счет майнинга криптовалюты, киберпреступники стали активно использовать его в своей деятельности. Исследователи безопасности обнаружили целый ряд взломанных сайтов, тайпсквоттинговых доменов и ресурсов, маскирующихся под техподдержку, со встроенным Coinhive. Когда жертва попадает на такой сайт, Coinhive использует мощности процессора ее компьютера для майнинга криптовалюты Monero.

Большой резонанс на прошлой неделе вызвало сообщение о бэкдоре в популярной утилите CCleaner от компании Avast. Не позднее 11 сентября на серверы производителя были загружены инфицированные версии CCleaner 5.33 и CCleaner Cloud 1.07.3191. Встроенный в утилиту бэкдор собирал, шифровал и отправлял на сервер злоумышленников информацию об имени компьютера, установленном программном обеспечении и запущенных процессах…

Еще одним громким событием на прошлой неделе стал взлом Комиссии по ценным бумагам и биржам США. Сам инцидент имел место еще в прошлом году, однако сейчас стали появляться свидетельства использования похищенной у регулятора информации для осуществления незаконных сделок. Причиной утечки является уязвимость в электронной системе подачи заявок

EDGAR.

На прошлой неделе о себе снова напомнили активисты Anonymous. На этот раз участники Anonymous Greece атаковали греческий правительственный сайт по продаже недвижимости должников банков…

Говоря о вымогательстве, нельзя не упомянуть новое вымогательское ПО nRansomware. В отличие от других программ-вымогателей nRansomware требует от жертв не деньги, а фотографии интимного характера.

Исследователи безопасности из Kromtech обнаружили утечку более полумиллиона записей компании SVR Tracking, специализирующейся на отслеживании местоположения автомобилей. База данных хранилась на незащищенном облачном сервере Amazon S3. В ней содержалась информация о 540 642 учетных записях клиентов, включая адреса электронной почты, хэши паролей, IMEI GPS-трекеров, номерные знаки, идентификационные номера транспортных средств (VIN) и пр…» ***(Обзор инцидентов безопасности за прошлую неделю // SecurityLab.ru (http://www.securitylab.ru/news/488716.php).-25.09.2017).***

***

«Венчурный фонд AVentures Capital инвестирует $500 тыс. в Spinbackup - поставщика решений для резервного копирования данных в "облачных" средах и обеспечения кибербезопасности для пользователей G Suite и Office 365.

Согласно пресс-релизу фонда, Spinbackup является официальным партнером Google. Ее продукты доступны для пользователей в официальном каталоге Google G Suite Marketplace. Компания имеет статус Advanced Technology Partner компании Amazon.

Большинство клиентов Spinbackup - компании среднего и малого бизнеса, а также учебные заведения, в числе которых - University of Tokyo, Gurnick Academy of Medical Arts, Sensys Gatso и др…

«Несмотря на то, что организации и частные лица во всем мире тратят более $74 млрд в год на решения для обеспечения кибербезопасности, большинство современных продуктов для защиты от потери и утечки данных не отвечает требованиям времени. Специалисты компании Spinbackup уверены, что человеческий фактор является главной угрозой для безопасности, надежности хранения данных, и готовы предложить новые решения для автоматического резервного копирования данных, включающие полный функционал для мониторинга использования информации, хранящейся в облаке», - говорится в пресс-релизе.

В нем подчеркивается, что AVentures Capital стал первым институциональным инвестором разработчика…

Spinbackup Inc., основанная в 2014 году, предлагает современные рыночные решения в области кибербезопасности…

AVentures Capital - венчурный фонд, основанный в 2012 году серийными

предпринимателями и финансовыми специалистами. Осуществляет инвестиции в проекты на ранних этапах. Ориентирован на сотрудничество с глобальными компаниями, имеющими НИОКР в Украине и странах Центральной и Восточной Европы.

Инвестиции фонда сосредоточены в таких технологических областях, как программное обеспечение, электронная коммерция, "облачные" сервисы, мобильные технологии, IoT и др…» ***(AVentures Capital инвестирует $0,5 млн в разработчика "облачной" защиты Spinbackup // Интерфакс-Украина (http://interfax.com.ua/news/economic/446844.html).- 07.09.2017).***

***

«Компания «РАМАКС Интернейшнл» сообщает об открытии Центра компетенций в области информационной безопасности (ЦКИБ) на базе одноименной практики. Задачами Центра являются создание, поддержание и аудит комплексных систем информационной безопасности клиентов компании.

Центр Компетенций в области информационной безопасности был создан в свете новых требований в области защиты информации у текущих клиентов компании, а также роста уровня опасности угроз и кибератак для бизнеса в целом… Центр безопасности помогает решить самые востребованные и актуальные задачи в области ИБ, такие как: предотвращение утечек информации, аутентификация доступа, защита от сетевых угроз, управление на уровне событий, контроль привилегированных пользователей, защита конфиденциальных данных, защита сети и каналов связи, противодействие системам социальной инженерии, разработка ИТ-стратегии, разработка рекомендаций о возможных угрозах, комплекса мер для защиты, подготовка документов для надзорных органов, разработка инструкций по соответствию требованиям ИБ для персонала, подготовка плана развития ИБ, разработка требований по внедрению систем ИБ, разработка рекомендаций по контролю процесса внедрения. Кроме того, ЦКИБ «РАМАКС Интернейшнл» предлагает особенно актуальные сейчас решения в области корреляции, прогнозирования, реакции и предупреждения событий на основе наработок псевдо-искусственного интеллекта, в том числе в сегменте Threat Intelligence. Все услуги предусматривают создание дорожной карты на 3-5 лет, для планирования и оптимизации затрат…» ***(«РАМАКС Интернейшнл» открывает Центр компетенций информационной безопасности // ООО "ИКС-МЕДИА"(http://www.iksmedia.ru/news/5436505-RAMAKS-Internejshnl-otkryvaet- Czent.html#ixzz4sShJlx9M).- (11.09.2017).***

***

«Компания Trend Micro Incorporated (TYO: 4704; TSE: 4704) мировой лидер в области решений для кибербезопасности, опубликовала отчет по информационной безопасности за первое полугодие 2017 года «Цена

компрометации» (The Cost of Compromise). В отчете представлены ключевые киберугрозы, которые продолжают бросать вызов развитию сферы информационных технологий…

В первой половине 2017 г. Trend Micro зафиксировала более 82 млн атак с использованием программ-вымогателей, а также более 3 тыс. попыток осуществления мошенничества с использованием корпоративной почты (BEC). Все это доказывает необходимость приоритизации мер по реагированию на возникающие угрозы. Несмотря на растущий уровень инвестиций в информационную безопасность, согласно последнему аналитическому отчету компании Forrester, на борьбу с увеличивающимся количеством корпоративных киберугроз все еще выделяется недостаточно средств...

В апреле и июне атаки с использованием программ-вымогателей WannaCry и Petya нарушили деятельность тысяч компаний из различных отраслей по всему миру. Общая сумма потерь от этих атак, включая последующее снижение производительности и расходы на устранение последствий, по разным подсчетам, составили порядка 4 млрд долларов США. Кроме того, по данным ФБР, мошенничество с использованием корпоративной почты обошлось компаниям в 5,3 млрд долларов США, все это – за первое полугодие 2017 г…

Другие выводы отчета:

·С начала года Trend Micro™ Smart Protection Network™ заблокировала более 38 млрд угроз, большинство из которых представляли вредоносные электронные письма.

·В первой половине года специалистами Zero Day Initiative в программных решениях популярных вендоров были обнаружены 382 новые уязвимости.

·Рост количества новых семейств программ-вымогателей замедлился: в первой половине 2017 г. было обнаружено порядка 28 новых семейств таких программ. При этом одна только программа-вымогатель WannaCry смогла заразить беспрецедентное количество компьютеров – 300 000 в 150 странах.

Подключенные устройства подвергают риску умные производства: один лиш ботнет Persirai, обнаруженный Trend Micro в апреле этого года, атаковал более 1 000 подключенных к сети IP-камер, при этом всего было обнаружено более 120 000 камер, уязвимых перед атаками вредоносной программы…» ***(Новый отчет по информационной безопасности от Trend Micro // ChannelForIT (http://channel4it.com/publications/Novyy-otchet-po-informacionnoy-bezopasnosti-ot- Trend-Micro--27677.html#).- 14.09.2017).***

***

«…В 2017 году расходы на обеспечение киберзащиты во всем мире вырастут на 8,2% в сравнении с прошлым годом и достигнут $81,7 млрд. К 2020 году объем рынка информационной безопасности превысит $100 млрд, говорится в свежем докладе аналитической компании IDC.

Для сравнения: в России с 2013 по в 2014 год рынок ИБ вырос на 13% и

составил только 59 млрд руб., то есть чуть меньше $1 млрд, свидетельствуют данные TAdviser…

По оценкам J'son & Partners Consulting, доля сервисов ИБ в России к 2018 году вырастет более чем в 4 раза в сравнении с 2014 годом, заняв до 40% рынка. Главной тенденцией станет рост спроса на интеллектуальные сервисы ИБ, предоставляемые по модели Security as a Service.

Становление рынка ИБ в России шло рука об руку с законодательными инициативами. Пожалуй, важнейшими вехами в его формировании стали:

·Законы «Об информации, информатизации и защите информации» (1995), Доктрина информационной безопасности РФ (2000),

·Закон «О персональных данных» (2006),

·Приказы Гостехкомиссии (ныне – ФСТЭК), которая ввела в действие многие из руководящих документов, и ФСБ РФ.

Принятие этих документов способствовало формированию, росту и устойчивому развитию многих направлений средств защиты информации (СЗИ).

В итоге к 2014 году, когда грянул валютный кризис, рынок ИБ в России сформировался. И как в расхожем выражении, валютные колебания сыграли отечественным компаниям на руку. Зарубежные разработки значительно выросли в цене, и многим компаниям пришлось переходить на отечественные аналоги. Это породило спрос.

В силу того, что цикл разработки решений ИБ в среднем занимает от 1,5 до 3 лет, пик появления лучших отечественных решений стоит ожидать как раз в период с 2016 по 2018 год…

…ключевым моментом последних лет стало утверждение новой Доктрины информационной безопасности в декабре 2016 года. Обновленная версия нацелена на превентивный ответ гибридным войнам, которые осуществляются не только на физическом, но также экономическом, политическом и информационном уровнях. За последние 16 лет изменились не только методы, но и масштабы угроз информационной безопасности…

Доктрина предусматривает необходимость обеспечения информационной безопасности не только технических составляющих (аппаратной и программной частей), но также «субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности», то есть подразумевает подготовку и переквалификацию сотрудников…» ***(Александр Атаманов. Свое вместо чужого: как формируется рынок информбезопасности России // Rusbase (https://rb.ru/opinion/svoe-vmesto-chuzhogo/).- 13.09.2017).***

***

«23 сентября на III международном форуме по кибербезопасности HackIT будет презентована новая криптовалюта Hacken, за которую на

одноименной платформе можно будет приобрести услуги «белых хакеров»…

«Криптовалюта Hacken будет работать в условиях «обратной эмиссии» — часть комиссии за транзакции будет «сжигаться», что приведёт к постоянному росту стоимости одного «бакена», — говорится в пресс-релизе…

Предпродажа началась 18 сентября. В открытый доступ хакены поступят 12 октября, и продажа продлится месяц.

Всего планируется выпустить 20 млн хакенов. Во время предварительной продажи будут проданы 1 млн хакенов, ещё 300 тысяч станут бонусом для участников предпродажи.

Остальные 18,7 млн будут доступны для покупки всеми желающими в октябре. Больше никаких эмиссий не будет» ***(Украинские "белые хакеры" представят собственную криптовалюту // TRISTAR.com.ua - твой финансовый навигатор!(http://tristar.com.ua/1/news/ukrainskie_belye_hakery_predstaviat_sobstvennuu_kriptov alutu_7987.html).- 21.09.2017).***

***

«В конце августа жители Индии из штатов Харьяна и Пенджаб обнаружили, что 2G, 3G, 4G, CDMA и GPRS перестали работать. Были отключены и СМС-сообщения. На несколько дней 50 млн человек остались без доступа к мобильному интернету…

…СМИ обратили внимание на документ, который был выпущен правительством Индии в начале августа. В нем описываются правила и процесс отключения интернета в стране.

Документ, изданный Министерством связи Индии, носит название «Временное приостановление обслуживания телекоммуникационных услуг ([в случае] чрезвычайных ситуаций или [в целях соблюдения] общественной безопасности)». Он был опубликован в рамках седьмого раздела «Закона о телеграфе» от 1885 года. По большому счету, он обеспечивает правовой механизм для «отключения» интернета…

Согласно новым правилам распоряжение о блокировке интернета может быть вынесено должностным лицом высшего уровня, отвечающим за внутреннюю безопасность, как на уровне страны, так и на уровне штата. Поводом для отключения могут быть «непреодолимые обстоятельства». Документ разрешает любому сотруднику Объединенного секретариата распорядиться о блокировке, если получение разрешения от Министерства внутренних дел «не представляется возможным». Запрет может сохраняться в течение 24 часов без разрешения Главного управления. Однако любое распоряжение о блокировке должно иметь под собой определенные основания.

Приказы передаются операторам связи либо в письменной форме, либо по защищенным каналам… Новые правила в Индии дополняют обширный список законов, регулирующих «отключение Интернета» во всем мире. Хотя

общественные организации, как правило, осуждают попытки властей контролировать доступ в Интернет, по состоянию на 2016 год в 27 странах были разработаны те или иные документы, позволяющие єто сделать…» ***(Индия приняла закон о «выключении» интернета // «Хабрахабр» (https://habrahabr.ru/company/vasexperts/blog/337584/).- 11.09.2017).***

***

Сполучені Штати Америки

«…Поскольку американское правительство продолжает расследование возможной связи между администрацией Дональда Трампа и Россией, Вашингтон считает, что продукты «Лаборатории Касперского» (ЛК) могут представлять угрозу внутренней безопасности США…

…Администрация общих служб (General Services Administration) уже удалила компанию из своего каталога доверенных поставщиков, а Сенат тем временем рассчитывает средства на оборону на 2018 финансовый год без учета закупок ПО от «Лаборатории Касперского»…

Проект бюджета запрещает использование программ «Лаборатории Касперского», но как быть с программными и аппаратными продуктами других производителей, в том числе Juniper и Microsoft, где используются технологии ЛК? Ответ на этот вопрос в законопроекте не предусмотрен...» (***Правительство США продолжает агрессивную политику по отношению к ЛК // SecurityLab.ru (http://www.securitylab.ru/news/488244.php).- 05.09.2017).***

***

«Суд в США частично отменил правило, согласно которому Facebook обязан был не разглашать фактов о получении администрацией соцсети ордеров с требованием раскрыть пользовательскую информацию.

…Апелляционный суд округа Колумбия опубликовал документ, в котором говорится, что правительство больше не может запрещать компаниям публично сообщать о подобных запросах.

Facebook вёл судебную тяжбу с правительством о законности правила «о неразглашении получения ордеров» (NDOs), запрещавшем сообщать кому-либо о запросах властей, с начала этого года. Всё началось с того, что представители федеральной прокуратуры направили в компанию запросы, касающиеся трех пользователей. Они также попросили не сообщать этим лицам о том, что данные из их аккаунтов будут раскрыты властям. Facebook боролся за отмену NDOs и поначалу проиграл, однако адвокаты соцсети попросили апелляционный суд округа Колумбия отклонить это решение, и суд удовлетворил их просьбу, назначив новое слушание. Но это пока не окончательная победа соцсети. Документ лишь говорит о том, что расследование «дошло до той точки, когда в запрете на уведомление пользователей больше нет необходимости».

Если Facebook удастся одержать верх на слушаниях в суде, пользователи будут получать уведомления, если информацией о них заинтересуется правительство. Сразу после получения ордера или поступления требования на раскрытие переписки и иных пользовательских данных, соцсеть будет отправлять соответствующее уведомление этому пользователю…» ***(Facebook получит право уведомлять пользователей о запросах властей по ним // РосКомСвобода (https://rublacklist.net/31993/).- 14.09.2017).***

***

«В Конгрессе представлен законопроект, предполагающий создание должности посла США по киберпространству, а также внедрение американской международной кибердипломатии…

В случае принятия закона, Госдепартамент США будет обязан включать в ежегодные доклады о соблюдении прав человека в мире оценки о свободе интернета.

В последнее время отношения России, Китая и США заметно ухудшились, особенно касаемо киберпространства. Соединённые Штаты обвиняют российские власти во вмешательстве в выборы Президента весной, летом и осенью прошлого года, выразившееся во взломе почты штаба кандидата в Президенты Хиллари Клинтон, а также создании фейковых аккаунтов в социальных сетях и попытках влиять на мнение избирателей через рекламу на Facebook…» ***(США вводит кибердипломатию для борьбы с российским и китайским влиянием на Сеть // РосКомСвобода (https://rublacklist.net/32018/).- 15.09.2017).***

***

«Схвалений сенатом США проект про витрати на оборону містить рекомендації щодо перегляду доктрини у сфері кібербезпеки…

Переглянута доктрина має передбачати, зокрема, положення про «роль кібервійськ у військовій стратегії США та плануванні», про «декларовану політику у сфері реагування США на кібератаки». Також йдеться про необхідність розробки кампанії щодо стримування загроз у кіберпросторі з боку Росії, Китаю, Ірану, КНДР та інших країн.

…сенатори пропонують повідомляти країни, що стали ціллю кібератаки, якщо США отримали таку інформацію…

…переважна більшість сенаторів схвалила законопроект. Тепер його передадуть на розгляд палати представників США» ***(Сенат США пропонує переглянути заходи з протидії кіберзагрозам і кампанію щодо стримування загроз із боку РФ і Китаю // Интерфакс-Украина (http://ua.interfax.com.ua/news/general/449582.html).- 19.09.2017).***

***

«…З початку нового століття в Сполучених Штатах робота щодо

нарощування потенціалу реагування на кіберзагрози проводиться дуже активно і системно. Не випадково у своїй «Стратегії національної безпеки» (редакція 2015 року) США нормативно закріпили свою «особливу відповідальність за мережевий світ» та наміри активно протидіяти будь-яким ворожим та протиправним діям у кіберпросторі або з використанням кіберпростору.

Нова американська адміністрація послідовно підтримує наведені зусилля.

Наприклад, наприкінці серпня у Вашингтоні було оголошено про зміну статусу Кіберкомандування ЗС США. Перш за все, цю структуру планується вивести з підпорядкування Стратегічному командуванню ЗС США та підняти її на рівень окремого функціонального командування збройних сил. Це дозволить централізувати керівництво кібернапрямом з боку Міноборони та Об'єднаного комітету начальників штабів США… Також було оголошено про відокремлення Кіберкомандування від Агентства національної безпеки. Не є таємницею, що до теперішнього часу посаду керівника обох відомств (на основі суміщення) займала одна людина. Але тепер очікується призначення двох окремих керівників…

Усвідомлення нових загроз разом з розумінням цінності власних операцій в кіберпросторі у вересні 2014 року призвело до появи директиви про створення фактично нового роду військ - Кіберкомандування сухопутних військ… Створення нового роду військ дозволило інтегрувати підрозділи для спільних дій та розширити можливості для активного впливу в кіберпросторі. На сьогодні Кіберкомандування сухопутних військ вже має у підпорядкування щонайменше дві бойові структури рівня бригади.

…крім бойових підрозділів було створено навчальний заклад - US Army Cyber School (Fort Gordon). Таке рішення крім підготовки кадрів дозволило отримати низку додаткових переваг. Наприклад, стало початком формування нової корпоративної культури в середовищі «кібербійців». А самі військовослужбовці отримали «зелене світло» в своїй кар'єрі, так як з'явилася нова інтегрована спеціальність замість низки попередніх…» **(Тетяна Попова. Кібербезпека на порядку денному//«Цензор.НЕТ» (https://censor.net.ua/blogs/6971/kberbezpeka_na_poryadku_dennomu).- 08.09.2017).**

***

Країни ЄС

«…Британская правозащитная организация Privacy International, занимающаяся вопросами защиты конфиденциальности и неприкосновенности частной жизни, разработала «Гид по международному праву и слежке» (Guide on International Law and Surveillance). В Руководстве затрагивается множество таких тем, как законность мероприятий по ведению массовой слежки, законодательство в области личных данных,

экстерриториальное применение прав человека в плане цифровой слежки, международное законодательство по части государственных взломов с целью наблюдения, «криптовойны», «тёмные» дискуссии и ответственность глобальных корпораций за неприкосновенность частной жизни [пользователей] и соблюдение прав человека…

Руководство состоит из шести глав:

·В первой главе рассматриваются положения в области прав человека договорное право;

·Вторая глава рассказывает о принципах прав человека, которые применяются к слежке, — такие, как принципы законности, необходимости и соразмерности;

·Третья глава рассматривает взаимодействие между слежкой и другими положениями в области прав человека — такими, как антидискриминация;

·Четвёртая глава касается массовой слежки;

·В пятой главе рассматривается дискуссия вокруг взлома и шифрования;

·Наконец, в шестой главе рассматриваются обязательства многонациональных корпораций в этой области…» ***(Privacy International представила «Гид по международному праву и слежке» // РосКомСвобода (https://rublacklist.net/31623/).- 01.09.2017).***

***

«Программное обеспечение, которое будет применяться во время электронного подсчета голосов на предстоящих выборах в Бундестаг, содержит существенные недостатки в плане безопасности.

Недостатки обнаружил немецкий союз хакеров Chaos Computer Club… Хакеры провели технический анализ самого программного обеспечения и установили, что эта программа достаточно легко поддается манипуляциям извне.

Эти манипуляции можно осуществлять как с результатами голосования на отдельных избирательных участках, так и в отдельных федеральных землях. Причем это можно делать даже не находясь на территории этих участков или федеральных земель…

Между тем председатель Федеральной избирательной кампании Дитер Заррайтер рассчитывает на то, что до 24 сентября, то есть до дня проведения выборов, выявленые недостатки удастся устранить…» ***(Хакеры обнаружили значительные недостатки программного обеспечения для выборов в ФРГ // Европейская правда (http://www.eurointegration.com.ua/rus/news/2017/09/7/7070663/).- 07.09.2017).***

***

«Еврокомиссия закрыла дело в отношении корпорации Microsoft по жалобе компании «Лаборатория Касперского»…

Напомним, в июне 2017 года «Лаборатория Касперского» обратилась с иском вЕвропейскую комиссию и Федеральное картельное ведомство Германии

(Bundeskartellamt) касательно злоупотребления корпорацией Microsoft доминирующим положением на рынке ОС, а также недобросовестной конкуренции на рынке продуктов по обеспечению защиты от компьютерных угроз.

13 июня в рамках антимонопольного разбирательства корпорация Microsoft получила предупреждение от Федеральной Антимонопольной Службы РФ (ФАС). Предупреждение было связано с нарушением корпорацией закона о защите конкуренции. В частности, техногигант создал условия, дискриминирующие производителей антивирусного ПО. Кроме того, Microsoft блокировала сторонние защитные решения в пользу собственного антивируса Defender, не поставив в известность пользователей и без их согласия. 18 июля корпорация Microsoft уведомила ФАС об исполнении предупреждения» ***(Еврокомиссия закрыла дело против Microsoft // "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=118561).- 11.09.2017).***

***

«…Президент Єврокомісії Жан-Клод Юнкер направив керівництву Європарламенту лист, в якому визначив 5 головних пріоритетів на 2018 рік. До першого пункту він відніс зміцнення європейської торгової програми…

Другим пунктом стало питання зміцнення промисловості та посилення її конкурентоспроможності. Юнкер наголосив, що особливо це стосується виробничої бази Європи та 32 млн працівників, які утворюють хребет промисловості…

Третім пунктом є лідерство Європи у боротьбі проти кліматичних змін…

Четвертий пріоритет зазначений Юнкером стосується інформаційного забезпечення та захисту європейців від кібер-атак.

«Кібер-атаки можуть бути більш небезпечними для стабільності демократії та економіки, ніж зброя та танки. Кібер-атаки не мають кордонів та ніхто не має проти них імунітету. Ось чому сьогодні Комісія пропонує нові інструменти, включаючи Європейське агентство з кібербезпеки, щоб захистити нас від таких нападів», - заявив Юнкер.

До п’ятого пріорітету він відніс питання міграції у Європі. За словами Юнкера, на сьогоднішній день значно ефективніше захищаються зовнішні кордони Європи…» ***(Ілля Жижиян. Президент Єврокомісії назвав п'ять пріоритетів для Євросоюзу на 2018 год // Інформаційне агентство «Українські Національні Новини» (Президент Єврокомісії назвав п'ять пріоритетів для Євросоюзу на 2018 год).— 13.09.2017).***

***

«У Бельгії висловлюють занепокоєння щодо забезпечення безпеки у кіберсфері своєї національної збірної на фінальній частині чемпіонату ФІФА з футболу, який має пройти у Росії у 2018 році…

Як уточнюється, загроза у сфері кібербезпеки може полягати у тому, що російські хакери намагатимуться викрасти онлайн-інформацію про порядок та тактику підготовки команд до чемпіонату.

Відтак, керівництво бельгійського футболу наголошує, що кібербезпека має стати найвищим пріоритетом для ФІФА на цьому етапі організації фінішної частини чемпіонату.

Слід зазначити, що національна збірна Бельгії вже кваліфікувалася для участі у чемпіонаті світу з футболу, який має відбутися в РФ у 2018 році…» ***(У Бельгії занепокоєні кібербезпекою на чемпіонаті світу з футболу в РФ // Укрінформ(https://www.ukrinform.ua/rubric-technology/2307693-u-belgii-zanepokoeni-kiberbezpekou-na-cempionati-svitu-z-futbolu-v-rf.html).- 18.09.2017).***

***

«Европейский союз представит во вторник в Брюсселе план конкретных действий в области кибербезопасности, заявил комиссар ЕС по внутренним делам Димитрис Аврамопулос… на конференции по международной безопасности киберпространства, которая была организована Францией на полях сессии Генеральной ассамблеи ООН в Нью-Йорке.

…Он подчеркнул, что предлагаемые в плане действия будут предприняты Евросоюзом, но в цифровом обществе, в котором живет современный мир, имеют глобальную перспективу. По мнению европейского комиссара, киберугрозы усилились и их характер изменился… Киберпреступность стала инструментом в геополитике и конфликтах (гибридных и иных)... Аврамопулос подчеркнул, что ни одна страна не может обеспечить кибербезопасность в одиночку. ЕС будет укреплять свое Агентство по сетевой и информационной безопасности (ENISA), которое базируется в Греции. ООН и НАТО должны, по мнению европейского комиссара, стать важнейшими площадками международного сотрудничества в борьбе с киберугрозами…» ***(Комиссар ЕС призвал к сотрудничеству в борьбе против киберугроз // ООО«АМ Медиа» (https://www.anti-malware.ru/news/2017-09-19-3/24109).- 19.09.2017).***

***

«Єврокомісія запропонувала низку заходів щодо посилення кібербезпеки, серед яких – створення Агентства ЄС з кібербезпеки…

Агентство буде створене на основі існуючого Європейського агентства з питань мережевої та інформаційної безпеки (ENISA).

Агентству буде надано постійний мандат, і воно матиме можливість надавати державам-членам ефективну допомогу та реагувати на кібератаки...

Агентство з кібербезпеки також допоможе запровадити загальноєвропейську систему сертифікації, яку Єврокомісія пропонує створити для забезпечення використання тільки захищеної продукції.

«Нові європейські сертифікати з кібербезпеки забезпечать надійність мільярдів пристроїв ("інтернету речей"), які мають відношення до

сьогоднішньої критичної інфраструктури, такої як енергетичні та транспортні мережі. Сертифікати кібербезпеки будуть визнані державами-членами, таким чином, знизяться адміністративні витрати та витрати для компаній», - йдеться у повідомленні…» ***(Єврокомісія оголосила про створення Агентства ЄС з кібербезпеки // Європейська правда (http://www.eurointegration.com.ua/news/2017/09/19/7071212/).- 19.09.2017).***

***

«В Європейському Союзі заявили планують змінити нову директиву, яка передбачає санкції за цифрові злочини, щоб дати можливість правоохоронцям боротися зі злочинами, пов'язаними з використанням криптовалют…

«Пропонована директива зміцнить можливість правоохоронних органів боротися з цією формою злочинності, розширивши сферу охоплення злочинів, пов'язаних з інформаційними системами, до всіх платіжних операцій, включаючи транзакції через віртуальні валюти», - пояснили в Єврокомісії.

Крім цього, можливі зміни в правилах ЄС, що стосуються криптоконверсій. Офіційні особи зазначають, що наразі у кримінальній статті «Шахрайство з негрошовими платежами» в ЄС не враховуються злочини, пов'язані з цією технологією…» ***(RomanK. У світі почали "полювання" на біткоін-шахраїв // BusinessUA.Com (http://businessua.com/finance/38179u-sviti-pochali-polyuvannya-na- bitkoin-shahraiv.html#).- 23.09.2017).***

***

«Представники Комітету з питань інформатизації та зв'язку за результатами діяльності робочої групи ЄС із законодавчого регулювання кібербезпеки продовжують вивчення зазначених питань на основі досвіду Республіки Польща.

Так, 26-27 вересня, делегація у складі голови Комітету Данченка О.І., першого заступника голови Комітету Лук'янчука Р.В. та члена Комітету Семенухи Р.С. спільно із головою Державної служби спеціального зв'язку та захисту інформації України Євдоченка Л.О. бере участь у навчальному візиті з питання ефективності управління кібербезпекою у м.Варшава, Польща.

Програма візиту передбачає низку зустрічей із колегами з Парламенту Польщі, зокрема в Комітеті з цифрових, інноваційних та сучасних технологій, а також у Міністерстві адміністрації і цифризації Польщі, в ході яких передбачено обговорення питання адаптації українського цифрового законодавства до норм ЄС, формування стратегії кіберзахисту та організації державно-приватного партнерства у сфері кібербезпеки, а також імплементації Директиви безпеки мережевих та інформаційних систем (NIS Directive).

Окрім того, з метою вивчення практичного досвіду польських фахівців з кібербезпеки заплановано візит до Національного центру кібербезпеки, який працює у відповідності до NIS Directive та чинного польського

законодавства…» ***(Делегація Комітету вивчає досвід Польщі у питаннях регулювання кібербезпеки // Народна Рада (http://narodnarada.info/news/delegaciya-komitetu- vivchae-dosvid-polschi-news-73851.html).- 27.09.2017).***

***

«Польские власти намерены потратить два миллиарда злотых на кибербезопасность. Об этом заявил министр обороны страны Антони Мачеревич во время выставки вооружения в Кельце… Конечно, это не очень большие средства, но это хорошее начало, — подчеркнул Мачеревич. Развивать это направление в Польше будет государственная компания Exatel… Ранее министр также заявлял, что втечение ближайших 14 лет Польша намерена потратить на оборону более 550 млрд злотых…» ***(2 млрд злотых будет потрачено Польшей на кибербезопасность // АМ Медиа (https://www.anti-malware.ru/news/2017-09-06-3/23975).- 06.09.2017).***

***

«В Финляндии открыли Европейский центр по борьбе против гибридных угроз.

Новая структура будет бороться с распространением ложной информации, атаками против информационных систем, а также другими видами атак с помощью современных технологий… Кроме Финляндии, соглашение о создании европейского центра противодействия гибридным угрозам ранее подписали Швеция, Норвегия, США, Франция, Германия, Великобритания, Испания, Польша, Эстония, Латвия и Литва. Все государства, подписавшие документ, вскоре отправят в финскую столицу своих сотрудников. Центр по гибридным угрозам также тесно сотрудничает с Евросоюзом и НАТО…

Ранее в отчете Европейского парламента о противодействии пропаганде также указывалось, что элементы гибридной войны можно заметить в действиях России во время украинского кризиса. РФ якобы воспользовалась отсутствием международных правовых актов в области кибербезопасности, а также использовала двусмысленность в свою пользу и влияла на общественное мнение в Европе…» ***(В Финляндии открыли Европейский центр по борьбе против гибридных угроз // АМ Медиа (https://www.anti-malware.ru/news/2017-09-07-3/23999).- 07.09.2017).***

***

Китайська Народна Республіка

«…Правительство КНР намерено создать национальную централизованную базу данных, в которой будет собрана вся информация о кибератаках…

Согласно указу Министерства промышленности и информатизации КНР, операторы связи, представители бизнеса и госорганы должны добавлять в национальную базу данных информацию об инцидентах безопасности, таких как атаки с использованием троянов, уязвимости в аппаратном обеспечении и контент, связанный с «вредоносными» IP-адресами.

Ответственность за создание платформы и устранение угроз ляжет на плечи самого министерства. Указ вступит в силу с 1 января следующего года. За его невыполнение операторы связи и компании будут получать соответствующие предупреждения и штрафы…» **(В Китае создадут национальную базу даннях киберугроз // SecurityLab.ru (http://www.securitylab.ru/news/488471.php).- 13.09.2017).**

***

«…Китайский закон о кибербезопасности, формально направленный на защиту данных китайских пользователей, может иметь разрушительные последствия для иностранных компаний и их технологий.

…анализ будет проводиться Центром оценки информационных технологий Китая (CNITSEC), который курируется Министерством государственной безопасности КНР.

Информация, полученная в результате анализа, проведенного CNITSEC, может быть использована для выявления уязвимостей в коде и использования их в разведывательных спецоперациях…

Действия китайского правительства можно расценивать как непрямой шантаж компаний, подпадающих под действие закона. Им придется делиться информацией о своих технологиях и интелектуальной собственностью, если компании хотят и дальше предлагать свои услуги на одном из крупнейших мировых рынков» ***(В Китае спецслужбы получат доступ к исходному коду любой программы // SecurityLab.ru (http://www.securitylab.ru/news/488223.php).- 04.09.2017).***

***

Російська Федерація

«Сбербанк предлагает создать в России Национальный центр кибербезопасности (НЦК) — главный орган по обеспечению информационной безопасности в стране… НЦК должен стать ключевой структурой по защите страны в информационном пространстве, следует из представленной в презентации Сбербанка архитектуры национальной системы кибербезопасности. Он будет получать информацию от международных центров безопасности, иностранных центров реагирования на инциденты в сфере информационной безопасности (computer emergency response team, CERT), правоохранительных органов и регуляторов. Согласно предложению

банка, НЦК будет куратором всех существующих институтов в сфере информационной безопасности страны. Под его контроль, в частности, должны перейти RU-CERT…, GOV-CERT…, Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак… и отраслевые CERT… Согласно предложенной банком схеме, аналогичные CERT предполагается создать и для обмена информацией среди предприятий энергетики и телекоммуникаций, чтобы они затем передавали данные в НЦК. Необходимость создания нового регулятора в банке объясняют низкой эффективностью механизмов борьбы с киберпреступлениями…

В документе также отмечается, что российские правоохранительные органы отстают в реагировании на кибератаки, а телеком-операторы не обязаны обеспечивать противодействие кибератакам. В итоге «организациям реально некуда обратиться в случае кибератаки»…» ***(Сбербанк предложил создать главный центр по борьбе с киберпреступлениями //Аналитический центр Anti-Malware.ru (https://www.anti-malware.ru/news/2017-09-01-3/23944).- 01.09.2017).***

***

«Центальный Банк РФ предложил принять ряд мер для повышения уровня безопасности при осуществлении денежных переводов в Сети. Соответствующие поправки планируется внести в положение №382-П от 9 июня 2012 года «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»…

В поправках приведен перечень ограничений по параметрам операций, определяемый оператором. В число параметров входит максимальное значение суммы денежного перевода, список получателей, время, а также местоположение устройства, использованного для проведения операции. Также оператор отвечает за защиту данных с помощью определенных технологических мер, обеспечивающих идентификацию клиента, аутентификацию сообщений при переводе средств и возможность контролирования реквизитов…

Оператор обязан проинформировать ЦБ о выявленных инцидентах кибербезопасности, а также сообщить регулятору о пресс-конференциях по поводу выявленных угроз за день до их проведения…» ***(ЦБ РФ введет новые меры безопасности при проведении online-платежей//Информационнаябезопасность (http://www.itsec.ru/newstext.php?news_id=118526).- 07.09.2017).***

***

«Российские IT-компании должны переходить на отечественное программное обеспечение, иначе государство не сможет использовать их

продукцию в некоторых сферах из-за высоких рисков для безопасности, заявил президент РФ Владимир Путин. На встрече главы государства с представителями информационно-коммуникационного кластера Пермского края в пятницу разговор зашел о том, каков объем отечественного программного обеспечения производимой ими высокотехнологичной продукции. Выяснилось, что это порядка 30%... «Надо стараться своих (программистов) «подтаскивать». По поводу безопасности есть вещи критически важные для государства, для жизнеобеспечения отдельных отраслей и регионов. И если вы будете все время в таком же объеме таскать и железо, и программное обеспечение, то в каких-то сферах государство вам неизбежно скажет: знаешь, мы не можем это взять, потому что где-нибудь там кнопку нажмут и все у нас отключится", — сказал Путин. По его словам, этого допустить нельзя, причем даже не в военных отраслях, а например, в сфере энергоснабжения…» ***(Александр Панасенко. Путин поручил IT-компаниям перейти на отечественное ПО // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-09-08-3/24013).- 08.09.2017).***

***

«…Комиссия по информационной безопасности при Совбезе РФ обсудила проблемы эффективности противодействия угрозам функционированию информационной инфраструктуры страны…

В рамках заседания Межведомственной комиссии состоялось обсуждение ряда вопросов по противодействию существующим и потенциальным киберугрозам…

Был предложен ряд мер по усилению защиты от информационных угроз, в частности по обнаружению, предупреждению и ликвидации последствий кибератак, а также по улучшению организации функционирования Рунета…» ***(Совбез РФ обсудил противодействие киберугрозам // SecurityLab.ru (http://www.securitylab.ru/news/488513.php).- 15.09.2017).***

***

«…Правительством РФ утвержден проект программы «Цифровая экономика». Ожидания руководства страны относительно толчка, который должны дать цифровые технологии российской экономике, исключительно велики. Не случайно на развитие этого сектора в 2018 году будет выделено 200 млрд руб… Между тем, как указывают эксперты инвестиционной компании ЦЕРИХ, с таким негативным последствием цифровой экономики, как киберпреступность, наши сограждане сталкиваются уже сегодня…

В ЦЕРИХ приводят данные статистики о росте кибермошенничества. К примеру, в 2016 году число краж средств с банковских карт граждан выросло по сравнению с 2015 годом на 43% и достигло 107 тыс. случаев. Суммарные потери банков и их клиентов в 2016 году составили 2 млрд руб. В 2017 году число краж денег с банковских карт может вырасти еще на 30%...

В подобных условиях развитие цифровой экономики в России обязательно должно включать разработку системы мер эффективной защиты информации, в первую очередь – персональных данных. Помимо технологических решений, изменения необходимо внести и в законодательную базу, чтобы сделать борьбу с киберпреступностью более действенной…» ***(ЦЕРИХ: Кибербезопасность должна стать базовой составляющей программы развития цифровой экономики // «Открытые системы» (https://www.computerworld.ru/news/TsERIH-Kiberbezopasnost-dolzhna-stat-bazovoy- sostavlyayuschey-programmy-razvitiya-tsifrovoy-ekonomiki-).- 17.09.2017).***

***

«Федеральная служба безопасности РФ получит расширенные полномочия по контролю над работой центров по обнаружению компьютерных атак. Соответствующий приказ президента РФ опубликован на официальном портале нормативных правовых актов…

Документ вносит изменения в указ президента РФ от 15 января 2013 года «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», предлагающие возложить на ФСБ функции не только создания, но и обеспечения контроля над госсистемой.

Согласно документу, ведомство будет организовывать и проводить работу по созданию и обеспечению функционирования госсистемы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ. Кроме прочего, спецслужба будет утверждать требования к информационным центрам, проводить их аккредитацию на соответствие требованиям, а также осуществлять мероприятия по оценке безопасности критической информационной инфраструктуры РФ (КИИ)…» ***(ФСБ возьмет под контроль центры по обнаружению кибератак // "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=118562).- 11.09.2017).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Польща виступає за розширення співпраці в ЄС і НАТО у сфері кібербезпеки.

Про це сказала прем'єр-міністр Польщі Беата Шидло під час зустрічі у Варшаві з прем’єрами Литви Сяулюсом Скверналісом та Латвії Марісом Кучінскісом…

За її словами, Польща та країни Балтії мають досвід, пов’язаний з гібридними загрозами, зокрема кібератаками…» ***(Польща хоче посилити співпрацю з ЄС і НАТО для кіберзахисту // Укрінформ***

(https://www.ukrinform.ua/rubric- world/2299230-polsa-hoce-posiliti-spivpracu-z-es-i-nato-dla-kiberzahistu.html).- 05.09.2017).

***

«…Глава финской дипломатии призвал развивать сотрудничество ЕС и НАТО в борьбе с гибридными угрозами и кибербезопасности в среду, во время семинара в Европейском центре борьбы с гибридными угрозами в Хельсинки… Он признал, что такая форма сотрудничества могла бы сработать также в других регионах, например в регионе Средиземного или Черного моря…

Глава Европейского центра борьбы с гибридными угрозами Мэтти Сареляйнен положительно отнесся к инициативе развернуть сотрудничество в районе Балтийского моря…

Во встрече в Хельсинки принимали участие также комиссар ЕС по вопросам безопасности Юлиан Кинг и заместитель генерального секретаря НАТО по вопросам разведки и безопасности Арндт Фрейтаг фон Лоринговен. Оба заверили в готовности поддержать инициативу министров Финляндии и Швеции…» ***(Финны разоблачают гибридные угрозы в районе Балтийского моря // bizresurs (http://bizresurs.com.ua/finny-razoblachayut-gibridnye-ugrozy-v.html).- 08.09.2017).***

***

«…Председатель Еврокомиссии Жан-Клод Юнкер (Jean-Claude Juncker) предложил создать Европейское агентство киберзащиты, которое будет защищать страны ЕС и европейские компании от информационных угроз…

По словам Юнкера, только за прошедший год в странах ЕС было зафиксировано более 4 тыс. кибератак. Порядка 80% европейских компаний сталкивались с киберугрозами различного рода. На данный момент Еврокомиссия ищет пути решения проблем с кибербезопасностью...» ***(Еврокомиссия предложила создать агентство по киберзащите // SecurityLab.ru (http://www.securitylab.ru/news/488472.php).- 13.09.2017).***

***

«Москва призвала Вашингтон рассмотреть предложение по формированию совместной группы по кибербезопасности, говорится в заявлении российского посольства в США… Вопрос о создании совместной группы по кибербезопасности обсуждался между президентами двух стран Владимиром Путиным и Дональдом Трампом на полях саммита «Большой двадцатки» в Гамбурге. Ранее Трамп подвергся резкой критике за предложение создать российско-американскую структуру. Кроме того, комитет сената по разведке одобрил законопроект, обязывающий американского главу государства получать разрешение конгресса на то, чтобы сотрудничать с

Россией в области кибербезопасности» ***(Александр Панасенко. Россия призвала США создать совместную группу по кибербезопасности // ООО «АМ Медиа» (https://www.anti- malware.ru/news/2017-09-14-3/24065).- 14.09.2017).***

***

«На третьому місяці президентства Дональда Трампа президент Росії Володимир Путін направив до Держдепу дипломата для передачі плану нормалізації відносин між країнами…

Згідно з планом, спецпредставник президента РФ з кібербезпеки Андрій Крутских повинен був зустрітися з американськими колегами для консультацій з «інформаційної безпеки»...

Крім того, Росія пропонувала провести зустрічі глав ЦРУ, ФБР, Ради нацбезпеки, Пентагону з російськими колегами, і відновити канали, «закриті» за часів президентства Барака Обами...

BuzzFeed зазначає, що в цьому документі є невисловлена пропозицію Москви про те, що Трамп не приділятиме багато уваги ймовірному втручанню Росії в американські вибори…

Видання повідомляє, що на сьогоднішній день тільки невелика частина із запропонованих планом зустрічей відбулася, і багато переговорів навряд чи вже будуть проведені, так як РФ і США знаходяться в стадії дипломатичного конфлікту.

Посольство Росії в Вашингтоні відмовилося обговорювати цей документ…» ***(Росія передала США план нормалізації відносин // Високий замок online (http://wz.lviv.ua/news/206743-zmi-rosiia-peredala-ssha-plan-normalizatsii-vidnosyn).- 13.09.2017).***

***

«Вопросы кибербезопасности обсуждались на международной конференции «ERP для МСБ. Cybersecurity. Комплексная безопасность», которая состоялась 14 сентября в Университете банковского дела.

Организатором мероприятия выступил международный Финансовый Клуб «Банкир». Лигу страховых организаций Украины на конференции представлял вице- президент ЛСОУ Сергей Тарасов…

По мнению вице-президента ЛСОУ Сергея Тарасова, рост влияния IT на бизнес-процессы «приведет к росту разрушительного потенциала кибератак, потребует систематических мероприятий по безопасности и совершенствования соответствующих стандартов» ***(ЛСОУ — спикер конференции по вопросам кибербезопасности // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/lsou-spiker- konferentsii-po-voprosam-kiberbezopasnosti).- 15.09.2017).***

***

«…Министр внутренних дел Томас де Майзиер открыл новое агентство кибербезопасности в Мюнхене, в рамках централизованной попытки борьбы с киберпреступностью и цифровым шпионажем, посредством массового телекоммуникационного наблюдения, шифрования данных и сбора массовых данных…

Задачи нового агентства будут также включать «цифровую судебную экспертизу», что означает разработку методов сбора данных из Интернета. ZITiS также будет изучать, и разрабатывать, новые стратегии надзора за телекоммуникациями для других агентств» ***(Германия открывает агентство по кибернадзору «ZITiS» // Бизнес-портал fdlx.com (http://fdlx.com/tech/97952-germaniya-otkryvaet-agentstvo-po- kibernadzoru-zitis.html).- 15.09.2017).***

***

«Международное сообщество в преддверии очередной, 72-й, сессии Генеральной Ассамблеи Организации Объединенных Наций. Подготовка идет практически во всех столицах 193 государств-членах.

Распоряжением Президента Российской Федерации В.В.Путина сформирована официальная делегация во главе с Министром иностранных дел С.В.Лавровым… Следуя многолетней традиции, Россия выступит в ходе Нью-Йоркской сессии с новой дипломатической инициативой, посвященной международному нормированию в сфере кибербезопасности. Подход российской дипломатии уже получил поддержку стран-членов БРИКС, ШОС, Организации Договора о коллективной безопасности. Много внимания ему уделяется в двусторонних контактах России с Китаем, США, другими государствами… Это предложение (подготовить проект соответствующей международной Конвенции) делается особенно актуальным с учетом того, что сегодня более 30 стран занимаются практической разработкой информационного оружия. ООН с подачи дипломатии Москвы призвана внести вклад в регулирование этого острого вопроса…» ***(Александр Панасенко. Россия предложит Генассамблее ООН новый подход к кибербезопасности // AM Медиа (https://www.anti-malware.ru/news/2017-09-07- 3/23998).-07.09.2017).***

***

«Сбербанк готов создать международную технологическую платформу по кибербезопасности, призванную обеспечить постоянный обмен между компьютерными группами реагирования на чрезвычайные ситуации в разных странах мира и обнаруживать кибератаки на ранних стадиях…

С учётом экспертизы и накопленных компетенций Сбербанк готов взять на себя создание глобальной международной технологической платформы обмена информацией. Её можно создать за относительно короткое время — 1–2 года…» ***(Сбербанк планирует выход на рынок кибербезопасности // ООО «ИКС-МЕДИА» (http://www.iksmedia.ru/news/5435899-Sberbank-planiruet-***

vyxod-na- rynok.html#ixzz4s4gl5Qdl).- 08.09.2017).

***

Кіберзахист критичної інфраструктури

«Банк России разработал новые требования к информбезопасности, соблюдая которые банки должны минимизировать риски киберугроз… На этой неделе на общественное обсуждение был вывешен проект документа Банка России «Управление риском нарушения информационной безопасности на аутсорсинге», в котором ЦБ указывает на риски для информационной безопасности банка от привлечения аутсорсеров и выдвигает требования по их минимизации. Риски от привлечения сторонних организаций, указывает регулятор, в том, что можно выбрать поставщика, не обладающего нужными знаниями или ресурсами, а также в том, что сам банк может слабо контролировать его действия. Результатом некачественной работы таких компаний может стать появление уязвимости в системе информзащиты банка и даже хищения средств кредитной организации. Стандарт вступит в силу уже с 1 января 2018 года…» ***(Александр Панасенко. ЦБ усиливает требования к кибербезопасности банков // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-09-14-3/24068).- 14.09.2017).***

***

«…Энергетический сектор в Европе и Северной Америке стал целью новой волны кибератак, в ходе которых хакерам удалось взять под контроль важные элементы управления системами энергетических компаний… Группа, стоящая за этими атаками, известная как Dragonfly, активна с 2011 года, а первые попытки кибератак на энергетический сектор были предприняты в конце 2015 года. В апреле 2017 года их интенсивность в очередной раз возросла…

…В июне текущего года правительство США предупредило промышленные фирмы о хакерской кампании, нацеленной на ядерный и энергетический секторы, в ходе которой злоумышленники рассылали фишинговые письма для сбора учетных данных и дальнейшего получения доступа к целевым сетям.

Десятки компаний по всему миру были скомпрометированы в ходе хакерской атаки, в том числе в США. Злоумышленникам удалось взять под контроль основные системы управления компаний, и при желании они могли совершить диверсию.

Dragonfly, также известная как Energetic Bear и Koala, проявляла наибольшую активность по всему миру в период с 2011 года по 2014 год. По мнению экспертов по безопасности, группа связана с российским правительством…» ***(Хакеры получили доступ к европейскому и***

американскому энергетическому сектору // SecurityLab.ru (http://www.securitylab.ru/news/488274.php).- 06.09.2017).

***

Кіберзлочинність та кібертерроризм

«Еще 600 Гбайт частных файлов из двух облачных хранилищ оказались в открытом доступе.

Хранилища принадлежат компании BroadSoft, занимающейся программным обеспечением и сервисами. Они содержали частную информацию сети кабельных телеканалов Time Warner Cable (TWC): базы данных SQL, фрагменты кода, журналы доступа, адреса и телефоны пользователей. Исследователи, обнаружившие утечку, сообщают, что в одном из файлов были найдены данные четырех миллионов клиентов TWC за последние 7 лет.

Информация хранилась в двух неправильно настроенных «корзинах» Amazon Web Services S3. Такие сервера по умолчанию защищены от взлома, но в данном случае доступ оказался публичным, и просмотреть их содержимое мог кто угодно...

Kromtech Security Center — компания, обнаружившая «корзины» — сообщает, что любой аутентифицированный пользователь мог скачать все данные прямо по ссылке.

Боб Дьяченко, директор компании по связям с общественностью, объявил об утечке в пятницу. Сотрудники Kromtech нашли уязвимость в июле, вскоре после обнаружения другого незащищенного сервера S3, принадлежавшего World Wrestling Entertainment…

В одном из текстовых файлов под названием User Profile Dump 07-07-2017 содержалась информация более чем о 4 миллионах пользователей TWC, в основном взятая из приложения MyTWC. В нем пользователи могут оплачивать счета, выбирать услуги, а также работать с голосовой почтой, списками каналов и настройками Wi-Fi. Информация о клиентах TWC с 26 ноября 2010 года по 7 июля 2017 года была доступна в едином файле и включала имена пользователей, MAC- адреса, серийные номера устройств, номера учетных записей, информацию об услугах, их категориях и идентификаторы транзакций...

Во вторник представитель BroadSoft сообщил Threatpost, что компания исправила проблему, как только узнала о ней…» ***(Четыре миллиона документов Time Warner Cable в неправильно настроенной «корзине» Amazon S3 // Threatpost (https://threatpost.ru/four-million-time-warner-cable-records-left-on-misconfigured-aws-s3/22197/).- 07.09.2017).***

***

«Компания ESET, разработчик антивирусного программного

обеспечения иэксперт в области кибербезопасности, сообщила о новой волне интернет-мошенничества: злоумышленники рассылают фишинговые письма от имени платежной системы Mastercard…

Для кражи данных пользователей мошенники используют взломанный сайт правительства Мексики…

Специалисты ESET сообщили об инциденте в Центр реагирования на компьютерные угрозы Мексики.

В Mastercard сообщили, что платежная система не направляет никаких сообщений или запросов физическим лицам…» ***(Интернет-мошенники атаковали банковские карты Mastercard // ИА "Олигарх Медиа" (https://oligarh.media/2017/09/06/internet-moshenniki-atakovali-bankovskie-karty-mastersard/).- 06.09.2017).***

***

«В Соединенных Штатах Америки бюро кредитных историй Equifax было подвержено кибератаке, в результате чего было похищено информацию 143 млн клиентов службы.

…Уже установлено, что подготовка к атаке началась еще а мае. Отмечается, что похитителям стали изветсны данные имен, номеров карт и шифров социальной страховки клиентов ведомства. Более 209 тыс кодов кредитных карт похищены киберпреступниками. Также хакерам стали открыты данные об водительских удостоверениях клиентов…» ***(В США произошла масштабная кибератака // Украинское рейтинговое агентство "УРА" (http://ura- 65 inform.com/ru/neformat/2017/09/08/v-ssha-proizoshla-masshtabnaja-kiberataka).- 08.09.2017).***

***

«…Футбольная ассоциация Англии (The Football Association, FA) порекомендовала игрокам английской сборной и обслуживающему персоналу не использовать Wi-Fi-сети в общественных местах и гостинницах во время ЧМ-2018, который пройдет в России, из-за угрозы хакерских атак...

Опасения относительно хищения данных возросли после взлома хакерской группировкой Fancy Bear электронной почты руководства FIFA в августе текущего года. Хакеры опубликовали в открытом доступе данные о футболистах, предположительно принимавших запрещенные препараты. Согласно опубликованным данным, в 2015 году 160 игроков не прошли допинг-контроль, а в 2017 году их число увеличилось до 200…» ***(Футбольная ассоциация Англии опасается атак российских хакеров во время ЧМ-2018 // SecurityLab.ru http://www.securitylab.ru/news/488390.php).- 12.09.2017).***

***

«Внаслідок хакерської атаки постраждали не лише топ-50 акаунтів, а

й профілі звичайних користувачів. Зловмисники намагаються продавати приватні дані…

За даними компанії RepKnight, що спеціалізується на кібербезпеці, атаки зазнали акаунти таких знаменитостей як: Емма Ватсон, Леонардо ДіКапріо, Вікторія Бекхем, Бейонсе, Леді Гага, Ріанна, Адель, Брітні Спірс, Зінедін Зідан, Девід Бекхем та інші.

Раніше повідомлялось, що хакери з OurMine зламали сайт WikiLeaks . Хакерське угрупування OurMine відоме тим, що у різний час зламало акаунти засновника соцмережі Facebook Марка Цукерберга, CEO компанії Google Сундара Пічаї, CEO Twitter Джека Дорсі, засновника компанії Niantic Labs та творця гри Pokémon Go Джона Ханке й сайту Buzzfeed. Також серед останніх «перемог» OurMine - акаунти телемережі HBO у Twitter та Facebook…» ***(Злам Instagram: хакери могли отримати доступ до 6 мільйонів акантів // Детектор медіа (http://osvita.mediasapiens.ua/web/cybersecurity/zlam_instagram_khakeri_mogli_otrim ati_dostup_do_6_milyoniv_akauntiv/).- 04.09.2017).***

***

«Эксперты отмечают всплеск числа атак на смартфоны и планшеты на базе Android. Во втором квартале 2017 г., по сравнению с тем же периодом прошлого года, этот показатель вырос почти на 40%.

Как говорится в новом исследовании компании Avast, среднемесячный показатель атак на смартфоны и планшеты на базе Android увеличился с 1,2 миллиона до 1,7 миллиона. Исследователи выяснили, что в месяц в среднем появляется 788 новых вариантов вирусов — на 22,2% больше, чем во втором квартале 2016 г. В отчете также указывается, что три самые распространенные мобильные угрозы — это ПО, разработанное для шпионажа и кражи личных данных («перехватчики root-доступа»), а также для показа пользователям нежелательной рекламы («загрузчики/дропперы» и «фейковые приложения»)…

Чтобы успешно бороться с современными киберугрозами, Avast обновила мобильные приложения Avast Mobile Security & Antivirus и AVG AntiVirus…»
(Число мобильных кибератак выросло на 40% // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5436593-Chislo-mobilnyx-kiberatak-vyroslo.html#ixzz4sSpkOE2d).- 12.09.2017).

***

«Група зловмисників експлуатує CDN-сервери Facebook для зберігання шкідливих файлів, які потім використовуються для інфікування систем користувачів банківськими троянами. В останні два тижні дослідники в області безпеки помітили кілька подібних кампаній…

Нова шкідлива кампанія була помічена експертом в області безпеки, відомим в Мережі як MalwareHunter. Зловмисники використовують CDN-сервери Facebook, оскільки домену Facebook «довіряє» більшість захисних

рішень…» ***(Хакери використовують CDN-сервери Facebook для обходу антивіруса // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2017/09/11/fb-sdn-servers- used.html).- 11.09.2017).***

***

«Стремясь защититься от хакеров, штат Вирджиния в США проводит замену электронных избирательных машин, которые используются для прямого голосования на выборах…

…штат установит такие аппараты, которые будут «продуцировать бумажное свидетельство» волеизъявления… Эти терминалы предлагают избирателю бумажный бюллетень, который он заполняет своей рукой, а аппарат потом сканирует и учитывает результат. Таким образом, с помощью бюллетеней можно будет в любой момент перепроверить результаты голосования в случае взлома электронной системы подсчета голосов.

Распоряжение о переоборудовании отдал Избирательный совет штата по рекомендации Департамента выборов. Власти мотивировали это тем, что в последнее время в США возросла опасность вмешательства хакеров в избирательный процесс, поэтому результаты голосования следует дополнительно сохранять на бумаге. Правительство опирается на многочисленные сообщения о подрывной деятельности иностранных держав на выборах президента США в 2016 г., которые циркулируют в американском информационном поле…» ***(Из-за хакеров штаты США меняют электронные избирательные машины на бумажные бюллетени//Информационнаябезопасность (http://www.itsec.ru/newstext.php?news_id=118578).- 11.09.2017).***

***

«Российские страховые компании наблюдают рост спроса на полисы страхования киберрисков после нашумевших атак WannaCry и NotPetya.

В США и Европе организации страхуют риски при работе с персональными данными (банковские карты, паспортные данные). В России же 8 из 10 запросов на страхование в области кибербезопасности касаются рисков простоя из-за киберинцидентов.

…стоимость услуг по страхованию от киберрисков варьируется от $100 тыс. для банков и крупных финорганизаций до менее $5 тыс. для средних компаний из других индустрий. Цена зависит от величины компании, сферы ее деятельности и рисков, которые необходимо покрыть…

Эксперты прогнозируют небольшой рост российского рынка киберстрахования в ближайшие 12 месяцев – на 5% в сегменте страхования от компьютерных инцидентов и на 15% в области комплексного страхования киберрисков…» ***(Спрос на страхование от кибератак вырос на фоне кампаний***

WannaCry и NotPetya // Информационная безопасность (http://www.itsec.ru/newstext.php?news_id=118588).- 12.09.2017).

***

«Федеральный суд Восточного округа штата Вирджиния вынес приговор 25-летнему Джастину Ливерману, участнику хакерской группировки Crackas With Attitude.

Группировка «прославилась» осенью 2015 года, когда смогла получить доступ кличным адресам электронной почты и телефонам нескольких крупных американских чиновников, включая тогдашнего директора ЦРУ Джона Бреннана, занимавшего пост директора Национальной разведки Джеймса Клэппера и заместителя директора ФБР Марка Джулиано…

В результате в руках участников Crackas With Attitude оказались некоторые конфиденциальные документы, которые были переданы организации WikiLeaks. Кроме того, хакеры принялись постоянно бомбардировать жертв письмами и SMS- сообщениями с оскорблениями и угрозами. Организация таких рассылок и была основной задачей Джастина Ливермана. В частности, он сильно осложнил жизнь Марка Джулиано. На протяжении месяца заместитель директора ФБР каждый час получал SMS с угрозами, причем касавшимися не только самого Джулиано, но и его жены и сына.

Разумеется, правоохранители не могли не отреагировать на такую дерзость… …суд приговорил хакера к максимально возможному в данной ситуации наказанию – 5 годам тюрьмы и штрафу в 145 тысяч долларов» ***(Не грози директору ФБР // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5436880-Ne-grozi-direktoru-FBR.html#ixzz4se1SgimO).- 12.09.2017).***

***

«По данным американской компании FireEye, занимающейся исследованиями в области кибербезопасности, северокорейские хакеры перешли на взлом криптовалютных бирж и похищение биткойнов и других криптовалют.

…если в 2016 году наблюдались многочисленные случаи хакерских атак при поддержке северокорейского государства в отношении банков и глобальной финансовой системы, то сейчас поднимается «вторая волна этой кампании: поддерживаемые государством исполнители похищают биткойны и другие виртуальные валюты». По мнению специалистов FireEye, причина активизации этих действий заключается как в ужесточении санкций, так и в росте популярности крипто валют.

С мая FireEye зарегистрировала по меньшей мере три попытки взлома южнокорейских криптовалютных бирж с целью похищения средств. Для взлома использовался выборочный фишинг, когда сотрудники этих бирж

получали по электронной почте письма с вредоносным ПО или текстом, который должен был ввести получателя в заблуждение и убедить его предоставить личные данные…» ***(Северокорейские хакеры меняют ориентацию // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5437073-Severokorejskie-xakery-menyayut- ori.html#ixzz4se1uiFRS).- 13.09.2017).***

***

«…Министерство обороны Швейцарии подверглось кибератаке. Об этом сообщило правительство страны. Кибератака была предпринята в июле нынешнего года.

В ходе хакерской атаки на ряд серверов минобороны и партнерской организации министерства иностранных дел Швейцарии злоумышленники использовали широко известное вредоносное ПО Turla, предназначенное для кибершпионажа. Как сообщается, специалистам удалось заметить и остановить нападение.

Правительство отказалось раскрыть информацию об источнике кибератаки и ущербе (в том числе возможной утечке данных), который она нанесла. Оборонное ведомство и МИД Швейцарии направили жалобу в федеральную прокуратуру. В настоящее время ведется расследование инцидента…» ***(Минобороны Швейцарии подверглось кибератаке // SecurityLab.ru (http://www.securitylab.ru/news/488529.php).- 17.09.2017).***

***

«…Британский хакер Шон Кэффри (Sean Caffrey), получивший несанкционированный доступ к данным спутниковой системы связи Минобороны США, получил условный тюремный срок. Хакер признал свою вину и был приговорен к 18 месяцам лишения свободы условно с испытательным сроком на тот же период.

Королевский суд Бирмингема признал, что Кэффри похитил учетные данные и адреса электронной почты более 800 пользователей системы спутниковой связи, а также пользователей 30 тыс. спутниковых телефонов.

По словам представителей Министерства обороны США, для восстановления систем после атаки 2014 года потребовалось порядка 50 часов и $628 тыс.

Кэффри был арестован в марте 2015 года. Как тогда сообщило Национальное агентство по борьбе с преступностью Великобритании (NCA), хакер взломал мобильную спутниковую службу, которую Пентагон использовал для связи со своими сотрудниками по всему миру…» ***(Взломавший спутниковую систему связи США хакер приговорен к 18 месяцам заключения // SecurityLab.ru (http://www.securitylab.ru/news/488510.php).- 15.09.2017).***

***

«…Музыкальный видеохостинг Vevo стал жертвой кибератаки. Хакеры опубликовали 3,12 ТБ внутренних документов, видео и рекламных материалов.

…Большинство утекших файлов Vevo представляли собой еженедельные музыкальные чарты, планы по распространению социального медиаконтента и различные подробности об исполнителях, однако часть документов содержала конфиденциальную информацию.

Ответственность за утечку взяла на себя хакерская группировка OurMine.

Группировка получила известность после серии громких хакерских атак, в том числе на WikiLeaks, HBO и исполнительного директора Google Сундара Пичаи.

Vevo - популярный музыкальный видеохостинг, совместный проект Universal Music Group, Sony Music Entertainment и Warner Music Group. Сервис предлагает порядка 250 тыс. официальных музыкальных видеороликов на официальном сайте и своем канале в YouTube…» ***(Видеохостинг Vevo стал жертвой хакерской атаки // SecurityLab.ru (http://www.securitylab.ru/news/488504.php).- 15.09.2017).***

***

«…Израильская компания в сфере кибербезопасности заявила, что опасное вредоносное ПО проникло в Google Play, атаковав 21 млн пользователей.

Согласно Fortune, аналитики Check Point Software Technologies сообщили в своем блоге о том, что атака состоит из десятков вредоносных приложений, которые отправляют мошеннические текстовые сообщения и выставляют пользователям счета за несуществующие услуги…

Вирус получил название «ExpensiveWall» в честь одного из мошеннических приложений «Lovely Wallpaper», который якобы предлагал различные фоновые изображения для смартфонов. Среди других взломанных приложений «I Love Filter», «Tool Box Pro» и «Horoscope».

По меньшей мере 50 приложений, которые пользователи Android загрузили около 4 млн раз, были взломаны новой формой вредоносного ПО, которое использовало метод «упаковки» – сжимание кода с помощью шифрования, что позволяет ему уклоняться от фильтров безопасности Google. Check Point опубликовала полный список известных вредоносных приложений на своем веб- сайте...» ***(Google Play поразил новый вирус, который атаковал 21 млн пользователей //PaySpaceMagazine «доступно о платежах» (https://psm7.com/news/google-play- porazil-novyj-virus-i-atakoval-21-mln-polzovatelej.html).- 15.09.2017).***

***

«Приложение CCleaner подверглось хакерской атаке, которая позволила похитить данные пользователей...

Вредоносный код обнаружили в 32-битной версии CCleaner 5.33.6162 (выпущена 15 августа) и версии CCleaner Cloud 1.07.3191 (выпущена 24 августа). О том, что эти версии программы ведут себя некорректно, стало известно 12 сентября. Тогда же были выпущены безопасные обновления.

Оба приложения после обновления до взломанных версий начинали отправлять имя компьютера, его IP-адрес, список установленных программ и сетевых адаптеров на специальный сервер на территории США. Этот сервер был отключен правоохранительными органами 15 сентября…

Кто стоит за атакой, неизвестно, но хакеры получили доступ к серверу, на котором создается очередная версия CCleaner. Атаку обнаружили специалисты антивирусной компании Avast…» ***(Хакеры взломали приложение для «чистки» компьютера CCleaner // Meduza(https://meduza.io/news/2017/09/18/hakery-vzlomali-prilozhenie-dlya-prilozhenie-dlya-chistki-kompyutera-ccleaner).- 18.09.2017).***

***

«Специалисты из FireEye подробно рассказали об активности кибершпионской группировки из Ирана APT33… Хакеры проявляют интерес, прежде всего, к аэрокосмическим и энергетическим промышленным предприятиям, а также к военным объектам.

Хакеры из APT33 действуют с 2013 года. Кибергруппировка осуществляет рассылку фишинговых писем. Обычно в письмах, замаскированных под объявления о работе, присутствует вредоносная ссылка. Если пользователь переходит по ней, то запускается процесс установки вредоносной программы на компьютер. Злоумышленники активно проводили фишинговые кампании на протяжении всего прошлого года.

Специалисты утверждают, что в APT33 действуют хакеры высокого уровня, которые даже зарегистрировали домены подставных фирм для создания видимости законной деятельности…

Исследователи выяснили, что APT33 пользуется утилитой собственной разработки DropShot для того, чтобы устанавливать на целевых устройствах вредоносную программу ShapeShift. Это модифицированный вариант программы Shamoon, которая в этом году атаковала саудовские нефтедобывающие компании…» ***(Хакеры из Ирана атаковали аэрокосмические и энергетические предприятия Саудовской Аравии // SecureNews (https://securenews.ru/apt33/).- 21.09.2017).***

***

«Команда экспертов по кибербезопасности MalwareHunterTeam обнаружила вирус nRansomware (Troj.W32.Inject.tnKf), который требует выслать фотографии ню за возможность получить доступ к заблокированным файлам.

Исследователи выложили скриншот, на котором запечатлены условия,

появляющиеся на экране зараженного PC (на фоне красуется паровозик Томас и играет композиция из ТВ-шоу «Умерь свой энтузиазм»)…» ***(Basil Naumov. Новый вирус вымогает интимные фото // Game2Day.org (https://game2day.org/news/23339/novyi-virus-trebuet-fotografii-nju-chtoby-razblokirovat-pc).- 24.09.2017).***

***

«Специалисты по кибербезопасности из компании McAfee назвали самого опасного персонажа интернета. Главным злодеем оказалась канадская певица Аврил Лавин, не выпускавшая альбомов с 2013 года, но исправно поставляющая в сеть вредоносный контент имени себя.

По результатам анализа, проведенного специалистами McAfee, именно в материалах, связанных с именем поп-панк-певицы, злоумышленники чаще всего размещают небезопасное ПО.

Аврил Лавин стала самой вредоносной знаменитостью, поскольку ссылки, которые поисковик выдает пользователям по запросу ее бесплатных MP3, с вероятностью в 22 процента приведут на вирусный сайт…» ***(Эксперты назвали самого опасного человека в интернете // ООО "Национальные информационные системы" (http://podrobnosti.ua/2200883- eksperty-nazvali-samogo-opasnogo-cheloveka-v-internete.html).- 25.09.2017).***

***

«…Хакери РФ атакували 21 штат США під час виборів американського президента 2016 року. Деякі системи кіберзахисту були прорвані, інформує «Голос Америки» з посиланням на Міністерство внутрішньої безпеки США.

У міністерстві не уточнили, чи змогли російські хакери впливати на результати волевиявлення американського народу. Адміністратор Виборчої комісії штату Вісконсін Майкл Гаас повідомив, що «кібергравці російського уряду» атакували систему реєстрації виборців штату...

Пізніше факт атак на виборчі системи підтвердили представники штатів Алабама, Огайо, Колорадо, Міннесота, Коннектикут і Вашингтон…

Раніше ЗМІ повідомляли, що за низкою гучних кібератак, швидше за все, стоїть російська хакерська група APT28, також відома як Fancy Bear, Pawn Шторм або Sofacy. Деякі фахівці з кібербезпеки стверджували, що угруповання Strontium працює на російську військову розвідку і несе відповідальність за злам електронних листів Демократичної партії США, зокрема виборчого штабу кандидата в президенти США Хілларі Клінтон…» ***(Кремлівські хакери атакували понад 20 американських штатів під час виборів — ЗМІ // Racurs.ua (http://ua.racurs.ua/news-94375-kremlivski-hakery- atakuvaly-ponad-20-amerykanskyh-shtativ-pid-chas-vyboriv-zmi).- 23.09.2017).***

***

«…В 2013 году Европейская комиссия заказала у голландской организации Ecorys исследование стоимостью €360 000 о том, как пиратство влияет на продажи музыки, книг, фильмов и игр в ЕС. Со временем об этом исследовании забыли, но в июле 2017 года депутат ЕС Джулия Реда подала заявку на получение доступа к информации о результатах исследования. Изучив материалы, она доказала, что за исключением недавно выпущенных блокбастеров, нет никаких доказательств в поддержку идеи о том, что нарушение авторских прав в Интернете негативно влияет на продажи контента.

Европейская комиссия прекратила исследование после того, как специалисты Ecorys заявили, что пиратство блокбастеров негативно влияет на их продажи. Они пришли к выводу, что на десять загрузок приходится примерно четыре посещения кинотеатра. В целом это уменьшает продажи определённых фильмов примерно на 4,4%. Членов Еврокомиссии такой результат удовлетворил, и они прекратили исследование…» ***(Еврокомиссия неожиданно пришла к выводу, что пиратство не вредит продажам // IGate (http://igate.com.ua/lenta/20076-evrokomissiya-neozhidanno- prishla-k-vyvodu-chto-piratstvo-ne-vredit-prodazham).- 25.09.2017).***

***

«…С января по март 2017 года количество кибератак в мире выросло в 4 раза. Такие данные содержатся в отчете по киберугрозам за первый квартал 2017 года, опубликованном компанией Microsoft...

Согласно исследованию, в первом квартале 2017 года 14,8% компьютеров в России столкнулись с вредоносным ПО, в то время как средний показатель по миру составил 9%. Тем не менее, исследователи отмечают тенденцию к снижению количества киберугроз в России с 17,2% в феврале до 12% в марте текущего года.

С ростом популярности облачных сервисов число атак на них также возросло. В частности, компания зафиксировала рост несанкционированных попыток входа в учетную запись Microsoft с вредоносных IP-адресов на 44%, став главной причиной заражения облачных сервисов (51%)…

По словам исследователей Microsoft, самым распространенным типом угроз в указанный период стали трояны (10,26%), инсталляторы нежелательного ПО (1,5%), вредоносные модификаторы браузеров (2,14%), дропперы (0,64%) и рекламное ПО (0,25%)» ***(В 1 квартале 2017 года Россия стала лидером по числу заражений вредоносным ПО // SecurityLab.ru (http://www.securitylab.ru/news/488675.php).- 22.09.2017).***

***

«…исследователи безопасности из Trend Micro зафиксировали новую массовую спам-рассылку с использованием вымогательского ПО Locky. Количество вредоносных писем уже преодолело отметку в несколько

миллионов.
В рамках кампании операторы Locky используют несколько типов спам-писем… Все письма содержат архив с расширением .7z. В архиве находится вредоносный VBS-скрипт, который при исполнении загружает вымогательское ПО Locky на компьютер пользователя.

По данным исследователей, основными объектами атак злоумышленников стали Чили, Япония, Индия и США. На долю России в среднем пришлось 6% от общего количества атак…» ***(Обнаружена новая масштабная спам-кампания по распространению Locky // Internetua (http://internetua.com/obnarujena-novaya-masshtabnaya-spam- kampaniya-po-rasprostraneniua-Locky).- 26.09.2017).***

***

«Западный мир готовиться к самой мощной за свою историю кибератаке…

«Самая мощная из всех возможных кибератак, кибератака «первой категории» произойдет в ближайшие несколько лет» - сообщает Национальный центр кибербезопасности (NCSC) Великобритании.

В своем докладе, направленному Центру правительственной связи, эксперты по кибербезопасности призвали правительство принять меры, чтобы защититься от злоумышленников…

Технический директор Национального центра кибербезопасности Ян Леви считает, что в ближайшее десятилетие произойдет самая мощная кибератака – атака первой категории – и единственный способ предотвратить ее – это изменить представление бизнеса и правительства о кибербезопасности.
Вместо того чтобы скупать антивирусный софт и выстраивать вокруг себя фаерволы, организации должны переосмыслить, какой информацией они владеют, какую ценность она несет и насколько большой бедой будет потерять ее, - считает Леви…

Ян Леви считает, что путь к спасению от хакеров – в переосмыслении отношения к персоналу…

Проблема состоит в том, что компьютерные системы создаются техниками для техников. И потому простые работники практически ничем не могут помочь в плане кибербезопасности, в то время как хакеры хорошо осведомлены о том, как работают программы. Леви же считает, что надо не искать готовых решений, покупая софт, а общаться с работниками и выявлять, что они могут сделать для безопасности компании…» ***(Дмитрий Малышко. Ян Леви: Грядет кибератака невиданной силы // Internetua (http://internetua.com/yan-levi--gryadet-kiberataka-nevidannoi-sili).- 25.09.2017).***

***

«В марте и мае этого года хакеры осуществили атаку на консалтинговую компанию «Deloitte», являющуюся лидером в сфере

кибербезопасности, и похитили конфиденциальную информацию миллионов американцев…

Среди ее клиентов банки, международные корпорации, мировые СМИ, фармацевтические гиганты и государственные учреждения…

Злоумышленники смогли скомпрометировать электронный адрес Deloitte через «учетную запись администратора». Взломать ее было проще простого, ведь учетная запись затребовала только один пароль и не имела «двухэтапной» проверки…

Есть подозрения, что в следствии кибератаки в марте и мае были украдены данные 143 млн. американцев и 400 тыс. британцев…

По всей видимости, атака была нацелена на американские компании. На данный момент, по крайней мере, шесть компаний-клиентов сообщили о том, что их информация была украдена.

На данный момент, не ясно, кто «хакнул» почту и по чьему заказу. Сейчас эксперты пытаются определить путь, по которому пришли хакеры. Компания наняла юридическую контору Хогана Ловелла, чтобы та оценила так называемый «случай нарушения кибербезопасности». Также над круглосуточным обеспечением безопасности клиентов работают эксперты из отдела кибер-расследований самой компании Deloitte..» ***(Дмитрий Малышко. Лидер в сфере кибербезопасности «Deloitte» стал жертвой хакеров // Internetua (http://internetua.com/lider-v-sfere-kiberbezopasnosti--Deloitte--stal-jertvoi-akerov).- 26.09.2017).***

***

«…В последнее время участились случаи утечек конфиденциальных данных с серверов Amazon S3…

Компании придерживаются ошибочного мнения, будто, если ссылка есть только у сотрудников, то никто посторонний получить доступ к хранилищу не может. Тем не менее, злоумышленники могут получить ее с помощью MitM-атаки на корпоративную сеть, брутфорс-атаки на доменные имена с целью выявления скрытых URL-адресов и другими способами. На первый взгляд задача кажется трудновыполнимой. Тем не менее, на GitHub представлены инструменты с открытым исходным кодом, упрощающие поиск открытых хранилищ S3 и ставящие под угрозу множество компаний.

По статистике компании Skyhigh Networks, у 7% от всех хранилищ S3 активирован неограниченных общественный доступ, а у 35% отсутствует шифрование. Судя по представленным данным, проблема приобретает характер эпидемии по всей инфраструктуре Amazon S3» ***(Обнаружена причина участившихся утечек данных из хранилищ Amazon S3 // SecurityLab.ru (http://www.securitylab.ru/news/488718.php).- 26.09.2017).***

***

«Конгресс США отложил слушания с участием Евгения

Касперского… Министерство внутренней безопасности США подозревает «Лабораторию Касперского» в кибершпионаже во время прошлогодних президентских выборов. Сам Касперский отрицает обвинения в работе на российское правительство…

Процедура дачи показаний должна была состояться 27 сентября. Вместе с Касперским в ней планировалось участие независимых американских экспертов по кибербезопасности» ***(В США отложили слушания с Касперским // «Открытые системы» (https://www.computerworld.ru/news/V-SShA-otlozhili-slushaniya-s-Kasperskim).- 22.09.2017).***

***

«…Россия вступила в спор с США за арестованного в Греции гражданина РФ Александра Винника. Американцы требуют его выдачи по заочному обвинению в отмывании $4 млрд через криптовалютную биржу BTC-E. В свою очередь, российские правоохранительные органы обвиняют господина Винника в мошенничестве более чем на 600 тыс. руб. По международному законодательству Россия имеет приоритетное право на возвращение своего гражданина, тем более что Александр Винник уже согласился на добровольную экстрадицию на родину.

Уголовное дело в отношении 38-летнего Александра Винника было возбуждено по ч. 3 ст. 159 УК РФ (мошенничество в крупном размере) следственным отделом ОМВД России по Останкинскому району Москвы. …основанием для этого стало заявление представителей одной из коммерческих структур. Ее представители заключили с господином Винником договор на поставку оборудования и перевели на его счет более 600 тыс. руб. Однако товар коммерсанты так и не получили…

10 августа 2017 года Александру Виннику предъявили заочное обвинение в мошенничестве и объявили его в розыск. ...через неделю Генпрокуратура России обратилась в Министерство юстиции, прозрачности и прав человека Греции с запросом о выдаче россиянина…

…если бы российская сторона оперативно не вмешалась в эту ситуацию, то господин Винник, скорее всего, уже давно был бы выдан США. …россиянина задержали по их запросу еще 25 июля в курортном поселке Уранополис в Халкидиках в одном из самых дорогих отелей, куда он приехал на отдых. По решению местной прокуратуры задержанного поместили под арест на максимально возможные два месяца до рассмотрения запроса об экстрадиции в США (срок содержания истек 25 сентября).

…Согласно данным ФБР, махинациями с криптовалютой господин Винник начал заниматься еще в 2011 году, конвертируя свои криминальные доходы в американский доллар и российский рубль через счета подконтрольных ему компаний. Именно тогда была взломана японская биржа Mt. Gox, что впоследствии привело к ее банкротству. Специалисты японской компании WizSec, занимающейся вопросами кибербезопасности и, в частности,

расследованием взлома биржи Mt. Gox, считают, что около 300 тыс. биткойнов ($800 млн) было выведено через BTC-E на различные счета, контролируемые господином Винником в банках Латвии и Кипра.

Впрочем, сам россиянин все обвинения США в свой адрес отрицает и от добровольной экстрадиции в эту страну, где ему грозит до 55 лет тюремного заключения и штраф в размере $12 млн, отказался. Его судьба, судя по всему, решится 29 сентября, когда в Греции состоится судебное заседание по делу об экстрадиции...» ***(Олег Рубникович. У каждого биткойна есть две стороны // Газета «Коммерсантъ» (https://www.kommersant.ru/doc/3422936).- 28.09.2017).***

***

«Банковский троян на операционной системе Android сумел во второй раз проникнуть в магазин приложений Google Play Store и инфицировать тысячи устройств, прежде чем был обнаружен… Приложение под названием BankBot впервые было обнаружено в магазине ранее в этом году, оно занимается кражей банковской информации при помощи поддельной страницы ввода данных. В апреле программа была убрана из магазина, но в начале сентября обнаружена снова…

Новая версия BankBot оказалась изощрённее первоначальной: улучшена обфускация кода и используется сервис специальных возможностей Android, как это делают другие банковские трояны…

Если раньше программа пыталась выдавать себя за некоторые банковские приложения, в которые пользователи вводят конфиденциальные данные, то теперь она имитирует Google Play. При запуске Google Play пользователю предлагается ввести данные кредитной карты…» ***(Алексей Алтухов. Банковский Android-троян BankBot стал опаснее прежнего//OSzone.net (http://www.oszone.net/31697/data_stealing_Android_malware_BankBot_is_back). - 28.09.2017).***

***

«Департамент киберполиции Украины задержал мошенника, который создавал сайты для кражи данных по банковским картам. Фишинговые сайты выманивали секретные данные по платежным картам, предлагая несуществующие услуги…

…фишинговые сайты работают по следующей схеме: отправитель указывает данные своей карты и номер карты получателя денег. В момент совершения перевода специальная программа переадресует операцию на легитимный ресурс для денежных переводов. Однако мошенническая программа подменяет номер карты получателя средств, а также меняет сумму транзакции…» ***(В Украине арестован преступник, который создавал фишинговые сайты //PaySpaceMagazine «доступно о платежах» (https://psm7.com/news/v-ukraine-arestovan-prestupnik-kotoryj-sozdaval-***

fishingovye-sajty.html).- 28.09.2017).

***

«Вирусы-вымогатели станут одной из главных киберугроз в 2017 году, говорится в докладе Европейского полицейского агентства…

Также в сообщении говорится об угрозе со стороны бот-сетей, действующих через инфицированные небезопасные устройства интернета вещей, а также со стороны теневого интернета» ***(Европол назвал главные киберугрозы 2017 года // АО «Газета.Ру» (https://www.gazeta.ru/tech/news/2017/09/27/n_10623236.shtml).- 27.09.2017).***

***

«Хакери, які працюють на угруповання "Ісламська держава", …створюють дуже недосконалі віруси та шифрувальні програми, які легко зламати, розповів дослідник з кібербезпеки Кайль Вілхойт на конференції DerbyCon…

У рамках свого дослідження він проаналізував три типи інструментів, створених хакерами з так званого Об'єднаного кібер-халіфату (UCC). Ця організація об'єднує 17 груп хакерів, які заявили про свою підтримку "ІД".

Ці інструменти мали такі проблеми:

Шкідливі програми містили велику кількість помилок.

Розроблена ними система електронної пошти сприяла витоку інформації про її користувачів.

Інструмент, який використовували хакери для атаки, не зміг досягти жодної цілі.

Крім того, спробами "ІД" збирати кошти через пожертви чи біткоїни скористалися шахраї: вони почали створювати веб-сайти, що імітують прохання "ІД" про фінансову допомогу, й збагачуватися на цьому…

Протягом останнього року UCC почала переходити на хакерські інструменти, які використовують західні кіберзлочинці…» ***(Дослідження: хакери "ІД" – дилетанти // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/dosl%d1%96djennia-hakeri-%d1%96d-diletanti.html).- 26.09.2017).***

***

«…Персональні дані українців продавав у інтернеті колишній працівник пенсійного фонду. Про це повідомляє департамент кіберполіції Нацполіції України.

Під час обшуків за місцем проживання 40-річного жителя Київщини правоохоронці вилучили комп'ютерне обладнання та мережеву техніку, за допомогою якої він розповсюджував дані…

Наразі встановлюється, яким чином чоловік отримував доступ до цих баз даних. Кіберполіція не виключає, що зловмисник, маючи відповідну технічну

освіту, самостійно втручався в роботу комп'ютерів користувачів і заражав їх шкідливим програмним забезпеченням для отримання необхідної інформації. Відкрито кримінальне провадження за ч.2 ст.362 (несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) КК України.

Також вирішується питання щодо відкриття провадження за ст.361 КК України (незаконне втручання в роботу комп'ютерів, систем та комп'ютерних мереж)…» ***(Колишній держслужбовець торгував в інтернеті персональними даними українців // Racurs.ua (http://ua.racurs.ua/news-94586-kolyshniy-derjslujbovec-torguvav-v-interneti-personalnymy-danymy-ukrayinciv-foto).- 27.09.2017).***

***

«Національне агентство поліції Південної Кореї повідомляє про спроби хакерів з КНДР зробити атаки на криптовалютні біржі країни. Розслідування інциденту веде відділ кібербезпеки правоохоронних органів Південної Кореї…

…хакери відправили 25 фахівцям, пов'язаним з чотирма bitcoin - біржами, листи з вірусами. Відправники видавали себе за поліцейських і співробітників державних установ.

У поліції також повідомили, що десять листів були відправлені в липні і серпні. Влада відзначає, що хакерам не вдалося нанести "реальні збитки"…» ***(У Південній Кореї заявили про кібератаки хакерів з КНДР на криптовалютні біржі // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/y-p%d1%96vdenn%d1%96i-kore%d1%97-zaiavili-pro-k%d1%96berataki-haker%d1%96v-z-kndr-na-kriptovalutn%d1%96-b%d1%96rj%d1%96.html).- 27.09.2017).***

***

«Группа киберпреступников Phantom Squad назвала дату массовой DDoS- атаки на тысячи корпораций по всему миру…

…массовый взлом назначен на 30 сентября… Хакеры требуют выкуп в размере 0,2 биткоина (около 720 долларов), в противном случае они грозят обрушить сайты компаний.

Тем временем, эксперты считают, что Phantom Squad лишь запугивают крупнейшие корпорации с целью обогащения, тогда как не обладают достаточной мощью для одновременного запуска DDoS-атак, рассчитанных на такое количество целей…» ***(Хакеры готовят массовую атаку на крупнейшие компании мира // "Херсон Daily" (https://khersondaily.com/news/hakery-gotovjat-massovuju-ataku-na- krupnejshie-kompanii-mira).- 29.09.2017).***

***

«В Таллинне в рамках неформальной встречи министров стран ЕС проходят киберучения для министров обороны…

Цель учений под названием EU CYBRID 2017 – отработка реакции ЕС на потенциальные атаки хакеров на военные структуры блока.

Согласно сценарию, хакеры осуществляют атаку на командование морской миссией ЕС в Средиземном море и начинают кампанию в социальных сетях, чтобы дискредитировать операции и вызвать протесты.

Каждый из министров обороны стран-членов ЕС будет пытаться устранить кризис во время проведения учений…» ***(В Таллинне проходят киберучения для министров обороны стран ЕС // Европейская правда (http://www.eurointegration.com.ua/rus/news/2017/09/7/7070635/).- 07.09.2017).***

***

«13 вересня Міністерство внутрішньої безпеки США заборонило федеральним компаніям користуватися програмним забезпеченням російської компанії Kaspersky Lab…

Влада США наголосила на тому, що антивірусні продукти компанії забезпечують широкий доступ до файлів і документів на комп'ютерах, на яких вони встановлені, та можуть бути використані зловмисниками для послаблення інформаційних систем, якими користуються чиновники в США.

У міністерстві заявили, що використання програмного забезбечення Kaspersky Lab у федеральних інформаційних системах несе в собі ризики для національної безпеки США.

Директива дає американським установам 30 днів на те, щоб визначити, чи використовують вони якісь продукти компанії Kaspersky Lab. Програмне забезпечення має бути вилучене з усіх інформаційних систем протягом 90 днів.

Генеральний директор компанії Kaspersky Lab Євген Касперський, що його компанія «не допомагала й не допомагатиме жодному уряду в світі в його кібершпигунстві чи спробах кібератак»…

За його словами, жоден достовірний доказ не був публічно представлений жодною організацією чи особою, оскільки обвинувачення базуються на фальшивих твердженнях та неточних припущеннях, якими є і твердження про вплив російських законів та політики на компанію. Пан Касперський заявив також, що Kaspersky Lab не підпадає під закони, про які йдеться в директиві США, а інформація, отримана компанією, захищена відповідно до законодавчих вимог та суворих галузевих стандартів, зокрема й за допомогою шифрування…» ***(США заборонила державним компаніям користуватися продуктами KasperskyLab // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/ssha_zaboronila_derzhavnim_kompani yam_koristuvatisya_produktami_kaspersky_lab/).- 14.09.2017).***

***

«Керівник російської компанії "Лабораторія Касперського" запрошений на слухання до Комітету Палати представників США з питань науки, космосу й технологій щодо можливості використання його антивірусів російськими спецслужбами…

Поява перед Конгресом – це відчайдушна спроба Касперського відповісти на давні звинувачення його фірми у причетності до шпигунської активності Кремля. Слухання також стануть можливістю дізнатися про нинішню напружену ситуацію у відносинах між США і РФ в кібер-просторі…

Крім того, на слуханнях виступатимуть американські урядові та приватні експерти в кібер-галузі…» ***(Касперського запросили дати свідчення в Конгресі США // Укрінформ (https://www.ukrinform.ua/rubric-world/2305576-kasperskogo-zaprosili-dati-svidcenna- v-kongresi-ssa.html).- 15.09.2017).***

***

«…28 вересня, Євросоюз почав перші навчання, з протидії гібридним загрозам і кібератакам…

Навчання PACE17 триватимуть тиждень і передбачають імітацію гібридної загрози державам-членам ЄС. Вони проводяться з метою оцінити, наскільки швидко ЄС може реагувати на такі загрози і наскільки скоординованими є країни та інституції…» ***(В ЄС почали перші навчання проти гібридних загроз і кібератак // Espreso.tv (http://espreso.tv/news/2017/09/28/v_yes_pochaly_pershi_navchannya_proty_gibrydnyk h_zagroz_i_kiberatak).- 28.09.2017).***

***

«Украина уже достигла значительного прогресса в сфере укрепление собственной кибербезопасности, но должна приложить еще больше усилий для своей защиты.

Об этом в интервью журналу "Тиждень" рассказал заместитель генерального секретаря НАТО вопросам новых вызовов безопасности Сорин Дукару.

По его словам, дальнейшие усилия требующая значений инвестиций, а также внимание на высшем стратегическом уровне.

Также Дукару подчеркнул, что критически важными шагами, учитывая скорость, с которой развеваются угрозы, является углубление партнерства с другими государствами, международными организациями, промышленностью и учеными…» ***("Но надо работать дальше": в НАТО отметили прогресс Украины // Вести-UA || Новости Украины | Новини України (https://vesti-ua.net/novosti/politika/47621-no-nado-rabotat-dalshe-v-nato-otmetili-progress-ukrainy.html).- 29.09.2017).***

***

Анонси наукових заходів з проблем кібербезпеки запланованих у 2017 році

«27 жовтня 2017 в Києві відбудеться ІІ Фінансовий форум, який служить адвокатам та представникам бізнесу платформою для обговорення та вирішення проблем у сфері фінансів…
Серед тем до обговорення:
Перспективні напрями фінансового ринку;
Блокчейн, біткоїни, ICO та інші нові фінансові інструменти;
Інформаційна та кібербезпека як must-have elements системи корпоративного управління бізнесом;
Лібералізація валютного контролю від НБУ…» ***(ІІ Фінансовий форум проведе ААУ // Закон і Бізнес (http://zib.com.ua/ua/print/129965-ii_finansoviy_forum_provede_asociaciya_advokativ_ukraini.html).- 30.08.2017).***

***

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

Європейські та міжнародні підходи до захисту прав людини : матеріали регіон. наук.-практ. конф., [Київ, 7 квіт. 2017 р.] / Київ. ун-т ім. Бориса Грінченка, Ф-т права та міжнар. відносин. - Київ, 2017. – 207 с.
Зі змісту:
·Кобилянська Л. Правові засади міжнародного співробітництва у сфері боротьби з кіберзлочинністю;
·Кравчук А. Право на безпечне інтернет-середовище в контексті становлення четвертого покоління прав людини;
·Кравченко О. Інформаційні війни: цілі, методи та засоби ведення;
·Тимошенко А. Політика США в галузі забезпечення інформаційної безпеки (2009-2017 рр.): загальні тенденції.
Шифр зберігання НБУВ: ВА812167.

***

Жовнір А.О. Упровадження медіаосвіти та формування медіакомпетентності як ключові фактори забезпечення інформаційної безпеки
громадянина та держави / А.О. Жовнір // Соціальні технології: актуальні проблеми теорії та практики. - 2017. - Вип. 73. - С. 179-193.
Розкрито теоретико-методологічний підхід та теорію медіаосвіти. Уточнено структуру та ключові елементи медіа компетентності. Висвітлено роль медіаосвіти в забезпеченні інформаційної безпеки держави.
Шифр зберігання НБУВ: Ж69919.

***

Закарпатські правові читання : матеріали IX Міжнар. наук.-практ. конф. (20-22 квіт. 2017 р., м. Ужгород). - Ужгород : РІК-У, 2017. - Т. 1. - 2017. - 546 с.

Зі змісту:

·Банж Р.О. Деякі питання правового регулювання інформаційної безпеки вУкраїні;

·Паш Б.В. Складові інформаційної безпеки держави: постановка питання. Шифр зберігання НБУВ: В356681/1.

***

Іншомовна підготовка працівників правоохоронних органів та сектору безпеки : матеріали всеукр. наук.-практ. конф., 21 квіт. 2017 р. / Ген. прокуратура України, Нац. акад. пед. наук України, Нац. акад. прокуратури України. - Київ, 2017. - 174 с.

Зі змісту:

·Бистрова Б.В. Загальні підходи до реформування системи вищої освіти в галузі підготовки бакалаврів із кібербезпеки у США.

Шифр зберігання НБУВ: ВС62487.

***

Курбан О. В. Інформаційні війни у соціальних он-лайн-мережах : [монографія] / Курбан О. В. ; Київ. ун-т ім. Бориса Грінченка. - Київ, 2017. - 392 с.

Розкрито історіографічний та теоретико-методологічні аспекти дослідження і розвитку інформаційних конфліктів. Визначено стратегію та тактику інформаційної війни. Подано базові прийоми та інструменти ведення інформаційної війни у соціальних он-лайн-мережах. Окреслено інформаційно-комунікаційні он-лайн- процеси у системі державної інформаційної безпеки.

Шифр зберігання НБУВ: ВА811504.

***

Матеріали Всеукраїнської науково-практичної конференції «Соціальні комунікації: інструменти, технологія і практика», 10-11 березня 2017 р. : [збірник] / Клас. приват. ун-т. - Запоріжжя, 2017. - 139 с.

Зі змісту:

·Євтушенко О.М. Нові медіа – нові герої: до питання про «кібергероїзм»;

·Катеринич П.В. Поняття інформаційної безпеки в польському та українському соціокультурних вимірах.

Шифр зберігання НБУВ: ВА811977.

***

Міжнародна науково-практична конференція «Законність і

правопорядок усучасному суспільстві», 10-11 березня 2017 р. : [зб. матеріалів] / НДІ публ. права. - Київ, 2017. - 119 с.
Зі змісту:
·Байдала О.В. Фішинг та інші методи шахрайства в інформаційному суспільстві.
Шифр зберігання НБУВ: ВА812029.

***

Якість і безпека: сучасні реалії : матеріали наук.-практ. конф., 02-03 берез. 2017 р. / Вінниц. нац. техн. ун-т, Вінниц. нац. аграр. ун-т, Вінниц. мед. коледж ім. Данили Заболотного. - Вінниця : ВНТУ, 2017. - 91 с.
·Ратушняк М.С. Основні вимоги до стратегії забезпечення кібербезпеки України Шифр зберігання НБУВ: СО35109.

***

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.