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

№ 11 (листопад)

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., 2017. – № 11 (листопад) . – 58 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.

© Науково-дослідний інститут інформатики і права Національної академії правових наук України,
© Національна бібліотека України імені В. І. Вернадського, 2017

ЗМІСТ

«Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий Верховною Радою України 5 жовтня 2017 року оприлюднили в парламентській газеті «Голос України»…

Законом визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки.

Документ також визначає основні об'єкти кіберзахисту, які в сукупності складають критичну інфраструктуру країни, принципи забезпечення кібербезпеки та національна система кібербезпеки. Згідно Закону, Президент України координує діяльність у сфері кібербезпеки через очолювану ним Раду нацбезпеки і оборони України…

В Законі враховано низку пропозицій експертів НАТО і Євросоюзу…» ***(Ілля Жижиян. Закон про кібербезпеку України опублікували в "Голосі України" // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1697646-zakon-pro-kiberbezpeku-ukrayini-opublikuvali-v-golosi-ukrayini).- 09.11.2017).***

***

«Операторы и провайдеры - члены ИнАУ 14 ноября, призвали экспертов Совета Европы помочь в «противодействии мошеннической практике подмены понятий в законодательстве о кибербезопасности»…

Недовольство операторов и провайдеров вызвали законодательные инициативы…– законопроекте об имплементации Конвенции о киберпреступности, правительственном законопроекте №7275 и уже принятом законе «О государственной поддержке кинематографии в Украине».

В законе о господдержке кинематографии в Украине, по мнению провайдеров, медиагруппы пролоббировали чрезмерные обязанности датацентров по досудебной блокировке контента…

В законопроект об имплементации Конвенции о киберпреступности… «представители силовых структур планируют добавить блокировки интернет-контента провайдерами, о чем в Конвенции нет и речи».

Правительственный законопроект №7275 по мнению провайдеров… фактически отменяет даже те механизмы противодействия изъятию серверов, что действуют сегодня. Законопроект также создает коррупционный механизм, когда правоохранители будут сами решать, удалять серверы, или копировать с них информацию…» ***(Владимир Кондрашов. Провайдеры заявляют о подмене понятий в законодательстве о кибербезопасности // Internetua (http://internetua.com/provaideri-zayavlyauat-o-podmene-ponyatii-v-zakonodatelstve-o-kiberbezopasnosti).- 15.11.2017).***

***

«На партнерской конференции Axis компания представила свое видение проблем обеспечения безопасности критических систем физической защиты…

Кибербезопасность стала центральной темой партнерской конференции. После инициированных ботнетом Mirai нашумевших DDoS-атак, в которых существенную долю «зомбированных» устройств составляли камеры видеонаблюдения, специалисты не могли не обратить пристального внимания на эту проблему…

Кибератака на систему видеонаблюдения может привести к подрыву физической защиты объекта, поэтому в Axis уделяют повышенное внимание вопросам кибербезопасности. Компания еще несколько лет назад выпустила руководство по усиления защиты Axis Hardening Guide, и оно постоянно обновляется. В систему управления Axis Camera Management добавлено управление сертификатами, чтобы доступ к камере мог получить только обладатель сертификата из доверенного источника. В ближайшие версии своих прошивок для камер Axis собирается внести ряд изменений для укрепления их защищенности: ввести ограничение на минимальную длину пароля, блокировать доступ к камере при массовых попытках входа, ввести проверку обновлений прошивок на подлинность и др…» ***(Axis защищает камеры видеонаблюдения // «Открытые системы» (https://www.computerworld.ru/articles/Axis-zaschischaet-kamery-videonablyudeniya).- 10.11.2017).***

***

«Парольная защита уже доказала свою ненадежность, поэтому технологические компании ищут новые способы аутентификации пользователей. К примеру, компания Google намерена предложить своим клиентам специальный аппаратный ключ (донгл) для авторизации в учетных записях.

Донгл представляет собой миниатюрное устройство, которое можно прицепить к связке обычных ключей. В набор входят два устройства – одно можно носить с собой в кармане или сумке, а второе хранить в надежном месте в качестве запасного. Стоимость каждого ключа составляет $20.

Донглы являются одной из ключевых составляющих программы Google Advanced Protection Program по усиленной защите пользователей, представляющих особый интерес для хакеров…

Подписаться на программу Advanced Protection Program может каждый, однако Google в первую очередь будет отдавать предпочтение пользователям, представляющим интерес для правительственных хакеров и спецслужб…» ***(Google защитит своих пользователей от хакеров с помощью донгла // SecurityLab.ru (http://www.securitylab.ru/news/489513.php).- 03.11.2017).***

***

«На сегодняшний день кибергигиена и кибербезопасность являются как никогда важными как для обычных пользователей мобильных телефонов, так и для крупнейших компаний…

Главный антивирусный эксперт Александр Гостев говорит, …что поскольку все больше людей используют свои мобильные телефоны в качестве хранилища своих данных, а номер мобильного телефона становится ключевым идентификатором - соответственно увеличивается риск, связанный со взломом мобильных телефонов…

Относительно кибератак на организации Гостев отметил, что они могут оставаться незамеченными, особенно когда злоумышленники точно знают, какую информацию они хотят получить.

Что касается предотвращения утечки, глава InfoWatch Group Владимир Шутёмов говорит, что для любой системы фильтрации контента легко выполнить перехват несанкционированных передач телефонных номеров по различным каналам…

Отмечается, что такая крупномасштабная передача данных, включая миллионы телефонных номеров, может быть выявлена, если существует государственная система для управления трафиком в сети.

«Компании, которые подвергаются утечке данных, должны незамедлительно уведомить своих клиентов об инциденте и о рисках, связанных с потерей их персональных данных», - сказал Шутёмов, добавив, что стоит лишь обучить пользователей основным принципам кибергигиены…» ***(Екатерина Шпачук. Эксперты по кибербезопасности: Никогда кибергигиена не была так важна, как сей час // Internetua (http://internetua.com/eksperti-po-kiberbezopasnosti--nikogda-kibergigiena-ne-bila-tak-vajna--kak-seicsas).- 01.11.2017).***

***

«Разработчики программы для управления паролями LastPass опубликовали отчет об использовании учетных данных сотрудниками различных компаний. Отчет сформирован на базе анонимных данных 30 тыс. пользователей LastPass.

Согласно приведенной в отчете информации, в среднем сотрудники используют порядка 190 паролей, которые они вводят около 150 раз в течение месяца. При этом 91% пользователей осведомлен о возможных рисках использования одних и тех же паролей в разных учетных записях, однако 61% пользователей продолжают подобную практику. Также в отчете указано, что 23% сотрудников используют одни и те же учетные данные для авторизации в социальных сетях и корпоративных системах и приложениях…

Согласно данным отчета, 100% компаний продолжают использовать пароли, несмотря на призывы отказаться от них или, по крайней мере, повысить безопасность с помощью комбинации паролей и других мер, таких как биометрия и использование публичных ключей шифрования» ***(Сотрудники компаний в среднем используют порядка 190 паролей в месяц // SecurityLab.ru (http://www.securitylab.ru/news/489475.php).- 02.11.2017).***

***

«Microsoft опубликовала новый список рекомендуемых стандартов безопасности для устройств под управлением Windows 10. Стандарты включают в себя ряд требований к аппаратному и программному обеспечению, гарантирующих максимальную защиту устройства.

Требования к аппаратному обеспечению разделены на 6 категорий: поколение процессора, архитектура процессора, виртуализация, криптографические спецификации Trusted Platform Module (TPM), верификация загрузчика и оперативная память.

Microsoft рекомендует использовать процессоры Intel и AMD 7-го поколения…

Еще одним рекомендуемым компонентом является криптографическая спецификация Trusted Platform Module - аппаратный модуль, интегрированный в компьютерный набор микросхем, либо приобретенный в виде отдельного модуля для поддерживаемых материнских плат, который отвечает за безопасное генерирование криптографических ключей, их хранение, безопасную генерацию случайных чисел и аппаратную аутентификацию.

Microsoft также подчеркивает важность функции верификации загрузчика платформы, которая не допускает загрузку прошивки, разработанной кем-либо, кроме производителя системы…» ***(Microsoft опубликовала стандарты безопасности для устройств на базе Windows 10 // SecurityLab.ru (http://www.securitylab.ru/news/489536.php).- 07.11.2017).***

***

«Microsoft опубликовала рекомендации по защите от кибератак с использованием протокола Dynamic Data Exchange (DDE).

Протокол DDE предназначен для обмена данными между Office и другими приложениями Windows…

Уязвимость в протоколе DDE эксплуатировалась множеством различных хакерских группировок, в том числе в ходе кампаний по распространению вымогательского ПО Locky.

В рекомендациях Microsoft подчеркнула, что DDE является легитимной функцией и предложила пользователям соблюдать определенные меры предосторожности для защиты от атак. В частности, для успешной атаки злоумышленникам необходимо убедить жертву отключить безопасный режим и подтвердить открытие вредоносных файлов в нескольких всплывающих окнах.

Помимо этого, Microsoft заявила, что пользователи Office могут также включить определенные ключи реестра, повышающие безопасность, в том числе ключ, отключающий автоматическое обновление данных из связанных полей…

Microsoft также рекомендует пользователям быть осторожными при открытии подозрительных вложений в электронных письмах, поскольку вредоносные документы, эксплуатирующие DDE, обычно доставляются по электронной почте…» ***(Microsoft опубликовала рекомендации по защите от DDE-атак // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=119687).- 10.11.2017).***

***

«Вьетнамская компания по кибербезопасности Bkav утверждает, что ей удалось обхитрить технологию распознавания лиц iPhone X Face ID с помощью маски. Маска сделана для того, чтобы обмануть технологию картирования лица Apple, поэтому она представляет собой что-то наподобие гибридной головы монстра с вырезами для глаз, носа и рта…

Стоимость изготовления маски составляет всего 150 долларов, сообщают в Bkav… В компании подчеркивают, что маска еще не доработана и нуждается в дополнительных исследованиях…» ***(Технологию распознавания лиц iPhone X взломали с помощью маски // PAYSPACE MAGAZINE (https://psm7.com/news/texnologiyu-raspoznavaniya-lic-iphone-x-vzlomali-s-pomoshhyu-maski.html).- 11.11.2017).***

***

«…Инновационную карту будущего, Da Vinci Choice, изобрел Саймон Хьюитт, бывший начальник отдела безопасности крупнейших банковских групп Австралии.

Новая карта представляет собой целый компьютер, обещает полностью устранить необходимость в паролях и трансформировать сферу платежей…

Чтобы воспользоваться картой, необходимо ввести пароль Da Vinci PIN – единственный пароль, который Вам потребуется — и выбрать карту, с которой будут списаны средства, так как пользователь может привязать к карте Da Vinci все уже имеющиеся у него платежные карты…

Для оплаты крупного счета (или снятия большой суммы в банкомате) на экране карты Da Vinci появится временный одноразовый ПИН-код, благодаря которому снижается риск мошенничества…

Da Vinci Choice поступит в продажу в начале 2018 года и будет стоить около 75 фунтов стерлингов» ***(Карта будущего: изобретена платежная карта с временным ПИН-кодом и экраном // PAYSPACE MAGAZINE (https://psm7.com/news/karta-budushhego-izobretena-platezhnaya-karta-s-vremennym-pin-kodom-i-ekranom.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29).- 14.11.2017).***

***

«Компания по кибербезопасности «Лаборатория Касперского info-icon» представила Polys — безопасную систему онлайн-голосования, основанную на технологии блокчейн и поддерживаемую прозрачными криптографическими алгоритмами, — на ежегодном мероприятии Cybersecurity Weekend компании в Дублине…

«Лаборатория Касперского» выпустила бета-версию Polys, которая должна получить ранние отзывы. Далее поэтапно будут разработаны версии рабочей системы голосования, которая, по мнению компании, «должна изменить способы голосования»…

В настоящий момент Polys предлагает бесплатную веб-панель для создания систем онлайн-голосования в двух вариантах: по большинству голосов, в которых выигрывает большинство голосов, и кумулятивное голосование где избиратель имеет несколько голосов, которые могут быть заданы по одному параметру, или разделены по нескольким опциям… Как только голосование будет создано на панели управления Polys, администраторы смогут выбрать, как принимать голоса.

В настоящее время поддерживаются опции электронной почты, уникальных кодов и публичного голосования. При голосовании по электронной почте Polys отправляет электронное письмо каждому избирателю с защищенной ссылкой для голосования. При открытом голосовании соответствующая ссылка открыта для всех, кто хочет её увидеть…

Помимо бесплатной панели управления, Polys предлагает платную версию, которая поддерживает маркировку, ребрендинг и возможность интеграции.

По данным «Лаборатории Касперского», надёжная система голосования должна обеспечивать анонимность избирателей, защиту от пустых голосов, торговли голосами и принуждения избирателей, а также позволить избирателям проверять, что их голоса зарегистрированы в блокчейне. Также важно шифровать результаты голосования, записанные в блокчейне, иначе промежуточные результаты могут стать доступны до окончания голосования, что часто противоречит закону…

После того, как системы голосования, основанные на блокчейне, смогут продемонстрировать надёжную безопасность, они смогут решить и задачу подсчёта ошибок и мошенничества на выборах…» (***Александр Панасенко. ЛК и Parity Technologies запускают систему голосования на блокчейне // ООО "АМ Медиа" (https://www.anti-malware.ru/news/2017-11-16-3/24792).- 16.11.2017).***

***

«Джон Макафи (John McAfeeinfo-icon), программист и основатель компании-разработчика антивирусного программного обеспечения McAfee, вошел в команду украинского стартапа для “белых” хакеров Hacken в качестве советника и партнера по развитию международного бизнеса…

На сегодня проект «этичных хакеров» привлек более $3 млн. Макафи, который давно стал легендой в сфере кибербезопасности, решил поддержать проект на партнерских условиях: он получит 10% от прибыли стартапа…

Команда проекта надеется, что Макафи привнесет с собой в проект дополнительную экспертизу экспертов в области кибербезопасности…» (***Александр Панасенко. Джон Макафи вошел в команду украинского стартапа для хакеров Hacken // ООО "АМ Медиа" (https://www.anti-malware.ru/news/2017-11-15-3/24776).- 15.11.2017).***

***

«…специалисты из ARM разработали проект архитектуры, которая должна обеспечить более высокую степень безопасности IoT-устройств за счет своевременной доставки обновлений по беспроводным каналам. Рабочий вариант концепции инженеры выложили на сайт IETF…

Авторы архитектуры считают необходимым регулярно обновлять программное обеспечение IoT-устройств по беспроводным каналам…

Автоматическая доставка обновлений по беспроводной связи для IoT-устройств может работать так же, как и в случае мобильных устройств…

Кроме того, концепция предусматривает «жесткие разрешения» на уровнях разработки кода, хранения, применения, подтверждения и квалификации обновлений. Для управления этими разрешениями и обновлениями цифровых сертификатов прошивки и публичных ключей IoT-устройств нужна инфраструктура открытых ключей…» ***(Alexandra Golovina. Инженеры ARM повышают безопасность IoT // Threatpost (https://threatpost.ru/iot_safety/23106/).- 07.11.2017).***

***

«…Аналитики компании Duo Security проверили 66 тысяч фишинговых ссылок и собрали такие «забытые» фишинг-паки, изучили их и опубликовали отчет. Всего было найдено 7,8 тысяч наборов, из которых уникальными оказалось всего 3,2 тысячи…

Аналитики отмечают, что многие архивы содержали бэкдор-скрипты, которые скрытно перенаправляли пользовательские данные, похищенные купившим такой пакет злоумышленником, еще и автору-разработчику пакета, а иногда позволяли перехватить управление чужой фишинговой площадкой…

Особое внимание аналитики уделили электронным адресам, по которым уходила украденная информация… Выяснилось, что 76% электронных адресов связаны всего с одним пакетом, а оставшиеся 24% получали данные сразу от нескольких. Самый популярный адрес был обнаружен в 115 уникальных паках.

Анализ площадок, на которых злоумышленники располагают фишинговые страницы, показал, что 3 из 10 скомпрометированных сайтов размещены на WordPress…

Важная деталь — 16% фишинговых страниц были найдены на HTTPS-сайтах. Это не говорит об уязвимости самого протокола, но служит предупреждением пользователям…

…Организациям, которые хотят защитить свои сайты от клонирования, авторы исследования рекомендуют внедрить систему многофакторной аутентификации…» ***(Anna Markovskaya. Фишинг быстрого приготовления // Threatpost (https://threatpost.ru/fishing-kits-analysis/23111/).- 07.11.2017).***

***

«Известные эксперты по безопасности Чарли Миллер (Charlie Miller) и Крис Валасек (Chris Valasek) заявили, что Интернет вещей не может быть безопасным, однако риски поддаются контролю…

…Эти высказывания были сделаны во время презентации на конференции Flight 2017, организованной компанией Black Duck Software.

По мнению исследователей, проблема заключается в том, что если охрана или обеспечение личной безопасности не являются основной задачей компании, то реализация мер защиты мирового уровня в ее продукции не может быть

рентабельной. Изготовители устройств не могут продавать высокий уровень IT-безопасности как одну из особенностей продукта и не могут перекладывать соответствующие затраты на покупателя…

…проблема состоит в том, чтобы количественно оценить степень безопасности, которая необходима для продукта. Например, существует большая разница между незащищенным подключенным тостером и камерами видеонаблюдения, угнанными с целью проведения DDoS-атаки. Определение необходимого уровня защиты для продукта — сложная задача…

Исследователи отметили, что в будущем особые задачи будут связаны с автономными автомобилями…

По мнению Миллера и Валасека, обеспечение безопасности должно иметь самый высокий приоритет при создании автономных автомобилей. Но для множества компаний, выпускающих подключаемые к Интернету устройства, безопасность не должна быть главной заботой.

«Если ваша компания опасается возможной атаки, то бояться следует не подключенных к Интернету лампочек. 145 миллионов человек пострадали от утечки персональных данных не из-за тостера Equifax», — говорит Валасек. Для противодействия взлому серверов и сетей прежде всего необходимы более традиционные средства защиты…» ***(Tom Spring. Интернет вещей небезопасен, и это данность // Threatpost (https://threatpost.ru/iot-is-insecure-get-over-it-say-researchers/23161/).- 09.11.2017).***

***

«Компания Cisco Systems опубликовала бюллетень безопасности, где предупреждает пользователей ключевых продуктов на основе программной платформы Cisco Voice OS об уязвимости, которая позволяет хакеру удаленно обойти авторизацию и получить привилегированный доступ к взломанным устройствам…

«Уязвимость проявляется в процессе восстанавливающего обновления (refresh upgrade) или выполнения миграции Prime Collaboration Deployment (PCD) на взломанном устройстве. После успешного завершения восстанавливающего обновления или миграции PCD остается включенным режим администрирования, позволяющий заполучить root-доступ к устройству с известным паролем», — пишут специалисты Cisco в своем бюллетене…

«Брешь закрывается, если впоследствии обновить затронутое устройство стандартным способом обновления до Engineering Special Release, сервисного обновления или нового крупного выпуска продукта», — сообщают специалисты Cisco…» ***(Tom Spring. Cisco предупреждает о критической бреши в Voice OS // Threatpost (https://threatpost.ru/cisco-warns-of-critical-flaw-in-voice-os-based-products/23278/).- 17.11.2017).***

***

«Компания Fujitsu запустила в странах региона EMEIA управляемый сервис, который… передает подробные отчеты о текущих и новых типах атак, а также об уязвимостях, требующих устранения.

…Согласно недавнему отчету, проведенному компанией Lloyds of London, атаки на операционные системы компьютеров, которым подвергаются многие компании, могут привести к убыткам в размере $28,7 млрд.

Для борьбы с подобного рода угрозами компания Fujitsu разработала сервис Cyber Threat Intelligence (CTI)… Сервис предлагает четкие указания о возможном ущербе для компаний от новых типов киберугроз, а также простые и эффективные рекомендации по обеспечению защиты… С помощью сервиса CTI компания Fujitsu стремится гарантировать работоспособность компаний даже в условиях самых серьезных кибератак…

Благодаря интеллектуальному подходу с участием экспертов компании, сервис CTI компании Fujitsu предоставляет более точные данные по сравнению с традиционными подходами без привлечения человеческих ресурсов…

Стоимость сервиса CTI зависит от предлагаемых услуг, уровней обслуживания и страны» ***(Fujitsu предлагает сервис защиты компаний от кибератак ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5450891-Fujitsu-zashhishhaet-kompanii-ot.html#ixzz4ysUrKquG).- 13.11.2017).***

***

«Компания Nokia анонсировала программное решение, которое помогает операторам в упреждающем порядке распознавать, прогнозировать и отражать угрозы заражения вирусами-вымогателями и другими вредоносными программными кодами…

Nokia NetGuard Security Management Center – это единое комплексное решение для управления безопасностью, аналитикой и реагированием…

Последняя версия этого решения… с новой информационной панелью (dashboard) и автоматическим механизмом управления процессами безопасности дает возможность операторам расследовать 100 % сигналов тревоги при сокращении расходов на 50 %, ликвидировать до 70 % ложных срабатываний, снижать сроки расследования более чем на 50 % и отражать угрозы до того, как хакер взломает систему безопасности и нанесет оператору большой ущерб…

Nokia Security Management Center консолидирует данные и получает из них полезную информацию для принятия решений. Данные собираются из различных источников, включая решение для безопасности Nokia NetGuard Endpoint Security и лабораторию Nokia Threat Intelligence Lab, которые собирают данные из фиксированных и мобильных сетей по всему миру. Nokia Security Management Center работает во взаимодействии с внешними системами безопасности и вместе с ними отслеживает состояние безопасности сетей, распознает уязвимости, управляет политиками безопасности и правилами доступа.

Версия Nokia Security Management Center, разработанная в рамках экосистемы Nokia Common Software Foundation с помощью облачных технологий, должна появиться на рынке в 1 квартале 2018 года» ***(Nokia предлагает ПО для борьбы с вирусами-вымогателями // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5451275-Nokia-predlagaet-PO-dlya-borby-s.html#ixzz4yseKLJ9N).- 14.11.2017).***

***

«Компания Shape Security разработала систему Blackfish, предназначенную для идентификации украденных логинов и паролей в Сети еще до того, как об утечке становится известно. Технология призвана помочь бизнесменам блокировать использование их паролей, украденных на некорпоративных ресурсах, и тем самым пресекать попытки захватов корпоративных аккаунтов…

На сегодняшний день клиентами Shape Security являются топовые банки, авиалинии, ведущие гостиничные сети и два министерства в США.

…На сайте разработчиков указывается лишь, что Blackfish задействует искусственный интеллект для идентификации атак с использованием угнанных паролей. В первую очередь, система смотрит, откуда именно злоумышленники пытаются получить доступ к интересующим их ресурсам…

В случае, если система убеждена, что пара логин-пароль скомпрометирована, то эта комбинация получает соответствующую пометку и деактивируется для всех клиентов Blackfish. Вдобавок система собирает информацию о возможных утечках и попытках эксплуатации краденых паролей своих клиентов, ускоряя обмен такой информацией и тем самым повышая общий уровень защищенности…» ***(Создана система, которая защитит бизнес от популярных паролей // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5451343-Sozdana-sistema-kotoraya-zashhitit.html#ixzz4ysenSUmj).- 14.11.2017).***

***

«…В октябре 2016 года производитель антивирусных решений Enigma Software Group (ESG) обратился в суд с жалобой на то, что конкурирующая компания Malwarebytes незаконно охарактеризовала ее антивирусное ПО как потенциально опасное для пользователей…

Адвокаты Malwarebytes обратились к редко используемому положению "Закона США о благопристойности в коммуникациях" (Communications Decency Act, CDA) от 1996 года. Речь идет о параграфе 230(c)(2)(B), обеспечивающем иммунитет производителям "технических средств для ограничения доступа" к непристойному контенту. Согласно заявлению Malwarebytes, поскольку компания является производителем инструментов для ограничения доступа к объектам, которые она считает неприемлемыми, у нее есть иммунитет согласно вышеупомянутому параграфу CDA.

Федеральный судья Окружного суда по Северному округу Калифорнии Эдвард Давила (Edward Davila) согласился с доводами Malwarebytes и отклонил жалобу ESG...» ***(Enigma Software Group проиграла дело против Malwarebytes // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=119690).- 10.11.2017).***

***

«Свыше 20 млн устройств Amazon Echo и Google Home, работающих под управлением ОС Android и Linux, уязвимы к атакам с эксплуатацией набора уязвимостей, получивших общее название BlueBorne.

О проблеме BlueBorne стало известно в середине сентября нынешнего года. Как сообщили тогда исследователи из компании Armis, уязвимости затрагивают реализации Bluetooth в более чем 8 млрд устройств по всему миру…

Исследователям удалось успешно проэксплуатировать уязвимости CVE-2017-1000251 и CVE-2017-1000250 в колонке Amazon Echo и CVE-2017-0785 в Google Home и получить контроль над виртуальным ассистентом…

По данным Armis, 82% компаний используют устройства Amazon Echo и Google Home в своих сетях. Хакеры могут перехватить управление уязвимыми гаджетами и использовать их для записи разговоров находящихся поблизости сотрудников либо как отправную точку для других атак. Эксперты проинформировали производителей об уязвимостях. Обе компании уже выпустили патчи, устраняющие проблему» ***(Более 20 млн устройств Amazon Echo и Google Home уязвимы к атакам BlueBorne // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=119794).- 16.11.2017).***

***

«Британський фахівець з кібербезпеки Марк Барнс розробив спосіб злому смарт-динаміка Amazon Echo, завдяки якому зловмисники зможуть дистанційно прослуховувати все, що відбувається в будинку власника цього пристрою. …злом працює поки тільки з пристроями, випущеними до 2017 року…

Метод злому, розроблений Барнсом, дозволяє завантажити на пристрій Echo модифіковану прошивку, яка може постійно вести аудіозапис і відправляти дані не тільки на сервера Amazon, як це і повинно бути, але і на будь-який інший сервер, вказаний зловмисником…

Зламаний пристрій Echo веде запис всього, що відбувається навколо нього постійно навіть без виголошення користувачем команди активації Alexa. Проте, за словами Барнса, запис на зламаному пристрої не ведеться, якщо натиснута кнопка примусового відключення мікрофона…» ***(Хакер перетворив Amazon Echo на домашнього шпигуна // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2017/10/11/Amazon-Echo.html).- 10.11.2017).***

***

«Програмна помилка в щонайменше 685 мобільних додатках ставить під загрозу порядку 180 млн смартфонів, попередили дослідники безпеки з компанії Appthority.

За словами дослідників, вразливість, яка отримала назву Eavesdropper, виникла через те, що розробники помилково вписали в код облікові дані для доступу до сервісів компанії Twilio Inc…

Проаналізувавши 1100 додатків, дослідники виявили 685 проблемних, пов'язаних з 85 порушеними обліковими записами Twilio.

Даний випадок є показовим для нового типу кіберзагроз, пов'язаних з використанням в мобільних додатках сторонніх сервісів, що надають функції передачі текстових повідомлень і голосових викликів…» ***(80 млн. смартфонів виявилися під загрозою через помилки в мобільних додатках // ООО "Центр***

інформаційної безпеки" (http://www.bezpeka.com/ua/news/2017/10/11/80-mln-mobiles-flawed.html).- 10.11.2017).

***

«Специалисты британской организации по защите прав потребителей Which? нашли уязвимости, которые позволяют хакерам говорить с ребенком, в «умных» игрушках…

В ходе исследования эксперты выяснили, что игрушки CloudPets, Furby Connect, i-Que Intelligent Robot и Toy-Fi Teddy могут применяться для общения с детьми.

В этих игрушках поддерживается незащищенное Bluetooth-соединение, для которого не установлен пароль или какие-либо другие механизмы аутентификации. Потенциальный злоумышленник может с легкостью осуществить взлом устройства и начать общение с ребенком…

Специалисты узнали, что при подключении данных игрушек через Bluetooth отсутствуют проверки подлинности, что дает хакерам возможность передавать ребенку голосовые сообщения и получать ответы…» ***(Хакеры могут говорить с детьми, используя «умные» грушки // SecureNews (https://securenews.ru/smart_toys/).- 14.11.2017).***

***

«Эксперты заявили, что под угрозой взлома находятся все машины, выпущенные с 2005 года. При этом каждое транспортное средство может стать оружием, способным убить несколько человек. К такому выводу пришли ученые Нью-Йоркского университета… По словам специалистов, хакеры могут получить удаленный доступ к запуску двигателя, рулевому управлению и тормозной системе автомобиля. Американский специалист по компьютерной безопасности назвал современные машины "легкой мишенью" для кибертеррористов и заявил, что это проблема национальной безопасности многих стран…» **(Хакеры могут убить миллионы человек с помощью кибератаки на автомобили // «Автоблог» (https://avtoblog.ua/news/hakery-mogut-ubit-milliony-chelovek-s-pomoschju-kiberataki-na-avtomobili).- 21.11.2017).**

***

«…Инженеры Mozilla работают над новой системой оповещений для браузера Firefox, которая будет отображать соответствующие уведомления при посещении пользователем сайтов, ставших жертвами утечки данных.

Новая система разрабатывается при участии основателя агрегатора утечек Have I Been Pwned? Троя Ханта (Troy Hunt) и будет использовать предоставленные ресурсом данные…

Пока разработка проекта находится только на начальной стадии. Сейчас он представлен в виде дополнения Breach Alerts и …станет прототипом будущей функции в Firefox, которая будет уведомлять пользователей о том, что их учетные данные возможно были скомпрометированы…

Сейчас Breach Alerts отображает уведомления при посещении ресурса, включенного в список Have I Been Pwned?, содержащего информацию об обнародованных утечках данных…

Двумя основными проблемами, по словам разработчиков, являются конфиденциальность пользовательских данных и технической архитектуры функционала…» ***(Firefox сообщит пользователям о сайтах, на которых происходили утечки даннях // РосКомСвобода (https://roskomsvoboda.org/33750/).- 23.11.2017).***

***

«…Согласно исследованию уровня защищенности корпоративных сетей российских компаний, проведенному компанией «Код безопасности», для 67% CIO и 77% ИБ-специалистов на первом месте по важности стоят стабильность работы и качественная техническая поддержка. Этот показатель актуален для финансовой сферы, сегмента информационных технологий, строительной отрасли и здравоохранения…

По данным исследования, в среднем на защиту корпоративных сетей компании выделяют 11% ИТ-бюджета. При этом далеко не каждая компания направляет часть этих ресурсов на создание профильного департамента.

Наибольшая доля компаний, имеющих выделенное подразделение сетевой безопасности, наблюдается в финансовой и промышленной отраслях…

По данным исследования, наибольшую опасность для корпоративной сети представляет атака на рабочие станции с использованием внешних носителей. Данную угрозу отметили 47% респондентов «Кода безопасности». 21% опрошенных видят существенный риск в фишинге – рассылке писем с вредоносным ПО…

Стандартным подходом к защите сетевой инфраструктуры является использование межсетевого экрана на периметре сети. Однако опрос показал, что специалистов по информационной безопасности беспокоят атаки на рабочие станции с использованием внешнего носителя в обход внешнего периметра сети.

Аналитики «Кода безопасности» выяснили, что только у 23% российских компаний имеется система мониторинга ИБ (SIEM), позволяющая централизованно собирать и анализировать поток событий информационной безопасности…

По данным исследования, у 88% участников опроса установлен межсетевой экран. VPN-шлюз есть у 59% респондентов…

Согласно результатам опроса, в 76% российских компаний существует потребность в обучении персонала, отвечающего за информационную безопасность…

Участниками проведенного исследования стали 200 ИБ-специалистов из 10 отраслей, а также 400 руководителей ИТ-служб» ***(На защиту корпоративных сетей российские компании выделяют 11% ИТ-бюджета // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5455109-Na-zashhitu-korporativnyx-setej-ros.html#ixzz4ze3Xa7Q8).- 27.11.2017).***

***

«…Компания ForeScout Technologies опросила более 2500 сотрудников 600 компаний по всему миру. И более 77% из них признали, что развитие интернета вещей создает серьезные проблемы для систем киберзащиты и является вызовом для всей сферы информационной безопасности. Еще 54% опрошенных признали, что испытывают серьезное беспокойство по поводу элементов сети ИВ. Такой высокий процент обеспокоенных сотрудников – это в целом хороший признак, так как позволяет ожидать, что перед развертыванием ИВ корпорации будут серьезно относиться к обеспечению эффективной защиты данных. Примерно 76% компаний готовы к тому, что при внедрении интернета вещей придется серьезно пересмотреть стратегию информационной защиты…

Сотрудники отделов кибербезопасности, согласно опросу ForeScout Technologies, считают серьезной проблемой отсутствие финансирования для повышения компетенций в сфере информационной защиты. Несмотря на частые кибератаки и громкое освещение этих тем в СМИ, многие руководители не готовы увеличивать траты на защиту сетей ИВ…

Опрос показал, что 40% специалистов по безопасности продолжают полагаться на свой традиционный подход к безопасности для защиты ИВ. Однако такой метод не позволяет идентифицировать все подключенные к сети устройства, что делает сети более уязвимыми перед "взломщиками". Так, 82% респондентов заявили, что не смогут идентифицировать все устройства, подключенные к их сети. Но при этом 59% заявили, что готовы работать при уровне риска безопасности от среднего до высокого при построении ИВ. Это серьезная проблема, поскольку 90% компаний ожидают, что количество подключенных устройств ИВ увеличится в течение следующих нескольких лет…» ***(Исследование ForeScout Technologies: бизнес видит в интернете вещей серьезный вызов кибербезопасности // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=119992).- 29.11.2017).***

***

Національна система кібербезпеки

«Украина недополучила 0,4% ВВП в связи с кибератакой вируса Petya, которому подверглись украинские компании в конце июня 2017 года. Об этом заявил создатель общественной организации "Гражданская кибероборона" Александр Кардаков…

В 2016 году ВВП Украины годовой составлял 93,27 млнд долларов. 0,4% от это суммы - 373 млн долларов, или около 10 млрд гривен…» ***(Из-за атаки вируса Petya Украина за полчаса потеряла 10 млрд гривен – експерт // информационный портал "ua.today". (http://ua.today/news/economy/iz_za_ataki_virusa_petya_ukraina_za_polchasa_poteryala_10_mlrd_griven_ekspert).- 03.11.2017).***

***

«Совсем скоро украинцев могут обязать регистрировать sim-карты, привязывая к ним свои личные данные…

Инициатива регистрировать всех мобильных абонентов появилась еще летом этого года, но, до недавнего времени отсутствовал четкий механизм. 17 октября Нацкомиссия регулирования связи и информатизации упростила процедуру регистрации абонентов мобильной связи. Для того, чтобы данная инициатива вступила в силу, парламент должен принять соответствующий законопроект Госслужбы спецсвязи и защиты информации.

Согласно утвержденной процедуре, абоненты смогут подавать заявление о регистрации как в электронной, так и бумажной форме, а идентифицировать их будут с помощью электронной цифровой подписи, дистанционной системы идентификации BankID и т.д…

Сейчас регистрация абонентов полностью добровольная и осуществить ее можно только в магазине компании, чьими услугами вы пользуетесь, с идентификационным кодом и паспортом. Возможность регистрироваться самостоятельно и в режиме онлайн и должна стать главным нововведением, которое упростит обязательную регистрацию.

После принятия проекта, у мобильных операторов будет девять месяцев, чтобы подготовить процедуру регистрации всех абонентов…

Украинцы опасаются, что регистрация повлечет за собой утечку их личной информации. Также один из рисков – это появление черных рынков sim-карт, зарегистрированных на подставных лиц. Опыт других стран показывает, что это распространенное явление после принудительной регистрации.

Опасения по поводу утечки конфиденциальной информации сложно назвать беспочвенными. Эксперты отмечают, что после регистрации у всех мобильных операторов появится полная база данных о клиентах…

…такая база может в любой момент подвергнуться хакерской атаке, так как в Украине существуют определенные проблемы с кибербезопасностью. Также нельзя исключать возможность утечки информации из-за сотрудников мобильных компаний, которые смогут использовать ее в корыстных целях.

Мобильные операторы наоборот уверяют, что регистрация не будет иметь негативных последствий для абонентов…» ***(Обязательная регистрация мобильных абонентов: чего ждать украинцам // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/202803-objazateljnaja_registratsija_mobiljnyh_abonentov_chego_hdatj_ukraintsam).-11.11.2017).***

***

«Информационное агентство Reuters, ссылаясь на слова руководителя Киберполиции Украины Сергея Демедюка, сообщило, что киберпреступники хотели заполучить доступ к конфиденциальной информации украинских организаций в рамках скрытой фишинговой кампании, которая проходила одновременно с атакой вымогательской программы BadRabbit…

По словам Демедюка, одновременно с этими атаками были зафиксированы более мощные скрытые нападения, целью которых была кража финансовой информации и конфиденциальных данных…

Демедюк сообщил, что целью параллельной атаки были пользователи платформы 1С, посредством которой хакеры распространяли фишинговые письма от имени разработчиков данного программного обеспечения. Одна из компаний-дистрибьюторов 1С признала, что их клиенты стали жертвами хакерских атак и посоветовал принять меры предосторожности…» ***(Украинские фирмы подверглись атаке фишеров, действовавших в одно время с BadRabbit // SecureNews (https://securenews.ru/badrabbit_2/).-03.11.2017).***

***

«Кіберзагрози залишаються актуальними для України і США, тому що обидві країни є одними з головних об'єктів для кібератак…

«Поки що немає єдиного рецепту, як уберегтися від кібератак. Кібербезпека — найважливіша галузь безпеки, яка ще не отримала належної уваги. І Америка, і Україна є одними з головних об'єктів атак з боку кіберзлочинців. Атаки, вчинені в Україні, мають на меті залякати її , а джерелом атак є найближчий північний сусід. Ми також страждаємо від кібератак з боку Росії», — зазначив Джуліані.

За його словами, головний потік небезпек виходить з Росії і Китаю.

«Збираючись працювати з Китаєм або Росією, необхідно розуміти, що ви наражатиметеся на небезпеку, що у вас спробують щось вкрасти, тому що вони не можуть нічого придумати. Потрібно давати їм хибну інформацію, як в старих фільмах епохи холодної війни. Тому ми іноді навмисно вдаємося до такої тактики — поставляємо неправдиву інформацію, яку вони активно використовують, після чого їх проекти лопаються як мильні бульбашки. Це свого роду урок», — додав Джуліані.

За його словами, в США «при президентові Трампі створено групу фахівців, яка займається питаннями забезпечення кібербезпеки...» ***(Джуліані заявив, що Україна та США є головними цілями для кібератак з боку РФ // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/dzhuliani-zayaviv-shho-ukrayina-ta-ssha-ye-golovnimi-tsilyami-dlya-kiberatak-z-boku-rf.html).- 20.11.2017).***

***

«…Хактивісти Українського Кіберальянсу, які відомі кібероперaціями проти російських політиків і військових, вирішили перевірити, чи посилили захист українські держустанови…

У рамках акції #FuckResponsibleDisclosure, хактивісти виявили відкриті сервери Головного управління Нацполіції в Київській області і НАЗК, де у відкритому доступі було викладено близько 150 гігабайт відсканованих декларацій співробітників…

Або сайт Судової влади України, який зберігав у відкритому доступі сертифікати і паролі для генерації ключів користувачів, а також аналітичні звіти по судах. Однак після публікації хактивістом сайт Судової влади закрив доступ до своїх даних протягом години.

Або сайт державної служби фінансового моніторингу України, який настільки застарів, що хактивісти не виключають можливості його скомпроментування до їх огляду…

Не всі департаменти «зраділи» виявленим недоліків. Наприклад, НАЗК офіційно заперечувало витік даних з сайту. У відповідь на офіційний запит від інтернет-ресурсу Цензор.НЕТ, НАЗК відповіло, що всі ці дані не є витоком, а лежать у відкритому доступі на сайті департаменту…

Хактивіст Шон Таунсенд зізнався, що Кіберальянс вже не раз намагався розповісти про жалюгідний стан кібер- і інформаційної безпеки України. Зазвичай, коли хактивісти виявляють «дірку» в кіберзахисті держдепартаментів і повідомляють про неї, то чиновники в кращому випадку по-тихому її «латають». У гіршому випадку, починають заперечувати наявність проблеми або звинувачувати волонтерів у зламі…

Чиновники закликають повідомляти про виявлені факти порушення в мережі кіберполіції. Однак хактивіст вважає, що відповідальність за кібер- та інформаційну безпеку має бути обопільною, тобто і з боку держави.

Наприклад, у ході огляду хакери Кіберальянсу з'ясували, що доки в жовтні Держспецзв'язку проводила кібернавчання, їхній сайт «лежав». Також помилково на сайті команди швидкого реагування на кіберзагрози CERT-UA було викладено пароль від одного з їхніх поштових акаунтів. Реакція на інцидент пішла лише через три доби. Цього разу хактивісти вирішили не повідомляти про інциденти, а відразу оприлюднити їх…

Не всі чиновники розуміють, що таке мережа і навіщо потрібно захищатися. Уже була ухвалена Інформаційна доктрина, а в жовтні закон «Про основні засади забезпечення кібербезпекі України», дія якого розпочнеться 9 травня 2018 року. Однак хактівіст звертає увагу на те, що, згідно з цим законом, кібербезпеку повинні забезпечувати всі, а значить ніхто, адже ніяких конкретних дій і покарань закон не передбачає…» ***(Українські хакери перевірили, як захищають сайти держустанов Читайте більше // Західна інформаційна корпорація (http://zik.ua/news/2017/11/23/ukrainski_hakery_pereviryly_yak_zahyshcheni_sayty_derzhustanov_spoyler__1211437).- 23.11.2017).***

***

«Национальная полиция и Microsoft Ukraine 22 ноября подписали меморандум о сотрудничестве в сфере информационной и кибербезопасности. Заключение соглашения стало результатом встречи заместителя главы Национальной полиции Украины Константина Бушуева и генерального директора Microsoft Ukraine Надежды Васильевой…

…в ходе встречи участники обсудили вопросы сотрудничества в области информационных технологий, информационной и кибербезопасности. Также обсуждалось о создание и модернизация информационной инфраструктуры, обеспечение автоматизации, прозрачности и контролируемости внутренних процессов…

Кроме того, участники встречи обсудили перспективу развития взаимоотношений между Национальной полицией и компанией-производителем программного обеспечения, в частности, речь идет о формировании с помощью Microsoft Ukraine своеобразного "ядра" из числа работников Национальной полиции, отвечающих за обеспечение информационной и кибербезопасности

ведомства» ***(Нацполиция и Microsoft подписали меморандум о сотрудничестве в сфере кибербезопасности // Internetua (http://internetua.com/nacpoliciya-i-microsoft-podpisali-memorandum-o-sotrudnicsestve-v-sfere-kiberbezopasnosti).- 23.11.2017).***

***

«Міністерство інфраструктури створило генеральний секретаріат цифрової інфраструктури та державне підприємство, яке буде опікуватися питаннями кібербезпеки, повідомив заступник міністра інфраструктури Юрій Лавренюк…

За його словами, на цьому етапі формується штат держпідприємства.

«Є директор, він формує свою команду. Є деякі напрацювання. Так, вони прописали концепцію захисту Одеського порту, порт підтримав цю ініціативу. Провели деякі торги, розробили відповідний програмний продукт і технічне забезпечення. Ми будемо ініціювати створення спільної робочої групи з представниками СБУ, які займаються питаннями кібербезпеки, а також Нацполіції, Державної служби захисту інформації, РНБО…», - сказав він.

«Щоб підприємство запрацювало, виділили близько 60 млн грн, це європейський грант», - повідомив Ю.Лавренюк» ***(Кібербезпекою об'єктів критичної інфраструктури опікуватиметься держпідприємство при Мінінфраструктури // Інтерфакс-Україна (http://ua.interfax.com.ua/news/general/465659.html).- 29.11.2017).***

***

Світові тенденції в галузі кібербезпеки

«Лидером по кибербезопасности в 2017 году признан Сингапур. США и Малайзия заняли вторую и третью строчку рейтинга МСЭ соответственно.

Россия оказалась на десятом месте в рейтинге 2017 года Международного союза электросвязи по индексу кибербезопасности, на один пункт опередив Японию и Норвегию, сообщили в Минкомсвязи РФ со ссылкой на отчет «Глобальный индекс по кибербезопасности» (The Global Cybersecurity Index, GIC).

По данным МСЭ за 2017 год Россия также опередила целый ряд других мировых лидеров в сфере ИКТ. Так, согласно рейтингу, Великобритания заняла 12 место, Южная Корея — 13-е, Финляндия — 16-е, Германия — 24-е, Италия — 31-е. Всего в исследовании приняли участие 193 страны…» ***(Россия заняла десятое место в «Глобальном индексе кибербезопасности» // «Открытые системы» (https://www.computerworld.ru/news/Rossiya-zanyala-desyatoe-mesto-v-Globalnom-indexe-kiberbezopasnosti).- 03.11.2017).***

***

«Компания Huaweiinfo-icon представила свое видение современной киберзащиты на 8-й Международной конференции «Доверие и безопасность в информационном обществе»…

С 29 октября по 3 ноября участники конференции посетили три крупнейших технологических центра Китайской Народной Республики – города Гуанчжоу, Шэньчжэнь и Гонконг…

Участники «Инфофорума» обсудили основные проблемы международной киберзащиты, представили существующие инфраструктурные проекты и ознакомились с инновационными разработками России и КНР в области информационной безопасности.

В программу мероприятия в Китае вошли пленарные и тематические заседания, экспертные встречи, посещение ситуационного центра полиции г. Шэнчьжэня и международной выставки China Public Security Expo-2017, знакомство с современной ИТ-инфраструктурой мегаполисов, встреча с представителями Бюро технологий и инноваций, посещение Science Park в Гонконге, посещение штаб–квартиры и производства компании Huawei в Шэньчжэне, а также знакомство с работой Центра реагирования на инциденты безопасности продуктов Huawei (PSIRT).

Последние разработки Huawei в инновационном центре компании и в PSIRT участникам конференции представил директор по информационной безопасности Huawei в России Александр Зубарев. По его словам, все больше вендоров прилагают максимум усилий к защите своей продукции… Компания Huawei уже сейчас имеет соглашения по кибербезопасности со всеми участниками цепочки поставок, а внутри компании защита охватывает все уровни разработки и стадии жизненного цикла продукции. Huawei не только минимизирует риски уязвимости продуктов Huawei, но и обеспечивает укрепление доверия клиентов к решениям и технологиям, построенным на их основе… Преимуществом для Huawei может стать внедрение российского стандарта ГОСТ шифрования в отдельные разработки с подтверждением оценки их соответствия требованиям ФСБ России, и компания намерена это реализовать…» (***Александр Панасенко. Huawei: необходимо объединение усилий для обеспечения кибербезопасности // ООО "АМ Медиа" (https://www.anti-malware.ru/news/2017-11-09-3/24717).- 09.11.2017).***

***

«Continental покупает израильскую компанию Argus Cyber Security, технология которой направлена против взлома автомобилей хакерами… Теперь Argus станет частью Elektrobit и будет продолжать коммерческие отношения со всеми поставщиками автомобильных компонентов…

Эксперты по кибербезопасности давно уже критиковали автомобильную промышленность за то, что та не смогла создать защиту внутренней связи транспортных средств с сетевыми функциями.

По их мнению, опасность заключается в том, что после нарушения внешней безопасности хакеры могут иметь свободный доступ к бортовым компьютерным системам, которые управляют всем — от двигателей и тормозов до кондиционеров и информационно-развлекательных систем» ***(Анатолий Гребенюк. Continental покупает израильскую кибер-компанию Argus // АвтоМания (http://avtomaniya.com/site/publication-full/15046).- 07.11.2017).***

***

«В Казахстане реализован проект по созданию комплексной ИБ-системы, основанной на решениях Cisco. Безопасность корпоративной сети «Евразийского банка» обеспечивают элементы архитектуры Cisco SAFE. Разработки Cisco позволили банку отразить ряд масштабных атак, совершенных на банковский сектор Республики Казахстан в 2017 году…

«Архитектура Cisco SAFE обеспечивает согласованность инструментов и позволяет решать операционные задачи на всем жизненном цикле атаки – до, во время и после, – рассказывает Владимир Илибман, эксперт Cisco по кибербезопасности. – Мы создаем целостную модель защиты не просто отдельных компонентов, а всей сети: такой метод позволяет идентифицировать начало нападения и проследить за его ходом, вовремя сформировать предупреждения и активно противодействовать атаке без участия пользователя. Модернизировав ИБ-инфрастуктуру, «Евразийский банк» сделал своего рода «долгосрочный вклад» в будущее. Надежная кибероборона обеспечивает сохранность данных и позволяет полностью сосредоточиться на достижении бизнес-целей».

На стадии внедрения находится технология TrustSec, которая необходима для защиты внутреннего периметра от несанкционированных подключений. Еще одна стратегическая цель – продолжить работу по интеграции установленных решений и подключению новых сервисов и модернизации сети.

Вместе с тем нельзя забывать, что человеческий фактор представляет наибольшую угрозу безопасности, а потому в банке регулярно проводятся обучающие мероприятия для сотрудников, призванные повысить уровень их осведомленности в вопросах ИБ» ***(Медуна. В одном из крупнейших банков Казахстана установлена система защиты информации на базе технологий Cisco // <META> (http://pr.meta.ua/read/54295).- 29.11.2017).***

***

Сполучені Штати Америки

«Бывший руководитель Yahoo Марисса Майер заявила на слушаниях в Сенате США, что 3 млрд аккаунтов сервиса были взломаны и украдены киберпреступниками из России…

Официальное государственное расследование утечки аккаунтов началось в январе. Несмотря на сотрудничество Yahoo и спецслужб США, механизм кибератаки определить так и не удалось…» ***(Бывший гендиректор Yahoo обвинила хакеров из России во взломе 3 млрд аккаунтов // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3461466?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0).- 09.11.2017).***

***

«Американське видання The Wall Street Journal повідомило, що щонайменше шість російських чиновників пов'язані зі зламом комп'ютерів Національного комітету Демократичної партії США минулого року…

За даними WSJ, Мінюст США уже зібрав достатньо доказів, аби пред'явити звинувачення шести російським посадовцям у справі про кібератаки.

Обговорення питання про офіційні звинувачення наразі перебуває на ранній стадії. Очікується, що чиновникам оголосять підозру наступного року. За даними газети, про арешт і ув'язнення поки не йдеться.

У разі, якщо російським чиновникам все таки оголосять звинувачення, для них становити проблему виїзд за межі РФ…» ***(До зламу серверів Демократичної партії США причетні 6 чиновників РФ — WSJ // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/do_zlamu_serveriv_demokratichnoi_partii_ssha_prichetni_6_chinovnikiv_rf_wsj/).- 03.11.2017).***

***

«…Сайт WikiLeaks опублікував вихідний код проекту під назвою «Вулик» (Hive). За його даними, «Вулик» маскувався під програми інших компаній, в тому числі «Лабораторії Касперського», і завантажував інформацію з вражених комп'ютерів. Навіть якщо користувачі знаходили вірус, вони не асоціювали його з ЦРУ… Спецслужби використовували сторонні й нічим непримітні домени та сервери, аби не викликати підозри…

Сайт також написав про принаймні три випадки, коли ЦРУ маскувалося під програми «Лабораторії Касперського».

Компанія поки офіційно ніяк не прокоментувала цю заяву, але її засновник Євген Касперський написав у Twitter, що у Лабораторії вивчили дані, опубліковані WikiLeaks, й що випущені ЦРУ сертифікати є підробленими…

Як раніше писав MediaSapiens, у вересні Міністерство внутрішньої безпеки США заборонило федеральним компаніям користуватися програмним забезпеченням Kaspersky Lab, остерігаючись її можливих зв’язків з російською розвідкою. Також нещодавно «Лабораторія Касперського» зізналася у тому, що випадково зкопіювала дані розвідки США.

…ЦРУ назвало Wikileaks «недержавною ворожою розвідувальною службою», на яку має вплив у тому числі Росія» ***(WikiLeaks стверджує, що ЦРУ маскувало свої віруси під «Лабораторію Касперського» // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/wikileaks_stverdzhue_scho_tsru_maskuvalo_svoi_virusi_pid_laboratoriyu_kasperskogo/).- 10.11.2017).***

***

«Сенсация от "Нью-Йорк таймс". У Агентства национальной безопасности США похищено кибер-оружие - сообщила газета…

Источники в АНБ подтвердили репортёрам - спецслужба, которая считается мировым лидером по взлому компьютерных сетей противника, не смогла защитить собственные секреты. Более того, до сих пор не способна установить, каким образом произошла утечка и замешан ли в ней кто-то из сотрудников…

По данным издания, все вирусы-вымогатели последнего времени - это только модификации похищенного у АНБ кибер-оружия, которое Штаты использовали для борьбы с терроризмом и проникновения в сети по всему миру - но теперь потеряли…

Лучшие силы сейчас охотятся на похитителей кибер-оружия, но пока никого не поймали. Чем американский скандал угрожает нам с вами - тоже теперь понятно…» ***(Дмитрий Анопченко . Вирусы на свободе: как американские спецслужбы проворонили свое новейшее кибер-оружие // ООО "Национальные информационные системы" (http://podrobnosti.ua/2210384-virusy-na-svobode-kak-amerikanskie-spetssluzhby-provoronili-svoe-novejshee-kiber-oruzhie.html).- 13.11.2017).***

***

«…В четверг, 16 ноября, компания Recorded Future опубликовала исследование, согласно которому Китай, если и не занимается сбором, то, по крайней мере, оттягивает раскрытие критических уязвимостей…

Вышеупомянутое исследование является продолжением более раннего исследования, демонстрирующего, что национальная база уязвимостей КНР (находится в ведении Министерства госбезопасности Китая) пополняется гораздо быстрее, чем ее американский эквивалент… Тем не менее, в некоторых случаях уязвимости попадают в нее позже…

В общей сложности исследователи проанализировали 300 случаев несвоевременного добавления уязвимостей в китайскую национальную базу. По их словам, они зафиксировали целый ряд примеров, когда уязвимости добавлялись вразрез со стандартной статистикой, и в некоторых случаях к оттягиванию добавления уязвимостей имело отношение Министерство госбезопасности КНР» ***(Китай оттягивает раскрытие уязвимостей с целью их эксплуатации // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=119811).- 17.11.2017).***

***

«… США разработали две стратегии на случай ракетной атаки Северной Кореи…

Один из них предусматривает серию кибератак или другие способы воздействий на пусковые системы баллистических ракет КНДР. Второй вариант нацелен на то, чтобы сбивать ракеты с помощью дронов и истребителей…

Обе стратегии пока экспериментальные и Белый дом планирует потратить на их разработку около $4 млрд. Утвердить выделение этой суммы должен Конгресс…» ***(В США разработали план на случай ракетной атаки Северной Кореи // Информационное агентство ЛІГАБізнесІнформ (http://news.liga.net/news/world/14856869-ssha_razrabotali_plan_na_sluchay_raketnoy_ataki_severnoy_korei.htm).- 18.11.2017).***

***

«Белый дом может вскоре запретить всем своим сотрудникам пользоваться персональными мобильными телефонами в рабочее время…

Инициатором запрета выступил глава аппарата Белого дома Джон Келли (John F. Kelly), чей персональный мобильный телефон ранее был скомпрометирован хакерами. Источники пока не указали точную дату введения запрета, поскольку решение по данному вопросу еще не принято.

Белый дом уже ввел превентивные меры в отношении личных беспроводных устройств, включая требование оставлять гаджеты за пределами конференц-залов, где проходят обсуждения конфиденциальной или засекреченной информации.

Высшие должностные лица пока не решили, стоит ли вводить запрет и будет ли он распространяться на всех сотрудников Белого дома…» ***(Сотрудникам Белого дома могут запретить пользоваться личными телефонами на работе // SecurityLab.ru (https://www.securitylab.ru/news/489854.php).- 28.11.2017).***

***

«…На общедоступном сервере Amazon исследователями в области безопасности была найдена информация, касающаяся армии США... Утечка, часть которой открыла внутренние данные виртуальной системы, относящиеся к «секретным сообщениям, включает примерно 100 гигабайт, якобы связанной с неудавшимся проектом военной разведки под кодовым названием «Красный диск» («Red Disk»). Этот образ принадлежит совместному проекту Разведывательного управления армии США и Агентства безопасности (АНБ), известному как INSCOM (United States Army Intelligence and Security Command).

Образ диска был оставлен на общедоступном сервере хранения Amazon Web Services без пароля, следовательно, его мог загрузить любой пользователь. Это, кстати, не первый инцидент с утечкой, связанный с такими хранилищами. Крис Викери (Chris Vickery), директор исследования киберрисков в фирме UpGuard, обнаружил эти данные и проинформировал правительство об утечке. Впоследствии хранилище защитили, однако его владелец остается неизвестным…

После распаковки и загрузки образ диска оказался датированным 2013 годом моментальный снимком файловой системы с Linux-сервера, являющегося частью облачной системы обмена разведданными под названием «Красный диск»…

Проект задумывался как легко кастомизируемая облачная система, способная удовлетворить требования масштабных и сложных военных операций. Предполагалось, что система Red Disk должна предоставлять американским солдатам в горячих точках данные прямиком из Пентагона, включая спутниковые снимки и видеотрансляцию с беспилотных летательных аппаратов.

…На разработку проекта Минобороны США потратило $93 млн, однако он так и не был до конца реализован» ***(Произошла утечка данных секретного проекта армии США и АНБ «Red Disk» // РосКомСвобода (https://roskomsvoboda.org/33925/).- 30.11.2017).***

***

«…командующий сухопутными войсками США в Европе Бен Ходжес во время дискуссии на Львовском форуме по безопасности… признал, что сейчас армия США в значительной степени ориентирована на интернет, однако история доказала, что менее эффективные "некомпьютерные" навыки также должны присутствовать в обучении для солдат.

"Мы сейчас снова учимся тому, как пользоваться картами и компасом, поскольку мы не можем быть уверенными в том, останутся ли сервисы, основанные на интернете, в период непрерывных кибератак", - пояснил он» ***(Армия***

США из-за кибератак возвращается к компасу и картам, - генерал // DsNews (http://www.dsnews.ua/world/armiya-ssha-iz-za-kiberatak-vozvrashchaetsya-k-kompasu-i-kartam--30112017230000).- 30.11.2017).

***

Країни ЄС

«Країни Євросоюзу затвердили рішення про посилення європейської кібербезпеки та кіберстійкості у всьому ЄС…

…затверджені сьогодні висновки підкреслюють необхідність того, щоб всі країни ЄС надавали необхідні ресурси та інвестиції для боротьби з кібербезпекою…

Інші заходи, виділені Радою, включають надання необхідних правоохоронних інструментів для боротьби з кіберзлочинністю, розробку скоординованої реакції ЄС на масштабні інциденти та кризові явища та кризові ситуації, а також проведення регулярних навчань із загальноєвропейської безпеки в галузі кібербезпеки.

Що стосується глобальних та дипломатичних аспектів кібербезпеки, Рада визнає важливість міжнародного співробітництва та вітає створення чітких рамок для використання політичних, дипломатичних та економічних інструментів, доступних для ЄС, як відповіді на шкідливу кіберактивність…» ***(ЄС затвердив заходи для посилення європейської кібербезпеки // Європейська правда (http://www.eurointegration.com.ua/news/2017/11/20/7073890/).- 20.11.2017).***

***

«…британская спецслужба занимающаяся радиоэлектронной разведкой и защитой информации правительственных органов и армии GCHQ, считает, что ФСБ России может использовать продукцию «Лаборатории Касперского» для сбора конфиденциальной информации в Великобритании. В частности, речь идет об антивирусной программе «Лаборатории Касперского», которую она предоставляет ряду крупных британских компаний и банков, в том числе Barclays, а те бесплатно предлагают ее своим клиентам. Barclays сотрудничает с «Лабораторией Касперского» еще с 2008 года, и антивирусное ПО компании использует 2 млн клиентов банка.

…в Barclays, рассматривается возможность прекращения сотрудничества с «Лабораторией Касперского». В банке объясняют это коммерческими причинами, не связанными с подозрениями GCHQ…

Мы никогда не получали никаких рекомендаций или указаний относительно "Касперского" ни от GCHQ, ни от Национального центра кибербезопасности»,— заявили FT в Barclays…

Это не первый случай, когда продукция «Лаборатории Касперского» вызвала подозрения у иностранных правительств. Так, в сентябре продукция компании была запрещена к использованию госорганами США как представляющая угрозу

для национальной безопасности…» ***(Алена Миклашевская. Британские спецслужбы подозревают «Лабораторию Касперского» в помощи ФСБ // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3466472?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).- 13.11.2017).***

***

«Національний криптологічний центр Іспанії, підпорядкований Національному розвідувальному центру, не виявив кібератак з боку РФ чи іншої країни під час кризи у Каталонії…

Під час кризи у Каталонії сайти державних органів Іспанії зазнали приблизно 70 атак, які вчинили кіберзлочинці і хакери, в тому числі міжнародне угруповання Anonymous.

Однак інші держави, зокрема Росія, за даними Національного криптологічного центру, за цими кібератаками не стояли…» ***(Розвідка Іспанії не зафіксувала кібератак з боку РФ під час кризи в Каталонії // Європейська правда (http://www.eurointegration.com.ua/news/2017/11/21/7073961/).- 21.11.2017).***

***

«Правительство Великобритании запустило программу Cyber Discovery, призванную заинтересовать школьников старших классов карьерой специалиста по кибербезопасности. Эта инициатива должна восполнить возрастающую нехватку квалифицированных кадров в стране.

В бесплатную программу входит несколько онлайн и оффлайн-мероприятий, посвященных технологиям предотвращения хакерских атак и противодействию взломам…

Заинтересованные старшеклассники должны будут заполнить онлайн-анкету и пройти тест, а лучшие из них смогут перейти к фундаментальному учебному плану…

В учебный план входит цифровое право, защита от хакерских атак, криптография, программирование и этика взлома. Онлайн-занятия перемежаются очным обучением, моделированием реальных ситуаций и проблем…

По оценкам аналитиков, к 2021 году спрос на специалистов по кибербезопасности возрастет до 3 млн человек…» ***(Британия вложит £20 млн в привлечение молодежи в кибербезопасность // Internetua (http://internetua.com/britaniya-vlojit-20-mln-v-privlecsenie-molodeji-v-kiberbezopasnost).- 23.11.2017).***

***

«Совет ЕС принял решение о создании европейской сертификационной системы мирового уровня для программных продуктов, связанных с обеспечением кибербезопасности…

В Совете ЕС подчеркнули, что потери экономики от кибератак уже составляют около €400 млрд каждый год…» ***(Александр Панасенко. В ЕС заявили***

о планах создать сертификационную систему кибербезопасности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-11-21-3/24843).- 21.11.2017).

***

«Правительство Германии рассматривает возможность внесения изменений в Конституцию страны для нанесения ответных ударов по хакерам, атакующим частные компьютерные сети…

По словам представителя Министерства внутренних дел ФРГ, соответствующие реформы планируется завершить в 2018 году. Под возможными мерами противодействия хакерам может пониматься отключение серверов, используемых злоумышленниками в атаках, считают эксперты…

Госсекретарь Клаус Витт (Klaus Vitt)итт также добавил, что многое будет зависеть от результатов коалиционных переговоров в парламенте Германии, в ходе которых в числе прочего будут обсуждаться и вопросы кибербезопасности.

В минувшем месяце чиновники немецких разведслужб сообщили парламенту о необходимости расширить их юридические полномочия для нанесения ответного удара в случае кибератак со стороны иностранных государств…» ***(В Германии могут внести изменения в Конституцию для ответного удара по хакерам // SecurityLab.ru (https://www.securitylab.ru/news/489874.php).- 28.11.2017).***

***

Китайська Народна Республіка

«…правоохранители китайского города Вэньчжоу (провинция Чжэцзян) арестовали 20 человек, которые подозреваются во взломе серверов авиакомпаний и хищении клиентской информации…

Полицейские выяснили, что хакеры продавали похищенные данные по 5 юаней (менее одного доллара) за запись. В течение одного года киберпреступникам удалось получить свыше 10 миллионов юаней (около 1,5 миллиона долларов).

Кража свыше 500 записей с персональными данными предполагает наказание в виде тюремного заключения сроком до 7 лет» ***(Китайская полиция арестовала 20 человек, подозреваемых в кибератаках на авиакомпании // SecureNews (https://securenews.ru/wenzhou/).- 13.11.2017).***

***

Російська Федерація

«Российский бизнес в целом по-прежнему не способен успешно противостоять кибератакам, выяснила PwC.

Многие компании в финансовом секторе, телеком- и IT-отрасли по-прежнему не способны противостоять кибератакам, следует из опроса PwC. В нем участвовали более 9,5 тыс. глав бизнес-подразделений и IT-служб из 122 стран, в

том числе 248 компаний из РФ. 40% респондентов из России признали отсутствие в компаниях общей стратегии информационной безопасности (во всем мире — 44%). В 48% российских компаний нет программы обучения, направленной на повышение осведомленности сотрудников в вопросах безопасности, в 56% отсутствует процедура реагирования на инциденты. По словам большинства респондентов из компаний, пострадавших от кибератак, они не в состоянии установить виновных. В способности идентифицировать личность правонарушителя полностью уверены только 19% участников исследования в России и 39% во всем мире. При этом почти четверть российских опрошенных считают причиной инцидентов в области ИБ использование мобильных устройств — этот фактор занял второе место после фишинговых атак…

Стремительный рост массового производства незащищенных устройств, подсоединенных к интернету вещей, приводит к появлению огромного количества уязвимых мест в системах кибербезопасности, что может вывести из строя критически важную инфраструктуру, полагает PwC… 57% российских компаний— участников опроса уже внедрили или внедряют стратегию в области безопасности в связи с применением «подключенных» устройств.

Уровень понимания ИБ зависит от размера компаний, считает представитель Cezurity Дмитрий Попович. По его словам, подавляющее число компаний имеет до 500 рабочих мест и зачастую руководители и владельцы вынуждены закрывать глаза на то, что инфраструктура не защищена от хакеров…» ***(Роман Рожков. Компании не справляются с хакерами // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3461367?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).- 09.11.2017).***

***

«Россия предложила Организации по безопасности и сотрудничеству в Европе (ОБСЕ) провести в 2018 году конференцию по повышению эффективности структуры в обеспечении информационной безопасности…

Официальная Москва полагает, что проведение этих мероприятий под эгидой ОБСЕ укрепит систему международной информационной безопасности, для чего в будущем году члены организации должны обсудить конкретные механизмы повышения эффективности своей работы по противодействию сетевым угрозам…» ***(Россия предложила ОБСЕ провести конференцию по кибербезопасности в 2018 году // «Парламентская газета» (https://www.pnp.ru/social/rossiya-predlozhila-obse-provesti-konferenciyu-po-kiberbezopasnosti-v-2018-godu.html).- 03.11.2017).***

***

«В Санкт-Петербурге в рамках Национальной технологической инициативы (НТИ) будет построен первый в России инжиниринговый центр кибербезопасности «СэйфНет». Открытие центра намечено на март 2018 года…

…Заявленными целями «СэйфНет» являются создание промышленного интернета, полигонов для обеспечения безопасности других проектов НТИ, а также

разработка защищенной инфраструктуры критических объектов для «Интернета вещей», «умной» энергетики, транспорта, телемедицины и пр…

Правительство Санкт-Петербурга выделило 84,9 млн рублей на реализацию проекта. В следующем году создатели центра рассчитывают получить дополнительное финансирование в виде гранта от Минэкономразвития…

В будущем такой же центр планируется построить в Новосибирске…» ***(В Санкт-Петербурге построят первый центр кибербезопасности в рамках НТИ // SecurityLab.ru (http://www.securitylab.ru/news/489467.php).- 02.11.2017).***

***

«Проект плана мероприятий разработанной по распоряжению Президента России Владимира Путина программы «Цифровая экономика» по разделу «Информационная безопасность» предлагает назначить единый государственный орган, ответственный за гармонизацию требований к информационной безопасности.

…В настоящее время вопросами лицензирования и сертификации в сфере информационной безопасности занимаются два ведомства: Федеральная служба технического и экспортного контроля (ФСТЭК) и Федеральная служба безопасности (ФСБ) в лице Центра по лицензированию, сертификации и защите и государственной тайны…

Как отмечается в плане мероприятий программы «Цифровая экономика» по разделу «Информационная безопасность», современные средства защиты информации носят комплексный характер и попадают под действие сразу обоих систем сертификации: ФСБ и ФСТЭК. Частично требования этих систем сертификации пересекаются: например, в части проверок на отсутствие незадокументированных возможностей, общих требований безопасности аппаратных платформ и операционных систем и пр…

Для определения единого госоргана в области требований к информационной безопасности кому-то - или ФСБ, или ФСТЭК - придется поделиться полномочиями, а никто из них этого не захочет делать…

Другое предлагаемое мероприятие в данной сфере - это государственная поддержка технических комитетов по направлению информационной безопасности. Сейчас деятельность таких комитетов осуществляется почти на общественных началах за счет средств компаний-экспертов…

Кроме того, предлагается создание системы добровольного декларирования уровня безопасности продуктов и услуг ИТК - Декларации информационной безопасности. Для этого необходимо создать положение о саморегулируемых организациях (СРО), действующих в сфере производства товаров и услуг в области информационной безопасности. К 2020 г. должно появиться три соответствующих СРО...» ***(Александр Панасенко. Единый регулятор ИБ возможно будет создан в рамках Цифровой экономики // ООО "АМ Медиа" (https://www.anti-malware.ru/news/2017-11-17-3/24811).- 17.11.2017).***

***

«Банк России начинает работу над изменениями в кодекс корпоративного управления, связанными с вопросам развития информационных технологий и кибербезопасности, сообщила директор департамента корпоративных отношений ЦБ РФ Елена Курицына…

«Настало время чтобы в российском кодексе корпоративного управления нашли свое отражение вопросы управления IT-технологиями и кибербезопасностью на должном уровне. Мы полагаем, что должна быть закреплена стратегическая роль совета директоров в том, чтобы организовывать систему управления рисками, связанными с развитием IT-технологий и вопросами кибербезопасности…», - сказала она.

Банк России опросил 84 российские компании из котировального списка первого и второго уровня Московской биржи. Чуть более 40 компаний ответили на вопросы ЦБ. Так, 73% компаний подтвердили, что вопросы кибербезопасности являются очень актуальной темой, 68% уже приняли внутренние документы, определяющие принципы работы IT и обеспечения кибербезопасности. Почти у половины избран директор в состав совета директоров, обладающий необходимыми компетенциями и навыками в сфере IT и кибербезопасности…» (***Александр Панасенко. ЦБ РФ внесет изменения в кодекс корпоративного управления связанный с ИБ // ООО "АМ Медиа" (https://www.anti-malware.ru/news/2017-11-16-3/24790).- 16.11.2017).***

***

«…В третьем квартале 2017 года эксперты «Лаборатории Касперского» расследовали 24 целевых атаки и кампании кибершпионажа, 10 из которых организовали группы хакеров, говорящих на китайском языке. Атаки в основном были направлены на разработчиков популярного программного обеспечения, а также на госструктуры и важные предприятия…

Одной из главных мишеней хакеров стали государственные проекты России с некоторыми азиатскими странами. Например, в июле специалисты в области интернет-безопасности выявили атаку IronHusky на компании из авиационного сектора России и Монголии…

Кроме этого, жертвами китайскоговорящих злоумышленников стали программы Netsarang и CCleaner. К них хакеры внедряли вредоносные коды.

Как отмечается в отчете, тенденция заражения организаций через производителей программного обеспечения, набирает все большие обороты...» ***(Антон Касс. Китайские хакеры активизировали действия против России // ООО Деловая газета «Взгляд» (https://vz.ru/news/2017/11/17/895775.html).- 17.11.2017).***

***

«…Россия может провести киберучения со странами ЕАЭС с 16 марта по 15 июня 2018 года… Проведение учений предусмотрено программой «Цифровая экономика», утвержденной премьер-министром Дмитрием Медведевым в конце июля. В соответствии с ней, во втором квартале 2018 года должны быть

определены перспективы проведения регулярных киберучений ЕАЭС, а сами учения планировались на 2020 год…

При этом в пресс-службе Евразийской экономической комиссии сообщили, что пока проведение киберучений не планируется, поскольку таких предложений от стран союза официально не поступало…

Появление «дорожной карты» с датами учений стало «формальным исполнением» распоряжения об их проведении при отсутствии инициативы со стороны собственно ЕАЭС и представителей ЕАЭС в рабочей группе, отмечает координатор кластера «Информационная безопасность» Российской ассоциации электронных коммуникаций Ирина Левова. Идея распространения стандартов информационной безопасности на страны ЕАЭС представляется странной, поскольку эти вопросы находятся «вне компетенции международной межправительственной организации торгово-экономического характера», добавляет она…» ***(Россия планирует провести киберучения со странами Евразийского союза // РосКомСвобода (https://roskomsvoboda.org/33639/).- 20.11.2017).***

***

«К ноябрю 2018 года «Росатом» планирует создать и ввести в эксплуатацию систему обнаружения и предотвращения компьютерных атак в корпоративном центре ГосСОПКА. Инвестировать в подобные проекты необходимо, чтобы исполнить требования закона о защите критической информационной инфраструктуры, вступающие в силу в 2018 году. 27 ноября АО «Гринатом» (обслуживает «Росатом») завершит сбор заявок на участие в тендере по созданию системы обнаружения и предотвращения компьютерных атак в корпоративном центре ГосСОПКА «Росатома». Максимальная сумма контракта — 11,6 млн руб. Аттестация системы и запуск в эксплуатацию запланированы к 1 ноября 2018 года, следует из документации «Гринатома»… Для структур «Росатома» это уже второй проект в области создания системы обнаружения кибератак…» ***(Александр Панасенко. Росатом создаст центр ГосСОПКА // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-11-24-3/24896).- 24.11.2017).***

***

«…По уровню осведомленности топ-менеджеров о киберугрозах Россия превзошла среднемировой показатель. Об этом сообщают «Известия» со ссылкой на международный опрос консалтинговой фирмы EY. В опросе приняли участие 1200 представителей компаний из более чем 20 секторов экономики.

Согласно результатам исследования, 30% российских предприятий считают, что смогут распознать потенциальную кибератаку и своевременно принять соответствующие меры. В мире данный показатель составляет всего 12%. Как следует из доклада, всего у 42% отечественных компаний нет единого центра обеспечения кибербезопасности, тогда как по всему миру данный показатель составляет 48%. В то же время 49% респондентов заявили о достаточном уровне подготовки топ-менеджмента в сфере кибербезопасности для управления связанными с ней рисками. Среднемировой показатель по данному вопросу

составил 17%. Помимо этого, 71% опрошенных отметили необходимость повышения расходов на защиту от киберугроз до 50%...» ***(Российские компании переоценивают свою защищенность от кибератак // SecurityLab.ru (https://www.securitylab.ru/news/489853.php).- 28.11.2017).***

***

«…Исследователи безопасности из компании Qrator Labs опубликовали отчет об информационной безопасности в финансовом секторе…

Согласно результатам отчета, 32% респондентов заявили об увеличении бюджета на обеспечение кибербезопасности в 2016 году, при этом 39% опрошенных сообщили, что бюджет остался неизменным, а 13%-ти кредитных организаций бюджет пришлось сократить. ..

Больше половины опрошенных (53%) назвали недостаточный уровень защиты в качестве причины для замены используемых решений для обеспечения кибербезопасности. Более четверти респондентов видят необходимость в замене используемых средств защиты при переходе на новые инфраструктурные решения, например, облачные технологии, где используемые ранее продукты перестают быть эффективными. Около 13% респондентов ответили, что в первую очередь склонны заменять импортные решения на российские аналоги.

Наиболее часто опрошенные компании сталкивались с фишингом (30%) и DDoS-атаками (26%)…

По статистике компании "Валарм", основными векторами атак на web-приложения в финансовой сфере являются внедрение SQLi-операторов (27%) и межсайтовая подделка запросов (26%). Повышенный интерес злоумышленников к данным типам атак связан с возможностью получения информации о базах данных клиентов и персональной информации пользователей, пояснили эксперты…» ***(Больше 50% российских банков недовольны своими средствами защиты от киберугроз // SecurityLab.ru (https://www.securitylab.ru/news/489916.php).- 29.11.2017).***

***

Міжнародне співробітництво у галузі кібербезпеки

«…Специализирующаяся на предотвращении и расследовании киберпреступлений компания Group-IB и Интерпол подписали соглашение об обмене информацией…

В рамках сотрудничества планируется наблюдение за изменениями тенденций в киберпространстве, появлением новых угроз и развитием существующих…

Первым опытом реального взаимодействия стала передача обнаруженных «цифровых следов» хакеров, причастных к атаке Bad Rabbit, спецподразделению Интерпола — Interpol Global Complex for Innovation» ***(Group-IB и Интерпол подписали соглашение о сотрудничестве в сфере кибербезопасности //***

«Открытые системы» (https://www.computerworld.ru/news/Group-IB-i-Interpol-podpisali-soglashenie-o-sotrudnichestve-v-sfere-kiberbezopasnosti).- 03.11.2017).

***

«Європі та Україні доцільно провести спільні навчання протидії кіберзагрозам та кібератакам. Про це 1 листопада, на пленарному засіданні ПА Євронест заявив у своєму виступі директор Національного інститут стратегічних досліджень Володимир Горбулін…

Як зазначив Володимир Горублін, для подолання та протидії таким загрозам країни ЄС та країни Східного партнерства мають поєднати зусилля, зосередившись на практичній площині: …«потрібні спільні навчання між Україною та єврпартнерами, якщо ми не хочемо, щоб агресор вдавався до тих провокацій, до яких вдається…Єдиний ефективний шлях протидіяти – розвивати національну спроможність і більше звертати уваги на дослідження у сфері кібербезпеки…» ***(Лілія Фоменко. У ПА ЄВРОНЕСТ заявили, що Україні та ЄС потрібні спільні навчання протидії кіберзагрозам // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1696299-u-pa-yevronest-zayavili-scho-ukrayini-ta-yes-potribni-spilni-navchannya-protidiyi-kiberzagrozam).- 01.11.2017).***

***

«Рада Європи і ряд великих технологічних компаній підписали угоду з метою забезпечення захисту прав людини і гарантії дотримання законів в Інтернеті.

Ініціативу підтримали такі всесвітньо відомі корпорації, як Apple, Deutsche Telekom, Facebook, Google, Microsoft, Orange і Telefonica…

Нинішня ініціатива - це частина прийнятої Радою Європи стратегії управління Інтернетом в 2016-2019 роках. Основна мета даної програми полягає в підтримці і захисті громадян у Всесвітній мережі. Мова, зокрема, йде про забезпечення рівності і свободи висловлювань, а також про боротьбу з кіберзлочинністю і тероризмом…» ***(Провідні IT-компанії допоможуть захистити права людини в Інтернеті // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2017/10/11/human-rights-online.html).- 10.11.2017).***

***

«29 октября – 3 ноября 2017 г. в Китайской Народной Республике состоялась 8-я Международная конференция «Доверие и безопасность в информационном обществе» (Инфофорум-Китай). Участники конференции посетили три крупнейших технологических и экономических центра Китая – города Гуанчжоу, Шэньчжэнь и Гонконг…

Программа Международной конференции «Инфофорум-Китай» вместила множество разнообразных мероприятий. По сути это был полноценный деловой тур, где участники получили возможность не только обменяться мнениями за круглым столом, но в режиме реального времени познакомиться с тем, как

организована работа и производство продукции передовых ИТ-компаний, как современные информационные решения используются на практике для организации безопасности и жизнедеятельности мегаполисов.

Так, помимо тематических заседаний и международных экспертных встреч, участники посетили международную выставку China Public Security Expo-2017, ситуационный центр полиции г.Шэнчьжэня, штаб–квартиру и демонстративный центр компании Huawei Technologies в Шэньчжэне и завод Huawei Technologies в Song Shan Lake. В Гонконге в рамках конференции состоялась встреча с руководством Science Park и с представителями Бюро инноваций и технологий Администрации Гонконга.

К участию в Международной конференции «Инфофорум-Китай» проявили интерес не только представители России и КНР, о своем участии также заявили представители Армении, Казахстана, Вьетнама и Малайзии…

Среди основных тем конференции были заявлены:

Цифровая экономика: международная практика, перспективы для России и Китая;

Умный город (регион): безопасная информационная инфраструктура мегаполиса;

Цифровое правительство: от электронных услуг к большим данным

Информационные технологии и проблема международного терроризма…»

(Инфофорум-Китай: сотрудничество России и КНР в области инноваций, информационных технологий и информационной безопасности // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5454676-InfoforumKitaj-sotrudnichestvo-Ross.html#ixzz4ze2HFnRy).- 24.11.2017).

***

Кіберзахист критичної інфраструктури

«Польша запустит пилотную программу по усилению кибербезопасности в сфере авиации…

«Мы хотим создать в секторе авиатранспорта единый пункт для координации всех действий по обеспечению кибербезопасности… для авиалиний, аэропортов и воздушного движения», – пояснил руководитель Управления гражданской авиации Польши Петр Самсон (Piotr Samson) на конференции «Кибербезопасность в гражданской авиации». Конференция проходила два дня в Кракове и проводилась совместно с Европейским агентством авиационной безопасности (European Aviation Safety Agency, EASA).

…Согласно заявлению польских властей, в рамках программы по усилению кибербезопасности планируется создать подразделение быстрого реагирования на инциденты» ***(Польша усилит кибербезопасность в сфере гражданской авиации // Internetua (http://internetua.com/polsha-usilit-kiberbezopasnost-v-sfere-grajdanskoi-aviacii).- 11.11.2017).***

***

«Представитель Министерства национальной безопасности США (DHS) объявил о том, что группа специалистов из правительственных структур, отраслевых экспертов и членов исследовательского сообщества еще год назад смогла провести успешную PoC-атаку на системы самолета Boeing 757. Как подчеркнули эксперты, справились они всего за два дня.

По словам представителя DHS Роберта Хики (Robert Hickey), проникнуть в системы самолета экспериментаторы смогли без помощи инсайдера, используя типовое оборудование, которое можно пронести на борт. … взлом произошел через радиочастотное оборудование, пока самолет находился на земле…

Возможность взломать бортовые системы самолета удаленно должна привести к пересмотру отношения к кибербезопасности на авиатранспорте. Как подчеркнул Хики, необходимо провести больше исследований, чтобы выявить все проблемы и определить пути их решения…» ***(Maxim Zaitsev. Boeing 757 можно взломать // Threatpost (https://threatpost.ru/boeing-757-proof-of-concept-hack/23199/).- 13.11.2017).***

***

«…Центральный банк Нидерландов (De Nederlandsche Bank, DNB) соберет команду из хакеров и ИБ-экспертов, чтобы они атаковали местную финансовую инфраструктуру. Ведомство таким образом хочет протестировать и усовершенствовать защитные механизмы нидерландских банков.

По словам представителей DNB, группа хакеров будет осуществлять скрытые атаки на банки, акционерные компании и клиринговые дома. Сейчас данный проект – Tiber (Threat Intelligence Based Ethical Red Teaming) – находится на пилотном этапе…

По замыслу регулятора, банки будут нанимать хакеров, которые войдут в так называемую «красную команду», самостоятельно, а атаки будут проходить под контролем DNB…» ***(Нидерландский Центральный банк привлечет хакеров для атак на финорганизации страны // SecureNews (https://securenews.ru/dnb/).- 15.11.2017).***

***

«SWIFT, глобальна система обміну повідомленнями, яка використовується для переведення трильйонів доларів щодня, попередила банки в середу про те, що загроза кібер-пограбувань зростає, оскільки хакери використовують все більш складні інструменти і методи для нових атак…

У новому попередженні на 16 сторінок, написаному спільно з підрозділом кібербезпеки BAE Systems Plc, докладно описані деякі нові методи, якими користувалися хакери…

SWIFT відмовилось розповідати про кількість атак, ідентифікувати жертв або сказати, скільки грошей було вкрадено. Проте, подробиці про деякі випадки стали загальнодоступними.

Наприклад, центральне інформаційне агентство Тайваню минулого місяця повідомило, що Далекосхідний міжнародний банк втратив 500 тисяч доларів через кібер-пограбування. BAE пізніше сказав, що атака була почата північнокорейської

групою хакерів, відомою як "Лазар" (Lazarus), яка, на думку багатьох компаній в області кібербезпеки, стояла за бангладешською справою…» ***(Юлія Шрамко. SWIFT попередила банки про підвищення загрози кібер-пограбувань // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1701452-swift-poperedila-banki-pro-pidvischennya-zagrozi-kiber-pograbuvan).- 29.11.2017).***

***

Кіберзлочинність та кібертерроризм

«…Аналитики Google вместе с учеными из Калифорнийского университета в Беркли представили исследование, посвященное тому, как хакеры взламывают аккаунты пользователей. Наблюдения велись с марта 2016 по март 2017 года, в центре внимания исследователей находились исключительно аккаунты в Google. Оказалось, что каждую неделю злоумышленники крадут до 250 тыс. паролей и других сведений об аккаунтах.

…самыми распространенными способами кражи данных оказались использование кейлогеров, фишинг и утечка данных через третью сторону. Кейлогер — это ПО, регистрирующее действия пользователя (нажатие клавиш, движение мышкой), число потенциальных жертв взломов с использованием такого ПО за год составило 790 тыс. 12,4 млн случаев взлома приходятся на фишинг (когда злоумышленники создают сайт, похожий на исходный, где пользователь вводит пароль). В случае с утечкой через третью сторону (1,9 млрд случаев) нередко речь идет о покупке данных пользователей на нелегальных площадках.

Исследователи также проанализировали, откуда был совершен последний вход в аккаунт, данные которого были украдены, то есть где, скорее всего, находились хакеры (хотя некоторые из них и могли шифровать свое местоположение). На первом месте и в случае применения кейлогера, и при фишинге находится Нигерия. За ней в первом случае следуют США, Марокко, ЮАР и Великобритания, в случае с фишингом — Бразилия, Сенегал, США и Малайзия…» ***(Google изучила хакеров // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5451004-Google-izuchila-xakerov.html#ixzz4ysdW72UC).- 13.11.2017).***

***

«Хакеры Fancy Bear, которых связывают с российскими спецслужбами, пытались взломать 4,7 тыс. аккаунтов пользователей Gmail на Украине, в России, Грузии и Сирии…

Агенство Associated Press провело собственное расследование, основанное на данных компании Secureworks, занимающейся кибербезопасностью. Информация Secureworks относится к периоду с марта 2015 года по май 2016 года. В США Fancy Bear пыталась получить доступ к 573 аккаунтам электронной почты. В списке целей хакеров фигурировали: бывший госсекретарь США Джон Керри, бывший

госсекретарь Колин Пауэлл, бывший верховный главнокомандующий силами НАТО в Европе Филип Бридлав и отставной генерал Уэсли Кларк…

На Украине Fancy Bear пытались взломать 545 ящиков электронной почты, в том числе, президента страны Петра Порошенко, его сына Алексея и некоторых бывших и нынешних министров…» ***(AP: хакеры Fancy Bear пытались взломать почту влиятельных людей на Украине, в США и в России // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3458622?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C).-02.11.2017).***

***

«Эксперты по кибербезопасности сообщили об обнаружении нового вируса, заражающего устройство без макросов: инфицирование вредоносным программным обеспечением (ПО) происходит через документы Microsoft Office.

Хакерами используется механизм Dynamic Data Exchange (DDE). Он позволяет использовать файлы Word для того, чтобы выполнять код, скрытый в другом файле, передает «Российская газета».

Компания Microsoft уже опубликовала инструкцию по защите от заражения, согласно которой самый простой способ избежать вируса - быть осторожным с незнакомыми окнами, всплывающими при открытии документа…» ***(Наталья Ануфриева. Обнаружен заражающий компьютеры через документы Word вирус // ООО «Деловая газета Взгляд» (https://vz.ru/news/2017/11/14/895141.html).-14.11.2017).***

***

«…Российские хакеры осуществляли атаки на СМИ и энергетический сектор Великобритании в течение 2016 года. Об этом заявил руководитель британского Национального центра кибербезопасности (NCSC) Кирен Мартин во время выступления в Лондоне…

…При этом он подчеркнул, что не может сообщить подробностей, поскольку все материалы засекречены…

По словам чиновника, сейчас центр активно сотрудничает с международными партнерами, представителями индустрии и обществом, чтобы как можно скорее ликвидировать угрозу. С момента своего запуска в прошлом году NCSC заблокировал уже десятки миллионов кибератак и отреагировал на 590 инцидентов…» ***(Руководитель центра кибербезопасности Британии заявил о хакерских атаках России на объекты энергетики и СМИ // Общественно-правовой портал «Ракурс» (http://racurs.ua/news-97135-rukovoditel-centra-kiberbezopasnosti-velikobritanii-zayavil-o-hakerskih-atakah-rossii-na-obekty).-15.11.2017).***

***

«…За даними видання Associated Press, розробник додатку керування артилерією, яку використовують українські військові проти російських

бойовиків на Донбасі, став одним із 545 членів політичної та військової еліти України, атакованих кремлівськими кіберзлочинцями Fancy Bear…

Виданню «Радіо Свобода» підтвердили, що електронна адреса, про яку йдеться, належить українському офіцеру Ярославу Шерстюку.

У розмові з «Радіо Свобода» Шерстюк розповів, що Associated Press повідомляли йому про ймовірну атаку хакерів, але сказав, що зламу його електронної скриньки не було.

Додаток управління артилерією Шерстюка був предметом багатьох суперечок відтоді, як у грудні 2016 року американська компанія з кібербезпеки CrowdStrike оприлюднила звіт про розроблену Fancy Bear шкідливу програму, ймовірно приховану в додатку. CrowdStrike стверджувала, що українські військові втратили 80% своїх радянських гаубиць Д-30 через здатність шкідливих програм отримувати повідомлення та локаційні дані від заражених пристроїв.

Шерстюк заперечив висновки CrowdStrike про те, що його програма опинилася під загрозою, а Міноборони України заперечило, що арсенал гаубиць було пошкоджено в обсязі, зазначеному у звіті компанії…» ***(Хакери Кремля намагалися зламати українську систему керування артилерією // ТзОВ "Редакційні системи" (http://expres.ua/news/2017/11/03/270046-hakery-kremlya-namagalysya-zlamaty-ukrayinsku-systemu-keruvannya-artyleriyeyu).- 03.11.2017).***

***

«Кіберполіція затримала і оголосила про підозру чоловікові, який за гроші допомагав вигравати торги в «Системі електронних торгів арештованим майном»…

… уродженець Кривого Рогу отримав доступ до електронної системи, вносив до неї зміни і за гроші допомагав вигравати торги. Він блокував всіх неугодних йому і його замовникам учасників, надаючи можливість зацікавленим особам виграти в торгах з мінімальними ставками. Такі махінації завдали збитки держбюджету на суму 2 млн грн…

Чоловіку оголосили про підозру у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 361 КК України (несанкціоноване втручання в роботу автоматизованих систем за попередньою змовою групою осіб). Йому загрожує до шести років позбавлення волі» ***(Хакер завдав збитків держбюджету на 2 млн гривень // Інформаційне агентство АСПІ (http://aspi.com.ua/ua/kriminal/item/4486-khaker-zavdav-zbitkiv-derzhbyudzhetu-na-2-mln-griven.html).- 06.11.2017).***

***

«Ряд стран по всему миру стали жертвами масштабной Ddos-атаки. Ботнет IOtroop/REAPER атаковал более 4,5 млн зараженных устройств в 200 странах, включая США, Великобританию, Канаду и Украину…

Кибермошенникам удалось организовать настолько масштабные атаки, начиная с октября, в результате того, что производителям IoT-устройств не удалось до конца устранить ошибки в безопасности.

Эксперты Ddos-Guard уточнили, что атаки осуществляются по принципу Pulse Wave, т. е. их мощность то спадает, то нарастает с одинаковой периодичностью и планомерным увеличением мощности. Объемы мусорного трафика на пике достигают отметки в 160 Gbps/150 Mpps. Боты генерировали HTTP-флуд на уровне L7» ***(Украина стала частью масштабной международной кибератаки // IGate (http://igate.com.ua/lenta/20480-ukraina-stala-chastyu-masshtabnoj-mezhdunarodnoj-kiberataki).- 14.11.2017).***

***

«Российский разработчик в сфере кибербезопасности Group-IB обнаружил более 500 мошеннических сайтов продажи нового iPhone, которые пытаются заработать на ажиотаже вокруг юбилейного смартфона Apple — iPhone X…

За последние два дня специалисты компании обнаружили более 500 мошеннических сайтов, на которых злоумышленники собирают предоплату, продают поддельные смартфоны, крадут конфиденциальные данные пользователей или могут заразить вирусом устройство, с которого жертва зашла на ресурс.

Доход одного такого ресурса в месяц может составлять до $68 тысяч, а в целом ущерб от них Group-IB оценила в $34 млн…

Активность мошенников связана с ажиотажным спросом на iPhone X…» ***(Валерий Вискалин. Group-IB обнаружила 500 мошеннических сайтов продажи новых iPhone X // Rusbase (https://rb.ru/news/group-iphone-x/).- 03.11.2017).***

***

«Компания «Доктор Веб» представила новую брошюру… «Троянцы-шифровальщики. Эпидемия с 2006 года». В ней она вспоминает историю развития этой угрозы и наиболее громкие атаки последних лет. Брошюра рассказывает о том, как обезопасить свой компьютер от заражения, содержит полезные ссылки на информационные и обучающие ресурсы компании «Доктор Веб», а также рекомендации о том, как себя вести, если ваши файлы все же оказались зашифрованы» ***(Что мы знаем о троянцах-вымогателях // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5450647-Chto-my-znaem-o-troyanczaxvymogatel.html#ixzz4ysURIy00.- 10.11.2017).***

***

«…Неизвестные хакеры атаковали… город Спринг Хилл в штате Теннесси (США). Один из служащих городской администрации по неосторожности открыл сообщение электронной почты с вредоносным вложением. В результате зловред распространился по всей компьютерной системе администрации, полностью ее заблокировав.

Жители города лишились возможности совершать любые платежи в городской бюджет онлайн, включая штрафы и коммунальные платежи. Хакеры требуют за разблокировку 250 тысяч долларов. Администрация Спринг Хилл отказывается выполнить их требования и рассчитывает, что IT-специалистам удастся восстановить работу системы, используя ранее созданные резервные копии

данных» ***(Хакеры обложили данью целый город // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5450897-Xakery-oblozhili-danyu-celyj-gorod.html#ixzz4ysd1zTZj).-13.11.2017).***

***

«Эксперты сообщили об обнаружении нового образца вредоносной программы Linux/Ebury – основного компонента ботнета Windigo. Исследование ESET подтвердило, что Ebury продолжает активно использоваться атакующими, и инфраструктура, предназначенная для кражи данных, все еще функционирует…

…в феврале 2017 года специалисты ESET обнаружили новый образец Ebury (версия 1.6), получивший ряд существенных доработок. Теперь Ebury использует новый алгоритм генерации доменов (DGA) для передачи украденных данных. Авторы малвари предусмотрели методы самомаскировки и новые способы внедрения в процессы, связанные с OpenSSH.

Кроме того, операторы Windigo изучают исследования поставщиков решений для безопасности и дорабатывают вредоносные инструменты, чтобы обходить индикаторы заражения и избегать обнаружения» (***Windigo в деле: обнаружены новые компоненты крупнейшего ботнета // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5452048-Windigo-v-dele-obnaruzheny-novye.html#ixzz4ysgp4C5q).- 15.11.2017).***

***

«…Group-IB сообщает о новой волне мошенничеств, совершаемых якобы от лица крупнейших российских финансовых организаций в социальных сетях. Киберпреступники традиционно используют комбинацию современных технологий и методов социальной инженерии для обмана пользователей и получения от них платежных реквизитов и других данных, которые впоследствии могут быть использованы с целью хищения денежных средств. В данном случае площадкой для поиска жертвы являются официальные группы банков в социальных сетях, предназначенные для поддержки пользователей.

Схема достаточно проста: пользователь публикует запрос в официальной группе банка. Тема обращения может быть любой: проблема с банковским сервисом, жалоба или просьба помочь с решением того или иного вопроса. Мошенники отслеживают подобные обращения и оперативно реагируют на них: представляясь сотрудником банка, они переводят диалог в личный формат, уходя от публичного обсуждения запроса, и в персональном сообщении предлагают свою помощь. Как показывают многочисленные примеры, в ходе общения мошенники пытаются различными способами, в том числе, с использованием приемов психологического давления, выманить информацию, которая позволит им получить доступ к деньгам жертвы. Чаще всего, они запрашивают номер и верификационный код карты, идентификатор пользователя, проверочный СМС-код и т.д…» ***(В социальных сетях появилась новая волна «банковского мошенничества» // ООО***

"ИКС-МЕДИА" (http://www.iksmedia.ru/news/5452056-V-socialnyx-setyax-poyavilas-novaya.html#ixzz4yshFcG2m).- 15.11.2017).

***

«Лаборатория Касперского» завершила внутреннее расследование инцидента, связанного с заявлениями ряда СМИ о том, что ПО компании якобы использовалось для поиска и скачивания засекреченной информации с домашнего компьютера сотрудника Агентства национальной безопасности США (АНБ)…

Итоговые результаты расследования таковы:

Защитное решение «Лаборатории Касперского» сработало ровно так, как и должно было сработать при обнаружении вредоносного кода. Оно уведомило аналитиков компании об угрозе на основании сигнатур ПО группировки Equation, деятельность которой на тот момент расследовалась уже шесть месяцев…

Информация, которая предположительно была секретной, была получена экспертами, потому что содержалась в архиве, на который отреагировало решение на основании сигнатур Equation.

Помимо вредоносных программ, указанный архив также содержал исходный код ПО группировки Equation и четыре текстовых документа с грифами секретности. «Лаборатория Касперского» не обладает какой-либо информацией о содержании этих документов, так как они были удалены после получения.

«Лаборатория Касперского» не может оценить, были ли соблюдены формальные процедуры обращения с секретными данными, соответствующие американскому законодательству. Эксперты компании не проходили инструктаж по обращению с засекреченными документами и не имеют юридических обязательств его проходить. При этом никакая информация из документов не передавалась третьим лицам.

В отличие от версии, озвученной в некоторых СМИ, не было найдено доказательств, что исследователи «Лаборатории Касперского» когда-либо пытались целенаправленно искать документы с пометками «совершенно секретно», «засекречено» и другими аналогичными.

Заражение компьютера бэкдором Mokes и потенциальное заражение другим вредоносным ПО указывает на возможность того, что доступ к данным пользователя мог получить неизвестный круг третьих лиц» (***Опубликованы полные результаты внутреннего расследования инцидента с исходным кодом ПО Equation // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5452518-Opublikovany-polnye-rezultaty-vnutr.html#ixzz4ysjoOAI4).- 17.11.2017).***

***

«Специалисты McAfee заблокировали доступ к вредоносной программе, распространение которой осуществлялось из сети самой компании.

Программа находилась на стороннем ресурсе, но распространялась посредством домена, связанного с сервисом McAfee ClickProtect. Примечательно, что задачей этого сервиса является защита пользователей электронной почты от фишинговых писем и вредоносных ссылок…

Троянская программа похищала с зараженной системы пароли и передавала их на командный сервер…» ***(Троянская программа распространялась с ресурса, связанного с защитным сервисом McAfee // SecureNews (https://securenews.ru/mcafee_2/).- 16.11.2017).***

***

«Банковская троянская программа Terdot, созданная на основе Zeus, получила новый функционал, с помощью которого отслеживает и меняет публикации в Facebook и Twitter, а также осуществлять перехват электронных сообщений.

Троянская программа начала активно действовать с середины прошлого года и в основном действует против австралийских, американских, британских, канадских и немецких пользователей. Вредоносное ПО может проводить атаки типа man-in-the-middle, добавлять код в веб-ресурсы, похищать из браузеров учетную информацию и данные банковских карт…

Terdot атакует разные социальные сети, но не «ВКонтакте», что может указывать на происхождение создателей программы.

Распространение троянской программы осуществляется посредством фишинговых писем со ссылкой на PDF-документ, которая запускает процесс загрузки Terdot на компьютер. Проникнув в систему, Terdot через браузерные процессы перехватывает трафик и загружает дополнительные шпионские программы для сбора данных и их передачи хакерам» ***(Банковская троянская программа Terdot шпионит за своими жертвами // SecureNews (https://securenews.ru/terdot/).- 17.11.2017).***

***

«ИБ-специалист Майкл Гиллеспи первым обратил внимание на вымогательскую программу Ordinypt после того, как один из пострадавших от шифровальщика опубликовал сведения об этом вредоносном ПО на ID-Ransomware. Чуть позже эксперты из G Data получили в свое распоряжение образец вымогательской программы, провели его анализ и выяснили, что Ordinypt атакует, прежде всего, немецких пользователей. На немецком языке написаны письма, содержащие вымогательскую программу, и уведомления с требованием выкупа…

…код вредоносной программы изучил реверс-инженер Филип Макенсен. Он пришел к выводу, что Ordinypt является не шифровальщиком, а вайпером.

Как утверждает эксперт, вредоносная программа вовсе не шифрует информацию, а заменяет данные на случайные комбинации символов и удаляет оригинальные версии файлов…

Специалисты считают, что создатели Ordinypt ведут целенаправленную киберкампанию для саботажа работы ряда компаний в Германии…» ***(Шифровальщик Ordinypt уничтожает информацию пострадавших пользователей // SecureNews (https://securenews.ru/ordinypt/).- 13.11.2017).***

***

«Эксперты из Google, Калифорнийского университета в Беркли и Международного института компьютерных наук провели исследование современных киберугроз…

Ученые провели анализ нескольких подпольных торговых площадок, на которых продавались аккаунты и учетная информация. Специалисты изучали данные, полученные за период с марта прошлого года по март текущего года.

Исследователи выявили свыше 788000 пар логинов и паролей, украденных посредством кейлогеров, 12400000 записей с учетными данными, украденными с помощью фишинга, а также чуть менее двух миллиардов пар логинов и паролей, попавших в открытый доступ в результате утечек. 12% аккаунтов, взломанных в ходе утечек, зарегистрированы в Gmail. Пользователи в 7% случаев повторно применяли свой пароль для аккаунта Google для другой учетной записи. Таким образом, сразу два аккаунта находятся под угрозой взлома…

По словам экспертов, фишинг является наиболее серьезной угрозой для пользователей, опережая кейлогеры и утечки данных. Риск взлома аккаунта жертвы фишинга в 400 раз больше вероятности компрометации среднего пользователя Google. Этот показатель в 10 раз меньше у пострадавших вследствие утечек информации и около в 40 раз меньше у жертв кейлогеров» ***(По мнению Google, фишинговые атаки более опасны, чем кейлогеры и утечки информации // SecureNews (https://securenews.ru/google_9/).- 10.11.2017).***

***

«Эксперты Symantec обнародовали отчет об активности кибергруппировки SowBug, которая действует как минимум с 2015 года…

Злоумышленники пользовались вредоносной программой Felisimus.

Впервые она была выявлена в марте этого года…

Используя эту вредоносную программу, киберпреступники могут поставить зараженную систему под свой полный контроль, передавать команды со своего сервера, осуществлять загрузку файлов и выполнять произвольный код…

Согласно отчету, сейчас Sowbug главным образом действует против правительственных органов в странах Южной Америки и Юго-Восточной Азии, в частности против аргентинских, бразильских, брунейских, малазийских, перуанских и эквадорских организаций. Хакеры имеют в своем распоряжении большие ресурсы, потому могут проводить атаки сразу на несколько целей. Зачастую кибернападения осуществляются не в рабочее время целевых организаций.

Пока что неясно, как хакеры проникли в компьютерные сети, но результаты анализа собранной информации позволили экспертам предположить, что злоумышленники задействовали фальшивые обновления для Windows и Adobe Reader…» ***(Кибергруппировка SowBug проводит скрытые атаки на госучреждения с 2015 года // SecureNews (https://securenews.ru/sowbug/).- 09.11.2017).***

***

«Американский Минюст в декабре собирается объявить о начале расследования нескольких дел, в том числе в отношении граждан Ирана…

По информации издания The Washington Post, иранские хакеры организовали кибератаку на телесеть HBO и завладели 1,5 Тб информации, в том числе — скриптами сериала «Игра престолов». В дальнейшем хакеры планировали получить от HBO деньги за отказ публиковать эти данные» ***(WP: минюст США обвинил Иран в кибератаке на телеканал HBO // Internetua (http://internetua.com/wp-minuast-ssha-obvinil-iran-v-kiberatake-na-telekanal-hbo).- 21.11.2017).***

***

«Служба безпеки України викрила банду хакерів, які встигли накрасти з банківських карток понад десять мільйонів гривень…

…шахраї проникали безпосередньо в банківські мережі, де, шляхом зчитування і дублювання інформації, отримували реквізити банківських карт. Четверо злочинців було затримано, в їх приміщенні під час обшуку виявили комп'ютерну техніку, понад мільйон гривень готівкою, а також зброю і патрони. Затриманим було оголошено про підозру у вчиненні злочинів за ст. 208 КК України…» (***У Києві «накрили» хакерів, які вкрали з банківських карт понад 10 мільйонів // ONLINE.UA https://novyny.online.ua/793124/u-kievi-nakrili-hakeriv-yaki-vkrali-z-bankivskih-kart-ponad-10-milyoniv/).- 20.112017).***

***

«…На протяжении ближайших нескольких лет количество направлений атак продолжит расти. В то же время возможности комплексного отслеживания и управления современными инфраструктурами снизятся.

Наблюдаются такие тенденции, как распространение подключенных устройств, имеющих доступ к персональным и финансовым данным, и появление новых подключений между самыми разными объектами — от скоплений устройств IoT и важных инфраструктур автомобилей, домов и офисов до комплексов «интеллектуальных городов»… Согласно нашему прогнозу, в 2018 г. эта тенденция усилится.

По результатам анализа таких изощренных атак, как Hajime, Devil's Ivy и Reaper, мы можем заявлять, что в будущем на смену ботнетам придут интеллектуальные скопления пораженных устройств — «роевые» сети… «Роевые» сети будут задействовать технологию самообучения в целях эффективного поражения уязвимых систем на беспрецедентном уровне. Устройства в составе этих сетей будут взаимодействовать друг с другом и согласованно принимать меры на основе обмена локальными данными. Помимо этого, интеллектуальные устройства-«зомби» будут самостоятельно выполнять команды без вмешательства оператора ботнета. Таким образом, количество устройств в составе «роевой» сети будет расти по экспоненте, как и в скоплениях роящихся насекомых. Эти устройства смогут одновременно атаковать множество целей, что существенно усложнит выявление и устранение угроз… В предыдущем квартале текущего года отдел FortiGuard Labs зафиксировал 2,9 миллиарда попыток установки связи между

ботнетами. Это свидетельствует о серьезности потенциальных последствий распространения «роевых» сетей и больших групп ботов.

…Количество атак при помощи червей-вымогателей и других типов программ за последний год увеличилось в 35 раз, однако это еще не предел. Вероятно, следующей целью программ-вымогателей станут поставщики облачных услуг и другие коммерческие организации, деятельность которых направлена на обеспечение регулярного поступления дохода. Поражение созданных поставщиками облачных услуг сложных гиперподключенных сетей может привести к нарушению деятельности сотен коммерческих организаций, государственных учреждений, важных инфраструктур и организаций здравоохранения…

…В скором времени, а возможно, и в следующем году мы столкнемся с вредоносным ПО, от начала до конца разработанным при помощи машин. При создании такого ПО будут использоваться технологии автоматизированного выявления уязвимостей и комплексного анализа данных. …злоумышленники начнут применять технологию искусственного интеллекта для создания сложных кодов, способных скрываться от обнаружения при помощи написанных машинами процедур. Используя возможности естественного развития уже существующих средств, злоумышленники будут разрабатывать специализированные эксплойты, направленные на максимально эффективное поражение определенных уязвимостей...

…Поставщики важных инфраструктур по-прежнему подвергаются наиболее существенному риску в связи со стратегическими и экономическими угрозами. Речь идет об организациях, которые обеспечивают функционирование сетей высокого значения, предназначенных для защиты важнейших служб и данных… В связи с высокой активностью злоумышленников, а также сближением эксплуатационных и информационных технологий обеспечение безопасности важных инфраструктур становится приоритетной задачей на 2018 г. и последующие годы.

…Согласно прогнозу, в связи с деятельностью организаций в составе инфраструктуры «Преступление как услуга», использующих передовые технологии автоматизации, в темной паутине станут доступными новые услуги. Уже зафиксированы случаи выставления на продажу на рынках темной паутины современных служб, разработанных на основе технологии машинного обучения. В состав некоторых предложений, к примеру, входит служба «полной невидимости» (Fully Undetectable, FUD). При помощи этой технологии разработчики угроз за определенную плату загружают коды атак и вредоносное ПО в службу анализа. Затем они получают отчет о возможности обнаружения угрозы средствами безопасности разных поставщиков…

…В связи с появлением новых технологий в сфере автоматизации и искусственного интеллекта перед изобретательными киберпреступниками открываются новые возможности для нанесения ударов по виртуальной экономике…

Система безопасности должна функционировать на скорости, не уступающей скоростям цифровых подключений, что требует автоматизации реагирования,

применения актуальных данных и внедрения функции самообучения. Благодаря этим мерам сети станут более эффективными и независимыми в принятии решений…

Кроме того, базовые меры защиты должны войти в состав основных протоколов безопасности…» ***(В 2018 бизнес столкнется с самообучающимися массированными кибератаками // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/206088-v_2018_biznes_stolknetsja_s_samoobuchajushchimisja_massirovannymi_kiberatakami).- 27.11.2017).***

***

«Вірус шифрувальник Scarab виявили фахівці, 24 листопада, зафіксували його розповсюдження за допомогою найбільшої спам-ботнет мережі "Necurs"…

Фахівці з кібербезпеки встановили, що з використанням "Necurs" було відправлено понад 12,5 млн електронних листів, в яких містилися файли з новою версією Scarab ransomware.

Електронні листи, в яких містився Scarab, були замасковані під архіви з відсканованими зображеннями…

Ці листи містили всередині архів 7Zip, з заархівованим Visual Basic скриптом. Після його спрацьовування на комп'ютер користувача завантажується і запускається EXE-файл - вірус Scarab ransomware…» ***Кіберполіція попередила про масове поширення вірусу Scarab // Gazeta.ua (https://gazeta.ua/articles/science/_kiberpoliciya-poperedila-pro-masove-poshirennya-virusu-scarab/805784).- 25.11.2017).***

***

«…Согласно отчету «Лаборатории Касперского», после «черной пятницы» общее количество переходов пользователей на фишинговые ссылки падает на 33% — наступает «серая суббота». Так, в 2016 году в «черную пятницу» системы «Лаборатории Касперского» зафиксировали 770 тыс. срабатываний системы «Антифишинг» на компьютерах пользователей, а на следующий день — 510 тыс. Начиная с «киберпонедельника», следующего за «серой субботой», активность фишеров снова начинает расти. Эксперты полагают, что такая тенденция сохранится и в этом году.

Уровень финансовых фишинговых атак стабильно высок в течение всего года, рассказали специалисты. Перед праздниками он становится еще выше, поскольку мошенникам легче обмануть пользователей в разгар акций, выяснили аналитики. По их словам, злоумышленники используют бренд «черной пятницы» в своих атаках, а также страхи пользователей, связанные с кибербезопасностью. Письма могут быть замаскированы под предупреждения о заражении, фальшивые обнаружения взлома я или сообщения, поощряющие осторожное поведение в Интернете…» ***(«Лаборатория Касперского»: вместе с ростом онлайн-покупок увеличивается число финансовых киберпреступлений // «Открытые системы»***

(https://www.computerworld.ru/news/Laboratoriya-Kasperskogo-vmeste-s-rostom-onlayn-pokupok-uvelichivaetsya-chislo-finansovyh-kiberprestupleniy).- 24.11.2017).

***

«Верховный суд Чехии не видит причин для отказа в выдаче США российского хакера Евгения Никулина, обвиняемого в киберпреступлениях, заявил председатель сената суда Карел Шемик…

Окончательно решение о том, в какую из двух стран будет выдан Никулин, примет министр юстиции.

Никулин был задержан в Праге в октябре прошлого года чешской полицией при содействии американского ФБР. Вашингтон обвиняет его за взлом важных серверов, в России он подозревается в интернет-хищениях…

Пражский горсуд весной этого года постановил, что Никулина можно выдать и в РФ, и в США. Обвиняемый обжаловал оба варианта, но затем согласился на экстрадицию в Россию» ***(Валерий Октябрёв. Суд в Чехии готов выдать российского хакера в США // «Парламентская газета» (https://www.pnp.ru/politics/sud-v-chekhii-gotov-vydat-rossiyskogo-khakera-v-ssha.html).- 24.11.2017).***

***

«…По данным агентства Bloomberg, еще в октябре 2016 года хакеры взломали компьютерную систему сервиса и похитили имена, адреса электронной почты и номера мобильных телефонов 50 млн пользователей Uber во всем мире. Кроме того, были похищены персональные данные 7 млн водителей.

Как предает агентство, Uber, вместо того чтобы сообщить о взломе регуляторам и водителям, заплатил похитителям 100 тыс. долларов, чтобы те удалили данные и оставили все в тайне…

В компании заявили, что хакеры не воспользовались полученной информацией. Также в Uber уверены в сохранности данных о кредитных картах, маршрутах поездок и другой информации.

По данным агентства, Uber нанял для расследования инцидента фирму по кибербезопасности Mandiant…» ***(Дмитрий Зубарев. Хакеры похитили данные 57 млн клиентов и водителей Uber // ООО Деловая газета «Вести» (https://vz.ru/news/2017/11/22/896295.html).- 22.11.2017).***

***

«Производитель решений в области информационной безопасности (ИБ) Check Point Software Technologies опубликовал результаты исследования кибератак на корпоративные устройства.

В Check Point сообщили, что все 850 опрошенных компаний столкнулись с вредоносным программным обеспечением в смартфонах и планшетных компьютерах. 89% организаций пережили хотя бы одну атаку вида "человек посередине" (Man-in-the-middle, MitM) на корпоративную сеть Wi-Fi, а 75% респондентов имеют в среднем 35 взломанных устройств, которые в зависимости

от платформы подверглись операции jailbreak (Apple iOS) или root (Android)…» ***(Все компании сталкиваются с кибератаками на мобильные устройства // Internetua (http://internetua.com/vse-kompanii-stalkivauatsya-s-kiberatakami-na-mobilne-ustroistva).- 25.11.2017).***

***

«20 ноября 2017 года были подвергнуты кибератаке и взлому некоторые информационные ресурсы организаций Узбекистана…

Массовой кибератаке было подвергнуто более 60 тысяч ресурсов в различных странах мира.

Центром UZINFOCOM и Центром информационной безопасности и содействия в обеспечении общественного порядка приняты оперативные меры по устранения источника атаки, создания резервных копий взломанных ресурсов для последующего изучения, а также восстановления последней актуальной версии системы с рабочими системными файлами и веб-сайтами организации.

В настоящий момент информационные ресурсы работают в штатном режиме. Последствия атаки полностью устранены…» ***(Сайты госорганов Узбекистана пострадали от кибератак // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5454440-Sajty-gosorganov-Uzbekistana-postra.html#ixzz4ze1lxzZg).- 23.11.2017).***

***

«…Вирусные аналитики компании «Доктор Веб» исследовали новую версию вредоносной программы, относящейся к широко известному семейству Trojan.Gozi.

Новый банковский троянец, получивший наименование Trojan.Gozi.64, основывается на исходном коде предшествующих версий Trojan.Gozi, который уже долгое время находится в свободном доступе. Как и другие представители этого семейства, Trojan.Gozi.64 может заражать компьютеры под управлением 32- и 64-разрядных версий Windows. Троянец имеет модульную архитектуру, но, в отличие от предыдущих модификаций, он полностью состоит из отдельных загружаемых плагинов. Также Trojan.Gozi.64 не имеет алгоритмов для генерации имен управляющих серверов — их адреса «зашиты» в его конфигурации, в то время как одна из первых версий Gozi использовала в качестве словаря текстовый файл, загружаемый с сервера NASA.

Создатели троянца заложили в него ограничение, благодаря которому он способен работать с операционными системами Microsoft Windows 7 и выше, в более ранних версиях Windows вредоносная программа не запускается…

Банковский троянец Trojan.Gozi.64 не представляет опасности для пользователей антивирусных продуктов Dr.Web, поскольку сигнатуры вредоносной программы и ее модулей добавлены в вирусные базы» ***(«Доктор Веб» исследовал нового банковского троянца // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5454815-Doktor-Veb-issledoval-novogo-bankov.html#ixzz4ze2zpayq).- 24.11.2017).***

***

«Кибергруппировка Cobalt получила известность благодаря атакам на банкоматы и европейские финансовые учреждения… В августе этого года от действий хакеров из Cobalt пострадало около 250 компаний, включая банки, биржи, инвестиционные фонды и страховые фирмы.

Как утверждают специалисты, сейчас кибергруппировка Cobalt использует уязвимость для заражения вредоносными программами компьютеров жертв. Так, Cobalt занимается распространением вредоносных RTF-документов, которые содержат эксплоит для данной уязвимости. Прежде всего, целями хакеров становились богатые и высокопоставленные люди.

Эксперты сообщают, что кибергруппировка начала работать с этой уязвимостью достаточно оперативно, что может быть вызвано скорой публикацией 4 PoC-эксплоитов (через несколько недель после релиза патча)…» ***(Кибергруппировка Cobalt пользуется уязвимостью в Microsoft Equation // SecureNews (https://securenews.ru/cobalt_3/).- 28.11.2017).***

***

Протидія зовнішній кібернетичній агресії

«Помощник генсека НАТО Сорин Дукару заявил в ходе выступления на конференции ОБСЕ по кибербезопасности о неспособности альянса самостоятельно справиться с киберугрозами.

По словам Дукару, …НАТО необходимо …сделать упор на сотрудничество с международными организациями, странами-партнерами, научными кругами и промышленным сектором для повышения уровня защиты, отметил он.

Также помощник генсека призвал выработать нормы безопасного поведения в киберпространстве, одновременно укрепляя данную сферу. По его словам, союз вложил ресурсы в создание системы централизованной защиты информационной сети…» ***(НАТО не в состоянии самостоятельно справиться с киберугрозами // SecurityLab.ru (http://www.securitylab.ru/news/489521.php).- 03.11.2017).***

***

«8 листопада міністри оборони країн-членів Північноатлантичного альянсу схвалили рішення про створення нової структури – Центру кібероперацій.

Про це заявив генеральний секретар НАТО Єнс Столтенберг…

Наразі триває розробка концепції нової командної структури НАТО й в рамках цього процесу було ухвалене відповідне рішення. Пан Столтенберг наголосив, що Центр кібероперацій буде військовою структурою, оскільки кібератаки нині становлять серйозну загрозу для безпеки країн-членів альянсу.

«Я вірю, що надалі в будь-якому військовому конфлікті буде кіберскладова. Через це нам необхідно інтегрувати наші кіберможливості... Ми повинні бути в кібер-сфері настільки ж ефективними, як на землі, на морі та в повітрі», – заявив генеральний секретар НАТО» (***Еспрессо. (НАТО створить Центр кібероперацій***

// MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/nato_stvorit_tsentr_kiberoperatsiy/).- 09.11.2017).

***

«Віце-канцлер міністерства внутрішніх справ Естонії Ерккі Коорт заявив, що органам правопорядку вдалося довести зв'язок зі спецслужбами РФ 20-річного громадянина Росії Олексія Васильєва, заарештованого за підготовку комп'ютерного злочину…

За його словами, під час кібератак 2007 року, пов'язаних з перенесенням пам'ятника "воїну-визволителю Талліна" (Бронзовий солдат), владі Естонії не вдалося нікого притягнути до відповідальності. "Тепер же було успішно доведено, що спецслужби іншої країни використовували агента для того, щоб проникнути в комп'ютерну систему Естонії, перебуваючи на території країни", - заявив віце-канцлер.

20-річний Васильєв був затриманий в Нарві 4 листопада і заарештований 6 листопада. Його підозрюють у скоєнні злочину ненасильницького характеру проти незалежності і суверенітету або територіальної цілісності Естонії, що передбачає покарання у вигляді позбавлення волі на строк від двох до 15 років…» ***(Естонія заявила про зв'язок арештованого за кібератаку росіянина зі спецслужбами РФ // Інтерфакс-Україна (http://ua.interfax.com.ua/news/general/462275.html).- 16.11.2017).***

***

«Канада та інші країни НАТО повинні більше робити для того, щоб протистояти використанню Росією засобів кібервійни, які зростають і розвиваються. Про це заявив Генеральний секретар НАТО Йєнс Столтенберг в ефірі CBC Radio…

«Раніше ми бачили більшість атак на кібермережі штаб-квартири НАТО, тепер ми спостерігаємо більше атак на мобільні телефони солдатів», - додав Генсек НАТО.

«Певною мірою кожна країна є сусідом Росії, тому що кіберпростір не визнає ніяких кордонів, тому також можна сказати, що Канада є сусідом Росії», - сказав міністр оборони Естонії Юрі Луйк.

Ця цифрова близькість, за словами Ю.Луйка, означає, що Канада не повинна дивуватися, якщо Росія спробує втрутитися в федеральні вибори в країні в 2019 році…» (***Юлія Шрамко. Генсек НАТО попередив Канаду про російські кібератаки // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1699563-gensek-nato-poperediv-kanadu-pro-rosiyski-kiberataki).- 20.11.2017).***

***

«…Видання Rzeczpospolita зазначає, що Захід лише зараз з жахом усвідомлює, що нова російська кіберзброя загрожує його інтересам. У Великій

Британії хочуть дізнатися, наскільки Москва вплинула на результат референдуму щодо Brexit у червні минулого року…

Уряд Іспанії теж усвідомив, що Москва стоїть за пропагандою в Інтернеті, яка переконала більшу частину світової спільноті щодо підтримки каталонських націоналістів. Прокурор Роберт Мюллер завершує розслідування щодо впливу Росії на перемогу Дональда Трампа в США, просуваючи "чорний образ" Хілларі Клінтон в мережі…

Як зазначає видання, стратегія Росії в кіберпросторі заснована на двох стовпах. З одного боку, за допомогою соціальних мереж, лідерів громадської думки, дружніх порталів Кремль поширює неправдиву інформацію. З іншого боку, російські хакери отримують стратегічну інформацію і навіть намагаються паралізувати ключову для безпеки держави інфраструктуру…

Відзначається, що російські хакери також дуже активні в Польщі: за останні півроку вони здійснили 2,5 мільйона атак на цілі в країні…» ***(Юлія Шрамко. Російські хакери атакували Польщу 2,5 млн разів за півроку // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1699594-rosiyski-khakeri-atakuvali-polschu-2-5-mln-raziv-za-pivroku).- 20.11.2017).***

***

«Служба безпеки України (СБУ) розробила концепцію захисту підприємств від кіберзагроз за принципом обміну інформацією між приватним бізнесом і державою…

«…СБУ напрацьовуватиме індикатори кіберзагроз і ділитиметься ними з об’єктами критичної інфраструктури, без будь-яких додаткових умов. Необхідна лише довіра до інфраструктури, тобто має бути довірений канал, яким підприємство може отримати інформацію про загрозу, й бажання захистити свою інфраструктуру», — повідомив агентству співрозмовник з СБУ, який побажав залишитися невідомим.

За його словами, така співпраця матиме й економічний ефект, давши змогу компаніям отримати захист від кіберзагроз без значних фінансових витрат…» (***СБУ розробила концепцію захисту підприємств від кібератак // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/sbu-rozrobila-kontseptsiyu-zahistu-pidpriyemstv-vid-kiberatak.html).- 30.11.2017).***

***

«В Эстонии в городе Тарту во вторник, 28 ноября, начались крупные киберучения Cyber Coalition Североатлантического альянса (НАТО)…

В учениях принимают участие свыше 700 специалистов по информационным технологиям, а также различные чиновники из 25 стран-членов НАТО и четырех стран-партнеров, включая Финляндию, Швецию, Швейцарию и Ирландию. Из них около 100 человек участвуют в маневрах в Тарту, а остальные 600 — находятся на своих рабочих местах в разных странах мира.

"Учения направлены на проверку способности стран — членов НАТО и стран-партнеров противостоять кибератакам, а также на отработку сотрудничества

экспертов кибербезопасности на внутригосударственном и международном уровне", — сказано в сообщении…» ***(В Эстонии проходят учения НАТО Cyber Coalition // mediahouse.com.ua (http://mediahouse.com.ua/v-yestonii-prokhodyat-ucheniya-nato-cyber-coalition/).- 29.11.2017).***

***

«Группа стран-союзников НАТО разрабатывает новые принципы кибервойны в связи с хакерскими атаками со стороны России, Китая и КНДР

Одним из них может стать использование ответных кибератак с целью уничтожить сеть противника…

Над стратегией работают США, Великобритания, Германия, Норвегия, Испания, Дания и Нидерланды. Стороны надеются закончить ее к началу 2019 года.

Доктрина может изменить подход НАТО - от обороны к конфронтации с хакерами, с помощью которых, как отметили чиновники Альянса, Россия, Китай и Северная Корея пытаются нанести ущерб западным правительства и украсть технологии…» ***(НАТО готовит мощный кибер-ответ российским хакерам // DsNews (http://www.dsnews.ua/world/nato-gotovit-moshchnyy-kiber-otvet-rossiyskim-hakeram-30112017160600).- 30.11.2017).***

***

«Российские силовые структуры уже приготовили механизмы, позволяющие совершить массивное кибервлияние в Украине.

…такое заявление озвучила эксперт по стратегическим коммуникациям ОО «Информационная безопасность», экс-замминистра информационной политики Украины Татьяна Попова. С ее слов, в России уже создано соответствующее подразделение, возможности которого растут с каждым днем.

«Стоит ожидать ужасные последствия. В том числе, во время «Ч» из-за противоправного вмешательства в системы управления и жизнеобеспечения киберпреступники смогут остановить работу атомных и других электростанций. Как результат, потребители останутся без электрической энергии. И если на промышленных объектах в ряде случаев есть резервные генераторы, то обычные граждане, особенно жители многоэтажных домов, такой возможности лишены», - говорит Попова.

Кроме того, прекратится функционирование транспортной инфраструктуры государства. В то же самое время, остановится банковская система – перестанут функционировать банковские карты» ***(Елена Клименко. Россия готова нанести мощную кибератаку на Украину – эксперт // Replyua (http://replyua.net/news/82066-rossiya-gotova-nanesti-moschnuyu-kiberataku-na-ukrainu-ekspert.html).- 30.11.2017).***

***

Актуальні питання протидії злочинності в сучасних умовах: вітчизняний та зарубіжний досвід : матеріали Міжнар. наук.-практ. конф. (17 берез. 2017 р., Дніпропетр. держ. ун-т внутр. справ) : у 2 ч. / Дніпропетр. держ. ун-т внутр. справ, Ген. прокуратура України, Нац. акад. прокуратури України. - Дніпро : Ліра ЛТД, 2017. - Ч. 1. - 255 с.

Зі змісту:

Надтока О.В. Інформаційна безпека в контексті протидії злочинності.

Шифр зберігання НБУВ: В356709/1.

***

Актуальні питання протидії злочинності в сучасних умовах: вітчизняний та зарубіжний досвід : матеріали Міжнар. наук.-практ. конф. (17 берез. 2017 р., Дніпропетр. держ. ун-т внутр. справ) : у 2 ч. - Дніпро : Ліра, 2017.- Ч. 2. - 303 с.

Зі змісту:

Булай Ю.Г., Булай Р.И. Киберпреступность, а также международные киберугрозы и их решение;

Гребенюк М.В. Європейський досвід оцінки загроз організованої кіберзлочинності (ЮСТА);

Гуцалюк М.В. Щодо протидії діяльності організованих злочинних угруповань, які використовують кіберпростір у своїх інтересах;

Кононець В.П., Карпенко А.В. Щодо зарубіжного досвіду протидії кіберзлочинності

Шифр зберігання НБУВ: **В356709/2**.

***

Комп'ютерні системи і мережні технології (CSNT-2017) : тези доп. X Міжнар. наук.-техн. конф., 20-22 квіт. 2017 р. / НАН України, Нац. авіац. ун-т, Навч.-наук. ін-т комп'ютер. інформ. технологій . - Київ, 2017. - 94 с.

Зі змісту:

Балакин С.В. Средства диагностирования несанкционированных воздействий и атак в компьютерной сети;

Галата Л.П., Пасічник П.В. Захист комп'ютерної мережі за допомогою протоколу PPTP

Шифр зберігання НБУВ: ВА812472.

***

Кузіна І. І. Роль інституту освіти в забезпеченні інформаційної безпеки держави (з позицій неоінституціонального підходу) / І. І. Кузіна // Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Соціологічні дослідження сучасного суспільства: методологія, теорія, методи. - 2017. - Вип. 38. - С. 31-34.

Розглянуто інститут освіти як дієвий інструмент, який може сприяти запобіганню або мінімізації наслідків загроз. Подано механізми, завдяки яким інститут освіти може виконувати функцію забезпечення інформаційної безпеки держави.

Шифр зберігання НБУВ: Ж29137/соц.

***

Наукові пошуки у ІІІ тисячолітті: соціальний, правовий, економічний та гуманітарний виміри : зб. тез ІІ Міжнар. наук.-практ. конф. (м. Кропивницький, 7-8 квіт. 2017 р.) / Кропивниц. ін-т держ. та муніцип. упр. - Кропивницький : КОД, 2017. - 348 с.

Зі змісту:

Цимбалюк В.С. Вплив кібер-права на перспективи удосконалення законодавства України про інформацію.

Шифр зберігання НБУВ: ВА813581.

***

Проблеми та напрями вдосконалення підготовки військових фахівців з урахуванням досвіду антитерористичної операції у східних областях України. XVI науково-методична конференція, Житомир, 25 травня 2017 року : тези доп. / Житомир. військ. ін-т ім. С. П. Корольова. - Житомир, 2017. - 175 с.

Зі змісту:

Завада А.А. Проблемні питання підготовки фахівців у галузі інформаційної безпеки;

Наумчак О.М. Обгрунтування необхідності підготовки фахівців у галузі кібербезпеки;

Павленко М.М. Сучасні шляхи забезпечення кібернетичної безпеки в комп’ютерних системах;

Сіленко В.П. Використання пакета програм при вивченні дисциплін спеціальності «Кібербезпека»;

Грищук Р.В. Особливості підготовки військових фахівців у Житомирському військовому інституті в галузях знань «Інформаційна безпека» та «Інформаційні технології»;

Дятел А.В. Особливості підготовки військових фахівців з інформаційно-психологічного впливу з метою інформаційної протидії в кіберпросторі;

Семчишин О.В. Пропозиції з удосконалення підготовки військових фахівців у сфері кібербезпеки;

Шкатула О.П. Кібернетичні загрози пізнавальній діяльності курсантів.

Шифр зберігання НБУВ: ВА812857.

***

Роль і місце національної спецслужби в історії українського державотворення : матеріали всеукр. наук.-практ. конф., 17 берез. 2017 р. / Служба безпеки України, Київ. нац. ун-т ім. Тараса Шевченка. - Київ, 2017. - 357 с.

Зі змісту:

Пальчик М.Л. Підвищення цифрової грамотності громадян та культури безпекового поводження у кіберпросторі як пріоритетний напрям забезпечення кібербезпеки України;

Рузик Д.М., Ковальчук С.П., Ваганій Н.В. Виготовлення вітчизняних технічних засобів як невідкладний захід із нейтралізації загроз кібербезпеці держави;

Сморжевська О.О. Кіберпростір: виклики гібридної війни для України;

Тронц В.М. Питання правового забезпечення міжнародного співробітництва у боротьбі з кіберзлочинністю;

Богуш В.М., Ковальчук О.В., Настралін В.П. Правове забезпечення сфери протидії кіберзлочинності;

Варенья Н.М., Смірнова В.О. Контррозвідувальна та слідча діяльність в аспекті контентного аналізу кіберпростору;

Верлінгер М.І., Гулак Г.М. Проблема регулювання господарської діяльності у сфері кіберзахисту;

Жуйкова К.В., Гулак Г.М. Кібербезпека як фактор впровадження інновацій;

Лигун В.К. Українські спецслужби на захисті кібернетичної безпеки України;

Присяжнюк М.М., Цифра С.І. Збезпечення кібербезпеки – проблема міжнародного рівня;

Рагнєв А.О. Кібернетичний простір як чинник еволюції діяльності спецслужб;

Щербань В.С., Гулак Г.М. Актуальні питання термінологічних визначень в галузі кібербезпеки.

Шифр зберігання НБУВ: ВА812536.

***

Справедливість у юриспруденції: теорія та практика : зб. матеріалів Міжнар. юрид. наук.-практ. конф. : тези наук. доп., (23 лют. 2016 р.). - Київ, 2017. - 154 с.

Зі змісту:

Сироїд Т.Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності

Шифр зберігання НБУВ: ВА812307.

***

Тези доповідей ІІ Міжнародної науково-практичної конференції «Міжнародні наукові та інноваційно-інвестиційні програми: досвід та результати» (17-18 травня 2017 року) / ДВНЗ "Укр. держ. хім.-технол. ун-т" [та ін.]. - Дніпро : ДВНЗ УДХТУ, 2017. - 274 с.

Зі змісту:

Федулова С.О., Чоп З. Інформаційна безпека та інформаційне суспільство;

Федорова Н.С. Кіберзлочинність як форма прояву інформатизації економіки.

Шифр зберігання НБУВ: ВА813318

***

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.