Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 10 (жовтень)

Київ - 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. – № 10 (жовтень) . – 79 с.

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

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

ЗМІСТ

«5 жовтня 2017 року Верховна Рада України прийняла Закон «Про основні засади забезпечення кібербезпеки України».

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів громадян, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Закон визначає, що об'єктами кіберзахисту є:

1. комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
2. об'єкти критичної інформаційної інфраструктури;
3. комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Забезпечення кібербезпеки покладається на міністерства та інші центральні органи виконавчої влади; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єктів оперативно-розшукової діяльності; Збройні Сили України; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єктів господарювання і громадян, які надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом…

Критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України – Національним банком України…

Так, Правління Національного банку України 28 вересня 2017 року прийняло Постанову № 95, якою затвердило Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України…

Постановою визначено обов'язкові вимоги щодо організації заходів інформаційної безпеки, які поетапно мають впроваджуватися банками:

– 1-й етап (основний – впровадження базових заходів інформаційної безпеки) – до 01 березня 2018 року,

– 2-й етап (впровадження додаткових заходів – для підвищення рівня зрілості інформаційної безпеки) – до 01 вересня 2019 року.

Зокрема вказані заходи безпеки інформації включають в себе: захист від зловмисного коду, заходи безпеки при використанні електронної пошти, контроль доступу до інформаційних систем банку, заходи безпеки в мережі банку, криптографічний захист інформації тощо…

Крім того, відповідно до провідного світового досвіду з питань інформаційної безпеки, документ передбачає призначення в банках відповідальної особи за інформаційну безпеку (Chief Information Security Officer, CISO) та наділення її повноваженнями, достатніми для прийняття управлінських рішень. Також банки повинні сформувати окремі підрозділи з інформаційної безпеки виключно зі штатних працівників банку, які безпосередньо підпорядковуються CISO…

Постанова набирає чинності з 01 березня 2018 року, крім розділу V «Додаткові заходи безпеки інформації», вимоги якого наберуть чинності з 01 вересня 2019 року…» ***(Страховщиков могут обязать обеспечить кибербезопасность и провести ее аудит - вице-президент ЛСОУ // TRISTAR.com.ua - твой финансовый навигатор! (http://tristar.com.ua/1/news/strahovshikov_mogut_obiazat_obespechit_kiberbezopasnost_i_provesti_ee_audit___vitse_prezident_lsou_8111_8112.html).- 10.10.2017).***

***

«Голова Верховної Ради України Андрій Парубій підписав три ухвалених парламентом закони «Про основні засади забезпечення кібербезпеки України», «Про електронні довірчі послуги» та «Про гастрольні заходи в Україні»…

…законопроект №2126а "Про основні засади забезпечення кібербезпеки України", законопроект №4685 "Про електронні довірчі послуги" та законопроект №6682 "Про гастрольні заходи в Україні" були ухвалені Верховною Радою 5 жовтня 2017 року…» ***(Парубій підписав закони про кібербезпеку, електронні довірчі послуги та про гастролі російських артистів // Інтерфакс-Україна (http://ua.interfax.com.ua/news/political/456315.html).- 20.10.2017).***

***

«Административную ответственность за нарушение законодательства в сфере технической и криптографической защиты информации могут ужесточить…

Так, за невыполнение требований законодательства по организации и обеспечению технической защиты государственных информационных ресурсов или информации, требование по защите которой установлено законом, предлагается наказывать наложением штрафа на должностных лиц органов власти, предприятий, учреждений и организаций независимо от формы собственности в размере от 50 до 100 необлагаемых минимумов доходов граждан.

Те же действия, совершенные повторно в течение года, повлекут за собой наложение штрафа в размере от 100 до 150 необлагаемых минимумов.

Комитет по вопросам законодательного обеспечения правоохранительной деятельности рекомендует Верховной Раде принять за основу соответствующий правительственный законопроект № 6711 «О внесении изменений в Кодекс

Украины об административных правонарушениях относительно невыполнения требований законодательства по организации и обеспечению защиты информации» ***(Руководителей предприятий хотят штрафовать за ненадлежащую защиту информации // Інформаційне агентство "ЛІГА:ЗАКОН (http://jurliga.ligazakon.ua/news/2017/10/6/165259.htm).- 06.10.2017).***

***

Організаційне забезпечення захисту інформації

«Новий відділ комп'ютерних мереж і кібербезпеки відкрили на базі провідної рівненської компанії у галузі інноваційних технологій "Ель-Роі"…

…спеціалісти відділу СКМ ТзОВ "Ель-Рої" пропонують жителям Рівненщини широкий спектр послуг у галузі інформаційної безпеки. Зокрема, проектування і монтаж структурованих кабельних мереж, доставку компонентів, створення і монтаж локальної обчислювальної мережі, а також комплекс послуг "під ключ" по створенню Wi-Fi мереж в офісах, виробничих приміщеннях, складах, відповідно до потреб замовника…» ***(У Рівному пропонують інноваційний підхід до кібербезпеки і збереження інформації // Інтернет-портал "ЧаРівне.інфо" (http://charivne.info/rivne-news/29776-u-rivnomu-proponuyut-innovatsijnyj-pidkhid-do-kiberbezpeky-i-zberezhennya-informatsiyi).- 20.10.2017).***

***

Технічні аспекти кібербезпеки

«На открытии ежегодной конференции Oracle OpenWorld в Сан-Франциско, которая начала работу вчера, председатель совета директоров и главный технологический директор Oracle Ларри Эллисон рассказал о новой разработке корпорации…

Oracle Autonomous Database Cloud — это первая в мире 100%-но самоуправляемая автономная база данных. …она использует алгоритмы машинного обучения и практически не требует администрирования и настройки, устраняя вероятность ошибки из-за «человеческого фактора» и функционируя подобно самоуправляемым автомобилям.

…решается весьма актуальная сегодня проблема кибербезопасности: базы данных могут сами себя защищать, выявляя аномальные события, например, если CFO вдруг войдет в систему из нетипичного региона. Полностью автоматизированная СУБД способна также обнаруживать и пресекать атаки, автоматически применять патчи в реальном времени: останавливать базу данных для этого не требуется.

…продукт практически полностью устраняет ручной труд по управлению базой данных (а это существенное снижение затрат), гарантирует доступность на

уровне 99,995% (не более 30 мин простоя в год), потребляет меньше системных ресурсов и обладает повышенной производительностью за счет автоматической тонкой настройки. Кэширование, индексирование, параллельное выполнение, распределение, сжатие данных — оптимизируются автоматически и система адаптируется к изменению данных…

Новый продукт сможет использоваться на платформе Oracle Exadata у заказчика, как облачный сервис в Oracle Cloud, а также в составе Oracle Cloud at Customer…

«Автономные сервисы» Oracle будут охватывать все нагрузки базы данных. Заказчкам будут доступны облачные сервисы Data Warehouse, OLTP Database, Express Database, NoSQL Database. Их отличия — автоматизация и высокая эффективность использования ресурсов. Планируется, что первая автономная база данных Oracle Autonomous Database Cloud будет доступна уже в конце 2017 года — для Data Warehouse…» ***(Ларри Эллисон объявил о создании самоуправляемой СУБД // «Компьютерное Обозрение» (http://ko.com.ua/larri_jellison_obyavil_o_sozdanii_samoupravlyaemoj_subd_121801). - 05.10.2017).***

***

«…Кібератаки стали головним болем сучасного життя. Але їхня історія значно давніша, ніж може здатися.

Про це у своїй статті пише заступник головного редактора The Economist Том Штендеж.

Він нагадує, що перша державна інформаційна мережа була збудована у Франції в 1790-х роках. Це була механічна телеграфна система, яка складалася з мережі веж, кожна з яких мала рухомі дерев'яні важелі на даху… Оператори в кожній вежі повинні були змінювати конфігурацію важелів, повторюючи їхнє розташування у попередній вежі, за якою вони спостерігали через телескоп…

У ті часи лише французька влада могла користуватися інформаційною мережею. Але в 1834 році двоє банкірів Франсуа і Жозеф Блан знайшли спосіб, …як використати телеграфну лінію. Вони підкупили оператора в місті Тур, щоб він робив умисні помилки в урядових повідомленнях через мережу…

Хитрість була викрита лише в 1836 році, коли продажний оператор вежі в Турі захворів і розповів про все другу… Братів Блан притягнули до суду, хоча їх не могли ні в чому звинуватити, оскільки не було закону, який би забороняв вносити додаткові дані в інформаційні мережі. На думку автора, вчинок французьких банкірів сотні років тому можна вважати першою в історії кібератакою.

Ця історія може послужити уроком для людства сьогодні, яке щодня зіштовхується з порушеннями в мережі. По-перше, варто уникати надмірної самовпевненості. Вторгнення в мережі на зразок тієї, від якої постраждала Yahoo, часто лишаються непоміченими впродовж багатьох років… Однак, розуміння загальної картинки масштабів кібератак лишається неправильним, і це проблема для кібербезпеки. Більшість організаторів атак, як і брати Блан, приховують своє втручання.

По-друге, попри розвиток технологій, безпека все одно схожа на ланцюг процесів. І людина в ньому завжди найслабша ланка… І це стосується так само сучасних систем. Ставлення до питання кібербезпеки як до суто технологічного виклику ігнорує важливу частину картинки: кібербезпека також залежить від встановлення правильного виконання соціальних і економічних ініціатив.

І по-третє, варто пам'ятати, що якими б новими не були винаходи, люди, такі як блати Блан, завжди будуть шукати спосіб використати їх для своїх злочинних намірів. Цей аспект людської натури вічний. І жодні технології не можуть його усунути…» ***(Перша в історії кібератака сталася більше 200 років тому і її урок актуальний досі - The Economist // «Дзеркало тижня. Україна» (https://dt.ua/TECHNOLOGIES/persha-v-istoriyi-kiberataka-stalasya-bilshe-200-rokiv-tomu-i-yiyi-urok-aktualniy-dosi-the-economist-256085_.html).- 05.10.2017).***

***

«Киберпреступность меняет свой облик и учится использовать социальные сети. К этому выводу пришли эксперты по кибербезопасности после обсуждения новых видов угроз.

Но это не означает, что можно забыть о вирусах-вымогателях или что атаки на критически важные инфраструктуры отошли на второй план. Эти угрозы по-прежнему несут огромный риск. Однако участники Кембриджского саммита по кибербезопасности пришли к заключению, что новые угрозы, такие как заказные, хорошо финансируемые атаки, начинают обретать узнаваемые черты…

По словам экспертов, в ландшафте угроз не только меняются способы взлома, вирусы-вымогатели и интеллектуальное воровство, но и появляется опасность для образа жизни. В качестве главного примера участники обсуждения привели использование социальных сетей для того, чтобы повлиять на итоги голосования или вызвать раскол между жителями страны через целевые рекламные кампании в Twitter и на Facebook…

В подобной ситуации использование платформы Facebook для формирования мнений с помощью сотен поддельных аккаунтов и целевой рекламы — это такой вид атаки, для противодействия которой нужны новые средства защиты.

Подобные угрозы особенно опасны по той причине, что Facebook и интернет-сервисы работают по всему миру. Следовательно, таким компаниям, как Facebook, приходится тщательно контролировать 2 миллиарда пользовательских аккаунтов, 80% из которых зарегистрированы за пределами США…

Крис Инглис (Chris Inglis), управляющий директор Paladin Capital Group и бывший заместитель директора Агентства национальной безопасности, считает, что поворотным моментом, который привел к появлению нестандартных методов, способных навредить ситуации в США, стал взлом Sony хакерами из Северной Кореи…

Из этого следует, что компаниям нужно пересмотреть ресурсы, которые требуют защиты…

Даже в случае с традиционными угрозами, такими как вирусы-вымогатели, целью атак все чаще становятся не люди, а организации и даже правительства…

Чтобы справиться с новым ландшафтом угроз, который становится все более глобальным и использует новые виды атак, необходимо наладить взаимодействие между частными организациями и правительственными учреждениями как внутри, так и за пределами США, считает Эндрю МакКейб (Andrew McCabe), заместитель директора Федерального бюро расследований…» ***(Злоумышленники находят новые цели и способы атак // Threatpost (https://threatpost.ru/attackers-redefining-objectives-approaches/22670/).- 09.10.2017).***

***

«Сервисы для трансляции видео уязвимы к кибератакам из-за проблемы в технологии MPEG-DASH. Злоумышленник может с точностью в 95% отследить просматриваемый пользователем контент, даже если сервис использует HTTPS-шифрование.

Данный тип отслеживания возможен из-за уязвимости в технологии MPEG-DASH, приводящей к утечке информации. Исправить уязвимость весьма сложно, поскольку для этого пришлось бы перестраивать всю технологию с нуля.

В начале эры интернета, если пользователь хотел просмотреть трансляцию видео в Сети, на его компьютер загружался весь файл. Для того чтобы избежать потери пропускной способности, были изобретены различные методы улучшения online-трансляций видео. Одним из них является технология MPEG-DASH (Dynamic Adaptive Streaming over HTTP), разбивающая исходное видео, хранящееся на сервере, на более мелкие сегменты, содержащие по несколько секунд видео…

Как выяснили исследователи, каждый сегмент видео достаточно уникален для создания "цифрового отпечатка". Уязвимость заключается в том, что каждый сегмент кодируется с разным битрейтом. Когда пользователь загружает данные файлы, формируется шаблон загрузки пакетов доступный каждому, кто имеет возможность просматривать сетевой трафик пользователя.

По словам исследователей, "отпечаток" виден даже в том случае, если трафик зашифрован. Злоумышленнику нужно лишь создать базу данных "цифровых отпечатков" для интересующих его видео.

Для слежки в подобных масштабах злоумышленник должен иметь возможность перехвата и анализа трафика пользователя. Необходимые для этого мощности есть у интернет-провайдеров, правительственных организаций, модераторов трафика, а также у вредоносных программ в небольших локальных сетях.

В среднем уровень успешности такой атаки составляет более 95%. В ходе тестирования исследователям в 99,5% случаев удалось идентифицировать видео, просматриваемое пользователем на YouTube, в 98,6% случаев на Vimeo, в 98,5% - на Netflix и в 92,5% - на Amazon…» ***(Взломщик может отследить контент в сервисах для трансляции видео с точностью до 95% // Информационная безопасность (http://www.itsec.ru/newstext.php?news_id=119117).- 06.10.2017).***

***

«Новый механизм информационной безопасности, разработанный при участии Национального института стандартов и технологий (NIST),

исправляет одну из критических уязвимостей, существовавшую в Интернете на протяжении четверти века...

Набор стандартов, известных под названием «Безопасная междоменная маршрутизация» (Secure Inter-Domain Routing, SIDR), призван снизить вероятность кражи данных при передаче их в глобальной сети. Документ опубликовало сообщество разработчиков Инженерного совета Интернета (IETF), которому содействовали NIST и Управление науки и технологий Министерства внутренней безопасности США (DHS).

Представленная разработка направлена на исправление протокола граничного шлюза (Border Gateway Protocol, BGP). Именно он ответственен за передачу информации на глобальном уровне — в частности, между интернет-провайдерами. Маршрутизаторы, используя этот динамический протокол, решают, как отправить информацию по сотням тысяч адресов через десятки тысяч сетей. Таким образом обеспечивается быстрая передача данных между веб-адресами и конечными пользователями в глобальном масштабе…

Предложенные разработки используют криптографические методы для верификации используемых маршрутов. Первый – Resource Public Key Infrastructure (RPKI) – позволяет облачному сервису или провайдеру устанавливать ограничения в приеме данных от других автономных сетей. Второй — BGP Origin Validation — дает маршрутизаторам возможность исключить неавторизованные BGP-оповещения при передаче данных. Третий — BGP Path Validation — устанавливает цифровые подписи для каждого маршрутизатора в сети.

Специалисты NIST помогут выстроить взаимодействие с коммерческими провайдерами: они распространят необходимую техническую документацию и окажут содействие в практическом использовании методик…» ***(Egor Nashilov. NIST опубликовал новые стандарты SIDR и закрыл брешь в BGP // Threatpost (https://threatpost.ru/nist-updates-bgp-security/22644/).- 06.10.2017).***

***

«Компания Google запустила бесплатную программу Advanced Protection для пользователей Gmail, Google Диск, YouTube и других сервисов, которые подвергаются особенно высокому риску целенаправленных кибератак.

В настоящее время программа Advanced Protection состоит из трех основных элементов. Во-первых, это защита пользователей учетных записей Gmail и Google от фишинговых атак. От пользователя потребуется двухфакторная аутентификация через токен (компактное устройство, предназначенное для обеспечения информационной безопасности пользователя), созданный аппаратным ключом безопасности. Ключи безопасности — это небольшие USB или беспроводные устройства. Они используют криптографию и цифровые подписи с открытым ключом, чтобы доказать Google, что это настоящий пользователь аккаунта. Злоумышленник, у которого нет ключа безопасности, автоматически блокируется, даже если у него есть пароль. Людям, которые будут участвовать в программе, придется приобрести у Google два совместимых ключа безопасности, USB-ключ будет стоить $20, Bluetooth — $25.

Во-вторых, это блокировка вредоносных приложений, захватывающих конфиденциальные данные, автоматически ограничивая полный доступ к Gmail и Диску только для приложений Google. Браузер Google Chrome будет на 60 секунд задерживать получение вложений и других файлов для более тщательного сканирования. В-третьих, снижение риска доступа к учетной записи Gmail будет реализовано с помощью добавления дополнительных шагов в процессе восстановления учетной записи.

Регистрация в программе доступна для всех, у кого есть учетная запись Google. Тем не менее в настоящее время она требует использования браузера Chrome от Google, потому что он поддерживает стандарт двухэтапной аутентификации в браузере через токен…» ***(Google усиливает безопасность // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3442111).- 18.10.2017).***

***

«Исследователь безопасности Кен Манро (Ken Munro) из компании Pen Test Partners опубликовал отчет об проблемах безопасности, обнаруженных в ходе исследования оборудования, установленного на кораблях.

…специалисту удалось обнаружить множество некорректно настроенного корабельного оборудования по всему миру.

Среди уязвимых устройств были, например, спутниковые антенны, установленные на судах для обеспечения круглосуточной радиосвязи, интернет-подключения, GSM и других коммуникаций… Такие антенны установлены не только на гражданских судах, но и на кораблях военно-морского флота, а также на вертолетах и самолетах. …исследователь обнаружил, что беспроводные спутниковые антенны Globe и частные терминалы KVH CommBox также некорректно настроены и доступны для подключений через интернет. Оба устройства обрабатывали логины через незащищенное HTTP-соединение, однако инструмент CommBox на странице входа в систему отображал название судна и даже имел специальную кнопку, нажав на которую можно было увидеть список всех активных пользователей и получить доступ к именам всего экипажа судна. Более того, злоумышленник может получить подробные сведения о частной сети, просто наведя указатель мыши на определенные элементы на странице входа. По словам исследователя, в настоящее время не сообщалось об инцидентах, связанных со взломом корабельных систем спутниковой связи, однако это только вопрос времени… Как сообщил исследователь, существует немало способов атаковать системы корабля, но система спутниковой связи уязвима больше остальных, поскольку практически всегда подключена к интернету. Безопасность данных систем должна стать первоочередной задачей. В частности, необходимо изменить пароли по умолчанию, использовать сложные пароли для всех учетных записей и протокол TLS для защиты форм входа, а также в обязательном порядке обновлять прошивку устройств» ***(Корабельные системы спутниковой связи уязвимы к кибератакам // Internetua (http://internetua.com/korabelnie-sistemi-sputnikovoi-svyazi-uyazvimi-k-kiberatakam).- 17.10.2017).***

***

«…На X ежегодном саммите по кибербезопасности McAfee MPOWER, который пройдёт с 17 по 19 октября в США, Xerox продемонстрирует свой комплексный подход к защите сетевой печатной техники…

Многоуровневые системы безопасности Xerox делятся на четыре ключевых составляющих:• предотвращение вторжений,• проверка целостности прошивки,• защита документов и данных,• использование интегрированных решений партнёров, таких как McAfee…

29 марта 2017 года Xerox запустил 29 принтеров и МФУ на обновлённой платформе Xerox® ConnectKey®. Они обладают удобными функциями защищённого мобильного подключения, могут работать с облачными сервисами и поддерживают дополнительные приложения, которые превращают обычные печатные устройства в умных сетевых бизнес-ассистентов…» ***(Xerox совместно с McAfee представит новейшие технологии защиты устройств и данных // Сервис размещения пресс-релизов (http://pr.adcontext.net/17/10/19/262738).- 19.10.2017).***

***

«Дослідник з бельгійського університету KU Leuven Меті Ванхоф (Mathy Vanhoef) виявив серйозну вразливість в протоколі шифрування бездротових мереж WPA2…

Учений стверджує, що таким чином зловмисники можуть отримати доступ до даних, що передаються між призначеним для користувача пристроєм і Wi-Fi-роутером. Ця технологія зламу отримала назву «перевстановлення ключа шифрування» (key reinstallation attacks, KRACKs).

З її допомогою хакери можуть отримати інформацію, яка раніше вважалася зашифрованою й убезпеченою. Це зокрема номери кредитних карток, паролі, чат-повідомлення, електронні листи, фотографії тощо.

Окрім того, залежно від типу мережі зловмисник зможе вводити дані та маніпулювати ними.

Небезпека атаки KRACK в тому, що вона стосується всього стандарту шифрування WPA2, а не конкретних пристроїв або операційних систем. Адже WPA2 найбільш поширений стандарт шифрування бездротових мереж. В ході дослідження Меті Ванхофа було з'ясовано, що атаки можливі в операційних системах Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys тощо.

Найбільш уразливими до цієї атаки виявилися пристрої з Linux та Android (версія 6.0 і пізніші)...» ***(Дані можуть перехопити через будь-яку Wi-Fi мережу – вчений // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/dani_mozhut_perekhopiti_cherez_budyaku_wifi_merezhu_vcheniy/).- 17.10.2017).***

***

«Во вторник 17 октября Google объявила о выпуске стабильной версии Chrome под номером 62.0.3202.62. В обновлении исправили 35 проблем безопасности… Кроме того, теперь в Chrome изменился подход к отображению незащищенных HTTP-сайтов…

В очередной версии Google требует от сайтов, содержащих любые веб-формы, наличие SSL-сертификата. Ресурсы без него получают приписку «не защищено» в адресной строке…

Кроме того, аналогичная приписка появится у всех HTTP-сайтов, открытых в режиме инкогнито…

Конечная цель разработчиков компании — снабдить сообщением о небезопасности соединения все HTTP-сайты и побудить владельцев сайтов к переходу на защищенный протокол HTTPS» ***(Alexandra Golovina. Вышла новая 62-я версия Google Chrome // Threatpost (https://threatpost.ru/channel-update-for-chrome/22874/).- 19.10.2017).***

***

«На прошлой неделе Google объявила о старте программы вознаграждения за поиск уязвимостей в самых популярных приложениях сторонних разработчиков. Искать пробелы в надежности программ будут хакеры, работающие через платформу HackerOne. За найденные уязвимости они будут получать от $1 тыс…

Google составила список из самых популярных программ в Google Play: пока это Dropbox, Duolingo, Line, Snapchat, Tinder, Alibaba, Headspace и Mail.ru. При этом на изучение хакерам отданы только «критичные и основополагающие сервисы» российской компании. Среди них: «Почта», «Календарь», «Код доступа» и «Облако Mail.ru»… Хакеры должны будут искать в указанном ПО сторонних разработчиков серьезные уязвимости и сообщать о них не Google, а самим компаниям—создателям приложений. После чего хакеры и представители службы компьютерной безопасности разработчиков вместе будут искать способы устранения проблемы. Как только решение будет найдено, а автор мобильного приложения подтвердит факт устранения проблемы, хакер сможет обратиться в Google за получением вознаграждения…» ***(Google отдаст популярные приложения в руки хакерам // IKSMEDIA.RU (http://www.iksmedia.ru/news/5445948-Google-otdast-populyarnye-prilozhen.html#ixzz4wPcznTBg).- 23.10.2017).***

***

«Исследователь безопасности Скотт Хелме (Scott Helme) обнаружил, что плагин uBlock Origin (uBO), основной задачей которого является блокировка нежелательной рекламы, также блокирует инструмент CSP (Политика защиты контента, Content security policy), предотвращающий внедрение вредоносного JavaScript кода и XSS-атак… По словам исследователя, он заметил данную функцию плагина, когда увидел, что ни один отчет CSP на его сайте не был отправлен. Проблема заключается в том, что web-сайты не получают предупреждения от браузеров о попытках осуществления XSS-атак, если uBO установлен и активен. Таким образом разработчики и администраторы сайта могут не знать о попытках эксплуатации уязвимостей в коде, а ресурс может быть скомпрометирован. Как заявил разработчик плагина Реймонд Хилл (Raymond Hill), данная функция является предусмотренной и, если пользователю необходимо,

чтобы отчеты CSP все же отправлялись, он может вручную добавить нужный ему скрипт в список исключений плагина. Хелме выступил против данной функции в плагине. По его словам, uBO может блокировать Google Analytics, не мешая отправке отчетов CSP. Хилл в свою очередь возразил, что отчеты CSP являются потенциальной проблемой конфиденциальности, поскольку данные отправляются на удаленный сервер… Спор вызвал оживленную дискуссию среди исследователей безопасности. К настоящему времени компромисс так и не был достигнут, однако Хилл заявил, что изучит данную проблему и посмотрит, возможно ли блокировать только определенные отчеты CSP…» ***(Плагин uBlock Origin блокирует уведомления о кибератаках // "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=119243).- 18.10.2017).***

***

«Европол призвал сотовых операторов и интернет-провайдеров отказаться от использования решения CGNAT (Carrier-Grade NAT, механизм трансляции сетевых адресов), так как технология затрудняет полицейским задачу отслеживания киберпреступников в интернете… Данная технология широко используется провайдерами, которые не хотят или не могут обеспечить переход к адресации IPv6. Проблема заключается в том, что в условиях исчерпания пула IPv4-адресов слишком большое число пользователей делят между собой один IP-адрес, в итоге полицейские не могут эффективно идентифицировать и отслеживать преступников. Правоохранительные органы могут обратиться к операторам связи с требованием раскрыть личность пользователей, однако, если расследование находится на ранней стадии и всего на нескольких IP-адресах "сидят" сотни тысяч пользователей, сделать это довольно сложно…

На сегодняшний день рассматривается несколько вариантов решения данной проблемы, в их числе заключение добровольного соглашения с операторами связи и провайдерами о сокращении использования CGN и количества пользователей, делящих один IP-адрес, или введение нормативных требований, обязывающих операторов и провайдеров вести подробные журналы, содержащие информацию о номерах исходных портов» ***(Европол призвал операторов связи и интернет-провайдеров отказаться от CGNAT // "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=119253).- 18.10.2017).***

***

«Центр безопасности коммуникаций Канады (Communications Security Establishment Canada, CSEC), ответственный за внешнюю электронную разведку, выложил в открытый доступ собственный инструмент для обнаружения вредоносного программного обеспечения. Спецслужба описывает свою разработку под названием Assemblyline как платформу для анализа вредоносных файлов. …Assemblyline генерирует информацию о каждом файле и присваивает ему уникальный идентификатор, позволяет пользователям добавлять собственные аналитические инструменты, а также выдает оповещения об обнаружении вредоносных файлов… Assemblyline создана на основе открытого программного обеспечения, однако большая часть кода разработана специалистами

CSEC… Инструмент распространяется под лицензией MIT…» ***(Канадская разведка обнародовала инструмент для выявления вредоносов// "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=119304).- 20.10.2017).***

***

«В iOS 11 найдена ошибка, которая дает хакеру возможность получить доступ к фото на смартфоне пользователя…

Чтобы получить доступ к галерее фото на заблокированном устройстве, киберпреступнику необходимо узнать номер телефона и позвонить по нему. Затем, не дожидаясь ответа, создать новое сообщение, состоящее из любых 3 эмодзи. Затем необходимо дать голосовому помощнику Siri команду на открытие любого приложения. При повторном звонке на заблокированном устройстве появится возможность ответить посредством сообщения, к которому можно прикрепить любые фото из галереи пользователя.

Ошибку выявили создатели Youtube-канала iDevices. Они уже сообщили представителям Apple о найденной уязвимости» ***(Благодаря ошибке в iOS 11, хакер может получить доступ к фотографиям в смартфоне // SecureNews (https://securenews.ru/ios_11/).- 20.10.2017).***

***

«Google обезопасит пользователей, являющихся потенциальными целями для кибератак.

Google намерена добавить в Gmail функции, обеспечивающие дополнительные уровни защиты для пользователей, являющихся потенциальными целями хакеров (например, госслужащих и журналистов)…

Учетные записи всех участников программы усиленной защиты пользователей будут регулярно получать обновления в соответствии с возникающими угрозами. Изначально Google предложит три уровня защиты, в том числе блокировку мошеннических учетных записей и защиту от фишинга. Кроме того, будет усложнен процесс восстановления пароля, чтобы хакеры не смогли выдавать себя за настоящих владельцев учетных записей…» ***(В Gmail появится дополнительная защита для госслужащих и журналистов // SecurityLab.ru (http://www.securitylab.ru/news/489152.php).- 17.10.2017).***

***

«Компанія Sirin Labs вирішила здійснити революцію блокчейн-пристроїв…

Першим революційним пристроєм… стане блокчейн-смартфон. Після цього слід очікувати на появу захищеного персонального комп'ютера.

…смартфон і комп'ютер буде працювати в автономній блокчейн-мережі, створеної на технології Tangle від IOTA. Для нового смартфона розробили операційну систему Shield OS. Особливість операційної системи є криптографічне ядро, що підтримує безліч криптовалютних гаманців, сервісів безпечних транзакцій, а також обмін між пристроями в мережі P2P. Вбудований гаманець буде мати три ступеня аутенфікації і безпечний обмін ресурсами між пристроями…

…вартість блокчейн пристрою складе $999...» ***(Нова реальність від Кенеса Ракишева // Gazeta.ua (https://gazeta.ua/articles/promotion/_nova-realnist-vid-kenesa-rakisheva/800674).- 29.10.2017).***

***

Національна система кібербезпеки

«Команда быстрого реагирования на компьютерные чрезвычайные события Украины (CERT-UA), которая функционирует в рамках Государственной службы специальной связи и защиты информации, предупреждает об угрозе схожей с вирусом Petya.A… в период с 13 по 17 октября.

Существует вероятность, что отдельные признаки кибератаки могут совпадать с соответствующими признаками вредного воздействия компьютерного вируса Petya.A, который атаковал информационные ресурсы ряда стран… Специалисты CERT-UA рекомендуют соблюдать требования кибербезопасности и следовать инструкциям по защите компьютерных систем от вируса Petya Ransomware, размещённым на сайте CERT-UA…» ***(Возможны новые кибератаки, - ГССС // Новости Украины. ЧАС.UA (http://timeua.com/news/2/57553.html).- 13.10.2017).***

***

«Національний Депозитарій розпочав модернізацію матеріально-технічної бази. Резервний Центр Обробки Даних (ЦОД) підвищить рівень захисту інформації та забезпечить безперебійну роботу центрального депозитарію при виникненні кібератак…

Модернізація ЦОД НДУ допоможе збільшити потужність існуючого ЦОД та підвищить швидкість роботи депозитарної системи. Повне резервування обладнання забезпечить мінімізацію ризику втрати даних центрального депозитарію та його клієнтів. У разі виходу з ладу частини апаратного забезпечення або при замаху на інформаційну безпеку центрального депозитарію країни, ядро інфраструктури продовжить роботу…

Загалом обсяг інвестицій, вкладених в модернізацію апаратної частини системи обробки інформації (СОІ), склав 11 млн грн.

…Оновлений резервний центр обробки даних планується запустити до кінця 2017 року…» ***(Яна Козиряцька. Національний Депозитарій підвищить рівень захисту інформації, щоб захиститись від кібератак // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1693648-natsionalnyi-depozytarii-pidvyshchyt-riven-zakhystu-informatsii-shchob-zakhystytys-vid-kiberatak).- 18.10.2017).***

***

«Вопросы киберстрахования были затронуты на состоявшемся 19 октября заседании Комитета по электронным коммуникациям при ТПП Украины.

..это касается «подготовки базовых требований к аппаратному и программному обеспечению, рекомендаций по внутренним правилам работы, подтверждению и фиксации кибератак, определению размера ущерба и проведению аудита информационных систем…» ***(В ТПП Украины обсуждался вопрос кибербезопасности и страхования киберрисков // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/v-tpp-ukrainyi-obsuzhdalsya-vopros-kiberbezopasnosti-i-strahovaniya-kiberriskov).- 25.10.2017).***

***

«У Секретаріаті Національної асоціації адвокатів України відбулася чергова робоча зустріч з розробниками програмного забезпечення Єдиного реєстру адвокатів України…

У ході зустрічі з фахівцями з програмування та інформаційного захисту були обговорені теми вдосконалення профайлу адвоката в ЄРАУ за рахунок нових візуальних можливостей та розширення текстових даних про адвоката у відкритій частині реєстру.

Також обговорювалося подальше посилення захисту даних реєстру в зв'язку із зростанням ризиків кібератак на інформаційні ресурси України...» ***(Єдиний реєстр адвокатів України хочуть убезпечити від хакерських атак // Інформаційно-правовий портал «Українське право» (http://ukrainepravo.com/news/ukraine/diniy-re-str-advokativ-ukraini-khochut-ubezpechiti-vid-khakerskikh-atak-/).- 27.10.2017).***

***

«…Розвиток національних комп'ютерних мереж і баз даних крім зрозумілих переваг, на жаль, має і зворотний бік. Вірусні атаки вже встигли стати звичним явищем в Україні, вони трапляються частіше, їхні наслідки дедалі серйозніші. Активність ворожої сторони та звичайних комп'ютерних шахраїв вимагає від української влади невідкладного розвитку національних засобів кібербезпеки.

Частиною цих зусиль є нещодавнє ухвалення Верховною Радою проекту Закону «Про основні засади забезпечення кібербезпеки України». …закон містить багато декларативних речей, які поки що в сучасних умовах країни буде складно реалізувати. Зокрема, розгортання національної системи кібербезпеки, адекватної характеру й масштабам реальних і потенційних загроз, а також застосування новітніх технологій і передового досвіду для поліпшення стану кіберзахисту об'єктів критичної інформаційної інфраструктури. Це потребує наявності достатніх ресурсів і, що більш важливо, достатньої експертизи в такому питанні…

Так, на думку директора із зовнішніх зв'язків асоціації RIPE NCC (регіон Східна Європа та Центральна Азія) Олексієм Семенякою, із зайвим контролем завжди є ризик створити аналог сумнозвісного російського «Роскомнадзора». Втім, державне регулювання мережі інтернет і суміжних сфер є необхідним, коли це

стосується процесів, які впливають на життя або здоров'я громадян, коли йдеться про керування обмеженим ресурсом або там, де можлива монополізація ринку… Проте, за словами Семеняки, у державного регулювання є низка проблем і поза наступом на свободу громадян заради національної безпеки. Так, експерт вважає, що регулювання завжди запізнюється, бо є реакцією керівних органів на події, фактично йдеться про відповіді на загрози, які вже відбулися… Іншою проблемою є сама природа державних органів. Що складніша система, то більше накопичується помилок між її рівнями. Інколи це призводить навіть до протилежного трактування чиновниками встановлених норм чи правил. Ускладнюють процес розвитку національної інформаційної системи й спроби сліпого копіювання чужого досвіду…

Тому в деяких країнах регулювання кіберсфери віддано недержавним організаціям, які представляють інтереси галузі. Таким шляхом пішли, наприклад, у Великій Британії, створивши Internet Watch Foundation — недержавну організацію операторів зв'язку. Саме вона виконує всю нормативну та регуляторну роботу, фактично шукає компроміс та консенсус між бізнесом і державними інтересами. IWF моніторить сайти й за потреби надає пропозиції щодо призупинення (для національних ресурсів) або блокування доступу (для іноземних). Крім того, організація приймає скарги на неприпустимий контент від поліції та звичайних громадян через спеціальну гарячу лінію. Хоча такі рекомендації не є обов'язковими й остаточне рішення залишається за операторами, більшість провайдерів беззаперечно виконує вказівки IWF. Для держави таке делегування повноважень теж вигідне, адже звільняє від додаткового навантаження відповідні органи національної безпеки, які можуть зосередитися виключно на своїх питаннях.

Таку саму думку має і Кауто Хуопіо, головний спеціаліст Фінського органу регулювання комунікацій (FICORA) та Національного центру кібербезпеки Фінляндії (NCSC-FI). Він зазначив, що створення сучасної системи кібербезпеки вимагає не лише активної роботи державних органів, а й залучення всіх суб'єктів галузі, особливо представників критичної інфраструктури… Крім того, експерт наголосив на важливості створення спеціальних груп для кожної окремої галузі промисловості, щоб оперативно обмінюватися специфічною інформацією щодо кіберінцидентів і знаходити способи їх подолати. Приклад Фінляндії показує, що в таких групах бажано мати представників державних органів, але виключно для початку комунікації між членами групи…

Щодо кібербезпеки, то до головних функцій Національного центру кібербезпеки належить інформування про можливі загрози. До того ж, як підкреслив Хуопіо, Центр не витрачає сили на кожну вірусну атаку, вони займаються лише більш-менш серйозними випадками, що оптимізує навантаження на експертів. Водночас, на його думку, дуже важливим є надання простої зрозумілої інформації для громадян, як-от проведення занять із населенням, спеціальних промо-кампаній, запуск відповідних веб-ресурсів. Це призводить до того, що у Фінляндії дуже великий відсоток населення обізнаний про необхідність встановлення й оновлення антивірусів, постійно перевіряється вся персональна

техніка — від комп'ютерів до смартфонів. Це робить країну загалом менш вразливою до масштабних комп'ютерних атак, що показали останні події…

На думку експерта, саме такий підхід може стати дуже ефективним для України в умовах обмеженого ресурсу... Адже більшість вірусних атак проти України показали, що зловмисники скористалися браком належного оновлення систем безпеки в мережах. До того ж, за словами експерта, такі заходи не потребують складного й дорогого обладнання, потрібні лише відповідні знання. Це допоможе залучити до загальної справи спільноту українських спеціалістів із кібербезпеки, які могли б надати власні рекомендації щодо пріоритетних заходів…» ***(Юрій Лапаєв. Подвійна істина кіберзахисту // Тиждень.ua (http://tyzhden.ua/Society/202550).- 27.10.2017).***

***

Світові тенденції в галузі кібербезпеки

«…В свежем докладе Международного валютного фонда (МВФ), посвященном финансовой стабильности, отмечается рост последствий и изощренности кибератак на финансовые институты, а также приводятся пугающие оценки, ну, например, экономический ущерб от потенциальной глобальной кибератаки может составить 53 млрд долларов. …только атака вируса NotPetya в июне этого года обошлась миру примерно в 850 млн долларов...

…На вопрос о масштабах киберпреступности пытается ответить недавний доклад — Европола. Эксперты организации отмечают: так называемые вирусы-вымогатели — WannaCry, Petya и NotPetya — сегодня затмили все прочие угрозы… По данным Европола, всего "эпидемия" затронула порядка 300 тысяч "жертв" более чем в 150 странах…

Эпидемия выявила проблему с огромным количеством устаревшего оборудования и программного обеспечения… К тому же налицо халатность со стороны системных администраторов различных компаний и госучреждений. О возможности атаки было известно за два месяца до ее начала, и никто не принял никаких мер… Только сейчас в ЕС собираются повышать штрафы за слабые меры киберзащиты.

Что еще беспокоит Европол? Это, к примеру, утечки данных: только за последние 12 месяцев были зафиксированы утечки, которые привели к раскрытию более 2 млрд учетных записей! Под ударом с некоторых пор и интернет вещей: в конце 2016-го зафиксирована первая массивная атака, проведенная с применением умных гаджетов и запущенная вредоносной программой Mirai. Тогда 150 тысяч взломанных роутеров и камер CCTV объединились в так называемый ботнет, или сеть, зараженную вредоносной программой…

Сила DDoS-атак за последний год многократно возросла. И защищаться от них становится все сложнее.

Цель таких атак …в банальной экономике: час простоя обходится фирме в миллионы долларов, что может использоваться в конкурентной борьбе, для

шантажа, да что там, даже в геополитическом противостоянии. В докладе Европола подтверждают: кибератаки зачастую проводят под конкретные события, например, бьют по флористам в преддверии Дня святого Валентина или по онлайн-букмекерам перед масштабными спортивными событиями. Еще вариант: преступники проводят слабую атаку и требуют выкуп, угрожая, что в следующий раз она будет мощнее, однако это оказывается блефом. Такие атаки "на удачу" стали особенно популярны, все дело в доступности DDoS-инструментария…

Чем жертвы расплачиваются с преступниками? Цифровой криминал подсел на криптовалюты: например, выкуп часто требуют в биткойнах, но и Monero, и Ethereum, и Zcash у киберкриминала тоже в чести. К тому же криптовалюта имеет хождение в даркнете, там, где на анонимных виртуальных рынках преступники закупают различные вредоносные программы…

…самое важное сейчас — разрушить романтический образ киберпреступников. Их основная масса — самый обыкновенный криминал, сросшийся с наркоторговлей, отмыванием денег и терроризмом. Различия между ними только в одном — одни с пистолетом, а другие — с клавиатурой» ***(Кирилл Журенков. Страшнее пистолета // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3428093).- 23.10.2017).***

***

«Американский разработчик ПО в области кибербезопасности Safe`n Sec Corporation подал в окружной суд Калифорнии иск к Сбербанку» а также компаниям Sberbank CIB, «СНС Холдинг» и «СНС Софт»… Компания обвиняет банк в незаконном использовании ее ПО, из-за которого она лишилась «миллионы долларов» выручки. Объем претензий компании превышает 450 тыс. долл.

Пресс-служба Сбербанка назвала иск незаконным и необоснованным. В банке заявили, что не использовали и не используют решения Safe`n Sec…» ***(Американский разработчик систем для защиты банкоматов подал в суд на Сбербанк // «Открытые системы» (https://www.computerworld.ru/news/Amerikanskiy-razrabotchik-sistem-dlya-zaschity-bankomatov-podal-v-sud-na-Sberbank).- 05.10.2017).***

***

«Компания Fortinet провела исследование, согласно которому 48% ИТ-руководителей полагают, что руководящий состав организаций не уделяет надлежащего внимания обеспечению информационной безопасности… По мнению 77% респондентов, ИТ-безопасность должна стать предметом пристального внимания руководящего состава.

Переходу информационной безопасности в разряд приоритетных направлений могут способствовать три ключевых фактора… Во-первых, это рост количества международных кибератак. За последние два года 85% организаций столкнулись с нарушениями безопасности. 49% ИТ-руководителей заявили, что международные кибератаки, например WannaCry, привлекли внимание руководящего состава… Во-вторых, увеличение давления со стороны

регулирующих структур. 34% респондентов заявили о росте количества нормативных требований. Например, в скором времени на территории Евросоюза вступят в силу «Общий регламент защиты данных», предусматривающие существенные штрафы. В-третьих, для многих организаций переход к облаку является частью процесса цифровой трансформации. Половина опрошенных респондентов (50%) в течение ближайших 12 месяцев планируют инвестировать средства в обеспечение облачной безопасности.

В исследовании принял участие 1801 респондент из 16 стран» ***(Fortinet: топ-менеджеры не уделяют должного внимания обеспечению информационной безопасности // «Открытые системы» (https://www.computerworld.ru/news/Fortinet-rukovodyaschiy-sostav-organizatsiy-ne-udelyaet-dolzhnogo-vnimaniya-obespecheniyu-informatsionnoy-bezopasnosti).- 19.10.2017).***

***

«В течение почти целого десятилетия компания Cisco публикует подробные отчеты о кибербезопасности…

…Наши эксперты в области безопасности… определили две тенденции, которые …препятствуют дальнейшему прогрессу и ведут нас в новую эру киберрисков и угроз.

…Получение дохода по-прежнему является главной целью большинства злоумышленников… Как сказано во введении к отчету Cisco по информационной безопасности за первое полугодие 2017 г. …такая вредоносная активность может предвещать появление нового и разрушительного типа атак …«прерывание обслуживания» (Destruction of service, DeOS). В течение прошлого года мы также фиксировали использование IoT-устройств при атаках DDoS. Недавняя активность IoT-ботнета дает основания предполагать, что некоторые злоумышленники уже готовят почву для широкомасштабной и высокоэффективной атаки, которая потенциально может уничтожить весь Интернет.

…Широта и глубина последних атак с целью вымогательства демонстрируют, как виртуозно злоумышленники используют бреши в безопасности и уязвимости на всех устройствах и сетях для максимального воздействия. Ограниченный мониторинг в динамических ИТ-средах, риски, представленные «теневыми ИТ-ресурсами», постоянный шквал уведомлений о безопасности и сложность среды обеспечения безопасности ИТ-инфраструктуры — вот лишь некоторые проблемы, с которыми сталкиваются группы обеспечения безопасности с ограниченными ресурсами при управлении современными изощренными и все более мощными киберугрозами» ***(Новый отчет Cisco по ИБ: атаки все искуснее, последствия все хуже // ChannelForIT (http://channel4it.com/publications/Novyy-otchet-Cisco-po-IB-ataki-vse-iskusnee-posledstviya-vse-huzhe-28039.html).- 17.10.2017).***

***

«Компания Hewlett Packard Enterprise позволила Минобороны России ознакомиться с программным обеспечением, которое использует Пентагон для защиты своих компьютерных сетей…

Систему ВПО под названием ArcSight используют для кибербезопасности большинство военных ведомств США. Она предупреждает аналитиков, когда обнаруживает, что компьютерные системы могут быть атакованы…

…Россия получила доступ к исходному коду, охраняемому внутренними инструкциями в отношении программного обеспечения, во время сертификации системы для продажи продукта российскому госсектору.

…изучение исходных кодов может помочь Москве выявить слабые стороны программного обеспечения. Это может помочь злоумышленникам сделать американских военных уязвимыми к кибератакам» ***(HP позволила России ознакомиться с системой кибербезопасности Пентагона, - Reuters // Espreso.tv (https://ru.espreso.tv/news/2017/10/02/nr_pozvolyla_rossyy_oznakomytsya_s_systemoy_kyberbezopasnosty_pentagona_reuters).- 02.10.2017).***

***

«В США создана антихакерская группа, включающая хакеров, ученых и американских губернаторов, главной целью которой будет предотвращение кибератак на электронные системы регистрации избирателей…

Антихакерская коалиция включает в себя организаторов прошедшей в текущем году в Лас-Вегасе хакерской конференции DEF CON, Национальной ассоциации губернаторов и Центра интернет-безопасности…

Проект будет анонсирован после того, как организаторы DEF CON опубликуют отчет об обнаруженных в июле уязвимостях в машинах для голосования и связанных с ними технологиях…

В качестве одной из возможных мер по противодействию кибератакам организаторы конференции DEF CON порекомендовали уменьшить долю аппаратного и программного обеспечения иностранного производства, используемого в машинах для подсчета голосов» ***(Хакеры и правительство США объединились для защиты выборов от кибератак // SecurityLab.ru (http://www.securitylab.ru/news/488980.php).- 10.10.2017).***

***

«Президент США Дональд Трамп має намір висунути на посаду міністра внутрішньої безпеки США Кірстієн Нільсен, яку вважають експертом у питаннях кібербезпеки…

Нільсен раніше була одним з головних помічників Джона Келлі, коли він ще очолював Міністерство внутрішньої безпеки, а після його призначення главою апарату перебралася в офіс в Білому домі. Вона вважається експертом з питань кібербезпеки…

Перед цим Нільсен працювала в експертному центрі з питань кібербезпеки університету Джорджа Вашингтона… Крім того, вона є експертом в питаннях

політики і стратегії внутрішньої і національної безпеки, а також у сфері захисту критично важливої інфраструктури…» ***(Трамп хоче призначити міністром експерта Білого дому з кібербезпеки // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/tramp-hoche-priznachiti-ministrom-eksperta-bilogo-domu-z-kiberbezpeki-256764_.html).- 12.10.2017).***

***

«…Эксперты по кибербезопасности считают, что Apple предоставила Uber разрешение скрыто следить за владельцами iPhone…

По их словам, мобильное приложение Uber имело доступ к закрытым личным данням пользователей iPhone…

Программа могла отслеживать владельцев "яблочных" смартфонов даже после удаления приложения Uber или сброса настроек iPhone к заводским установкам» ***(Компания Uber может шпионить за пользователями iPhone // AOinform(http://www.aoinform.com/news/kompanija_uber_mozhet_shpionit_za_polzovateljami_iphone/2017-10-09-20090).- 09.10.2017).***

***

«Співробітники ізраїльської розвідки, що стежать за російськими хакерами, виявили, що вони використовують антивірусне програмне забезпечення "Лабораторії Касперського", яке також використовується 400 мільйонами людей у всьому світі, в тому числі державними агентствами США…

Це призвело до прийняття у Вашингтоні в минулому місяці рішення про те, щоб програма Kaspersky була видалена з урядових комп'ютерів.

…ізраїльські шпигуни також виявили в мережевих атаках інструменти Kaspersky, які могли б отримати тільки від Агентства національної безпеки США.

Після розслідування, NSA виявив, що ці інструменти знаходяться в російському уряді…

В кінці минулого місяця Національна рада розвідки США завершила секретний звіт, який він розділяє з союзниками по НАТО, в якому говориться, що розвідувальна служба ФСБ Росії мала "ймовірний доступ" до баз даних і вихідних кодів Касперського…

Цей доступ може допомогти активувати кібератаки проти урядових, комерційних і промислових мереж США…

Поки що не відомо, які інші секрети США можуть виявити російські хакери, перетворивши програмне забезпечення Касперського в свого роду пошук Google для отримання конфіденційної інформації…» ***(Альона Мазуренко. США дізналися про хакерські атаки РФ від ізраїльських розвідників // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1692377-ssha-diznalysia-pro-khakerski-ataky-rf-vid-izrailskykh-rozvidnykiv).- 11.10.2017).***

***

«Скандал вокруг «Лаборатории Касперского» в США получил продолжение: сразу два американских издания — The Washington Post и The Wall

Street Journal — сообщили, что российские хакеры использовали антивирус для кражи секретных данных.

По данным СМИ, кибершпионы, связанные с правительством России, проникли в компьютер одного из сотрудников Агентства национальной безопасности США: в нем содержалась информация о том, как АНБ защищает собственные компьютерные сети и проникает в сети других государств. Инцидент якобы произошел в 2015-м году, но Штатам стало о нем известно лишь весной этого года...

..Руководитель агентства кибербезопасности Евгений Лифшиц уверен, что антивирусные программы могут использоваться для получения практически любой информации…

Информация о краже данных АНБ при помощи российского антивируса может привести к репутационным потерям, отметил вице-президент компании «Лаборатория Касперского» Антон Шингарев:

«„Лаборатория Касперского“ не получила никаких свидетельств, подтверждающих связь компании с инцидентом, описанным в этих статьях. Мы считаем крайне прискорбной ситуацию, при которой в результате недоказанных и недоказуемых утверждений в СМИ мы снова сталкиваемся с беспочвенными обвинениями в свой адрес. Мы являемся частной компанией и не имеем политических связей ни с одним государством в мире, включая Россию… Безусловно, меня расстраивает возможный репутационный ущерб. Со всеми, у кого есть вопросы по поводу ведения нашего бизнеса, мы стараемся быть максимально открытыми, готовы сотрудничать вплоть до предоставления исходного кода, потому что абсолютно уверены в нашей правоте. Это часть геополитического конфликта»…» ***(Альбина Хазеева. Антивирусная атака // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3432995).- 06.10.2017).***

***

«По словам бывших сотрудников Агентства национальной безопасности США, у американской шпионской службы есть серьезная проблема – ее секреты очень легко украсть. К примеру, на прошлой неделе ряд зарубежных СМИ сообщили о взломе Tailored Access Operations (TAO) – элитного хакерского подразделения АНБ. За последние пять лет это уже четвертая масштабная утечка данных агентства.

…TAO представляет собой всю хакерскую мощь АНБ. У подразделения есть доступ к самой секретной информации из закрытых сетей противника, а его сотрудники разрабатывают и используют сложные эксплоиты для уязвимостей в маршрутизаторах, операционных системах и т.д., которые могут спровоцировать настоящий хаос, если окажутся не в тех руках.

Однако вышеупомянутые инструменты отнюдь не хранятся под замком. «В TAO данные весьма свободно перемещались между разными сетями», - сообщил один из источников, работавший в подразделении после похищения данных Эдвардом Сноуденом в 2013 году…

«Большинство операторов знали, как при желании из засекреченных сетей и интернета можно получить все, что нужно, даже без USB», - отметил источник.

По словам второго собеседника, также некогда работавшего в ТАО, главная мера безопасности заключалась в том, что сотрудники все время проверяли наличие у коллег бейджика…» ***(АНБ США испытывает серьезные трудности с безопасностью даннях // SecurityLab.ru (http://www.securitylab.ru/news/489062.php).- 12.10.2017).***

***

«В США проводится масштабная модернизация оборудования на избирательных участках в разных штатах…

Отмечается, что меры по повышению безопасности и надежности избирательных систем предпринимаются на фоне предполагаемых попыток хакеров, связанных с Россией, вмешаться в ход голосования на предыдущих выборах президента США.

В некоторых штатах избирательные комиссии нанимают специалистов по кибербезопасности…

Эксперты многие годы предупреждали о недостаточной безопасности системы голосования как на федеральном, так и на уровнях штатов, однако избирательные комиссии из-за недостатка средств зачастую отказывались от модернизации оборудования.

Как известно, следующая крупная избирательная кампания — промежуточные выборы в Конгресс — пройдет в США ноябре 2018 года…» ***(Для защиты от хакеров Кремля: В США проводят масштабную модернизацию избирательных участков // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/197374-dlja_zashchity_ot_hakerov_kremlja_v_ssha_provodjat_masshtabnuju_modernizatsiju_izbirateljnyh_uchastk).- 15.10.2017).***

***

«Соцмережа Twitter видалила повідомлення та дані користувачів, які потенційно могли б бути важливими для слідчих у справі маніпуляцій соціальних платформ під час виборів 2016 року у США..

Росія створювала армії ботів, фейкових користувачів, скандальні хештеги та фальшиві рекламні кампанії для створення історій на підтримку Трампа та проти Клінтон.

Однак велику частину цієї аналітичної інформації було втрачено назавжди, вважають аналітики кібербезпеки.

Причина цього – стандарт захисту споживачів. Згідно з ним, якщо споживач видаляє повідомлення чи платну рекламну кампанію, тоді і Twitter та приватні компанії, які користуються соцмережею для маркетингу на платній основі, повинні видалити у себе ці самі дані…

Наразі інженери намагаються з’ясувати, яка інформація доступна і яку можна поновити, намагаючись знайти способи відновлення пакетів даних, які було повністю видалено…» ***(Twitter видалив дані, важливі для розслідування дій Росії під час президентських виборів у США // Espreso.tv***

(https://espreso.tv/news/2017/10/13/twitter_vydalyv_dani_vazhlyvi_dlya_rozsliduvannya_diy_rosiyi_pid_chas_prezydentskykh_vyboriv_u_ssha).- 13.10.2017).

***

«Бывший координатор по вопросам киберпространства Госдепартамента США Крис Пэйнтер считает, что государствам необходимо принимать более оперативные и эффективные меры в отношении государств, занимающихся кибератаками…

В 2014 году, когда Пэйнтер еще работал в Госдепартаменте, были взломаны компьютерные системы компании Sony Pictures. После расследования ФБР объявило, что за взлом отвечает Северная Корея, и президент Обама подписал указ о новых экономических санкциях против связанных с ней людей и организаций. Однако санкций, считает Пэйнтер, недостаточно. Возможно, требуются как дипломатические и экономические средства сдерживания, так и ответные действия в киберпространстве, полагает он. При этом власти должны действовать без задержки, не дожидаясь появления абсолютно бесспорных доказательств причастности другого государства…» ***(Эксперт госдепартамента: ответ на кибератаки, организуемые государствами, должен быть жестче // «Открытые системы» (https://www.computerworld.ru/news/Expert-gosdepartamenta-otvet-na-kiberataki-organizuemye-gosudarstvami-dolzhen-byt-zhestche).- 16.10.2017).***

***

«…Помощник министра обороны США по вопросам внутренней и глобальной безопасности Кеннет Рапуано (Kenneth Rapuano) заявил, что США усиленно следит за деятельностью некоторых государств в киберпространстве, в частности, речь идет о Китае, Иране, КНДР и особенно России…

Как сообщил помощник министра, главной задачей Киберкомандования США, насчитывающего более 6 тыс. сотрудников, является обеспечение защиты компьютерных сетей Министерства обороны США от киберугроз. В случае необходимости Пентагон готов направить все имеющиеся у него ресурсы на отражение кибератаки…» ***(Пентагон выразил обеспокоенность деятельностью РФ в киберпространстве // SecurityLab.ru (http://www.securitylab.ru/news/489245.php).- 20.10.2017).***

***

«…Министерство внутренней безопасности США опубликовало обязательную к выполнению директиву, в соответствии с которой все федеральные агентства должны начать использовать технологии HTTPS, DMARC и STARTTLS в течение следующих нескольких месяцев для защиты государственных web-сайтов и электронной почты.

В течение следующих 30 дней учреждениям предписано разработать план действий по выполнению требований Директивы 18-01 (Binding Operational Directive (BOD) 18-01).

Агентствам также предоставляется 90 дней на подготовку всех серверов электронной почты, для использования STARTTLS - протокола, позволяющего пользователям создать зашифрованное соединение (TLS или SSL) прямо поверх обычного TCP-соединения.

Министерство также требует постепенного внедрения DMARC (Domain-based Message Authentication, Reporting and Conformance) - протокола проверки подлинности электронной почты и отчетности, предназначенного для обнаружения и устранения фишинговой почты и спама…

По распоряжению министерства, все принадлежащие агентствам домены второго уровня должны использовать расширение SPF (Инфраструктура политики отправителя, Sender Policy Framework) и метод аутентификации электронной почты DKIM (DomainKeys Identified Mail), позволяющие организациям указывать серверы, которые могут отправлять электронные письма, используя их домен.

Согласно требованию ведомства, федеральные агентства должны отключить протоколы SSLv2 и SSLv3, а также алгоритмы 3DES и RC4. На выполнение этой задачи госструктурам предоставлено 120 дней. Вышеуказанные протоколы и алгоритмы также должны быть отключены на всех web-серверах, а все публичные web-сайты должны использовать HTTPS-соединение и механизм HTTP Strict Transport Security (HSTS)…» ***(МВБ США обязало федеральные агентства использовать DMARC и HTTPS // SecurityLab.ru (http://www.securitylab.ru/news/489158.php).- 19.10.2017).***

***

«Сенатор Джон Маккейн предложил рассмотреть вопрос о направлении повестки координатору Белого дома по кибербезопасности Робу Джойсу – с тем, чтобы наиболее высокопоставленный сотрудник администрации в данной области дал показания влиятельному сенатскому Комитету по делам вооруженных сил…

Роб Джойс не явился в Комитет по делам вооруженных сил для участия в слушаниях, посвященных киберугрозам, с которыми сталкиваются в США…

Белый дом отказался разрешить Робу Джойсу, входящему в состав Совета по национальной безопасности, выступить на слушаниях, сославшись на привилегию исполнительной власти, которая дает представителям исполнительной власти не разглашать некоторую конфиденциальную информацию…

Маккейн, оставивший пустой стул за столом свидетелей, чтобы подчеркнуть отсутствие Джойса, назвал отказ Белого дома допустить Джойса на слушания проявлением «фундаментального расхождения между авторитетом и подотчетностью, которая наблюдается сегодня в нашем правительстве, когда речь идет и кибербезопасности».

На слушании выступили несколько других высокопоставленных чиновников в сфере кибербезопасности, в том числе замдиректора отдела кибербезопасности ФБР Скотт Смит, заместитель министра обороны по внутренней обороне и глобальной безопасности Кеннет Рапуано и и.о. замминистра по внутренней безопасности Кристофер Кребс.

По словам Рапуано, общие усилия соответствующих ведомств позволили властям получить более полное представление о новых киберугрозах для страны, хотя признал, что «мы по-прежнему сталкиваемся со сложностями, когда речь идет о реагировании на киберинциденты в крупном масштабе»…

Смит, в свою очередь, заявил, что, хотя у ведомства множество ресурсов, нацеленных конкретно на борьбу с киберпреступностью, есть и некоторые другие подразделения, «которые ФБР может задействовать в случае киберинцидента»...» ***(Маккейн отправит повестку координатору Белого дома по кибербезопасности // Инфомационное агентство «IP News» (https://www.ipnews.in.ua/news/world/138861-makkejn-otpravit-povestku-koordinatoru-belogo-doma-po-kiberbezopasnosti).- 20.10.2017).***

***

«Ежедневная американская газета The New York Times… решила провести эксперимент в области безопасных коммуникаций и сделать свою страничку nytimes.com доступной для сервиса Tor Onion…

Команда NYT, стремясь обеспечить доступ к своим материалам, решила изучить пути улучшения доступа для своих читателей, предпочитающих использовать Tor. Одним из таких способов стало создание собственной странички в этой анонимной сети — https://www.nytimes3xbfgragh.onion/.

Этот «луковый» адрес доступен только через сеть Tor, а также специальное программное обеспечение — такое, как Tor Browser. Такие инструменты гарантируют читателям NYT свободный доступ, без страха за блокировки и правительственный мониторинг…» ***(The New York Times запускает свой сайт в анонимной сети Tor // РосКомСвобода (https://rublacklist.net/33111/).- 27.102017).***

***

Країни ЄС

«…В конце прошлой недели Комитет Европейского парламента по гражданским свободам, правосудию и внутренним делам проголосовал за Положение о конфиденциальности e-Privacy. Данное Положение — «эволюционировавшая» в более строгий для исполнения документ одноимённая Директива…

…если ранее в e-Privacy Directive был заложен запрет для проводных и телефонных операторов связи на выполнение каких-либо действий вмешательства (прослушивание, запись, хранение, мониторинг и пр.) при телефонных разговорах или пересылках sms без согласия пользователей, то теперь это требование должно распространиться и на связь с помощью интернет-соединений.

Кроме этого, в обновлённом документе зафиксировано требование, чтобы по умолчанию все функции возможного «вмешательства» были отключены и могли быть включены только по явному согласию со стороны пользователя. Комитетом также были одобрены положения, защищающие использование шифрования и

требующие корпоративной подотчётности от компаний в виде периодических публикаций…

E-Privacy призвано облегчить пользователям предоставление и снятие согласия, позволяя выполнять его согласно настройкам браузера вместо всплывающих окон cookie…

«Несмотря на огромные усилия лоббистов, Комитет проголосовал за чёткие правила по защите конфиденциальности, — комментирует принятие документа исполнительный директор European Digital Rights (EDRi) Джон МакНэйми. — Мы приветствуем такой подход, поскольку он не только защитит граждан, но и поспособствует конкуренции и инновациям».

В настоящее время люди, занимающиеся сёрфингом Сети, используют приложения на своём мобильном, или подключенные устройства, которые отслеживаются и профилируются. Огромные объёмы данных, генерируемых этими устройствами, создают риски для конфиденциальности, безопасности, а также демократии как таковой.

EDRi считает, что четкие правила, основанные на согласии и прозрачности, помогут уйти от дисфункционального рынка, который подрывает доверие и безопасность…» ***(Европа в шаге от принятия «Правила e-Privacy» по защите данных пользователей // РосКомСвобода (https://rublacklist.net/32955/).- 23.10.2017).***

***

«В среду, 18 октября, в рамках антитеррористического пакета Европейская комиссия предложила странам-участницам Евросоюза помогать друг другу во взломе зашифрованных устройств…

…в случае необходимости страны ЕС будут оказывать друг другу помощь в вопросах взлома шифрования. …у некоторых стран есть больше технических возможностей, и Еврокомиссия намерена сделать так, чтобы никто не оказался в невыгодном положении. Поэтому правоохранительные органы стран ЕС будут помогать друг другу в проведении экспертизы. Как к данной инициативе относятся сами правоохранители, и захотят ли они делиться своим опытом и технологиями с зарубежными коллегами, пока неизвестно…» ***(Еврокомиссия предложила странам ЕС помогать друг другу во взломе шифрования// "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=119279).- 19.10.2017).***

***

«Четыре миллиона евро выделила Еврокомиссия в качестве награды победителям конкурса на разработку надежных, обеспечивающих конфиденциальность и доступных каждому методов проверки личности пользователя (аутентификации) на персональных электронных устройствах.

Власти ЕС объявили об этом проекте по случаю проводимого уже пятый год в октябре в странах ЕС месячника кибербезопасности…

Согласно обнародованному в понедельник коммюнике Еврокомиссии, в рамках месячника пройдет широкая информационная кампания по распространению знаний о киберугрозах и о защите от них.

Около 300 мероприятий в области кибербезопасности пройдут в октябре во всех странах ЕС. Их организуют Агентство по сетевой и информационной безопасности ЕС (ENISA) совместно с Еврокомиссией и более чем 300 партнерами, включая местные органы власти и организации» ***(ЕК выделила 4 млн евро в награду разработчикам простого и надежного способа проверки личности в электронных устройствах // Интерфакс-Украина (http://interfax.com.ua/news/general/452425.html).- 03.10.2017).***

***

«… «ЄС повинен більше інвестувати в кібербезпеку, щоб запобігати атакам на критичну інфраструктуру та протистояти намірам дестабілізувати суспільство», - йдеться в ухваленій у вівторок резолюції Європарламенту…

Як зазначається, 80% європейських компаній мали під час своєї діяльності щонайменше один інцидент у сфері кібербезпеки.

Відтак парламентарії пропонують покращити систему обміну інформацією між відповідними агентствами ЄС, провести кампанію із підвищення рівня обізнаності громадян з кібербезпеки, організувати підготовку висококваліфікованих ІТ-фахівців, створити базу даних для реєстрації кіберзлочинів, удосконалити законодавство ЄС у цій сфері…» ***(У ЄС хочуть збільшити витрати на кібербезпеку // «iPress» (http://ipress.ua/news/u_yes_hochut_zbilshyty_vytraty_na_kiberbezpeku_228297.html). - 03.10.2017).***

***

«…В правительстве Польши планируют создать департамент по вопросам кибербезопасности. Об этом сообщила премьер-министр Польши Беата Шидло во время открытия Европейского форума по кибербезопасности в Кракове, … задачей которого будет мониторинг проблем в этой сфере и формирование экспертного тыла для главы правительства Польши….

Возглавит новое ведомство государственный секретарь в канцелярии председателя Совета министров Польши Павел Шефернакер…» ***(В правительстве Польши планируют создать департамент по вопросам кибербезопасности // «РБК-Украина» (https://www.rbc.ua/rus/news/pravitelstve-polshi-planiruyut-sozdat-departament-1507558321.html).- 09.10.2017).***

***

«Польская армия для противодействия угрозам в киберпространстве будет насчитывать тысячу человек.

Об этом во время форума по кибербезопасности Cybersec-2017 в Кракове заявил министр обороны Польши Антоний Мацеревич, сообщает "Укринформ"...

Он добавил, что на создание этих войск министерство обороны выделит 2 млрд злотых (более $550 млн).

Он обосновал необходимость создания польской киберармии, в частности, угрозой со стороны России…» ***(Польша выделяет $550 млн на создание киберармии // Espreso.tv***

(https://ru.espreso.tv/news/2017/10/09/polsha_vydelyaet_550_mln_na_sozdanye_kyber armyy).- 09.10.2017).

***

«…В связи с сообщениями СМИ о хакерских атаках с помощью софта "Лаборатории Касперского", Федеральное ведомство по безопасности в сфере информационной техники (BSI) ФРГ заявило, что у него нет оснований предостерегать от пользования программным обеспечением этой компании…

Ранее американские СИМ сообщили, что российские хакеры использовали антивирусное программное обеспечение Касперского для шпионажа против американских ведомств…

BSI, однако, заявило, что на данный момент оно не располагает информацией о том, что факты, изложенные в американских СМИ, действительно имели место. В ведомстве отметили, что BSI находится в контакте с американскими партнерами и другими спецслужбами.

В BSI указали, что антивирусные программы играют важную роль в обеспечении безопасности IT-систем, и для обеспечения надежной защиты такие программы, как правило, должны иметь полный доступ ко всем данным, хранящимся в компьютере. Эти права доступа необходимы для обнаружения хорошо замаскированных вредоносных программ… В BSI добавили, что ведомство для проведения технических анализов пользуется и продукцией Касперского» ***(Сергей Ромашенко. Германское ведомство кибербезопасности доверяет продуктам Касперского // Deutsche Welle (http://www.dw.com/ru/%D0%B3%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D1%81%D0%BA%D0%BE%D0%B5-%D0%B2%D0%B5%D0%B4%D0%BE%D0%BC%D1%81%D1%82%D0%B2%D0%BE-%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%D0%B8-%D0%B4%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D0%B5%D1%82-%D0%BF%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82%D0%B0%D0%BC-%D0%BA%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE/a-40913714?maca=rus-rss-MetaUA_rus_V_Mire-3045-xml-mrss).- 11.10.2017).***

***

«Еврокомиссия готовит к запуску кампанию по защите подростков от кибератак в интернете. Об этом заявил еврокомиссар по вопросам безопасности в ЕС Джулиан Кинг на пленарной сессии Европарламента в Страсбурге. «Еврокомиссия думает о том, чтобы запустить панъевропейскую кампанию по безопасности в интернете и кибербезопасности для подростков», — цитирует Кинга РИА Новости…» ***(Александр Панасенко. ЕС проведет кампанию по безопасности в интернете для защиты подростков // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-10-03-3/24253_.- 03.10.2017).***

***

«…**Масштабна кібератака на парламент, здійснена в червні, тривала більше 12 годин і скомпрометувала близько 90 облікових записів електронної пошти.** Загалом же вражені були понад 9 тисяч акаунтів. Спочатку вважалося, що за атакою стоїть Росія, але зараз розвідка покладає відповідальність на Іран. Це була перша істотна кібератака Ірану проти Великої Британії. Мотив атаки невідомий, але висловлюються припущення, що Корпус вартових ісламської революції міг використовувати кібератаку, щоб підірвати ядерну угоду, оскільки націлений на продовження розробки Іраном ядерної зброї» ***(Виктор Шуляр. До кібератаки на британський парламент причетний Іран // «Публичные люди» (http://pl.com.ua/do-kiberataki-na-britanskij-parlament-prichetnij-iran/).- 14.10.2017).***

***

«Власти Финляндии не исключают возможности привлечения российских специалистов по кибербезопасности к работе Европейского центра по противодействию гибридным угрозам. Об этом заявил ..глава финского МИДа Тимо Сойни… По словам господина Сойни, «Финляндия не чувствует угрозы со стороны России и ничего не боится»… «…При этом мы состоим в ЕС, в ООН, в Северном совете, у нас партнерство с НАТО и так далее. И мы думаем, что подобное многостороннее сотрудничество, основанное на взаимных договоренностях и международном законодательстве,— вот, что хорошо для любой небольшой страны»,— отметил министр. Европейский центр по противодействию гибридным угрозам был открыт в Хельсинки в сентябре… Среди стран-учредителей, помимо Финляндии, еще 11 государств, в том числе США, Великобритания, Германия и Швеция. Целью центра была названа работа по исследованию гибридных угроз — например, связанных с атаками против информационных систем и распространением ложной информации…» ***(Александр Панасенко. Финляндия готова сотрудничать с Россией по вопросам кибербезопасности// ООО "АМ Медиа" (https://www.anti-malware.ru/news/2017-10-20-3/24468).- 20.10.2017).***

***

«У міністерстві закордонних справ Фінляндії буде запроваджено посаду посла з питань гібридних загроз.

Про це заявив МЗС Фінляндії Тімо Сойні…

За його словами, новий посол покликаний сприяти виявленню і відображенню гібридних загроз.

Він наголосив, що балтійський регіон повинен мати кращу готовність відповідати на гібридні загрози, а суспільства має бути краще поінформоване про них.

Коли саме буде запроваджено нову посаду міністр не уточнив…» ***(В МЗС Фінляндії створять посаду посла з питань гібридних загроз // Європейська правда (http://www.eurointegration.com.ua/news/2017/10/20/7072560/).- 20.10.2017).***

***

Китайська Народна Республіка

«Hikvision, ведущий мировой поставщик инновационных продуктов и решений для видеонаблюдения, и консалтинговая компания EY China, провели совместную конференцию, целью которой является запуск проекта развития информационной безопасности в Ханчжоу, Китай.

Благодаря опыту консультативной группы по вопросам рисков в области информационной безопасности, EY помогает Hikvision в разработке систем управления информационной безопасностью в ответ на растущие риски кибербезопасности. Команда проекта EY использует свои умения и знания в области кибербезопасности для поддержки Hikvision в проведении оценок информационной безопасности на уровне групп и научно-исследовательского центра. Кроме того, в рамках этого сотрудничества EY будет постоянно делиться передовыми технологиями для дальнейшего содействия Hikvision в решении проблем, которые возникают в результате трансформации рисков кибербезопасности…» ***(Hikvision и EY провели совместную конференцию по информационной безопасности // «Security-News.Today» (https://www.security-news.today/hikvision-ey-proveli-sovmestnuyu-konferentsiyu-po-informatsionnoj-bezopasnosti/).- 27.10.2017).***

***

Російська Федерація

«…Директор Федеральной службы безопасности РФ Александр Бортников выступил с предложением расширить сотрудничество при реагировании на киберинциденты и рассмотреть возможность запрета создания вредоносного ПО на международном уровне. Об этом он заявил в рамках XVI совещания руководителей спецслужб органов безопасности и правоохранительных органов иностранных государств…

Бортников отметил, что эффективность противодействия кибератакам, многие из которых носят международный характер, в значительной степени определяется уровнем взаимодействия национальных субъектов, реагирующих на компьютерные инциденты. В этой связи ведомство предложило расширить практическое сотрудничество при реагировании на компьютерные инциденты и рассмотреть возможность создания международного правового режима запрета на разработку вредоносного ПО…

Также глава ведомства отметил, что в ФСБ «изучают и считают необходимым к распространению передовой международный опыт в сфере информационной безопасности», в частности «меры по запрету анонимности в интернет-мессенджерах», а также запрет оборота анонимных SIM-карт» ***(ФСБ***

предложила запретить разработку вредоносного ПО на международном уровне // SecurityLab.ru (https://www.securitylab.ru/news/488868.php).- 04.10.2017).

***

«Північна Корея відкрила новий інтернет-зв'язок із зовнішнім світом, на цей раз через Росію, що, за словами експертів у галузі кібербезпеки, зміцнить Інтернет в середині країни та його здатність здійснювати кібератаки…

Компанія Dyn Research, яка відстежує підключення до інтернету у світі, заявила, що російська телекомунікаційна компанія TransTeleCom почала підтримувати північнокорейський трафік приблизно з 9:00 за Гринвічем у неділю.

Раніше трафік оброблявся через китайську компанію China Unicom. TransTeleCom не зміг надати оперативного коментаря щодо цієї інформації.

Інтернет Північної Кореї обмежений кількома сотнями з'єднань. Але ці зв'язки є життєво важливими для координування кібератак, сказав Брайс Боланд, голова технічного відділу компанії FireEye по Азіатсько-Тихоокеанському регіону…

Болан заявив, що російська лінія доступу посилить здатність Північної Кореї керувати майбутніми кібератаками.

За його словами, багато хто з кібератак, що здійснюються Пхеньяном, проводяться за межами Північної Кореї шляхом використання захоплених комп'ютерів хакерами, які територіально знаходяться в КНДР…» ***(Російська компанія підвищила здатність КНДР до здійснення кібератак – експерти // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/ros%d1%96iska-kompan%d1%96ia-p%d1%96dvishila-zdatn%d1%96st-kndr-do-zd%d1%96isnennia-k%d1%96beratak-eksperti.html).- 02.10.2017).***

***

«…Уже через два года в России начнут выдавать аттестаты специалистов в области кибербезопасности в финансовой сфере. Об этом в среду, 11 октября, сообщил заместитель начальника главного управления безопасности и защиты информации Банка России Артем Сычев.

По словам Сычева, в настоящее время уже разработаны квалификационные требования, а также программа по магистерской специальности и по повышению квалификации…

В будущем также планируется ввести требование об обязательном наличии аттестатов нового типа для работающих в банках специалистов в области кибербезопасности, однако этого не стоит ожидать в ближайшем будущем…

Как пояснил Сычев, обучение специалистов будет проводиться в трех наиболее популярных направлениях – методология, технология и юриспруденция в кибербезопасности. Правда, кто будет обучать новые кадры и выдавать аттестаты, пока неизвестно…» ***(В РФ начнут выдавать аттестаты специалистов по кибербезопасности в финансовой сфере // SecurityLab.ru (http://www.securitylab.ru/news/489051.php).- 12.10.2017).***

***

«…План мероприятий по кибербезопасности на 2017-2024 годы по программе «Цифровая экономика» предусматривает создание в России отечественной операционной системы, на которой будут базироваться устройства Интернета вещей и Промышленного интернета. Это следует из документа, разработанного рабочей группой, которую возглавляет Сбербанк. Разработка ОС должна завершиться до 31 декабря 2021 года, к этому же сроку планируется выбрать пилотную отрасль для внедрения системы, а также отрасли для ее тиражирования.

Согласно документу, в результате должна быть создана «отечественная свободная ОС для использования во всех видах киберфизических систем, превосходящая зарубежные ОС по ключевым параметрам быстродействия, безопасности и отказоустойчивости».

Ответственными исполнителями указаны Минпромторг, Минкомсвязь, а также отечественные автопроизводители и разработчики программного обеспечения.

…Согласно документу, прототипы таких ОС должны быть разработаны к четвертому кварталу 2018 года. Сами ОС и центр компетенций по вопросам межмашинного взаимодействия, включая киберфизические системы и Интернет вещей, должны появиться в третьем квартале 2020 года.

Кроме того, в четвертом квартале 2019 года планируется принять национальные стандарты межмашинного взаимодействия для киберфизических систем.

Если использовать имеющиеся наработки, то стоимость такого проекта составит около 200 млн руб., если же брать деньги на разработку у государства, то стоимость может вырасти до 1,5 млрд руб…» ***(В России создадут национальную операционную систему для Интернета вещей // «Открытые системы» (https://www.computerworld.ru/news/V-Rossii-sozdadut-natsionalnuyu-operatsionnuyu-sistemu-dlya-Interneta-veschey).- 10.10.2017).***

***

«…Міжнародна організація кримінальної поліції (Інтерпол) і російська «Лабораторія Касперського» підписали нову угоду про співпрацю у сфері боротьби з кіберзлочинністю…

Першу таку угоду вони уклали в 2014 році. В Інтерполі заявляють, що фахівці «Лабораторії Касперського» регулярно ділилися інформацією про нові кіберзагрози з правоохоронцями країн, що входять до організації. Зокрема, Інтерпол стверджує, що експерти російської компанії брали участь в операціях з ліквідації ботнетів — мереж заражених комп'ютерів, якими можна керувати дистанційно без відома власників.

Як стало відомо The Wall Street Journal, за згодою компанії в антивірусну програму були внесені модифікації, що дозволяють таємно сканувати комп'ютери по всьому світу. Російський уряд використовував «Касперського» для шпигунства за класифікованими урядовими документами США і надсекретною інформацією. Внесені модифікації дозволяли знаходити на комп'ютері засекречені файли, в тому числі файл під грифом «Top Secret» («цілком таємно»). У компанії в свою чергу

спростовують причетність до шпигунства на користь РФ, заявивши про готовність взаємодіяти з американською владою…» ***(Інтерпол підписав нову угоду у сфері кібербезпеки з «Лабораторією Касперського» // Громадсько-правовий портал «Ракурс» (http://ua.racurs.ua/news-95442-interpol-pidpysav-novu-ugodu-u-sferi-kiberbezpeky-z-laboratoriieu-kasperskogo).- 12.10.2017).***

***

«Дочерняя компания Сбербанка BI.ZONE выходит на новый этап сотрудничества с международной правоохранительной организацией Интерпол — стороны подписали официальное соглашение о расширении сотрудничества по борьбе с международной киберпреступностью.

В рамках данного соглашения компания BI.ZONE будет оказывать оперативную поддержку деятельности Интерпола по борьбе с преступлениями в киберпространстве и предоставлять международной организации актуальные данные о новейших угрозах и деятельности организованных преступных групп…

Компания BI.ZONE — визионер российского рынка кибербезопасности, предлагающий услуги по защите активов и репутации бизнеса в сети Интернет, основанные на кибербразведке и постоянном мониторинге информационных потоков в публичных и теневых сегментах киберпространства…» ***(Сбербанк и Интерпол расширяют сотрудничество по борьбе с киберпреступлениями // IKSMEDIA.RU (http://www.iksmedia.ru/news/5445939-Sberbank-i-Interpol-rasshiryayut.html#ixzz4wPcWdsBL).- 23.10.2017).***

***

«На Всемирном форуме молодежи и студентов зампред правления Сбербанка Станислав Кузнецов выступил с лекцией «Кибербезопасность — как защититься в мире киберугроз?», в ходе которой он назвал сайт объявлений Avito одной из центральных площадок для киберпреступлений…

Господин Кузнецов показал слайд, на котором была описана схема обмана: мошенник-автор просит потенциального покупателя прислать номер банковской карты или ее фотографию, чтобы «внести предоплату или полную сумму перевода», после чего подключает СМС-банк на телефон мошенников либо передает им пароль для регистрации в интернет-банке. Затем со счета потенциального покупателя похищаются средства.

«Заявление господина Кузнецова в наш адрес абсолютно некорректно. Делать подобные заявления — все равно что обвинять интернет в том, что он является причиной возникновения киберпреступности. В этой логике можно допустить аналогичный вывод о том, что Сбербанк является основной площадкой для мошенничества с банковскими картами, являясь лидером по их эмиссии»,— заявил «Ведомостям» представитель Avito…» ***(Сбербанк назвал Avito одной из центральных площадок кибермошенников // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3446800).- 21.10.2017).***

***

«Результаты исследования показали, что электронная почта является по-прежнему наиболее используемым онлайн-сервисом в России… Второе место занимают соцсети «ВКонтакте» и Facebook. 22,2% респондентов заявили, что им приходилось сталкиваться с кражей персональных данных. 66,6% сомневаются, что их личная информация надежно защищена. 35,4% россиян ни разу не меняли пароль после взлома. 81,2% же изменили пароль для взломанного аккаунта, но не для других сайтов.

Наиболее популярными у хакеров сервисами оказались Amazon (43,7% взломов), Dropbox (42.3%) и Snapchat (41,7%). Далее идут электронная почта, LinkedIn, WhatsApp, Facebook и Twitter…» ***(Большинство россиян ничего не предпринимают для защиты своих персональных данных // «Открытые системы» (https://www.computerworld.ru/news/Bolshinstvo-rossiyan-nichego-ne-predprinimayut-dlya-zaschity-svoih-personalnyh-dannyh).- 20.10.2017).***

***

«…Программа «Цифровая экономика», подготовленная Минкомсвязью по поручению Президента России Владимира Путина и утвержденная Правительством, содержит целый ряд мер по развитию импортозамещения и технологической независимости России в сфере информационно-коммуникационных технологий (ИКТ). Эти предложения входят в раздел «Информационная безопасность».

Кроме всего прочего, в начале 2019 года в рамках программы планируется законодательно установить требования к использованию отечественного компьютерного, серверного и телекоммуникационного оборудования на объектах инфраструктуры обработки данных. Планируется разработать и внедрить модель центра обработки данных (ЦОД), на котором обеспечено преимущественное использование данных видов оборудования отечественного производства…

В сфере информационной безопасности в начале 2018 г. для инвестиционной поддержки будет определен перечень перспективных информационных технологий в области информационной безопасности…

В начале 2019 г. будет создана система добровольного декларирования уровня безопасности продуктов и услуг ИКТ («Декларация информационной безопасности»). Тогда же будет создана система стимулов создания российской продукции в области информационной безопасности и увеличения ее доли в условиях цифровой экономики

Во II квартале 2019 г. будет законодательно обеспечена предустановка отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории стран Евразийского экономического сотрудничества (ЕАЭС).

Во II квартале 2020 г. будут разработаны национальные стандарты информационной безопасности в системах, реализующих облачные, туманные, квантовые технологии, системах виртуальной и дополненной реальности и технологий искусственного интеллекта.

В том же году будет обеспечен контроль применения и развития перспективных технологий идентификации участников информационного

взаимодействия, включая технологии биометрической идентификации, многофакторной идентификации на основе ЕСИА и иных технологий идентификации…» ***(Программа «Цифровая экономика» может отрицательно повлиять на развитие отечественного IT // РосКомСвобода (https://rublacklist.net/32895/).- 19.10.2017).***

***

«С 2018 года российские банки каждые три месяца будут отчитываться перед регулятором обо всех без исключения кибератаках, даже самых мелких…

В конце сентября предполагалось, что будет установлена минимальная сумма ущерба, которую банки должны будут отражать в своей отчетности. Это избавило бы их от расходов на расследование незначительных случаев кибератак. Тратить на разбирательство больше, чем было потеряно, для банков экономически нецелесообразно…

Теперь Центробанк решил отказаться от этого ограничения. По мнению экспертов, оставленные без внимания мелкие кибератаки могут обернуться большими потерями в будущем…

О проблемах, возникших при переводе денег клиентов, финансовые организации должны информировать Центробанк с 2013 года. Фиксироваться должны все случаи такого рода — например, кража данных пластиковой карты при оплате счета, случаи скимминга или фишинга. На основании этих данных регулятор составляет статистику по киберпреступлениям.

Сейчас в отчет включаются механизм мошенничества, дата, оператор платежной системы и меры, принятые по устранению ущерба. Однако с 2018 года в документах появятся точные финансовые сведения о сумме хищения и о возвращенных клиенту деньгах. При этом в отчет необходимо будет включать даже самые мелкие атаки, ущерб от которых минимален» ***(Egor Nashilov. Центробанк ужесточает требования к отчетности о кибератаках // Threatpost (https://threatpost.ru/cb-hardens-requirements-for-reports-on-cyberattacks/22917/).- 23.10.2017).***

***

«Глобальный специалист по страхованию и управлению рисками компания Marsh подписала меморандум о взаимопонимании с «Лабораторией Касперского»…

…рамках меморандума обе компании будут сотрудничать в области аудита кибербезопасности, который включает в себя первоначальный анализ и услуги по расследованию инцидентов. В рамках соглашения Marsh предложит крупным российским компаниям страховые решения и метод расчета возможных потерь…» ***(Marsh и Kaspersky Lab подписали меморандум в сфере аудита кибербезопасности // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/marsh-i-kaspersky-lab-podpisali-memorandum-v-sfere-audita-kiberbezopasnosti).- 31.10.2017).***

***

«…«Лаборатория Касперского» запустила глобальную инициативу по информационной открытости (Global Transparency Initiative). В рамках этой инициативы «Лаборатория Касперского» намерена предоставить исходный код своих продуктов, включая код обновлений ПО и антивирусные базы, для анализа независимым экспертам…

На начальном этапе реализации инициативы по информационной открытости предусмотрены следующие шаги:

– независимый анализ исходного кода (старт до конца первого квартала 2018 года) с последующим аналогичным анализом программных обновлений и антивирусных баз;

– независимая оценка процесса безопасной разработки и стратегии по минимизации рисков в цепочке поставщиков и в программном обеспечении (старт до конца первого квартала 2018 года);

– разработка дополнительных механизмов контроля процесса обработки данных – совместно с независимыми экспертами, которые смогут оценить соответствие принятых в компании практик заявленным требованиям (старт до конца первого квартала 2018 года);

– открытие трех Центров прозрачности (Transparency Centers) по всему миру с целью решения любых вопросов в сфере кибербезопасности совместно с клиентами, партнерами и государственными органами. В этих центрах партнеры компании смогут получить информацию о программном коде «Лаборатории Касперского», обновлениях продуктов, антивирусных базах и пр. Первый центр планируется открыть в 2018 году; всего же к 2020 году Центры прозрачности будут работать в Азии, Европе и США;

– увеличение размера вознаграждения в программе bug bounty до 100 тысяч долларов за обнаружение наиболее серьезных уязвимостей в программном обеспечении «Лаборатории Касперского» – этот шаг станет дополнительной мотивацией для независимых исследователей, работающих в рамках программы компании по скоординированному раскрытию уязвимостей (до конца 2017 года).

Кроме того, компания приглашает всех представителей сообщества по информационной безопасности и других заинтересованных лиц присоединиться к проработке второго этапа инициативы Global Transparency Initiative, который начнется во втором квартале 2018 года…» ***(«Лаборатория Касперского» станет прозрачнее // IKSMEDIA.RU (http://www.iksmedia.ru/news/5446257-Laboratoriya-Kasperskogo-stanet-pro.html#ixzz4wPdxxL9r).- 24.10.2017).***

***

«Лаборатория Касперского» рассказала о случаях кибершпионажа, в которых жертвами преступников становились их же «конкуренты» — другие группировки, занимающиеся целевыми атаками…

Несколько примеров того, как хакеры могут использовать чужие технологии в собственных целях:

1. …Установка бэкдора (инструмента для удаленного управления компьютером жертвы) во взломанной сети позволяет атакующим постоянно

следить за операциями другой группы. «Лаборатория Касперского» обнаружила как минимум два примера подобных атак. Первый — в 2013 году при анализе сервера китайскоговорящей группировки NetTraveler, атакующей активистов и организации в Азии. Второй нашли в 2014 году при расследовании взлома группировкой Crouching Yeti одного из веб-сайтов… Исследователи заметили, что в течение некоторого времени панель управления сетью командных серверов была изменена при помощи тэга, который указывал на китайский IP.

2. …В 2016 году исследователи «Лаборатории Касперского» обнаружили, что взломанный корейскоязычной группировкой DarkHotel сайт также содержал эксплойты другой APT-группировки — ScarCruft. Жертвами последней в основном становились российские, китайские и южнокорейские организации. Атака DarkHotel произошла в апреле 2016 года, а ScarCruft — месяцем позже. Это позволяет предположить, что преступники из ScarCruft следили за операциями DarkHotel, прежде чем приступать к собственным.

3. …использование в операциях инфраструктуры и сведений группировок, которые хорошо знают конкретный регион или индустрию. При этом некоторые преступники предпочитают не воровать у других цели, а «делить» их. В ноябре 2014 года «Лаборатория Касперского» обнаружила, что принадлежащий ближневосточному исследовательскому институту сервер, известный как «Магнит для угроз», одновременно содержал импланты групп Regin, Equation Group (англоговорящие), Turla, ItaDuke (италоговорящие), Animal Farm (франкоговорящие) и Careto (испаноговорящие)…» ***(Как киберпреступники воруют друг у друга технологии // IKSMEDIA.RU (http://www.iksmedia.ru/news/5446241-Kak-kiberprestupniki-voruyut-drug.html#ixzz4wPeEBFzB).- 24.10.2017).***

***

«…«Считаю, что нужно усилить персональную ответственность руководителей за обеспечение информационной безопасности», — заявил Путин в ходе заседания Совбеза России.

Российский лидер также отметил рост угроз в информационном пространстве…

Он также отметил необходимость активнее содействовать созданию международной системы безопасности» ***(Путин заявил о необходимости усилить ответственность чиновников за кибербезопасность // Автономная некоммерческая организация «ТВ-Новости» (https://russian.rt.com/science/news/443301-putin-otvetstvennost-chinovniki-kiberbezopasnost).- 26.10.2017).***

***

«…Владимир Путин уверен в необходимости повышения безопасности российского сегмента Глобальной сети. Об этом глава государства заявил в четверг, 26 октября, на заседании Совбеза РФ…

Говоря о повышении безопасности Рунета, Путин также отметил, что при этом не должно создаваться никаких барьеров и фильтров для законопослушных граждан…

Глава государства также отметил повышение уровня угроз и рисков в киберпространстве и глобальный масштаб кибератак. В частности Путин выразил обеспокоенность по поводу возможных хакерских атак на системы в сферах государственной обороны, управления и финансов, а также по поводу утечек электронных документов, способных «обернуться самыми тяжелыми последствиями».

По словам российского главы, вопросы безопасности в киберпространстве имеют для РФ стратегическое значение как фактор обеспечения суверенитета, обороноспособности и безопасности государства, эффективного развития экономики, социальной сферы и госуправления» ***(Путин выступил против создания барьеров в киберпространстве // SecurityLab.ru (http://www.securitylab.ru/news/489353.php).- 27.10.2017).***

***

«…в рамках правительственной программы «Цифровая экономика» готовится создание масштабного рынка страхования от киберрисков. Полис информационной безопасности может стать обязательным с 2020 года для всех стратегических отраслей — от банковской сферы до машиностроения. Примеров организации управления киберрисками в таком объеме нет ни в одной стране, и РФ может стать мировым лидером в этой отрасли…

Рабочую группу по этому направлению программы возглавляет Сбербанк. План предполагает к 2020 году введение индустриального стандарта по обязательному аудиту информационной безопасности (будет описывать условия страхования и сбора статистики, модели актуарных расчетов тарифов и т. д.) — и требование обязательного страхования таких рисков предприятиями отдельных отраслей экономики (включая банковскую сферу, аэропорты, вокзалы и стратегические отрасли промышленности — металлургию, машиностроение, судостроение, авиапром и др.)… Для реализации проекта предлагается внести поправки в закон об организации страхового дела (добавляется новый вид страхования). Расходы на него должны будут снижать налоговую базу — для этого предлагается внести поправки в НК.

Текущее положение дел в этой сфере документ описывает так: «Страхование информационных рисков является неизвестным и непонятным для большинства потребителей этой услуги». За всю историю страхования киберрисков в РФ заключено менее 20 договоров страхования, большинство из которых оформлено предприятиями с иностранным участием у иностранных страховщиков…

…По оценке директора по развитию решений промышленной кибербезопасности «Лаборатории Касперского» Андрея Суворова, средняя сумма убытка среди корпоративных заказчиков компании от кибератак составляет $497 тыс. По данным Group-IB для России и СНГ, в интернет-банкинге у юридических лиц с использованием вредоносных программ в день совершают две успешные атаки со средней суммой хищения 1,25 млн руб. За год с июля 2016 по июль 2017

года у юрлиц украли 622,5 млн руб. (на 35% меньше, чем годом ранее). Рынок страхования от хакерских атак в РФ только формируется, говорит Алексей Новиков, руководитель экспертного центра безопасности PT Expert Security Center. По его словам, страховщики не готовы брать на себя такую ответственность из-за сложной оценки потерь.

В первую очередь услуга киберстрахования востребована банками и финансовыми организациями, во вторую — провайдерами, в третью — компаниями, занимающимися обработкой персональных данных… При этом у компаний, в первую очередь технологичных, постепенно нарастает понимание того, что проблема есть и что можно страховаться от таких рисков. В страховой компании «Альянс», страхующей клиентов от киберрисков, отметили, что после распространения вирусов WannaCry и Petya зафиксировали рост спроса на услуги страхования от киберугроз — по оценке компании, мировой оборот этого рынка составляет $2,5 млрд.

Бизнес к идее страховой защиты киберрисков отнесся по-разному. В Абсолют-банке “Ъ” заявили, что сейчас банки такие риски не страхуют, но идею назвали своевременной… Глава департамента нефинансовых рисков и финансового мониторинга Росевробанка Марина Бурдонова относится к идее обязательного кибераудита банков положительно, а обязательное страхование также считает избыточным. Собеседник из правоохранительных органов, знакомый с позицией Банка России по этой теме, назвал аудит информационной безопасности «здравой идеей» — он «выявит проблемы в банках, которые необходимо закрывать». Страховку он также считает «лишней тратой денег»…» ***(Татьяна Гришина, Кристина Жукова, Юлия Тишина, Елена Черненко, Вероника Горячева, Елизавета Кузнецова. Полис на всякий вирус // «Коммерсантъ» (https://www.kommersant.ru/doc/3450079?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).- 30.10.2017).***

***

«…глава Минобрнауки Ольга Васильева заявила, что основам кибербезопасности начнут учить школьников и учителей, соответствующие программы будут разработаны ведомством. По ее словам, говорить школьникам об этом нужно в стандартах начального образования и на уроках информатики, обществознания, права, ОБЖ, а также во внеурочной деятельности.

Учебник по кибербезопасности, по которому в дальнейшем будут учиться российские школьники, напишут ученые факультетов психологии и журналистики Московского государственного университета им. Ломоносова…

Некоторые шаги в направлении интернет-ликбеза для школьников делаются уже давно. Например, 30 октября в российских школах прошёл Единый урок кибербезопасности в интернете, а в некоторых учебных заведениях в частном порядке были проведены лекции с участием местных чиновников и представителей некоторых организаций, на которых хотелось бы заострить внимание отдельно…» ***(Детский омбудсмен: блокировки не помогают, надо ввести уроки***

кибербезопасности в школах // РосКомСвобода (https://rublacklist.net/33145/).-30.10.2017).

***

Республіка Білорусь

«Обзор законодательства Республики Беларусь в сфере информационной безопасности – Часть 6: Техническая и криптографическая защита информации…

В Республике Беларусь вопросы криптографической защиты информации, не содержащей сведений, отнесенных к государственным секретам, регулируются:

– Законом «Об информации»;

– Законом Республики Беларусь от 28 декабря 2009 г. «Об электронном документе и электронной цифровой подписи»;

– Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», которым утверждено Положение о технической и криптографической защите информации в Республике Беларусь;

– приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации» (далее – Приказ № 62)…

Приказом № 62 было утверждено специальное Положение о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и критически важных объектов информатизации (далее – Положение о порядке криптографической защиты информации).

Криптографическая защита информации осуществляется путем применения средств криптографической защиты информации, а также комплекса организационных мер.

К средствам криптографической защиты информации относятся технические, программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

К объектам, на которых осуществляется криптографическая защита информации в соответствии с Положением о защите информации, относятся:

– государственные информационные системы в части обеспечения целостности и подлинности электронных документов (решение об организации защиты принимается собственником (владельцем) таких систем при использовании в этих системах электронных документов);

– информационные системы, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (решение об организации защиты принимается собственником (владельцем) таких систем при реализации комплекса мероприятий по созданию системы защиты информации (на этапе проектирования системы защиты информации информационной системы));

– критически важные объекты информатизации (далее – КВОИ) (в соответствии с Положением об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации, утвержденным Указом Президента Республики Беларусь от 25 ноября 2011 г. № 486…

Работы по криптографической защите информации в организации проводятся подразделением технической защиты информации или иными подразделениями (должностными лицами), выполняющими функции по криптографической защите информации, либо, при необходимости, могут привлекаться организации, имеющие специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и услуг.

…Техническая защита информации – деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации (абзац 8 пункта 3 Положения о защите информации).

Под средствами технической защиты информации следует понимать – технические, программные, программно-аппаратные средства защиты информации, предназначенные для защиты информации от ее утечки по техническим каналам, несанкционированного доступа, несанкционированных воздействий на информацию, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля эффективности ее защищенности.

К объектам, на которых осуществляется техническая защита информации в соответствии с Положением о защите информации, относятся:

– объекты информатизации, предназначенные для обработки информации, содержащей государственные секреты;

– информационные системы, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (в отношении данных объектов ОАЦ было принято Положение о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденное Приказом № 62);

– КВОИ…

К субъектам, на которых возложены требования по соблюдению требований положений по технической и криптографической защите информации относятся:

– собственники (владельцы) КВОИ, объектов информатизации, предназначенных для обработки информации, содержащей государственные

секреты, а также собственниками (владельцами) государственных информационных систем в части обеспечения целостности и подлинности электронных документов;

– собственники (владельцы) информационных систем, в которых обрабатываются служебная информация ограниченного распространения, информация о частной жизни физического лица и персональные данные;

– государственные органы и иные государственные организации, хозяйственные общества в отношении которых Республика Беларусь либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами, являющимися собственниками (владельцами) информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

– иные собственники (владельцы) объектов информатизации (в том числе информационных систем) – вправе руководствоваться требованиями по технической и криптографической защите информации, если иное не предусмотрено законодательными актами…» ***(Обзор законодательства Республики Беларусь: Техническая и криптографическая защита информации // Digital.Report (https://digital.report/obzor-zakonodatelstva-respubliki-belarus-kryptografia/).- 12.10.2017).***

***

«Обзор законодательства Республики Беларусь в сфере информационной безопасности – Часть 8: Борьба с киберпреступностью…

Киберпреступление – вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации, например информации по банковским счетам…

Условно, подобного рода противоправные деяния можно разбить на несколько групп:

– преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых (такие действия рассматриваются как посягательства на собственность и квалифицируются по статьям гл. 24 УК РБ);

– преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д. (такие действия рассматриваются как преступления против информационной безопасности и квалифицируются по статьям гл. 31 УК РБ);

– преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве средства совершения корыстного преступления, и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной

информации (такие действия рассматриваются как хищение путем использования компьютерной техники и квалифицируются по ст. 212 УК РБ)…

…В Министерстве внутренних дел Республики Беларусь создано и функционирует специальное подразделение по борьбе с киберпреступностью – Управление по раскрытию преступлений в сфере высоких технологий (Управление «К»).

В структуре компьютерной преступности доля преступлений против информационной безопасности за последние годы увеличивается (к примеру, в 2012 году такая доля составляла 5,5%).

Рассмотрим составы основных киберпреступлений:

– основной состав преступления, предусмотренного статьей 212 «Хищение путем использования компьютерной техники» предусматривает два способа хищения:

  - хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных;
  - хищение путем введения в компьютерную систему ложной информации…

– статья 349 УК «Несанкционированный доступ к компьютерной информации» предусматривает ответственность за несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда. Понятие «существенный вред» законодателем не раскрывается…

– деятельность по изменению информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности охватывается составом преступления, предусмотренного статьей 350 УК «Модификация компьютерной информации»…

– компьютерный саботаж (статья 351 УК) представляет собой умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя…

– статья 352 УК предусматривает ответственность за несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда.

– статья 353 УК предусматривает ответственность за изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети.

– за разработку компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения,

блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработку специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами – предусмотрена ответственность статьей 354 УК…

– статья 355 УК предусматривает ответственность за умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда…

По данным Министерства внутренних дел Республики Беларусь общий уровень раскрываемости киберпреступлений в 2015 году составил 55,5% (в 2014 году – 56,2%)… Установленный материальный ущерб составил 69,47 миллиардов рублей, из которых возмещено 31,5%» ***(Обзор законодательства Республики Беларусь: Борьба с киберпреступностью // Digital.Report (https://digital.report/obzor-zakonodatelstva-respubliki-belarus-kiberprestupnost/).- 12.10.2017).***

***

«Национальный банк Беларуси создает подразделение по кибербезопасности. Планируется, что оно начнет действовать в 2018 году. «Мы сейчас создаем подразделение, которое занимается кибербезопасностью, находимся на первом этапе: определили направления деятельности, сейчас создана комиссия с участием банков, которые наиболее прогрессивны в этой части, и всех заинтересованных служб Нацбанка. Планируется, что это подразделение (Центр мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере) будет запущено в 2018 году", - сообщил первый заместитель председателя правления Национального банка Беларуси Тарас Надольный…» ***(Александр Панасенко. Нацбанк Беларуси создает подразделение по кибербезопасности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-10-26-3/24548).- 26.10.2017).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Представники Федерального резервного банку Нью-Йорка та Нацбанку домовилися розширити співпрацю у сфері кібербезпеки… та частіше зустрічатись для консультацій щодо діяльності центральних банків України та США, а також впливу глобальних тенденцій на фінансові системи наших країн…

Під час зустрічі в. о. голови НБУ Яків Смолій розповів про масштабну внутрішню реорганізацію Національного банку, а також про кроки, які регулятор здійснив для реалізації реформ…» ***(Нацбанк співпрацюватиме з США у сфері кібербезпеки // «iPress»***

(http://ipress.ua/news/natsbank_spivpratsyuvatyme_z_ssha_u_sferi_kiberbezpeky_228453.html).- 04.10.2017).

***

«Сполучені Штати Америки нададуть Україні понад 5 мільйонів доларів на зміцнення здатності запобігати кіберзагрозам.

Про це йшлося під час першого двостороннього діалогу щодо кібербезпеки, що відбувся у п'ятницю у Києві…

Крім того, учасники діалогу обговорили захист критичної інфраструктури та військових систем, зміцнення довіри у сфері кібербезпеки в ОБСЄ…» ***(США нададуть Україні понад $5 млн на заходи кібербезпеки // Джерело: Високий замок online (http://wz.lviv.ua/news/207716-ssha-nadadut-ukraini-ponad-usd5-mln-na-zakhody-kiberbezpeky).- 30.09.2017).***

***

«Під час міністерської зустрічі щодо цифрової економіки у Таллінні були визначені ключові пріоритети цифрової спільноти Україна-ЄС.

…Міністр економічного розвитку і торгівлі Степан Кубів, який також брав участь у зустрічі, підтвердив пріоритетність цифровізації України як частини її інтеграції до Європейського Союзу…

Він зазначив, що найбільш важливими напрямками співпраці у цифровій сфері для України є розвиток широкосмугового доступу до Інтернету та технологій 4G і 5G, кібербезпека, розвиток інновацій та розбудова інноваційної екосистеми, електронна ідентифікація, електронне урядування та розвиток електронної торгівлі.

Міністр додав, що Україна зацікавлена у посиленні двостороннього цифрового діалогу з ЄС і розглядає його як логічне продовження Угоди про вільну торгівлю…

За результатами зустрічі сторони схвалили спільну декларацію, у якій визначили 6 ключових напрямків спільної роботи у цифровій сфері та деталізували плани щодо реалізації пріоритетних дій до 2020 року» ***(У Таллінні визначили 6 пріоритетів для створення цифрової спільноти Україна-ЄС // Європейська правда (http://www.eurointegration.com.ua/news/2017/10/5/7071918/).- 05.10.2017).***

***

«З 29 жовтня по 1 листопада ц.р. у Києві в приміщеннях Верховної Ради України пройшла чергова Шоста сесія Парламентської Асамблеї ЄВРОНЕСТ, у якій взяли участь народні депутати України, європарламентарії та представники парламентів країн Східного Партнерства (Україна, Азербайджан, Вірменія, Грузія, Молдова)…

Під час сесії були обговорені наступні ключові теми:

- свобода та об’єктивність ЗМІ;
- молодіжне безробіття;
- енергетична складова реалізації паризької кліматичної угоди 2015;
- жінки на ринку праці;

– кібербезпека в країнах ЄС та країнах Східного Партнерства…» ***(З 29 жовтня по 1 листопада ц.р. у приміщеннях Верховної Ради України проходитиме чергова VI сесія ПА ЄВРОНЕСТ, у якій візьмуть участь народні депутати України, європарламентарії та представники парламентів країн Східного Партнерства // Народна Рада (http://narodnarada.info/news/jovtnya-listopada-primischennyah-verhovnoji-news-78012.html).- 26.10.2017).***

***

«Японских специалистов направят в центр кибербезопасности НАТО, который находится в столице Эстонии. Об этом … заявил генеральный секретарь НАТО Йенс Столтенберг, который 29 октября начинает визит в Японию... По словам Столтенберга, согласование этого вопроса находится сейчас в финальной стадии. Он также отметил, что рассматривается вопрос широкого участия японской стороны в учениях НАТО по кибербезопасности сообщает…» ***(Александр Панасенко.Эстонский центр кибербезопасности НАТО защитят японцы // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-10-30-3/24577).- 30.10.2017).***

***

Кіберзахист критичної інфраструктури

«НБУ установил минимальные требования к кибербезопасности банков. Так, банки обязаны внедрить систему управления информационной безопасностью, а также процесс управления рисками.

В банке будет назначаться уполномоченное лицо, ответственное за информационную безопасность (Chief Information Security Officer). К его полномочиям отнесен определение направлений развития информационной безопасности банков, а также контроль за внедрением мер кибербезопасности.

Также все сотрудники банка будут проходить специальное обучение, при разработке программы которого будут учитываться произошедшие кибератаки.

Кроме того, банки должны обеспечить защиту пользователей в информационных системах банка…

Меры кибербезопансости также включают криптографическую защиту информации, защиту от вредоносного кода, меры безопасности при использовании электронной почты и меры безопасности в сети банка.

Положение об организации мер по обеспечению информационной безопасности в банковской системе Украины утверждено постановлением НБУ от 28 сентября 2017 года № 95. Постановление вступает в силу с 1 марта 2018 года, кроме раздела V «Дополнительные меры безопасности информации», требования которого вступят в силу с 1 сентября 2019 года» ***(Определены требования к кибербезопасности банков // Інформаційне агентство "ЛІГА:ЗАКОН (http://jurliga.ligazakon.ua/news/2017/10/5/165201.htm0.- 05.10.2017).***

***

«Спецслужбы США обнаружили хакерскую группировку, которая с мая 2017 года совершала кибератаки на энергетические и промышленные предприятия. Об этом заявили Федеральное бюро расследований (ФБР) и Министерство внутренней безопасности (МВБ) в распространенном совместном заявлении…

Ведомства не уточнили, в какой стране хакеры пытались взломать компьютерные сети промышленных предприятий. Однако отметили, что киберпреступники смогли получить доступ как минимум к одному генератору энергии. Свое заявление американские спецслужбы сопроводили шестью техническими документами, в которых описывается используемое хакерами вредоносное программное обеспечение. В этих документах говорится, что кибератаки проводились при помощи отправки электронных писем с вредоносными программами. Также в этих письмах предлагалось перейти по ссылкам на сайты и ввести конфиденциальные данные пользователя. Жертвами злоумышленников становились подрядчики, работающие на государственные предприятиями и имеющие доступ к их компьютерным сетям, пояснили американские спецслужбы…» ***(США выявили кибератаки на энергетические и промышленные предприятия // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3447075).- 22.10.2017).***

***

«…Департамент внутрішньої безпеки США та Федеральне бюро розслідувань попередили у своїй доповіді, поширеній електронною поштою, про те, що ядерні, енергетичні, авіаційні, водні та критично важливі промислові підприємства, поряд з державними структурами, були ціллю хакерських атак, скоєних в травні і раніше.

Агентства попередили, що хакери змогли зламати деякі мережі, але не розкрили дані про конкретні жертви атак.

Представник відділу з питань національної безпеки Скотт Макконнелл відмовився викласти подробиці щодо поширеної інформації в повідомленні або пояснити, чому уряд повідомляє про це зараз…

ФБР відмовилося коментувати звіт, який, за словами дослідників безпеки, описує ескалацію атак на інфраструктуру в Європі і Сполучених Штатах…

У звіті говориться, що зловмисники ті ж самі, що описані компанією Symantec у вересневому звіті, в якому попереджали, що просунуті хакери проникли в системи, які контролюють операції деяких американських і європейських енергетичних компаній…» ***(США попередили енергетичні компанії про хакерські атаки // Високий замок online (http://wz.lviv.ua/news/209008-ssha-poperedyly-enerhetychni-kompanii-pro-khakerski-ataky).- 22.10.2017).***

***

«Россия и Китай намерены рассмотреть вопросы создания доверенного телекоммуникационного оборудования, способного противостоять возможным кибератакам извне. Об этом вице-премьер РФ Дмитрий Рогозин сообщил по

итогам 21-го заседания Российско-китайской комиссии по подготовке регулярных встреч глав правительств…

Рогозин добавил, что Россия прекрасно понимает, что "если идет такая волна критики абсурдной, доведенной до идиотизма со стороны США по поводу якобы российского кибервмешательства, это [реализуется] известная формула "держите вора!".

"Тот, кто больше всего кричит, что якобы на него напали, что-то у него украли, собственно говоря и готовится к такого рода кибератакам, - заметил зампред российского правительства. - Мы делились этой информацией с нашими китайскими коллегами, делились информацией о количестве киберпроисшествий против Китая и против России, и считаем, что в рамках БРИКС есть все основания эту тему поднять и создавать систему защиты критически важной инфраструктуры» ***(Рогозин: РФ и КНР обсуждают создание системы киберзащиты критически важной инфраструктуры // ТАСС (http://tass.ru/ekonomika/4686672).- 30.10.2017).***

***

Кіберзлочинність та кібертероризм

«В современном мире предприятия и государственные учреждения работают в динамичной информационной среде, где характер киберугроз постоянно изменяется, следовательно, должны меняться и методы защиты от них…

…О современном ландшафте угроз и методах противодействия, защите от целенаправленных атак на государственные органы и крупный бизнес (Deep Discovery), инструментах и партнерских программах шла речь на конференции Security TRENDs – 2017, которая проходила в Киеве в конце сентября. Участниками конференции стали представители ведущих заказчиков и ИТ-бизнеса страны, которым был представлен самый полный обзор проблем в области кибербезопасности и современных решений для защиты информационных систем предприятий…

Кибератаки на информационные системы и сервисы сегодня входят в число пяти наиболее существенных рисков, с которыми сталкивается мировой бизнес. Только одна успешная атака приносит злоумышленникам в среднем $5,9 млн, при этом, по данным исследования The Global State of Information Security Survey, 63 % профессионалов в области кибербезопасности уверены: атака на системы их предприятий – лишь вопрос времени. В 2016 году было зафиксировано 82 млрд атак, а число новых семейств программ-вымогателей выросло на 750 %.

Ключевые спикеры Security TRENDs отметили, что наиболее привлекательными для киберпреступников сегодня становятся сложные корпоративные сети, облачные системы и виртуальные среды, а также пользовательские устройства, в том числе мобильные. Это обстоятельство требует внедрения специальных средств защиты, направленных на предотвращение

вмешательства в работу корпоративных систем на наиболее уязвимых направлениях...» ***(На конференции Security TRENDs – 2017 рассказали об инновациях в сфере кибербезопасности // hi-Tech.ua (https://hi-tech.ua/na-konferentsiys-security-trends-2017-rasskazali-ob-innovatsiyakh-v-kiberbezopasnosti/).-13.10.2017).***

***

«…The New York Times выпустила статью о северокорейских хакерах, которые становятся новыми террористами. Публикуем сокращенный перевод материала.

По словам сотрудников безопасности США и Великобритании, в кибермармии Северной Кореи работает более шести тысяч хакеров, которые крадут сотни миллионов долларов и устраивают в мире хаос. Сейчас внимание западных аналитиков сосредоточено на ядерной программе страны, и многие недооценивают ее киберпотенциал. Инфраструктура Северной Кореи неплохо защищена от ответных кибератак, кроме того ее хакеры в основном действуют за пределами страны, так что санкциями их не остановить…

По сообщениям разведки, ежегодно Северная Корея зарабатывает сотни миллионов долларов благодаря программам-вымогателям, грабежам цифровых банков, взлому аккаунтов в видеоиграх и криптовалютных бирж Южной Кореи. Представитель руководства британской разведки сообщил, что кибератаки приносят стране около миллиарда долларов в год, то есть одну треть от своих объемов экспорта…

…Недавний анализ агентства по кибербезопасности Recorded Future показал, что основная активность корейских хакеров исходит из Индии, Малайзии, Новой Зеландии, Непала, Кении, Мозамбика и Индонезии…

В августе 2012 года иранские хакеры атаковали нефтяную компанию Saudi Aramco, заразив вирусом около 30 тысяч ее компьютеров и 10 тысяч серверов. Вирус удалил все данные и оставил вместо них часть изображения с горящим флагом США. Через полгода хакеры из Северной Кореи провели похожую атаку из Китая, заразив компьютеры трех главных банков и двух крупнейших телеканалов Южной Кореи.

Возможно, корейские хакеры просто скопировали модель иранцев, но специалисты полагают, что Иран, скорее всего, помогает Северной Корее, пишет The New York Times.

…Главная задача корейских хакеров — защитить образ 33-летнего лидера страны Ким Чен Ына. В августе 2014 года они атаковали британский телеканал Channel Four, после того как тот сообщил, что снимет сериал о британском ученом, которого взяли в плен в Пхеньяне для разработки ядерного оружия.

Сначала корейцы обратились к британскому правительству, назвав сериал «скандальным фарсом». Жалобу проигнорировали, после чего власти обнаружили, что корейские хакеры смогли проникнуть в систему телеканала. Кибератаку подавили до того, как она нанесла какой-либо ущерб, а представители канала пообещали продолжить съемки сериала…

В сентябре 2014 года корейские хакеры проникли в сеть Sony, но сама компания и американские спецслужбы этого не заметили. 24 ноября корейцы начали кибератаку на Sony… Вредоносный код уничтожил 70% информации на компьютерах и ноутбуках Sony Pictures…

Затем Северная Корея решила заработать на своих кибератаках, и под удары попали онлайн-банки. В октябре 2015 года хакеры атаковали Филиппины, в конце того же года — банк Tien Phong во Вьетнаме и Центральный банк Бангладеша. Кибератаки стали еще более изощренными: например, на сайте финансовой инспекции Польши появилась вредоносная программа, которая заражала компьютеры определенных пользователей — сотрудников банков Польши, Бразилии, Чили, Эстонии, Мексики, Венесуэлы и даже США…

Американские эксперты опасаются, что в нарастающей кибервойне с Северной Кореей противник может применить не только кибероружие, но и ядерное. На данный момент непонятно, кто же руководит кибератаками со стороны Северной Кореи…» ***(Вероника Елкина. The New York Times: На Северную Корею работает 6 тысяч хакеров // Rusbase (https://rb.ru/story/korean-cyberarmy/).- 25.10.2017).***

***

«…Верховный суд Испании удовлетворил запрос американских властей на экстрадицию гражданина России Петра Левашова в США, где ему предъявлены обвинения в хакерстве, в том числе в управлении мощным ботнетом. На обжалование решения суда у россиянина есть три дня…

Напомним, 36-летний Левашов был задержан в апреле 2017 года в Испании, где проводил отпуск. В США против россиянина выдвинуты обвинения по восьми пунктам. В частности он обвиняется в управлении ботсетью Kelihos, насчитывающей свыше 100 тыс. инфицированных систем и использующейся киберпреступниками для распространения вредоносного ПО, программ-вымогателей, фишинговых писем и пр. Прокуратура требует для Левашова наказания в виде 52 лет лишения свободы, однако сам обвиняемый свою вину отрицает…» ***(Испанский суд решил выдать русского «спам-короля» властям США // SecurityLab.ru (https://www.securitylab.ru/news/488852.php).- 04.10.2017).***

***

«В ходе расследования утечки данных клиентов бюро кредитных историй Equifax исследователи безопасности из компании Mandiant выявили, что утечка оказалась масштабнее, чем предполагалось ранее. Если до этого речь шла о 143 млн человек, то теперь общее число затронутых клиентов составляет 145,5 млн человек.

В ходе утечки хакерами была похищена конфиденциальная информация, в том числе адреса, даты рождения, номера телефонов и номера социального страхования…

В причастности к атаке подозревают китайских хакеров… В общей сложности хакеры установили порядка 30 бэкдоров. Один из них, China Chopper, широко используется китайскими хакерами.

В ходе анализа трафика иследователи обнаружили, что группировка, изначально взломавшая Equifax, не смогла обойти межсетевые экраны компании, и оперативно передала эстафету более опытной команде. Вторая группировка использовала специальные средства туннелирования для обхода межсетевых экранов, анализа и взлома одной базы данных за другой… Высокий уровень организации может говорить о причастности хакеров, предположительно связанных с армией и правительством КНР, отмечают эксперты» ***(Стали известны новые подробности утечки данных Equifax // SecurityLab.ru (http://www.securitylab.ru/news/488837.php).- 03.10.2017).***

***

«Россия может быть причастна к хакерским атакам на телефоны военных НАТО, которые расквартированы в странах Прибалтики…

По мнению чиновников, …цель взлома смартфонов — сбор оперативной информации, измерение силы войск НАТО и запугивание солдат.

Чиновники уверены, что координация хакерских атак проводится на "государственном уровне", а для их осуществления используют оборудование, недоступное большинству гражданских лиц, в том числе дроны и установленную на них технику для слежки.

По словам одного из военных НАТО, который находится в Польше с июля, он нашел свой айфон "взломанным". У хакера, который это сделал, был российский IP-адрес, утверждает военнослужащий…

Еще несколько его сослуживцев также пожаловались на "странные вещи", которые происходят с их телефонами.

Неподалеку от места расположения сил НАТО в Польше находится российская военная база.

По мнению экспертов по кибербезопасности, российские военные могут получить доступ к телефонам солдат НАТО с целью установить, есть ли разница между официально заявленным количеством расквартированных военных альянса и их реальным числом.

Накануне стало известно, что Министерство обороны России изучило код системы ArcSight, которая лежит в основе кибербезопасности большинства подразделений американской армии» ***(WSJ узнала о подозрениях НАТО в хакерской атаке России на телефоны военных // Каспаров.Ru (http://www.kasparov.ru/material.php?id=59D4D23FC45CE).- 04.10.2017).***

***

«Провайдер предоставил ФБР журналы активности мужчины, подозреваемого в киберпреследовании…

Речь идет о деле Райана Лина (Ryan Lin), 24-летнего мужчины из штата Массачусетс (США), обвиненного в киберпреследовании 24-летней женщины Дженнифер Смит (Jennifer Smith, имя изменено) в период с апреля 2016 года и вплоть до его ареста 5 октября 2017 года.

Согласно материалам следствия, женщина подверглась многочисленным хакерским атакам, угрозам и случаям кибersталкинга после того, как Лин стал ее

соседом по квартире. Следователи полагают, что Лин получил доступ к профилям Смит на ряде ресурсов, а также к учетной записи в Apple iCloud и на Google Диске. Для того чтобы скрыть свою личность, подозреваемый использовал ProtonMail, VPN-сервисы и Tor.

После почти года расследования местная полиция обратилась в ФБР за помощью. Агенты бюро обнаружили первые доказательства вины подозреваемого у одного из бывших работодателей Лина. После того, как он уволился, компания переустановила рабочий компьютер Лина, однако ФБР смогло найти различные свидетельства, показывающие, что подозреваемый использовал VPN для преследования.

Тем не менее, самые убедительные доказательства появились после того, как ФБР удалось получить журналы активности Лина от двух VPN-провайдеров - PureVPN и WANSecurity. Журналы показали, как один и тот же IP-адрес VPN подключился к двум почтовым ящикам Gmail, принадлежащих Лину, один из них был настоящим, а другой использовался для угроз. Также следователям удалось выявить учетную запись на сайте Rover.com, созданную Лином для того, чтобы получить номер телефона Смит. Позднее PureVPN смог связать преступную деятельность Лина с его домашним и рабочим IP-адресами…» ***(VPN-провайдер предоставил ФБР журналы активности для поимки киберпреступника // SecurityLab.ru (http://www.securitylab.ru/news/488966.php).- 09.10.2017).***

***

«Disqus – досить зручна форма для коментування статей і більшість сайтів її вже давно підключили. Але, як стало відомо, конфіденційну інформацію про користувачів атакували хакери…

Витік даних торкнувся таких відомостей, як імена користувачів і пов’язані з ними адреси електронної пошти, датовані ще 2007 роком. Також хакерами був отриманий доступ до інформації про дати приєднання до сервісу і останньої авторизації, яка зберігалася в звичайному текстовому вигляді і торкалася 17,5 млн користувачів…

Як відзначають у компанії, про витік стало відомо лише в минулий четвер, коли фахівець з питань кібербезпеки Трой Хант повідомив компанію про те, що він отримав у своє розпорядження копію інформації. Після цього протягом 24 годин компанія усунула уразливість, почала розсилати повідомлення постраждалим користувачам і примусово скинула їхні паролі…» ***(Грицина Вікторія. Компанію Disqus було атаковано хакерами // Pingvin.Pro (https://pingvin.pro/gadgets/news-gadgets/kompaniyu-disqus-bulo-atakovano-hakeramy.html).- 10.10.2017).***

***

«В результаті хакерської атаки на системи інтернет-гіганта Yahoo в 2013 році було викрадено особисті дані всіх 3 млрд користувачів, зареєстрованих на сервісах цієї компанії…

…в інтернет-компанії вважали, що злом торкнувся близько одного млрд облікових записів. Але розслідування виявило, що масштаби хакерської атаки були значно більше.

У 2016 році компанія Yahoo повідомила про дві масові крадіжки даних своїх користувачів. Крім кібератаки в серпні 2013 року, в компанії зафіксували ще один схожий епізод: в кінці 2014 року хакери зламали не менше 500 млн акаунтів Yahoo.

В одному з зломів звинувачують співробітників ФСБ РФ.

В обох випадках зловмисники могли отримати доступ до імен, адрес електронної пошти, телефонних номерів, дат народження та іншої інформації. Хакери зуміли також дістатися до зашифрованих і незашифрованим перевірочних питань і відповідей, які використовуються при відновленні забутого пароля…» ***(У 2013 році через кібератаку були викрадені дані трьох млрд користувачів Yahoo // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1691155-u-2013-rotsi-cherez-kiberataku-buly-vykradeni-dani-trokh-mlrd-korystuvachiv-yahoo).- 04.10.2017).***

***

«За шесть месяцев 2017 года в мире произошла утечка 7,78 млрд записей с персональной и платежной информацией, что почти в восемь раз выше показателя за аналогичный период 2016 года (1,06 млрд записей). Соответствующие данные приводятся в отчете компании InfoWatch…

Больше всего информации (98%) было потеряно в результате крупных кибератак, уточнили в InfoWatch. За полгода компания зафиксировала 20 хакерских атак, в результате которых злоумышленники получили более 10 млн записей конфиденциальных данных… По мнению аналитиков, на увеличение числа утечек влияют новые возможности, связанные «с использованием информации в цифровом мире»: перевод услуг в электронный вид, e-commerce (электронная коммерция), электронные деньги, а также объекты исключительных прав (интеллектуальная собственность) в цифровом виде…

Чаще всего от утечек информации страдали медучреждения (17,4%), госорганы (15,2%) и организации из торговой отрасли (12,2%). По количеству скомпрометированных записей лидируют ИТ-компании (33,9%), торговые предприятия (20,2%) и госорганы (15,8%)…

InfoWatch уточняет, что отчет компании охватывает не более 1% всех утечек данных, так как основан на анализе публичной информации…» ***(Объем утечек конфиденциальных данных в мире за год увеличился в восемь раз // АО «Коммерсантъ». (https://www.kommersant.ru/doc/3434638).- 10.10.2017).***

***

«Расположение ключевых военных и стратегических объектов инфраструктуры, электростанций, а также план совместных действий войск США и Южной Кореи на случай войны с КНДР — все эти засекреченные данные оказались в руках северокорейских хакеров… Кража документов произошла еще год назад, но южнокорейские специалисты до сих пор выясняют, какие именно данные оказались в распоряжении КНДР…

Хакерская атака произошла еще в сентябре прошлого года. Однако известно о ней стало только сейчас. О случившемся изданию рассказал один из депутатов парламента Южной Кореи и представитель правящей в стране Демократической

партии Ли Чхоль Хи. Ссылаясь на данные официальных лиц военного ведомства, господин Хи заявил, что общий объем украденных документов составил 235 Гб. Причем содержимое 80% документов еще предстоит установить. В Министерстве обороны страны появившуюся информацию комментировать отказались…» ***(КНДР украла военные документы США и Южной Кореи // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3434811).- 10.10.2017).***

***

«Хакеры взломали широко распространенный международный стандарт безопасности Wi-Fi - протокол шифрования WPA2…

Как сообщили эксперты подразделения Национального управления кибербезопасности США (US-CERT), в WPA2 есть "несколько ключевых уязвимостей, связанных с управлением", которые в свою очередь "будут затронуты большинство или даже все операции с применением стандарта".

В результате такой уязвимости хакеры смогут перехватывать информацию, которую пользователи сети интернет передают посредством протокола Wi-Fi...

Эксперты по кибербезопасности поясняют, что сотни миллионов как частных, так и публичных Wi-Fi-роутеров, стали уязвимы для взломщиков. Тем, кто заботится о безопасности своей информации, эксперты безопасности советуют использовать HTTPS-соединения для посещения различных сайтов и подключения к интернет-сервисам». ***(Стало известно о глобальном взломе протокола безопасности Wi-Fi // Апостроф (https://economy.apostrophe.ua/news/transport-i-svjaz/2017-10-16/stalo-izvestno-o-globalnom-vzlome-protokola-bezopasnosti-wi-fi/110342).- 16.10.2017).***

***

«Президент компанії Microsoft Бред Сміт заявив, що уряд Північної Кореї несе відповідальність за створення комп'ютерного вірусу WannaCry, який атакував всесвітню мережу на початку цього року…

"Я думаю, що на цьому етапі всі, хто уважно слідкує за подіями, знають, що WannaCry був створений Північною Кореєю за допомогою кіберінструментів чи зброї, що була викрадена з Агентства національної безпеки Сполучених Штатів", - зазначив Б.Сміт…

Голова Microsoft також відзначив, що кібератаки з боку держав стали частішими та більш суворими…» ***(Саша Картер. Президент Microsoft назвав КНДР відповідальною за створення вірусу WannaCry // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1693184-prezydent-microsoft-nazvav-kndr-vidpovidalnoiu-za-stvorennia-virusu-wannacry).- 15.10.2017).***

***

«21 жовтня, напередодні спеціального засідання уряду щодо обмеження автономії Каталонії, хакери зламали сайт Конституційного суду Іспанії…

Сайт суду припинив роботу після масових DDoS-атак, відповідальність за здійснення яких взяло на себе з угруповання Anonymous.

Хакери оголосили у мережі про запуск «Компанії за звільнення Каталонії», у межах якої вони анонсували інші акції впродовж 21 жовтня – у день, коли іспанський уряд планував запустити процес обмеження автономії провінції Каталонія, яка прагне стати незалежною.

Напередодні, 20 жовтня, Департамент внутрішньої безпеки Іспанії у Twitter підтвердив початок такої хакерської кампанії, зазначивши, що протягом останніх тижнів сторінки державних органів зазнали інших кібер-атак.

Раніше на відеохостингу Youtube з акаунту AnonymousVideos було опубліковано ролик, де йдеться про початок «Операції "Каталонія"» (#opCatalunya)…» ***(Сайт Конституційного суду Іспанії зламали напередодні обговорення урядом каталонського питання // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/sayt_konstitutsiynogo_sudu_ispanii_zlamali_naperedodni_obgovorennya_uryadom_katalonskogo_pitannya/).- 23.10.2017).***

***

«Хакеры Anonymous продолжили атаковать правительственные сайты Испании, протестуя против действий местных властей, желающих урегулировать кризис в Каталонии.

…был атакован веб-ресурс печатного органа правительства Испании Boletín Oficial del Estado (BOE)…

Сайт был атакован хакерами примерно в то же время, когда там был опубликован документ о том, что испанский парламент одобрил меры по урегулированию кризиса в Каталонии согласно со статьей 155 Конституции Испании, которая при необходимости дает возможность приостанавливать автономию региона…» ***(Сайт официальной газеты испанского правительства атакован Anonymous // SecureNews (https://securenews.ru/catalonia/).- 30.10.2017).***

***

«Лаборатория Касперского» обнаружила ПО для кражи денег из банкоматов, свободно продающееся в Даркнете. Оно дает злоумышленникам возможность получить деньги из банкомата в случае физического доступа к устройству. Цена такой программы на одной из закрытых сейчас площадок составляла 5 тыс. долл…

Программа была обнаружена 27 марта 2017 года. Однако «Лаборатория Касперского» выяснила, что ее самые ранние образцы были известны сообществу по кибербезопасности еще с июня 2016 года. В то время он был загружен в Сеть на территории Украины, впоследствии загрузки осуществлялись также из других стран. Кто стоит за этим вредоносным кодом, до сих пор неизвестно.

Программа не требует от злоумышленников практически никаких существенных знаний и навыков в области информационных технологий, что создает новую угрозу для финансовых организаций, считают эксперты. Для защиты от таких угроз они рекомендует по умолчанию запретить запуск любой неавторизованной программы в системе банкомата, ограничить возможности соединения с неавторизованными устройствами и установить специализированное защитное ПО» ***(«Лаборатория Касперского»: в Сети можно купить ПО для***

кражи денег из банкоматов // «Открытые системы» (https://www.computerworld.ru/news/Laboratoriya-Kasperskogo-obnaruzhila-v-Darknete-PO-dlya-krazhi-deneg-iz-bankomatov).- 19.10.2017).

***

«У Польщі зросла кількість кібератак на інституції. Про це повідомив міністр оборони Польщі Антоні Мацеревич…

«Якщо мова йде про останні півроку, більш-менш раз на тиждень маємо справу зі посиленими, істотними атаками на кібербезпеку чи самого міністерства, чи ширше – різних інституцій також в Польщі. Деякі з цих загроз мають характер загальноєвропейський, навіть всесвітній», – сказав Мацеревич.

Повідомляється, що останнім часом кіберзлочинці намагалися "хакнути" комп'ютери Міністерства оборони Польщі…» ***(Яна Козиряцька. У Польщі повідомили про збільшення кількості кібератак // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1693726-u-polshchi-povidomyly-pro-zbilshennia-kilkosti-kiberatak).- 18.10.2017).***

***

«Експерти ESET виявили перший шифратор з функцією блокування екрану, атакуючий смартфони та планшети на базі Android. За розблокування пристрою шкідлива програма вимагає заплатити 0,0130 біткоіни (більше 70 доларів).Оплата повинна бути здійснена протягом 24 годин. Якщо викуп не буде перерахований, дані залишаться зашифрованими. Шифратор DoubleLocker побудований на базі мобільного банківського трояна для Android-пристроїв. Проте, у нього відсутні функції, призначені для збору банківських даних користувачів… DoubleLocker поширюється переважно під виглядом Adobe Flash Player через скомпрометовані сайти...» ***(Android почав атакувати новий вірус // BusinessUA.Com (http://businessua.com/telekom/38850android-pochav-atakuvati-novii-virus.html#).- 18.10.2017).***

***

«Фейкові повідомлення про запобігання замаху на президента України Петра Порошенка, які невідомі зловмисники розповсюджували від імені прес-центру СБУ, розсилалися з румунських ір-адрес…

В СБУ підтвердили цю інформацію, повідомивши, що лист було відправлено з "сусідніх країн".

"Служба безпеки України спростовує інформацію, яка увечері 23 жовтня була нібито розповсюджена з електронної пошти прес-служби. Фейкове повідомлення про попередження СБУ замаху на Президента України, було надіслано з однієї з сусідніх країн з пошти anonymousemail@orbit.eternalimpact.info з підміною справжньої адреси прес-служби відомства. Жодних фактів зламу офіційних поштових та веб ресурсів СБ України не зафіксовано", - повідомили у відомстві» ***(Стало відомо, звідки розсилалося фейкове повідомлення про замах на Порошенка // ТСН.ua (https://tsn.ua/nauka_it/stalo-vidomo-zvidki-rozsilalosya-feykovoe-povidomlennya-pro-zamah-na-poroshenka-1020285.html).- 23.10.2017).***

***

«По наблюдениям ИБ-экспертов, киберпреступники развернули активный поиск слабых приватных ключей SSH на тысячах серверов с веб-сайтами на WordPress. Ежедневно злоумышленники прочесывают около 25 тыс.ресурсов.

«Наше внимание привлекла жалоба клиента, который мониторил свой трафик в реальном времени и увидел, что кто-то сканирует его на наличие SSH-ключей, — сообщил Threatpost Марк Мондер (Mark Maunder), генеральный директор WordFence. — Мы проверили собственные ловушки для хакеров (honeypot) и обнаружили, что случай не единичный: ежедневно сканируется около 25 тысяч систем»…

Злоумышленники анализируют серверы по ключевым словам root, ssh или id_rsa в надежде найти веб-каталоги с приватными ключами SSH, по ошибке хранящиеся в свободном доступе…

«Сканирование общедоступных каталогов на наличие приватных ключей SSH — далеко не новая техника. Но наблюдаемый всплеск активности вызывает опасения», — сообщил Джастин Джетт (Justin Jett), руководитель контрольно-ревизионного отдела Plixer.

По мнению Джетта, очень немногие компании следуют надлежащим практикам безопасности SSH. И это весьма опасно, поскольку, в отличие от цифровых сертификатов с ограниченным сроком годности, ключи SSH действуют постоянно, а пароли пользователи меняют редко…

…специалисты Venafi также отметили рост числа сканирований SSH-ключей как в общедоступных каталогах, так и в Git, SVN (или Subversion) и других репозиториях.

Несмотря на то, что приватные ключи нельзя хранить в общедоступных каталогах, администраторы слишком часто забывают за этим следить и публикуют в Сети как общедоступные, так и приватные ключи…» ***(Tom Spring. Новая волна атак на SSH-ключи // Threatpost (https://threatpost.ru/hackers-take-aim-at-ssh-keys-in-new-attacks/22924/).- 23.10.2017).***

***

«ФБР призывает организации, ставшие жертвами DDoS-атак, сообщать о подробностях этих инцидентов…

Пострадавшим следует обращаться в местные отделения ФБР независимо от масштабов атаки и финансовых последствий для организации… ФБР просит компании сохранять IP-адреса, связанные с атакой, сетевой трафик и журналы захвата пакетов, а также электронные письма и любые другие сообщения преступников.

Помимо этого, правоохранителей интересуют подробности любых понесенных в результате атаки потерь и, если компания заплатила выкуп, номер криптокошелька или адрес электронной почты, использованные для перевода денег.

Данная просьба ФБР входит в более масштабное предупреждение, адресованное предприятиям в связи распространением нагрузочных бутер- и стрессер-сервисов, часто выступающих в роли ключевого звена DDoS-атаки.

Эти сервисы продаются преступникам и хактивистам на теневых форумах и служат для автоматизации и повышения мощности атак…

В отдельном заявлении ФБР предупреждает, что в связи с прогнозируемым ростом числа IoT-устройств с 20 до 50 млрд к 2020 году угроза DDoS-атак через них станет еще более актуальной.

Все больше опасений вызывает возможность взлома подключенных медицинских устройств, систем автоматизации зданий, «умных домов» и других подключенных к Интернету бытовых устройств, способных повлиять на физическую безопасность и здоровье человека…

ФБР призывает владельцев таких устройств и их производителей принять ряд мер по защите своих устройств: сменить стандартные имя пользователя и пароль, изолировать IoT-устройства в защищенную сеть и поддерживать актуальность ПО, устанавливая патчи и другие обновления» ***(Michael Mimoso. ФБР просит организации делиться подробностями DDoS-атак // Threatpost (https://threatpost.ru/fbi-asks-businesses-to-share-details-about-ddos-attacks/22913/).- 23.10.2017).***

***

«Check Point Software Technologies в сентябре зафиксировал значительное увеличение числа атак Locky. По результатам Global Threat Impact Index, вымогатель поразил 11,5% организаций во всем мире.

Locky… сентябре 2017 стремительно поднялся, оказавшись на втором месте при помощи ботнета Necurs, который тоже вошел в рейтинг, заняв 10 место...

...Тот факт, что в сентябре каждая десятая организация во всем мире была поражена хотя бы одним видом вымогателей, говорит о том, что существующие вредоносные программы могут быть так же опасны, как и абсолютно новые варианты.

Самые активные зловреды сентября 2017:

- RoughTed — крупномасштабная кампания вредоносной рекламы, используется для переадресации пользователей на зараженные сайты и загрузки мошеннических программ, эксплойт-китов и программ-вымогателей. Зловред может быть использован для атаки на любые типы платформ и операционные системы; способен обходить блокировку рекламы.

- Locky — вымогатель, который начал свое распространение в феврале 2016 года, распространяется в основном с помощью спам-писем, содержащих загрузчик, замаскированный под вложение Word или Zip, которое затем загружает и устанавливает вредоносное ПО, которое шифрует файлы пользователя.

- Globeimposter — вымогатель, замаскированный под шифровальщик Globe ransomware. Был обнаружен в мае 2017 года и распространялся с помощью спам-кампаний, вредоносной рекламы и эксплойт-китов. После шифрования программа добавляет расширение .crypt к каждому зашифрованному файлу.

HackerDefender — пользовательский руткит для Windows, который был третьим по распространенности вредоносным ПО в августе, покинул первую десятку.

Самым популярным вредоносным ПО для атаки мобильных устройств в сентябре стал Triada, который поднялся с третьего места, за ним следуют Hiddad и Lotoor…» ***(Вымогатель Locky снова взлетел в рейтингах вредоносных программ // IKSMEDIA.RU (http://www.iksmedia.ru/news/5446014-Vymogatel-Locky-snova-vzletel-v-rej.html#ixzz4wPdKk1ao).- 23.10.2017).***

***

«Хакеры взломали сайт компании-разработчика Eltima и распространяли зараженные трояном OSX/Proton версии популярных приложений: мультимедийного плеера Elmedia Player и менеджера закачек Folx.

Эксперты ESET обнаружили зараженные приложения на сайте Eltima 19 октября. После предупреждения разработчики устранили угрозу и сообщили о возобновлении раздачи легитимного софта.

– OSX/Proton – троян для удаленного доступа (Remote Access Trojan, RAT), который продавался на подпольных форумах с марта 2017 года. В нем предусмотрены функции для кражи данных, включая информацию о пользователе и операционной системе, список установленных приложений, данные браузеров, номера криптовалютных кошельков, данные связки ключей macOS, сохраненные логины и пароли…» ***(Выявлена кибератака на пользователей Mac // IKSMEDIA.RU (http://www.iksmedia.ru/news/5446070-ESET-vyyavila-kiberataku-na-polzova.html#ixzz4wPegcHT1).- 23.10.2017).***

***

«В Южно-Африканской Республике произошла крупнейшая за всю историю страны утечка данных.

Как сообщает обнаруживший утечку исследователь безопасности Трой Хант (Troy Hunt), миллионы персональных записей о гражданах, имеющих выданный в ЮАР идентификационный номер, оказались в Сети.

"Обычно я каждый день получаю множество файлов, связанных с утечками данных, но в этом файле меня поразил размер – 27 ГБ", – сообщил Хант…

По словам Ханта, южноафриканская утечка является худшей из всех, с которыми он когда-либо сталкивался на разных уровнях. Вероятным источником утечки является южноафриканская компания Dracore Data Sciences, специализирующаяся на сборе и обработке данных..» ***(В ЮАР произошла крупнейшая за всю историю страны утечка данных // "Информационная безопасность" (http://www.itsec.ru/newstext.php?news_id=119246).- 18.10.2017).***

***

«21 октября в ходе подсчета голосов на парламентских выборах хакеры организовали DDoS-атаки на сайты, принадлежащие Центральному статистического управлению Чехии.

Как сообщила пресс-служба ведомства, произошли сбои в работе сайтов volby.cz и volbyhned.cz…

Меры, оперативно принятые ИТ-специалистами, позволил полностью ликвидировать последствия кибератак и восстановить нормальную работу пострадавших сайтов. Хакеры не внесли изменений в результаты подсчета голосов. Также злоумышленники не смогли взломать инфраструктуру, которая применяется для того, чтобы подсчитывать голоса и обрабатывать полученную информацию…» ***(Чешские правительственные интернет-порталы атакованы хакерами // SecureNews(https://securenews.ru/czech/).- 23.10.2017).***

***

«ИБ-эксперты Proofpoint рассказали о возросшей активности кибергруппировки Leviathan, которая распространяет вредоносные программы для кражи конфиденциальной информации у корпораций, работающих в сфере кораблестроения и сотрудничающих с военно-морскими силами…

Киберпреступники воспользовались уязвимостью, которая дает возможность внедрять код для активации скриптов, содержащих команды PowerShell, и устанавливать вредоносные программы. По словам специалистов, киберкампания Leviathan была начата несколько дней спустя выявления этой уязвимости.

Взломав систему, хакеры устанавливали утилиту Orz (Core), которая может выполнять команды, а также осуществлять сбор данных, загрузку и обновление файлов. Кроме того, злоумышленники использовались троянскую программу NanHaiShu, которая дает возможность передавать данные с зараженного устройства на командный сервер…» ***(Военные предприятия в США и странах Европы атакованы хакерами // SecureNews (https://securenews.ru/leviathan/).- 18.10.2017).***

***

«Эксперты из BAE Systems рассказали, что ответственность за кибернападения на тайваньский банк Far Eastern International Bank (FEIB) могут нести хакеры из северокорейской кибергруппировки Lazarus.

Хакеры на минувшей неделе пытались украсть около 60 миллионов долларов у FEIB, но в действительности они похитили не более чем 500000 долларов, поскольку сотрудники банка быстро зафиксировали подозрительные транзакции и смогли вернуть большую часть денег.

Киберпреступники в ходе своих атак пользовались вредоносными программами, имитирующими уведомления о денежных переводах в банковской системе SWIFT. Для взлома системы злоумышленники пользовались различными утилитами, включая редкий вариант вымогательской программы Hermes. Возможно, вымогательская программа применялась для того, чтобы отвлечь внимание банковской службы безопасности от кражи.

Кибератака на FEIB имеет сходство с аналогичными инцидентами в Банках Бангладеш и Филиппин…» ***(Хакеры из КНДР могли украсть у одного из тайваньских банков 60 миллионов долларов // SecureNews (https://securenews.ru/dprk_hackers_5/).- 17.10.2017).***

***

«После кибератаки в 2016 году хакеры могли похитить данные клиентов офшоров на Бермудских островах. Об этом говорится в заявлении юридической консалтинговой компании Appleby Global, обслуживающей клиентов бермудских офшоров…

«После того как были проведены соответствующие мероприятия, а их результаты протестированы командой Forensics (ИТ-компания, занимающаяся, в том числе, вопросами обеспечения кибербезопасности), мы уверены в том, что данные наших клиентов находятся в безопасности", — говорится в сообщении Appleby Global…» ***(Хакеры могли украсть данные клиентов бермудских офшоров // mediahouse (http://mediahouse.com.ua/khakery-mogli-ukrast-dannye-klientov/).- 25.10.2017).***

***

«Шведський суспільний мовник SVT вистежив кіберзлочинців, які блокують комп'ютери в 31 країні, й пізозрює, що вони координуються з Росії…

SVT отримала доступ до бази даних хакерів у результаті витоку інформації.

Телеканал повідомив, що анонімна група хакерів, чия діяльність, імовірно, координується з російського Санкт-Петербурга, розіслала по електронній пошті понад 1,6 млн листів. Вони мали вигляд розсилки від шведської телекомунікаційної компанії Telia і поштового оператора PostNord.

Після переходу за посиланнями, вказаними в листах, комп'ютери користувачів блокуються. За зняття блокування хакери-здирники вимагають викуп.

За даними репортерів, хакери атакували таким чином комп'ютери в 31 країні, зокрема Швеції, Австралії, Польщі, Іспанії, Італії, Туреччині та Індії. Розмір викупу в більшості випадків коливався від 410 до 620 євро. Хакери пропонували перерахувати його в біткоіни...

Телеканал SVT повідомив, що пов'язує кібератаки з Росією через те, що отримане в результаті витоку інформації листування хакерів велося російською мовою. У ньому йшлося про банківські рахунки, заражені комп'ютери та обсяги коштів, які вдалося заробити.

Крім того, SVT стверджує, що використовувана злочинцями «програма шифрування посилає спеціальний ключ на сервер в Росії». IP-адреса, з якого координується діяльність хакерів, також «управляється з підключення в центрі Санкт-Петербурга»…» ***(Телеканал SVT виявив хакерів-здирників, які ймовірно координуються в Росії // MediaSapiens (http://osvita.mediasapiens.ua/web/cybersecurity/telekanal_svt_viyaviv_khakerivzdirnikiv_yaki_ymovirno_koordinuyutsya_v_rosii/).- 30.10.2017).***

***

«26 октября был взломан хакерский форум Basetools.ws, предназначенный для продажи украденной информации банковских карт, персональных данных и спам-утилит. Вследствие взлома в распоряжение злоумышленника попала база данных веб-ресурса, части которой он опубликовал на сайте вместе с требованием выкупа.

Злоумышленник потребовал, чтобы администрация Basetools выплатила выкуп в 50000 долларов, в противном случае угрожая передать данные ФБР, Министерству внутренней безопасности, Министерству юстиции и Министерству финансов США…

Вскоре после того, как появилось сообщение с требованием выкупа, форум Basetools стал недоступен для пользователей…» ***(Хакерский форум Basetools взломан вымогателем, который потребовал выкуп в 50000 долларов // SecureNews (https://securenews.ru/basetools/).- 27.10.2017).***

***

«Как сообщает ресурс The Hacker News, хакеры, известные как n3tr1x и str0ng, взломали официальный блог популярной библиотеки JavaScript – jQuery, которая применяется на множестве сайтов…

Пока что нет никаких свидетельств взлома сервера jQuery. Хакеры лишь изменили внешний вид блога и опубликовали небольшое сообщение.

Вероятнее всего, хакеры взломали аккаунт одного из разработчиков jQuery Ли Силбер с помощью ее пароля, полученного в ходе утечки. Кроме того, нельзя исключать, что хакеры могли заполучить доступ к сайту, используя уязвимость в сервере или в системе WordPress.

Разработчики jQuery удалили сообщение хакеров сразу же после взлома, но пока что не сделали никаких заявлений по данному инциденту» ***(Хакеры взломали блог библиотеки jQuery // SecureNews (https://securenews.ru/jquery_2/).- 27.10.2017).***

***

«С помощью уязвимости в Windows хакеры могут украсть хеши паролей NTLM, не взаимодействуя с пользователем. Воспользоваться уязвимостью достаточно просто, а для проведения атаки не нужно обладать особыми техническими навыками. Необходимо лишь внедрить вредоносный SCF-файл в общедоступный каталог Windows…

Уязвимость выявил исследователь информационной безопасности из Колумбии Хуан Диего. В апреле Диего проинформировал о своей находке Microsoft, которая выпустила соответствующий патч в октябре, предназначенный лишь для Windows 10 и Server 2016. Таким образом, другие версии операционной системы все еще уязвимы…» ***(Пароли Windows могут быть похищены хакерами скрытно от пользователей // SecureNews (https://securenews.ru/windows_2/).- 30.10.2017).***

***

«Израильские эксперты по кибербезопасности сообщают, что компьютерные сети уже начал атаковать новый вирус, до этого неизвестный.

Сам вирус является массивным ботнетом, то есть состоит из отдельных независимых хостов с запущенными ботами…

Новый вирус может влиять на работу не только домашних компьютеров, но и роутеров, веб-камер. Заражённые устройства начинают распространять вирус на всю остальную электронику, когда к ним подключаются другие гаджеты.

Если угрозу не остановить в кратчайшие сроки, вирус погубит весь интернет. Эксперты рекомендуют пользователям отключать неиспользуемую технику, чтобы та не заразилась через интернет-канал…» ***(Новый вирус в состоянии «поломать» весь мировой Интернет // Новости планеты (http://www.planetanovosti.com/news/novyj_virus_v_sostojanii_polomat_ves_mirovoj_internet/2017-10-25-17021).- 25.10.2017).***

***

«Исследователи Cisco Talos обнаружили атаку российских кибершпионов с помощью фишинга, содержащего документы, ссылающиеся на конференцию НАТО по кибербезопасности.

По мнению Talos за атакой стоит российская группа APT28, также известная как Pawn Storm, Fancy Bear, Sofacy, Group 74, Sednit, Tsar Team и Strontium. Их целью стали люди, интересующиеся конференцией CyCon по кибербезопасности, организованной НАТО. APT28, спонсируемые РФ, использовали документы с контентом, скопированным с официального сайта CyCon в качестве приманки…

Информация об обнаруженной атаке была опубликована на сайте центра киберзащиты НАТО: «Информация с нашего сайта была использована с целью заражения пользователей вредоносной программой. Это атака, когда легитимная информация используется для привлечения внимания».

Звучит весьма серьезно, если бы не одно обстоятельство. Участники конференции, на которых была нацелена кибератака, являются экспертами в области кибербезопасности и «велика вероятность того», что они знают, что такое фишинг, вредоносное ПО и т.д. Для такой аудитории рассылки фишинговых писем с документами Word, содержащими макросы, может оказаться недостаточно.

Скорее всего, после приступа веселья, эксперты НАТО по безопасности разрешили выполнение макроса в изолированной среде, чтобы убедиться в загрузке и установке Seduploader…» ***(Российские хакеры из APT28 атаковали экспертов НАТО по принципу «на авось» // ChannelForIT (http://channel4it.com/publications/Rossiyskie-hakery-iz-APT28-atakovali-ekspertov-NATO-po-principu-na-avos-28148.html#).- 25.10.2017).***

***

Хакерська атака за допомогою вірусу «Bad Rabbit»

«..Команда реагування на комп'ютерні надзвичайні події України CERT-UA Державної служби спеціального зв'язку та захисту інформації України повідомляє про початок нової хвилі кібератак на інформаційні ресурси України…

У відомстві відзначили, що фахівці поки встановили поодинокі випадки хакерських атак. Йдеться про міжнародний аеропорт «Одеса» та метрополітен Києва.

Команда CERT-UA закликала українських інтернет-користувачів та власників інформаційно-телекомунікаційних систем та інших інформаційних ресурсів дотримуватися посилених вимог кібербезпеки…

У кіберполіції заявили, що масштабної кібератаки в Україні немає. Над усуненням технічних неполадок, що виникли через дії хакерів, працюють підрозділи кіберполіції, Служба безпеки та Державна служба спеціального зв'язку та захисту інформації…

У спецслужбі вважають, що мета хакерів — порушити штатне функціонування інформаційних систем, що може дестабілізувати ситуацію в країні.

Експерти СБУ дізналися, що хакерська атака може бути здійснена з використанням оновлень, у тому числі загальнодоступного прикладного програмного забезпечення. Механізм її реалізації буде подібним до кібератаки, проведеної в червні 2017 року, коли віруси паралізували значну частину державних та приватних установ…» ***(У Держцентрі кіберзахисту заявили про початок нових хакерських атак в Україні // Racurs.ua (http://ua.racurs.ua/news-96051-u-derjcentri-kiberzahystu-zayavyly-pro-pochatok-novyh-hakerskyh-atak-v-ukrayini).- 24.10.2017).***

***

«Вчора хакери намагалися поширити свою кібератаку на Міністерство інфраструктури, втім воно не постраждало завдяки вчасному попередженню спецслужб

…Коментуючи кібератаку, яка сталася 24 жовтня, міністр інфраструктури Володимир Омелян зазначив, що міністерство у першій половині дня отримало інформацію від спецслужб, що планується кібератака. Тоді у відомстві вирішили на деякий час вимкнути сайти.

За його словами, жодних втрат від нового нападу немає, всі системи працюють стабільно…» ***(Кібератаку в Україні спрямували і проти одного з міністерств // Espreso.tv (https://espreso.tv/news/2017/10/25/kiberataku_v_ukrayini_spryamuvaly_i_proty_odnogo_z_ministerstv).- 25.10.2017).***

***

«Кіберполіції проаналізувала дії вірусу-шифрувальника «BadRabbit», який атакував Україну і Росію 24 жовтня, і виявила в ньому відсилання до культового серіалу «Гра престолів».

…Наприклад, заплановані завдання мають імена трьох драконів з серіалу: Drogon, Rhaegal, Viserion. Раніше подібні послання до популярної фентезійної саги були помічені світовими експертами в складі одного з скриптів, який використовувався для поширення відомого шифрувальника «Locky», — повідомляє кіберполіції…

«Bad Rabbit» для поширення в якості основного вектора використовує ураженні сайти, з яких користувачами завантажувалося фальшиве оновлення «Flash»…

Фахівці СБУ зазначили, що для попередження несанкціонованого блокування інформаційних систем необхідно дотримуватись таких рекомендацій: щоденно оновлювати системне програмне забезпечення, не відкривати вкладення до електронної пошти форматів.doc та.rtf, що надійшли від неперевіреного відправника, дотримуватися загальних правил інформаційної безпеки, зокрема, створювати резервні копії.

…Новий вірус Bad Rabbit вразив у вівторок, 24 жовтня, сервери декількох російських ЗМІ: «Інтерфакс» і «Фонтанка»…

Також хакери атакували кілька державних установ, зокрема системи київського метрополітену, міністерства інфраструктури і аеропорту Одеси…

При завантаженні системи зараженого комп'ютера відбувається активація вірусу. Замість звичного робочого столу користувач бачить чорний екран, на якому червоними літерами написано про шифрування всіх файлів комп'ютера.

Щоб їх розшифрувати, зловмисники просять перейти на onion-адресу (яка індексується тільки за допомогою браузера Tor), де відвідувач отримує номер біткоін-гаманця. На нього зловмисники вимагають перевести 0,05 біткоінів (близько 7 тисяч гривень), щоб дешифрувати файли. На даний момент на біткоіни-гаманець не було переведено жодних коштів…

Співробітник чеської компанії ESET, яка виробляє антивірусне ПЗ, Іржі Кропак в своєму акаунті в Twitter повідомив про те, що вірус поширюється через фальшивий файл оновлення для програми Adobe Flash, яка встановлена практично на кожному комп'ютері з системою WIndows…» ***(У коді нового вірусу Bad Rabbit знайшли імена драконів з «Гри престолів» // Високий замок online (http://wz.lviv.ua/world/209157-kompiuternyi-virus-bad-rabbit-zdiisnyv-nyzku-potuzhnykh-kiberatak).- 26.10.2017).***

***

«Стали відомі подробиці про вірусу Bad Rabbit, який 24 жовтня вразив мережі аеропорту в Одесі, Міністерства інфраструктури та Київського метрополітену

Експерти у сфері кібербезпеки Group-IB з’ясували, що вірус Bad Rabbit використовував для проникнення на комп’ютери підроблені сертифікати американської компанії Symantec, що виробляє програмне забезпечення…

Фахівці з’ясували, що Bad Rabbit — це вдосконалений варіант вірусу Petya, який також шифрує дані жорсткого диска, але використовує нові способи ураження.

Зараження здійснювалося через спеціальний сайт, де користувачам пропонували оновити Flash-плеєр. Цей сайт був пов’язаний із поширенням спаму.

Згідно з оцінками антивірусу ESET, 24 жовтня вірус Bad Rabbit атакував комп’ютери у кількох країнах, а саме в Росії — 65%, Україні — 12%, Болгарії — 10%, Туреччині — 6% і Японії — 4%.

Наразі поширення вірусу зупинено…» ***(Кіберексперти з'ясували нові подробиці про атаку вірусу Bad Rabbit в Україні // Racurs.ua (http://ua.racurs.ua/news-96067-kibereksperty-z-yasuvaly-novi-podrobyci-virusu-bad-rabbit).- 25.10.2017).***

***

«…Кибератаки под условными названиями Locky1024 и BadRabbit, которые произошли в Украине 24 октября, могут оказаться отвлекающим маневром. К такому выводу пришли эксперты компании ISSP…

…Єксперты ISSP Labs сейчас работают над анализом поступивших в лабораторию образцов Locky1024 и BadRabbit. В данный момент они могут с уверенностью сказать, что образец Locky1024 не используется для получения паролей и не распространяется дальше по локальной сети. Это означает, что этот вектор не аналогичен Petya/NotPetya, как поспешно сообщали некоторые эксперты и компании по кибербезопасности.

"Данный вектор атаки может выступать прикрытием для другой, скрытой атаки, которая осталась незамеченной за всеобщим вниманием к шифровальщикам (такая же вероятность существует и по вектору BadRabbit)", - отмечают в ISSP Labs…» ***(Целью вчерашних кибератак могло быть отвлечение внимания // Информационное агентство ЛІГАБізнесІнформ (http://biz.liga.net/all/it/novosti/3714513-tselyu-vcherashnikh-kiberatak-moglo-byt-otvlechenie-vnimaniya-.htm).- 25.10.2017).***

***

«…Центр кибербезопасности «Ростелекома» при появлении первых сообщений о заражениях вирусом Bad Rabbit оперативно оповестил всех клиентов, пользующихся сервисами по информационной безопасности, об угрозе заражения новым вирусом-шифровальщиком и мерах противодействия ему.

В ходе кибератаки Центр кибербезопасности изучал все данные о новом вирусе, принимал технические меры по выявлению попыток заражения клиентов, как в реальном времени, так и ретроспективно… Благодаря круглосуточному мониторингу и комплексу превентивных мер, принятых Центром кибербезопасности, клиенты "Ростелекома" не пострадали от вируса…» ***(«Ростелеком» отразил атаки вируса Bad Rabbit на сети корпоративных клиентов компании // «Коммерсантъ» (https://www.kommersant.ru/doc/3453430?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).- 27.10.2017).***

***

«Комп'ютерний вірус, який раніше цього місяця порушив роботу ряду організацій та установ України, включаючи київське метро та міжнародний аеропорт Одеси, вживав коди, раніше вкрадені з Агентства національної безпеки США (NSA)…під назвою EternalRomance…

Цей протокол переводить дані між комп'ютерами Windows і дозволяє хакерам більш ефективно розповсюджувати коди з однієї ураженої машини до іншої.

Початковий власник EternalRomance NSA втратив контроль за цією важливою технологією в квітні, коли її, якимось чином, викрала група хакерів під назвою «The Shadow Brokers» («Тіньові брокери»)… » ***(Закордонні ЗМІ розповіли про вірус-здирник, який вразив київське метро // Конфликты и законы (http://k-z.com.ua/tekhnologii/44447-zakordonni-zmi-rozpovili-pro-virus-zdirnik-yakiy-vraziv-kiyivske-metro).- 30.10.2017).***

***

«Эксперты Group-IB обнародовали отчет о недавних атаках вымогательской программы Bad Rabbit. Специалисты выяснили, что ответственность за атаки с использованием шифровальщиков Bad Rabbit и NotPetya (Petya.A) несет одна и та же кибергруппировка.

Как утверждают исследователи, код Bad Rabbit был создан на основе NotPetya. Так, в Bad Rabbit есть уникальный функционал вычисления хэша, а также методика распространения программы и удаления журналов…

По словам экспертов, распространение Bad Rabbit осуществлялось с помощью методики drive-by download, а для доставки вредоносной программы применялись сайты популярных российских и украинских СМИ. Кроме того, специалисты обнаружили, что хакеры получили доступ к этим веб-ресурсам в ходе целенаправленной атаки.

…Как утверждают исследователи, целью киберкампании NotPetya, вероятнее всего, являлся саботаж, так как вредоносная программа располагала лишь одним кошельком для выкупа. В ходе киберкампании Bad Rabbit для каждого устройства автоматически создается уникальный ключ, для которого существует отдельный кошелек. Кроме того, в случае с Bad Rabbit использовалось доменное имя, которое ранее фиксировалось в хакерских атаках, осуществлявшихся с целью фишинга и перехвата трафика. Благодаря анализу файлов на Tor-сайте, эксперты выяснили, что этот ресурс был создан еще 19 октября.

Эксперты также обратили внимание на то, что киберкампания была спланирована со всей тщательностью и, вероятнее всего, ее запуск изначально был намечен на 25 октября…» ***(Киберкампании Bad Rabbit и NotPetya организованы одной и той же хакерской груп пой // SecureNews (https://securenews.ru/bad_rabbit_notpetya/).- 27.10.2017).***

***

«По словам экспертов из «Лаборатории Касперского», незначительные операционные ошибки разработчиков Bad Rabbit позволяют некоторым пострадавшим вследствие активности вымогательской программы восстановить файлы без выплаты выкупа.

Основной проблемой является то, что Bad Rabbit не осуществляет удаление теневых копий с инфицированной системы. Вредоносная программа создает копию файла, шифрует ее и удаляет оригинальную версию. В это время все

зашифрованные файлы имеют статус «в работе», а на диске хранятся их копии, которые были созданы сервисом теневого копирования Windows. Теневые копии находятся на диске, пока есть свободное место, то есть в течение неопределенного времени…

Большая часть вымогательских программ стирает теневые копии, чтобы в дальнейшем копии оригинальных файлов нельзя было обнаружить посредством программного обеспечения для восстановления диска. По словам исследователей «Лаборатории Касперского», разработчики Bad Rabbit не внедрили в свою программу функционал удаления теневых копий. Сохранение теневых копий, однако, не является гарантией полного восстановления всех файлов, принадлежащих жертве, но дает возможность получить доступу хотя бы к части зашифрованной информации.

Еще одна ошибка, найденная исследователями, относится к паролям для дешифровки файлов. Bad Rabbit осуществляет шифрование файлов жертв посредством шифрования MFT и подменяет главную загрузочную запись на свой экран загрузки…

Главная загрузочная запись – это код и данные, которые нужны для загрузки операционной системы, размещенные в первых физических секторах на жестком диске или другого носителя информации.

Специалисты «Лаборатории Касперского» получили во время отладки пароль, генерируемый вредоносной программы. Исследователи попытались воспользоваться им после того, как инфицированная система была заблокирована и перезагружена. Пароль сработал, вследствие чего загрузка системы продолжилась. Однако, данная методика дает возможность обходить лишь кастомизированный загрузчик. После загрузки операционной системы файлы остаются зашифрованными…» ***(Обнаружен способ восстановления файлов, затронутых программой Bad Rabbit // SecureNews (https://securenews.ru/bad_rabbit_2/).-30.10.2017).***

***

Протидія зовнішній кібернетичній агресії

«Міжнародна спільнота має об'єднатися у протидії кібервійні, яку ініціювала Російська Федерація.

Про це заявив заступник глави Адміністрації Президента Дмитро Шимків в ході XIII конференції з кібербезпеки, яку проводить Українська група інформаційної безпеки…

За його словами, Україна залишається "експериментальним полігоном" для різних видів кіберзброї та кіберзагроз, щотижня спеціалісти виявляють різні модифікації вірусів. Але Україна вчиться, зазначив Шимків і висловив задоволення проведенням заходів, які серйозно підвищують компетенцію ІТ- фахівців та всіх, хто причетний до кібербезпеки…» ***(Світ має об'єднатися проти кібервійни, розпочатої Росією – Шимків // Укрінформ (https://www.ukrinform.ua/rubric-***

society/2328264-svit-mae-obednatisa-proti-kibervijni-rozpocatoi-rosieu-simkiv.html).- 20.10.2017).

***

«Стів Возняк, співзасновник Apple, і Філіп Циммерман, творець першого програмного забезпечення для шифрування електронної пошти, приїхали в Київ і розповіли, як Україні будувати систему кібероборони, де шукати "білих" хакерів і як зупинити відплив за кордон фахівців з кібербезпеки…

Стів Возняк: «Як Україні захистити свій кіберпростір:

По-перше, зрозуміти, як кіберзлочинці проникають в інформаційну мережу країни, як вони вражають економіку, які наслідки мають ці атаки. Вже потім необхідно формувати підходи для розробки системи захисту…

По-друге, необхідно розподіляти, а не централізувати інформаційні системи. Централізований контроль означає, що можна вразити пункт контролю і тоді можна вразити всю систему…

Чи вплинули російські хакери на вибори президента США?..

Думаю, росіяни це справді зробили. Хакери втручаються у виборчі процеси в усьому світі. З такою точкою зору згодні всі розвідувальні агентства...

Багато людей вважають, що наступною війною буде кібервійна, бо існує дуже багато, так би мовити, кіберзброї. Якщо ми говоримо, що якась країна маніпулює вашою країною, то, звичайно, вона це робить за допомогою такої кіберзброї».

Філіп Циммерман: «…Я із США і ми маємо дещо спільне з Україною: на нас напав уряд Росії. Отже, кібербезпека зараз має в певному сенсі геополітичний вимір.

Ви живете в середовищі, яке має великі загрози з точки зору кібербезпеки. Це означає, що для вас дуже важливо розвивати свої навички в кібербезпекових засобах. Ви повинні розробити власні засоби відбиття кібернападів…

Можу відзначити, що у вас є дуже багато талановитих інженерів. Вам потрібно зібрати їх, щоб привернути до них увагу. Їх також необхідно залучити до розробки кібербезпекової оборони країни.

…Тому у вас є передумови стати в Європі центром компетенції в галузі кібербезпеки…

У США урядові розвідувальні відомства самі займаються заходами з кібербезпеки. Вони не використовують для цього приватний бізнес. Не думаю, що вони наймають співробітників з кола хакерів. АНБ має великий набір спеціалістів, які розвили гарні навички. Більшість з них пов'язана з нападами, а не захистом.

Проте є частина АНБ, яка займається захистом, зокрема, питаннями криптографії. Вони закуповують обладнання, програмні продукти для використання урядовими відомствами…

Вам необхідно формувати пул інженерів і на місцевому рівні розвивати навички з кібероборони. Ви можете взаємодіяти з хакерами з інших країн, особливо з країн Західної Європи. Перед ними стоять ті ж загрози, що і перед вами…» ***(Всеволод Некрасов. Не до жартів. Україна може стати європейським центром з кібербезпеки // Економічна правда (http://www.epravda.com.ua/publications/2017/10/3/629730/).- 03.10.2017).***

***

«Збитки України від кібератак Російської Федерації (РФ) оцінюється в десятки мільйонів доларів. Про це заявив секретар Ради нацбезпеки і оборони України (РНБО) Олександр Турчинов в ході зустрічі з помічником президента США з кібербезпеки Джошем Стайнманом, передає прес-служба РНБО…

Згідно з інформацією прес-служби, Турчинов заявив, що РФ вже четвертий рік веде проти України гібридну війну, одним з елементів якої є кіберагресія…

За його словами, для забезпечення системної протидії кіберзагрозам РНБО України ухвалив стратегію кібербезпеки. У той же час, з метою координації структур, що відповідають за різні аспекти цієї проблематики, створено Національний координаційний центр кібербезпеки при РНБО.

Турчинов підкреслив, що розгортається національна телекомунікаційна мережа і створюється захисний ІТ-контур, який повинен захистити державні інформаційні ресурси і об'єкти критичної інфраструктури…» ***(Збитки від кібератак РФ на Україну оцінюються в десятки мільйонів доларів, – Турчинов // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/zbitki-v%d1%96d-k%d1%96beratak-rf-na-ykra%d1%97ny-oc%d1%96nuutsia-v-desiatki-m%d1%96lion%d1%96v-dolar%d1%96v-tyrchinov.html).- 30.09.2017).***

***

«В Литве в понедельник начались национальные учения "Cyber Shield 2017", в них примут участие около 200 представителей из 50 компаний страны…

Учения, организованные Службой кибербезопасности и телекоммуникаций при Министерстве национальной обороны, будут изучать процедуры Национального плана управления киберинцидентами и развивать взаимодействие между учреждениями и предприятиями.

В первый день маневров представители литовских компаний на уровне руководителей в Вильнюсе будут отрабатывать управление киберинцидентами, согласно созданной в Литве базе кибернетической безопасности.

С 3-4 октября участники маневров разделятся по командам, и приступят к отражению кибератак в специально созданной для учений виртуальной информационной инфраструктуре…» ***(В Литве начались учения по кибербезопасности // Европейская правда (http://www.eurointegration.com.ua/rus/news/2017/10/2/7071731/).- 02.10.2017).***

***

«За период с июня 2014 по сентябрь 2017 активисты Украинских кибер войск заблокировали на счетах террористов из ОРДЛО около 21 миллиона долларов (больше 550 миллионов гривен по нынешнему курсу).

Об этом на своей странице в Facebook сообщил основатель и руководитель Украинских кибер войск Евгений Докукин…

По информации активиста, в общей сложности было заблокировано 490 счетов террористов в гривнах, рублях, долларах, евро и других валютах в десятке популярных платёжных систем…

Среди заблокированных значатся счета в поддержку «Харьковской народной республики», «для помощи народу Донбасса», «одесского подполья» и других…

На сегодняшний день больше всего "похудели" кошельки «ДНР/ЛНР» в WebMoney – 270 кошельков (87 счетов). На втором месте – Яндекс.Деньги (ровно 200 счетов)…» ***(Владимир Кондрашов. Кибервойска заблокировали на счетах террористов полмиллиарда гривен // Internetua (http://internetua.com/kibervoiska-zablokirovali-na-scsetah-terroristov-polmilliarda-griven).- 12.09.2017).***

***

«Служба безпеки України попереджає про підготовку нової хвилі масштабної кібератаки на державні структури та приватні компанії…

За інформацією спецслужби, цілями зловмисників визначені великі державні та приватні компанії, основна метою яких є - порушити штатне функціонування інформаційних систем, що може дестабілізувати ситуацію в країні…

Для попередження несанкціонованого блокування інформаційних систем необхідно дотримуватись таких рекомендацій:

- оновити сигнатури антивірусного ПЗ на серверах і робочих станціях;
- здійснити резервування інформації, що оброблюється на комп'ютерному обладнанні;
- забезпечити щоденне оновлення системного програмного забезпечення, у т.ч. OS Windows усіх без винятку версій» ***(Ілля Жижиян. СБУ попередила про нову масштабну кібератаку в Україні // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1692608-sbu-poperedylo-pro-novu-masshtabnu-kiberataku-v-ukraini).- 12.10.2017).***

***

«НАТО намерена интегрировать потенциал стран-членов по противодействию киберугрозам в структуру командования альянса, заявил генсек НАТО Йенс Столтенберг, …. выступая на заседании Парламентской ассамблеи НАТО в Румынии.

…«Большая часть сил и средств НАТО не является собственностью НАТО, а находится в собственности стран-членов, но у нас есть общие рамки, командование и управление, интегрирующее национальные возможности в совместные рамки НАТО", — заявил Столтенберг…» ***(Александр Панасенко. НАТО интегрирует национальные кибервозможности в свою структуру // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-10-09-3/24319).- 09.10.2017).***

***

«Росія вже втретє здійснила кібератаку на Польщу, яка була успішно відбита. Про це заявив міністр оборони Польщі Антоні Мацєревич…

…За словами міністра, кібератака була здійснена на філіали українських підприємств, які мають також відділення на території інших країн ЄС…» ***(Тетяна Калякіна. Польща відбила чергову кібератаку з РФ // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1692940-polshcha-vidbyla-cherhovu-kiberataku-z-rf).- 13.10.2017).***

***

Анонси заходів з проблем кібербезпеки запланованих у 2017 році

«В седьмой раз в Москве 16-17 ноября 2017 года пройдет конференция по кибербезопасности ZeroNights.

Впервые на ZeroNights будет два ключевых докладчика: … Thomas Dullien/Томас Даллиен (aka Halvar Flake) из Google и Shay Gueron/Шей Герон из Amazon. Томас Даллиен в своем выступлении поднимет тему использования машинного обучения в сфере атакующих исследований («Машинное обучение, атака и будущее автоматизации»), а Шей Герон сосредоточится на проблемах безопасности пользовательских данных в виртуализированной облачной среде («Атаки на зашифрованную память: За пределами одного бита»).

Также мы представляем вам первые несколько докладов основной программы:…

1) Абдул-Азиз Харири, Брайан Горенц, Ясиль Спелман (США, Канада) представят доклад под названием «Во имя всеобщего блага: использование интерфейса RPC VMware для веселья и пользы»…

2) Джеймс Форшоу (Великобритания) выступит с докладом «Использование токенов доступа для обхода системы UAC»…

3) Игаль Гофман и Марина Симаков (Израиль) представят доклад «Вредоносный JIT: использование концепции администрирования «точно в срок» при попытке избежать обнаружения»...» ***(На ZeroNights 2017 – два keynote спикера! // SecurityLab.ru (http://www.securitylab.ru/news/488968.php).- 09.10.2017).***

***

«7 ноября в Киеве состоятся XVII Payments EMA Conference и X Security EMA Conference. Эти две масштабные конференции объединят специалистов по противодействию мошенничеству и киберпреступности, а также профессионалов карточного и платежного рынка стран СНГ и Восточной Европы…

В программе XVII Payments EMA Conference («Платежи и инновации-2017»):

– Уникальный анализ продуктов поставщиков платежных услуг (топ-15 банков)

– Ключевые инициативы в сфере карточных, электронных и мобильных платежей…

В программе X Security EMA Conference («Восточно-европейской Конференции «EMA» по противодействию мошенничеству и киберпреступности – 2017»):

– Итоги 2017 года в сфере кибермошенничества, по данным Ассоциации EMA и European CyberCrime Centre

– Актуальные угрозы для банков и прогноз на 2018 год

– Анализ и примеры логических атак на банкоматы

– Кибератаки: как укрепить безопасность и уменьшить риски

– Социальная инженерия – статистика и результаты Национальной программы содействия безопасности электронных платежей и карточных расчетов Safe Card

– Лучшие практики предотвращения киберпреступлений, алгоритмы эффективного взаимодействия банков и правоохранителей…» ***(В Киеве пройдут две крупнейшие конференции в сфере платежей и кибербезопасности // PaySpaceMagazine «доступно о платежах» (https://psm7.com/event/v-kieve-projdut-dve-krupnejshie-konferencii-v-sfere-platezhej-i-kiberbezopasnosti.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29).- 31.10.2017).***

***

«Конференция "Код информационной безопасности", охватывающая в этом году 5 стран (26 городов), состоится в деловом доме "Петр Столыпин" 9 ноября. К бесплатному участию в конференции приглашаются руководители и специалисты отделов ИТ и ИБ, а также представители СМИ. Специалисты обсудят главные тренды, нюансы управления ИБ, лучшие практики и технологии…» ***(Александр Панасенко. В Тюмени пройдет масштабная конференция по информационной безопасности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-10-30-3/24592).- 30.10.2017).***

***

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

Актуальні питання кримінального процесу очима молодих дослідників : матеріали VIII Всеукр. наук. конф. студентів і аспірантів (Харків, 17 трав. 2017 р.). - Харків : Право, 2017. - 257 с.

Зі змісту:

Степанов А.В. Участь спеціаліста в розслідуванні комп'ютерних злочинів.

Шифр зберігання НБУВ: Ва812493.

***

Бистрова Б.В. Особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки в ВНЗ США / Бистрова Богдана Василівна // Вісник Черкаського університету. Серія : Педагогічні науки. - 2017. - № 6. - С. 15-17.

Розглянуто особливості формування системи професійної підготовки майбутніх бакалаврів з кібербезпеки у ВНЗ США. Проаналізовано інноваційний підхід, що стає в сучасних умовах методологічною платформою для організації дослідницької та проектної роботи студентів. їх наукового спілкування з професійним товариством.

Шифр зберігання НБУВ: Ж69408/пед.н.

***

Добринін І.С. Вдосконалення методики факторного аналізу інформаційних ризиків / І.С. Добринін, Н.О. Мальцева // Системи обробки інформації. - 2017. - Вип. 3. - С. 146-150.

Запроповавано методику оцінки ризиків, яка базується на методиці факторного аналізу інформаційних ризиків з імплементацією до міжнародного стандарту ISO/IEC 27001:2013.

Шифр зберігання НБУВ: Ж70474.

***

Лисенко С.О. Зарубіжний досвід адміністративно-правового регулювання інформаційної безпеки підприємств з точки зору компаративістики / С. О. Лисенко // Наукові праці МАУП. Серія : Юридичні науки. - 2016. - Вип. 4. - С. 35-44.

Досліджено зміст поняття «компаративістика» у контексті адміністративно-правового регулювання інформаційної безпеки підприємств. Визначено основні положення проекту Доктрини інформаційної безпеки України.

Шифр зберігання НБУВ: Ж72223/юрид.

***

Мельник М.О. Аналіз побудови моделі політики інформаційної безпеки підприємства / М.О. Мельник, Г.Д. Нікітин, К.О. Мезенцева // Системи обробки інформації. - 2017. - Вип. 2. - С. 126-128.

Розглянуто основні моделі політик та типів політик інформаційної безпеки. Виявлено особливості організації моделі політики безпеки, яка дозволить захистити дані компанії від несанкціонованого доступу.

Шифр зберігання НБУВ: Ж70474.

***

Мельник М.О. Організація захисту інтернет-ресурсу від несанкціонованого доступу та програмний захист авторських прав / М.О. Мельник, Н.С. Константинова, О.В. Бескупський // Системи обробки інформації. - 2017. - Вип. 2. - С. 122-125.

Проаналізовано платформу для створення як персональних сайтів, так і комерційних порталів – CMS WordPress. Зпропоновано план захисту та індивідуальне програмне рішення з урахіванням виявлених недоліків.

Шифр зберігання НБУВ: Ж70474.

***

Мельник М.О. Організація захисту сайту, створеного на платформі WordPress за допомогою плагіна iThemes Security / М.О. Мельник, Р.В. Дудко, А.Д. Поліщук // Системи обробки інформації. - 2017. - Вип. 2. - С. 118-121.

Доведено, що саме за допомогою плагіна iThemes Security можна подолати будь-які загрози безпеки сайту.

Шифр зберігання НБУВ: Ж70474.

***

Підлісний С.А. Метод підвищення цілісності відеоінформації для інформаційних технологій протидії кібератакам: автореф. дис. ... канд. техн. наук : 05.13.06 / Підлісний Сергій Анатолійович ; Черкас. держ. технол. ун-т. - Черкаси, 2017. - 20 с.

Системно досліджено питання підвищення цілісності відеоінформаційного ресурсу для заданого часу його доставки в умовах дії кібератак. Розглянуто існуючі методи протидії кібератакам. Запропоновано метод підвищення цілісності відеоінформації на основі структурно-ентропійного флотування пари компонент трансформанти.

Шифр зберігання НБУВ: Ра430382.

***

Семенов В.В. До питання боротьби з кіберзлочинністю в Україні / В.В. Семенов, М.С. Дзігора // Прикарпатський юридичний вісник. - 2016. - Вип. 6. - С. 174-178.

Розглянуто заходи, вжиті у законодавчій, інституційній сфері в Україні, напрями науково-криміналістичного забезпечення, які спрямовані на боротьбу з кіберзлочинністю.

Шифр зберігання НБУВ: Ж74200.

***

Традиції та новації юридичної науки: минуле, сучасність, майбутнє : матеріали Міжнар. наук.-практ. конф., 19 трав. 2017 р. : у 2-х т. - Одеса, 2017. - Т. 1. - 2017. - 787 с.

Зі змісту:

Задерейко О.В. Cyberspace and strategy of state cybersecurity;

Логінова Н.І. Захист кіберпростору як фактор безпеки країни;

Трофименко О.Г. Аналіз законодавчої бази щодо забезпечення кібербезпеки України.

Шифр зберігання НБУВ: В356734/1.

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.