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

№ 12 (грудень)

Київ - 2017

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л. Литвинова, 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. – № 12 (грудень) . – 82 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

«…Директор департамента МИД РФ по вопросам новых вызовов и угроз Илья Рогачев назвал Будапештскую конвенцию по киберпреступлениям устаревшей и требующей пересмотра…

По словам Рогачева, принятая в 2001 году конвенция не предусматривает должных мер в отношении современных киберугроз, таких как спамерская деятельность, сетевое мошенничество и ботнеты…

Дипломат также подчеркнул, что одной из основных проблем, не позволяющих России присоединиться к конвенции, является в частности содержание ст. 32, согласно которой участники механизма получают трансграничный доступ к данным другой стороны без необходимости уведомлять власти государства, располагающего соответствующей информацией.

Как заявил Рогачев, данная статья позволяет нарушать фундаментальные гражданские права в отношении личных данных граждан…» ***(Будапештскую конвенцию по киберпреступлениям посчитали устаревшей // SecurityLab.ru (https://www.securitylab.ru/news/490042.php).- 05.12.2017).***

***

Технічні аспекти кібербезпеки

«Исследователи Positive Technologies Марк Ермолов и Максим Горячий на конференции Black Hat Europe в Лондоне рассказали об уязвимости в Intel Management Engine 11, которая открывает злоумышленникам доступ к большей части данных и процессов на устройстве…

Уязвимость затрагивает Intel Management Engine — подсистему, которая с 2015 года встраивается в большинство чипов Intel для обеспечения эффективной работы системы. Intel ME функционирует во время запуска компьютера, его работы и режима сна, обеспечивая практически всю коммуникацию между процессором и внешними устройствами. Таким образом, она располагает доступом почти ко всем данным на устройстве.

Исследователи Positive Technologies обнаружили уязвимость в критически важном модуле Intel ME, эксплуатируя которую злоумышленник может обойти криптографическую и аппаратную защиту. Переполнение буфера в стеке, которое возникает, когда программе приходится записывать объем данным больше допустимого, приводит к риску внедрения зловредного кода. Исследователи нашли способ обойти защиту от переполнения стекового буфера и смогли запустить произвольный код, используя технику Return Oriented Programming…» ***(Уязвимость в микросхемах Intel позволяет злоумышленнику получить контроль даже над выключенным компьютером // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/288711/).- 07.12.2017).***

***

«Американский поставщик решений для шифрования и защиты конфиденциальной информации выпустил патчи для двух критических уязвимостей своих продуктов…

Уязвимость CVE-2017-14377 затронула веб-агенты EMC RSA, которые обеспечивают аутентификацию на сайтах на базе Apache Web Server. Эти программные элементы запрашивают у посетителя SecurID-информацию, передают ее на центральный сервер и, в зависимости от полученного ответа, разрешают или блокируют вход. Как следует из комментария к патчу, если агент отправлял данные по TCP, злоумышленник мог вызвать специфическую ошибку, чтобы получить неавторизованный доступ к веб-ресурсам.

Вторая брешь — CVE-2017-14378 — потенциально представляет более серьезную угрозу, поскольку касается всех приложений, разработанных в SDK агентов аутентификации RSA для C. Проблема была связана с реализацией асинхронного режима TCP, который ускоряет обработку сетевых данных с разным битрейтом — например, при передаче в одном канале текста, голоса, аудио- и видеосигналов. Эта уязвимость также открывала взломщику доступ из-за сбоя механизма обработки ошибок…» ***(Egor Nashilov. RSA исправила критические уязвимости агентов аутентификации // Threatpost (https://threatpost.ru/rsa-patches-for-authentification-tools/23601/).- 06.12.2017).***

***

«Компания HP Inc. устранила уязвимость, позволяющую злоумышленникам превратить код для отладки, случайно оставленный на сотнях моделей ноутбуков, в клавиатурный шпион.

Брешь, связанную с использованием драйвера сенсорной панели Synaptics Touchpad, обнаружил Майкл Минг (Michael Myng)…

Компания HP подтвердила наличие проблемы и выпустила обновление, которое удаляет опасный код, представляющий собой отладчик препроцессора трассировки программного обеспечения Windows (WPP). По данным HP, уязвимость присутствует более чем на 460 моделях ноутбуков, включая модельные ряды EliteBook, HP Pavilion и ZBook…

Обновление программного обеспечения можно скачать на сайте HP. Также оно будет доставляться на компьютеры в составе обновлений Windows…» ***(Tom Spring. Отладчик, забытый на ноутбуках HP, может служить кейлоггером // Threatpost (https://threatpost.ru/leftover-debugger-doubles-as-a-keylogger-on-hundreds-of-hp-laptop-models/23732/).- 13.12.2017).***

***

«Исследователи компании GuardSquare выявили опасную уязвимость ОС Android, которая позволяет злоумышленникам распространять вредоносные приложения под видом легитимных.

Уязвимость, получившая название Janus, распространяется на приложения, в которых реализована первая версия схемы цифровой подписи Android APK. ОС Android, начиная с версии 5.0, использует способ проверки файлов APK и DEX, при котором проверяется не вся цифровая подпись приложения, а лишь

определенная последовательность байтов. Зная об этом, киберпреступники могут подменять легитимные приложения с высоким уровнем привилегий вредоносными, не нарушая цифровой подписи и успешно проходя проверку.

Уязвимость устранена в декабрьском пакете обновлений Google, однако может потребоваться немалое время, прежде чем многочисленные производители Android-устройств выпустят собственные обновления и доведут их до пользователей…» ***(Выявлена новая опасная уязвимость в Android // ООО "ИКС-МЕДИА"(http://www.iksmedia.ru/news/5458445-Vyyavlena-novaya-opasnaya-uyazvimos.html#ixzz51ECwYS90).- 11.12.2017).***

***

«Лаборатория Касперского» представила комплексный сервис активного поиска угроз Kaspersky Threat Hunting, повышающий эффективность защиты от целевых атак.

В комплекс вошли два продукта: услуга круглосуточного наблюдения и реагирования на инциденты Kaspersky Managed Protection и сервис обнаружения целевых атак Targeted Attack Discovery…

Kaspersky Managed Protection – это экспертный сервис проактивного и непрерывного обнаружения сложных угроз, направленных на компанию. Команда аналитиков «Лаборатории Касперского» внимательно изучает данные, собранные установленными в корпоративной сети решениями Kaspersky Endpoint Security для бизнеса и Kaspersky Anti Targeted Attack Platform. В случае выявления каких-либо аномалий эксперты проводят тщательное исследование: изучают поток событий в системе и анализируют поведение подозрительных программ…

В свою очередь, Targeted Attack Discovery – аналитический сервис, направленный на выявление следов целевых атак, которые происходят внутри инфраструктуры компании в текущий момент или были совершены раньше. Эксперты «Лаборатории Касперского» изучают взаимосвязи собранной в корпоративной сети информации с открытыми и частными базами данных по киберугрозам. Этот анализ позволяет выявить подозрительную активность, определить возможные источники инцидентов и скомпрометированные устройства. Сервис также позволяет компаниям получить план действий по устранению последствий инцидента и рекомендации по поддержке информационной безопасности предприятия в будущем…

Сервис Kaspersky Threat Hunting расширяет и дополняет возможности платформы для защиты от целевых атак Kaspersky Anti Targeted Attack Platform…» ***(«Лаборатория Касперского» запустила сервис активного поиска кибератак // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5458608-Laboratoriya-Kasperskogo-zapustila.html#ixzz51EDe3HKQ).- 12.12.2017).***

***

«В программируемых логических контроллерах (ПЛК) производства немецкой компании WAGO обнаружена серьезная уязвимость, позволяющая получить доступ к внутренней сети предприятия, где используются уязвимые ПЛК…

Уязвимость связана с использованием в ПЛК WAGO программы CODESYS Runtime Toolkit 2.4.7.0. Данное встраиваемое ПО от немецкого разработчика 3S-Smart Software Solutions используется несколькими вендорами в сотнях логических и других промышленных контроллерах. Уязвимость в CODESYS Runtime Toolkit была обнаружена несколько лет назад, и в августе нынешнего года компания WAGO была уведомлена о проблеме, однако так и не выпустила исправление…

Поскольку на ПЛК WAGO из серии PFC200 протокол SSH включен по умолчанию, неавторизованные атакующие могут проэксплуатировать уязвимость, переписать содержащий хеши паролей файл etc/shadow и получить на устройстве права суперпользователя…» ***(Уязвимость в ПЛК WAGO ставит под угрозу безопасность корпоративных сетей // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120119).- 06.12.2017).***

***

«ИБ-эксперты из Forcepoint Security выявили новый вариант троянской программой Quant, снабженный функционалом, который дает возможность атаковать кошельки с криптовалютой…

Продажа этой программы осуществляется на русскоязычных хакерских сайтах пользователями, которые известны как DamRaiX и MrRaiX. Quant является загрузчиком, который имеет функционал географического таргетинга, а также может выполнять файлы форматов dll и exe…

По словам специалистов, обновленная версия Quant имеет ряд новых опций. Так, в троянской программе теперь есть различные вредоносные файлы, которые по умолчанию загружаются на инфицированное устройство…

В новом варианте Quant также присутствует функционал спящего режима, позволяющий уклоняться от обнаружения программы антивирусными решениями» ***(Троянская программа Quant может атаковать кошельки с криптовалютой // SecureNews (https://securenews.ru/quant/).- 07.12.2017).***

***

«Эксперты компании Fox-IT представили написанный на Python скрипт, позволяющий восстановить записи в журнале событий, удаленные утилитой eventlogedit на скомпрометированных компьютерах. Eventlogedit является частью предполагаемого хакерского инструмента Агентства национальной безопасности (АНБ) США под названием DanderSpritz, который в числе других программ был выложен в открытый доступ кибергруппировкой The Shadow Brockers в минувшем году…

На самом деле утилита не удаляет или изменяет записи в журнале, а только совмещает их, делая "удаленную" запись частью предыдущей. По умолчанию, DanderSpritz совмещает одну или две "компрометирующие" записи с "чистым" логом. Таким образом при чтении подделанного файла Журнал событий прочитает чистую запись, увидит конечный тег и проигнорирует весь "плохой" контент, пояснили исследователи. Этот ловкий трюк позволяет злоумышленникам скрыть свои действия на скомпрометированных устройствах.

По словам специалистов, разработанный ими скрипт позволит другим исследователям восстановить оригинальные записи и отследить "отпечатки" злоумышленников…» ***(Создан скрипт для восстановления удаленных хакерским инструментом АНБ логов // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120246).- 12.12.2017).***

***

«…Группа ученых из Калифорнийского университета в Сан-Диего — Джо ДиБлазио (Joe DeBlasio), Стефан Сэвидж (Stefan Savage), Джоффри Волкер (Geoffrey M. Voelker) и Алекс Снорен (Alex C. Snoeren) — создали Tripwire, чтобы любой мог отследить взлом своих учетных записей. Для этого утилита заводит аккаунты на одном или более ресурсах, используя один и тот же уникальный email-адрес. Везде устанавливается одинаковый пароль, совпадающий с паролем почтового ящика. Задача Tripwire — регулярно отслеживать входы в почту. Если кто-то проник в специально созданный ящик, значит, взломали одну из привязанных к нему учеток.

В ходе тестового запуска команда зарегистрировалась на 2300 сайтах, использовав более 100 тысяч контрольных email-адресов. По итогам исследования выяснилось, что 19 ресурсов взломали, причем на одном из этих ресурсов зарегистрировано 45 миллионов учетных записей…

Примечательно, что утилита также помогает определить ресурсы, которые хранят пароли в виде открытого текста или кодируют их через слабые алгоритмы шифрования…» ***(Egor Nashilov. Ученые раскрыли утечку на сайте с 45 миллионами учеток // Threatpost (https://threatpost.ru/tripwire-test-run-discovers-19-leaks/23774/).- 15.12.2017).***

***

«Компания Microsoft выпустила обновление пакета MS Office, отключающее функцию Dynamic Data Exchange (DDE) в приложении Word, которая ранее неоднократно эксплуатировалась хакерами для установки вредоносного ПО на компьютеры пользователей.

Протокол DDE используется для обмена информацией между программами пакета Office, которые используют общие данные или общую память…

…В октябре 2017 года эксперты предупредили, что особенности работы протокола DDE могут быть проэксплуатированы хакерами для создания документов, загружающих вредоносное ПО со стороннего сервера. Данный метод может использоваться в качестве замены макросам в атаках с использованием документов. Месяцем позже Microsoft выпустила рекомендации по защите от атак с использованием протокола DDE…

…На этой неделе компания представила обновление Office Defense in Depth Update ADV170021, добавляющее новый ключ в реестр Windows, управляющий статусом DDE в Word. По умолчанию он отключает функцию. Помимо этого, ADV170021 также включает обновления для уже неподдерживаемых версий Word - 2003 и 2007…» ***(Microsoft отключила функцию DDE в Word для предотвращения***

кибератак // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120307).- 15.12.2017).

***

«…Бывший подрядчик американских спецслужб Эдвард Сноуден совместно с другими разработчиками представил приложение, призванное защитить от слежки Android-устройства, в особенности старые и дешевые модели…

…Haven представляет собой мобильное приложение с открытым исходным кодом, работающее по примеру системы видеонаблюдения. Оно использует камеру смартфона, микрофон и акселерометр для определения подозрительной активности и предупреждения пользователя…

Помимо своего прямого предназначения Haven также может выполнять функцию домашней системы безопасности для защиты от грабителей и вандалов…

В настоящее время Haven находится на ранней стадии разработки, и у него есть ряд недостатков. К примеру, для отправки предупреждений ему нужен постоянный доступ к интернету. Кроме того, приложение является весьма энергозатратным и может выдавать ложноположительные результаты» ***(Сноуден представил приложение для защиты Android-устройств от слежки // SecurityLab.ru (https://www.securitylab.ru/news/490508.php).- 25.12.2017).***

***

«…Управление перспективных исследовательских проектов Министерства обороны США (Defense Advanced Research Projects Agency, DARPA) объявило о намерении выделить $3,6 млн на разработку компьютера, аппаратное обеспечение которого станет «неразрешимой головоломкой». Проект, получивший название MORPHEUS, должен стать серьезной альтернативой современному подходу к кибербезопасности, заключающемся в регулярном обновлении ПО.

…MORPHEUS будет быстро и в произвольном порядке «перемешивать» хранящуюся на компьютере информацию…

Согласно DARPA, если убрать некоторые недостатки в аппаратном обеспечении, можно избежать эксплуатации до 40% уязвимостей (ошибки шифрования, инъекции кода, раскрытие информации и пр.)…

Когда атакующий получает доступ к системе, он должен выявить и проэксплуатировать уязвимость в ПО. После успешной эксплуатации ему достаточно определить, где на системе хранятся нужные ему данные, похитить их и скрыться. Как правило, данные всегда находятся в одном и том же месте, поэтому, обнаружив уязвимость и место хранения информации, миссия атакующего наверняка завершится успешно.

Материнские платы MORPHEUS будут в произвольном порядке перемешивать данные, непрерывно меняя их местоположение, поэтому, даже обнаружив уязвимость в ПО, злоумышленник не сможет добраться ни до нее, ни до данных…» ***(Способный перемешивать данные компьютер сделает 40% атак***

бесполезными // SecurityLab.ru (https://www.securitylab.ru/news/490461.php).- 21.12.2017).

***

«…Німецька компанія з області кібербезпеки SYSS змогла обійти захист на старих версіях операційної системи… Windows 10 і на різних пристроях.

SYSS провела досліди на Microsoft Surface Pro 4, на якому було встановлено торішнє оновлення для Windows 10 – Anniversary Update. Проти злому не встояла навіть спеціальна система захисту, яку користувач може активувати при включенні Windows Hello.

Навіть установки останньої версії Fall Creators Update, в якій уразливість системи захисту Windows Hello виправлена недостатньо. Якщо ви налаштовували лицьове розпізнавання на старій версії Windows 10, то ваш комп'ютер уразливий. Тому експерти радять тим, хто користується системою, перейти в параметри ОС і налаштувати розпізнавання обличчя заново.

Для злому потрібна роздрукована на принтері фотографія власника облікового запису, зроблена на інфрачервону камеру…» ***(Владимир Ігор. Windows Hello зламали роздрукованою на принтері фотографією // Pingvin.Pro (https://pingvin.pro/gadgets/news-gadgets/windows-hello-zlamaly-rozdrukovanoyu-na-prynteri-fotografiyeyu.html).- 25.12.2017).***

***

«Пользователь под ником Specter опубликовал в Сети эксплойт под названием namedobj, созданный для обхода защиты Sony PlayStation 4 с версией прошивки 4.05. Как утверждает хакер, программа будет работать на приставке с любым кодом, а также вносить изменения в систему на уровне ядра.

С помощью данной программы пользователи смогут сделать джейлбрейк системы и обойти антипиратскую защиту Sony. Эксплойт также позволит запускать на PlayStation 4 сторонние homebrew-программы, которые не будут нарушать закон об авторском праве.

Стоит отметить, что эксплойт от Specter работает только с версией ПО 4.05. На PlayStation 4 со всеми последующими версиями, а также с последней версией 5.03 код работать не будет» ***(Александр Лазарчук. Хакеры взломали PlayStation 4 // MobiDevices.ru (https://mobidevices.ru/hackers-broke-into-playstation-4).- 29.12.2017).***

***

«…Исследователи из Университета Принстона обнаружили, что они могут сломать HDD, воздействуя на него при помощи аудиоустройства, которое производит звуковые волны на определенной частоте. Звук создает резонансный эффект, который усиливает вибрацию работающего жесткого диска и выводит его из строя...

Поскольку HDD используются во многих устройствах (например, в системах видеонаблюдения, PC, банкоматах и так далее), при должном уровне подготовки хакеры могут провести сокрушительную атаку. Так, в ходе эксперимента

исследователям удавалось вызвать BSOD в PC, а также отключить камеру видеонаблюдения» ***(Basil Naumov. Хакеры научились уничтожать жесткие диски при помощи звука // Game2Day.org (https://game2day.org/news/24857/eksperty-hakery-mogut-unichtojit-hdd-pri-pomoshi-zvuka).- 29.12.2017).***

***

Організаційне забезпечення захисту інформації

«В 2017 году 60% компаний сталкивались с серьезным киберинцидентом.

Всего 15% компаний из нефтегазовой отрасли имеют оформленную программу реагирования на киберинциденты, свидетельствуют результаты исследования, проведенного экспертами британской аудиторско-консалтинговой компании Ernst & Young. Как показал опрос, в котором приняли участие 40 респондентов, хотя вопрос кибербезопасности является приоритетным для предприятий, они более чем когда-либо обеспокоены растущим масштабом и сложностью ландшафта киберугроз.

Согласно результатам опроса, 60% компаний сталкивались с серьезным киберинцидентом, при этом только 17% предприятий считают, что смогут обнаружить сложную кибератаку в будущем. 78% респондентов в числе наиболее вероятных источников атак назвали неосторожных сотрудников, 63% отметили, что не намерены увеличивать бюджет по кибербезопасности после инцидентов, не причинивших никакого вреда.

Причиной 43% значительных утечек стала неосторожность конечных пользователей, ставших жертвами фишинга, следует из отчета. При этом 97% компаний не проводят оценку финансовых последствий от серьезных утечек.

По признанию 87% опрошенных, текущие планы и стратегии их компаний не в полной мере учитывают последствия инцидентов безопасности, как отметили 95% респондентов, реализованные меры кибербезопасности не соответствуют нуждам их организаций.

Согласно оценкам британского аналитического агентства Juniper Research, в течение последующих пяти лет общий ущерб компаний и организаций по всему миру от утечек данных достигнет $8 трлн, в том числе из-за неадекватных мер защиты, реализуемых предприятиями…» ***(Только 15% нефтегазовых компаний имеют программу реагирования на киберинциденты // SecurityLab.ru (https://www.securitylab.ru/news/490337.php).- 17.12.2017).***

***

«Почему непрерывно растут потери от киберпреступников и что с этим делать, пытались разобраться на панельной дискуссии «Эволюция щита и меча», состоявшейся в рамках международного форума Antifraud Russia 2017 по борьбе с мошенничеством в сфере высоких технологий…

«…Мы научились бороться с вирусами, хакерами и предотвращаем попытки мошенничества с высокой эффективностью. Сейчас основную опасность представляет социальная инженерия, на которую приходится 80% всех атак на клиентов», — заявил Сергей Лебедь, глава службы кибербезопасности Сбербанка. По его данным, за 2016 год в МВД зарегистрировано 60 тыс. киберпреступлений. Однако подавляющее число преступников остаются безнаказанными. Только 19% дел было направлено в суд, и 45% из этих дел развалились уже в суде по различным причинам.

За год в «черных списках» Сбербанка накапливается около 50 тыс. записей по мошенникам, но эта информация не востребована правоохранительной системой… …По его мнению, проблема в том, что МВД отказывается заниматься профилактикой преступлений.

«Мы оказываемся на месте преступления, когда в стене безопасности зияет огромная дыра, и наша задача – найти пушку и тех, кто из нее выстрелил. А вот для укрепления стены надо действовать вместе, и эффективность зависит от обмена информацией, но делиться ею желают далеко не все», — принял эстафету Александр Вураско, заместитель начальника отдела БСТМ МВД России…

Как отметил Вураско, масштабные атаки шифровальщиков стали возможными благодаря революции в способах распространения троянов… Любой человек может приобрести в Интернете готовый инструментарий, позволяющий совершать технически сложные преступления. Трояны для банкоматов продаются с видеоинструкцией по использованию, и стоят они около 5 тыс. долл. – вполне подъемную сумму. А если кто-то хочет совершить атаку на мобильные устройства, ему не нужно задумываться о том, как технически это реализовать, — можно арендовать ботнет с «дружественным» интерфейсом…

«Оператор связи может делать очень многое. К сожалению, когда мы продумываем свои мероприятия по борьбе с преступниками и защите клиентов, приходится думать еще и о том, чтобы нас за это в лучшем случае не уволили, а в худшем – не посадили», — высказался Сергей Хренов, руководитель департамента по гарантированию доходов и управлению фродом «МегаФона». Оператор связи может легко блокировать серверы управления клиентской программой, обезвредив все трояны, но не имеет права делать этого: над ним висит дамоклов меч лишения лицензии. Он может делать очень интересные алгоритмы блокировок мошеннических SMS-рассылок, но не имеет права обращаться к текстам сообщений: статья 138 УК РФ предусматривает ответственность за разглашение тайны связи. Есть много нюансов, которые требуется урегулировать на законодательном уровне…

«Мы пытаемся решить сверхзадачу: защитить от мошенничества тех, кто защищаться не хочет. Банки должны работать с клиентами, защищая их, но хотят ли клиенты знать то, что до них хотят донести?», — задался вопросом Алексей Сизов, руководитель направления противодействия мошенничеству компании «Инфосистемы Джет». Большинство людей просто не знают, как устроен процессинг операций по банковским картам, не понимают смысл оказываемых им услуг и их работу на техническом уровне… К сожалению, ни в одном банковском договоре вместе с описанием услуг не указывается список соответствующих

рисков…» (***Николай Смирнов. Борьба с киберфродом: кто виноват и что делать? // «Открытые системы» (https://www.computerworld.ru/articles/Borba-s-kiberfrodom-kto-vinovat-i-chto-delat).- 18.12.2017).***

***

«…Эксперты по кибербезопасности призвали к улучшению образования в сфере ИБ, поскольку из-за острой нехватки специально обученных кадров компании беззащитны перед хакерскими атаками. Согласно недавнему исследованию, проведенному рядом рекрутинговых агентств, 81% опрошенных ожидают увеличение спроса на ИБ-экспертов, однако только 16% считают, что этот спрос будет удовлетворен…

Росту спроса способствовал ряд крупных кибератак, имевших место в нынешнем году… Необходимо как можно скорее восполнить нехватку специалистов, способных противостоять киберпреступности, считает директор по внешним связям Британского компьютерного общества Адам Тилторп (Adam Thilthorpe).

«…Правительство и бизнес должны разработать комплексную стратегию в области образования. Мы должны брать на незаполненные должности больше женщин и этнических меньшинств, а также [переквалифицировать] пожилых работников», - отметил Тилторп» ***(Рекрутеры сетуют на острую нехватку ИБ-специалистов // SecurityLab.ru (https://www.securitylab.ru/news/490533.php).- 20.12.2017).***

***

«…Центр правительственной связи GCHQ (спецслужба Великобритании, ответственная за ведение радиоэлектронной разведки и защиту правительственных каналов связи) заявил, что испытывает проблемы с вербовкой новых сотрудников. Едва ли не все специалисты высокой квалификации, которые требуются для работы в спецслужбах, предпочитают отправлять резюме в Apple, Google или Facebook. Технические гиганты платят специалистам по кибербезопасности в 4-5 раз больше, чем способен предложить GCHQ…

В 2013 году GCHQ предпринимала попытки привлечь специалистов по кибербезопасности гибкой системой поощрений. Однако, это не возымело должного эффекта: карьерному росту они предпочитают несравнимо более высокий заработок. В наборе 2015 года был дефицит сотрудников в размере 22%. В 2016 году на службу поступил 51 новый шпион, но GCHQ обещает, что к 2018 году их будет уже 110. В ближайшие годы количество сотрудников спецслужбы должно увеличиться на 14%, достигнув 6639 человек …» ***(Британских шпионов переманивают на работу ИТ-компании // Finance.ua (https://news.finance.ua/ru/news/-/417862/britanskih-shpionov-peremanivayut-na-rabotu-it-kompanii).- 28.12.2017).***

***

«Итоги года в сфере кибербезопасности в Украине подвели в ходе круглого стола эксперты, представители профильных ассоциаций и государственные чиновники…

Обсуждались законодательные изменения в этой сфере, реальные действия в различных секторах за год, затраты на кибербезопасность в государственном и частном секторах и т.д.

R&D директор компании "IT Интегратор", член Комитета по Кибербезопасности АПКБУ Владимир Кург напомнил о создании Национального координационного центра кибербезопасности летом этого года. Однако, отметил он, информация о деятельности комитета в открытом доступе отсутствует.

При этом позитивом можно считать то, что положения о защите критической инфраструктуры в указанном документе дали толчок для создания отраслевых центров кибербезопасности, в частности, Мининфраструктуры и Укрэнерго.

Директор представительства Cisco в Украине Олег Боднар считает, что за последнее время в данной сфере было сделано больше, чем за 15 - 20 лет…

Операционный директор компании 10Guards, член Комитета по Кибербезопасности АПКБУ Виталий Якушев подчеркнул, что в Украине существуют стандарты комплексной защиты информации, однако они устарели...

По его словам, за законом "Об основных принципах обеспечения кибербезопасности Украины", который должен вступить в силу в мае следующего года, и закрепляет основные понятия в данной сфере, необходимо будет принять еще один нормативный акт, в котором будут определены конкретные направления и действия…

Глава набсовета "Октава Капитал", создатель общественной инициативы "Гражданская кибероборона", глава Комитета Кибербезопасности АПКБУ Александр Кардаков акцентировал внимание на том, что если в направлении государственного сектора определенные шаги предпринимаются в этой сфере, то в отношении остальных секторов экономики позитивных сдвигов нет…» ***(Круглый стол "Итоги года в сфере кибербезопасности. В Новый Год со старыми бедами?" // Информационное агентство ЛІГАБізнесІнформ (http://press.liga.net/releases/kruglyy_stol_itogi_goda_v_sfere_kiberbezopasnosti_v_novyy_god_so_starymi_bedami_/).- 11.12.2017).***

***

«Национальная комиссия регулирования связи Украины (НКРСИ) утвердила новые правила регистрации абонентов операторов мобильной связи. В настоящий момент правила переданы на утверждение в Министерство юстиции…

В августе текущего года украинские власти разработали законопроект, предусматривающий обязательную регистрацию абонентов мобильной связи, а также регистрацию оборудования по международным идентификаторам…

Поданные на утверждение в Минюст правила отводят девять месяцев на подготовку всех технических и административных средств, необходимых для

добровольной регистрации» ***(Украинские власти начали борьбу с анонимностью в мобильных и интернет сетях // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120038).- 01.12.2017).***

***

«Видання The Atlantic заявляє, що є свідчення про ймовірну атаку на енергомережу України…

«Деякі свідчення вже показують, що може готуватися нова атака. Роберт Лі, засновник та керівник компанії з промислової кібербезпеки Dragos розповів, що останніми тижнями він помітив незвичне зростання діяльності в Україні тієї ж групи розробників, які скоїли напад у 2016 році», - йдеться в статті.

За словами Лі, ця група майже не провадила діяльності в Україні з моменту останньої атаки і до листопада…

В The Atlantic зазначають, що, можливо, ця активізація роботи є розвідкою та підготовкою до наступної операції або спробою налякати загрозою хакерської атаки» ***(ЗМІ попереджають про ймовірну кібератаку в Україні // Українська правда (http://www.pravda.com.ua/news/2017/12/18/7165980/).- 18.12.2017).***

***

«Український кіберальянс», який раніше оприлюднював зміст електронної скриньки радника президента Росії Владислава Суркова, оголосив флешмоб проти безвідповідальної, як вони кажуть, політики кібербезпеки українських державних структур…

Близько двох місяців тому активісти розпочали флешмоб #FuckResponsibleDisclosure і за цей час вони «перевірили» роботу сайтів і баз даних Міністерства оборони, Національної поліції, Міністерства внутрішніх справ, обласних державних адміністрацій, Конституційної комісії, РНБО, Державної служби спеціального зв'язку та захисту інформації й інших державних служб та відомств.

Суть флешмобу полягає в оприлюдненні в соціальних мережах несекретних документів зі службових комп'ютерів, демонстрації ненадійності сайтів окремих міністерств та службових баз даних підприємств і об'єктів критичної інфраструктури. Активісти не використовують суто хакерські методи – зазвичай достатньо лише пошуку в Google, пише речник УКА під ніком Шон Таунсенд у своїй колонці про підсумки флешмобу.

…дехто закриває вразливості швидко, а дехто ігнорує повідомлення хакерів. Втім, після їхніх «перевірок» правоохоронці відкрили щонайменш два кримінальних провадження, одне з яких стосується російських хакерів. Їм вдалося прорватися на поштовий сервер МВС…

У відкритому доступі можна було знайти списки офіцерів і базу даних сайту академії МВС. Тепер ці дані закрили. Команді швидкого реагування при Держспецзв'язку знадобилося п'ять днів для реагування на повідомлення, проте після цього вразливість також прикрили, зазначає представник хакерської спільноти.

Швидко відреагували на вразливість сайту РНБО, зазначає Таунсенд, і на діру в безпеці на сайті Конституційної комісії…

Ще донедавна (станом на 20 грудня 2017 року) не працював сайт Міністерства освіти і науки України. За словами хакерів – через флешмоб, який виявив відкритий доступ до бази даних міністерства. Зараз (26 грудня 2017 року) сайт працює, в прес-службі міністерства на запитання щодо заходів кібербезпеки поки не відповіли.

В грудні хакери оприлюднили документи з комп'ютерів офіцерів Збройних сил України – дані з одного стосуються розмінування, з іншого – бронетехніки. В Міністерстві оборони Радіо Свобода повідомили, що за фактом можливого зламу проводиться службове розслідування…

Остання «жертва» флешмобу українських хакерів – це державне підприємство «Енергоатом». Підставою їхньої «перевірки» стала жовтнева публікація російськими хакерами з групи «Кіберберкут» декількох документів про нібито «новий Чорнобиль» і наступну інформаційну атаку на «Енергоатом». Пізніше у Фейсбуці представники «Енергоатому» заявили, що російські хакери зламали Міністерство екології, а не їхнє підприємство…

На державному підприємстві «Енергоатом» внаслідок флешмобу проводять внутрішнє розслідування. Попередньо можна сказати, що активістам вдалося отримати доступ до службової інформації, яка не є конфіденційною, говорить директор ДП «Енергоатом» з інформаційних технологій Олександр Лісовий в коментарі Радіо Свобода…

Флешмоб #FuckResponsibleDisclosure допоміг виявити проблеми, визнає він, проте інформаційний вплив оприлюднення даних був негативним…

На думку одного зі спеціалістів американської компанії з кібербезпеки Comodo Group, що раніше працював у декількох відділах комп'ютерної безпеки державних органів, проблеми з кіберзахистом державних агенцій пов'язані не тільки із низькою комп'ютерною культурою, а й з низькою зарплатою…

Експерт з інформаційної безпеки Дмитро Снопченко каже Радіо Свобода , що будь-які дані з тих, що хакери оприлюднили, в соціальних мережах, можна назвати критичними…

Його ставлення до флешмобу двояке. З одного боку, ця публічна критика могла привернути увагу справжніх хакерів, які тепер більш активно будуть шукати вразливості у державних служб. З іншого боку, флешмоб допоміг викрити недоліки кібербезпеки, а після зламу засоби кібербезпеки зазвичай підсилюють.

У минулорічному інтерв'ю Радіо Свобода Шон Таунсенд казав, що хакерська спільнота воює з Росією. І у відповідь на запитання, чи готові вони «ламати» українських політиків, сказав, що внутрішні українські проблеми мають вирішуватися демократичним шляхом. Не відмовляється він від своїх слів і сьогодні. «Так званий full disclosure, який ми робимо, – це доволі демократичний засіб, який вирішує більше технічні проблеми. Проте неадекватна реакція на це іноді дивує», – зазначив Шон Таунсенд…» ***(Українські хакери оприлюднили службові документи військових, енергетиків і урядовців // PERSONA.TOP (https://persona.top/2017/12/26/ukrayins-ki-hakeri-oprilyudnili-sluzhbovi-dokumenti-vijs-kovih-energetikiv-i-uryadovtsiv/).- 26.12.2017).***

***

«Национальная полиция на примере атаки вируса Petya смогла выявить пробелы в кибербезопасности страны и принять меры для устранений выявленных недостатков

Об этом на годовой итоговой пресс-конференции заявил председатель Нацполиции Сергей Князев…

По словам Князева, в 2017 году эффективность работы Департамента кибербезопасности НПУ существенно увеличилась. В частности, удалось предотвратить или свести к минимуму нанесенный хакерами ущерб…» ***(Князев рассказал о последствиях атаки вируса Petya для полиции // DsNews (http://www.dsnews.ua/politics/knyazev-rasskazal-o-posledstviyah-ataki-virusa-petya-dlya-politsii-26122017153700).- 26.12.2017).***

***

Світові тенденції в галузі кібербезпеки

«Краткий обзор главных событий в мире ИБ за период с 4 по 10 декабря 2017 года…

… На минувшей неделе жертвой хакеров стал крупнейший web-сервис для майнинга криптовалют Nicehash, лишившийся более 4 тыс. биткойнов. Злоумышленникам удалось похитить только средства, хранящиеся на локальных кошельках NiceHash…

На минувшей неделе сотрудники Европола, Евроюста и ФБР при участии ИБ-экспертов пресекли деятельность крупнейшей сети ботнетов Andromeda, распространявшей вредоносное ПО Gamarue, также известное как Wauchos. Сеть состояла из 464 отдельных ботнетов и заражала порядка 1,1 млн компьютеров ежемесячно. В рамках правоохранительной операции было отключено около 1,5 тыс. доменов и IP-адресов, использовавшихся в C&C-инфраструктуре…

Несмотря на усилия правоохранительных органов, в Сети продолжают появляться новые ботнеты. В частности, эксперты компании Qihoo 360 Netlab зафиксировал и всплеск активности ботнета Satori (одного из вариантов Mirai), включающего порядка 280 тыс. активных устройств…

Порядка 31 млн пользователей популярной виртуальной клавиатуры AI.type стали жертвами утечки данных из-за разработчика приложения, который не защитил сервер должным образом. Сервер работал без парольной защиты, в результате доступ к клиентской базе данных компании, включавшей свыше 577 ГБ конфиденциальной информации, мог получить кто угодно…» ***(Обзор инцидентов безопасности за прошлую неделю // SecurityLab.ru (https://www.securitylab.ru/news/490208.php).- 11.12.2017).***

***

«Краткий обзор событий в мире ИБ за период с 11 по 17 декабря 2017 года…

…12 декабря крупнейшая гонконгская криптовалютная биржа Bitfinex сообщила о серии мощных DDoS-атак, приведших к сбоям в работе сервиса. …специалисты Fortinet зафиксировали новую фишинговую операцию, в рамках которой преступники распространяют троян для удаленного доступа (RAT) Orcus через вредоносную рекламу, предлагающую установить легитимный бот Gunbot, предназначенный для торговли на бирже.

На минувшей неделе эксперт Роберт Ли (Robert Lee) предупредил о возможной кибератаке на энергосистемы Украины, аналогичной инцидентам, произошедшим в 2015 и 2016 годах… Как полагает специалист, хакеры могут провести новую атаку в декабре 2017 года.

О хакерской атаке на ряд своих клиентов сообщила нидерландская компания Fox-IT. Согласно уведомлению, неизвестный злоумышленник осуществил атаку «человек посередине» и следил за ограниченным числом пользователей. Хакер перехватывал трафик, предназначавшийся для домена Fox-IT, с помощью SSL-сертификата читал передаваемые по HTTPS данные, а затем перенаправлял пользователей на настоящий сервер Fox-IT.

На минувшей неделе группа экспертов описала новый вариант криптографической атаки Даниэля Бляйхенбахера, позволяющий получить закрытые криптографические ключи для расшифровки HTTPS-трафика при определенных условиях. К новой атаке под названием ROBOT, уязвимы некоторые продукты ряда производителей, в том числе Cisco, Citrix, F5 и Radware, а также 27 сайтов из рейтинга Alexa Top 10, включая Facebook и PayPal.

…CERT Эстонии (Computer Emergency Response Team, компьютерная группа реагирования на чрезвычайные ситуации) заявила об утечке учетных данных, затронувшей порядка 200 тыс. эстонских пользователей…» ***(Обзор инцидентов безопасности за прошлую неделю // SecurityLab.ru (https://www.securitylab.ru/news/490360.php).- 18.12.2017).***

***

«Компания Trend Micro Incorporated (TYO: 4704; TSE: 4704), мировой лидер в разработке решений для кибербезопасности, опубликовала ежегодный отчет с прогнозами по информационной безопасности на 2018 год "Изменения парадигмы: прогнозы по информационной безопасности 2018" (Paradigm Shifts: Trend Micro Security Predictions for 2018)…

Основные выводы:

– По прогнозам экспертов, глобальные потери от BEC-атак в 2018 году превысят сумму в $9 млрд.

– Киберпреступники начнут использовать технологии машинного обучения и блокчейн в своих методиках взлома. DAO (Decentralized Autonomous Organization), первый децентрализованный венчурный фонд, построенный на базе блокчейна Ethereum, подвергся крупной масштабной атаке. В результате эксплуатации ошибки в коде DAO со счетов проекта исчезли более $50 млн электронной наличности.

– В 2018 году программы-вымогатели останутся основным инструментом получения прибыли, хотя и другие виды киберпреступлений будут набирать обороты.

– В 2018 году киберпреступники найдут новые способы использовать бреши в устройствах класса IoT для получения собственной выгоды. Кроме DDoS-атак, злоумышленники будут использовать IoT-устройства для создания прокси-серверов с целью скрыть свое настоящее местоположение и веб-трафик. Причина подобной тенденции в том, что при проведении расследований полиция чаще всего опирается на IP-адрес в журналах. Все больше устройств, таких как биометрические трекеры, дроны, аудиоколонки и голосовые помощники будут взломаны с целью извлечения накопленных данных, проникновения в жилища и т.д.

– Корпоративные приложения и платформы будут подвержены риску нецелевого использования и уязвимостям. SAP и другие системы планирования ресурсов предприятия могут быть взломаны. Если обрабатываемые данные были модифицированы или отправлена неправильная команда в системе ERP, вычислительная техника может стать инструментом саботажа, приводя к ошибочным решениям, таким как неверные объемы ресурсов, нежелательные переводы денег и даже перегрузка систем.

– Кампании киберпропаганды станут более отточенными, благодаря использованию уже опробованных методик спам-рассылок.

– Большинство компаний начнут соблюдать правила европейского закона о защите персональных данных акта (General Data Protection Regulation, GDPR) только после первого громкого судебного процесса» ***(Trend Micro представила прогнозы в области информационной безопасности на 2018 год // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120302).- 15.12.2017).***

***

«…По оценкам экспертов по кибербезопасности из компании SCO, общая сумма ущерба от кибератак в 2017 году составила $86,4 млрд. Но и это не предел. По оценкам экспертов, к 2021 году сумма ущерба может перевалить за $6 триллионов. А вот пять главных угроз кибербезопасности, которые поджидают нас в 2018 году

Принудительный майнинг криптовалют

…Некоторые пользователи продолжают майнить биткоины, скупая видеокарты и выстраивая монструозные и энергоемкие “майнинг-фермы”. Но нашлись и те, кто предпочитает добывать криптовалюту чужими руками.

В этом году популярными стали трояны-майнеры. Это, по сути, вирус, который проникает на компьютер пользователя и использует его вычислительные ресурсы для добычи биткоинов в кошелек злоумышленника. Также для майнинга могут использоваться замаскированные скрипты на сайтах…

Эксперты SCO считают, что в 2018 году количество попыток подобного недобросовестного майнинга (его также называют “криптоджекингом”) многократно возрастет. Следует ожидать появления новых, еще более изощренных способов майнинга за чужой счет.

PowerShell-атаки

В последнее время хакеры, целью которых являются конкретные компании, чаще всего прибегают к так называемым PowerShell-атакам. Атаки используют встроенный инструмент автоматизации Windows PowerShell…

В 2017 году такой метод атаки стал очень популярен среди злоумышленников. В 2018 количество PowerShell-атак продолжит расти.

Киберпреступное подполье

…Уже сегодня формируется теневой рынок услуг и инструментов, пользоваться которыми могут даже люди, не имеющие специальных технологических знаний. Любой, у кого найдется достаточная сумма, может приобрести готовый ботнет или другой инструмент для проведения атаки или взлома.

Кроме того, на базе крупных киберпреступных группировок все чаще формируются структуры, напоминающие старую добрую организованную преступность…

Защитное программное обеспечение само станет целью

…Хакеры могут пытаться находить бреши в продуктах безопасности, либо, если речь идет о каких-либо облачных решениях, перехватывать облачный трафик. По мере того, как о подобных инцидентах будет узнавать широкая публика, доверие пользователя к защитному программному обеспечению будет снижаться. И это, опять таки, будет играть на руку злоумышленникам.

Более активная киберзараза

…Эксперты считают, что в 2018 году количество активно атакующих червей возрастет, а значит, нас ждет не одна киберэпидемия» ***(Роман Черный. 5 главных угроз кибербезопасности в 2018 году // IGate (http://igate.com.ua/news/20752-5-glavnyh-ugroz-kiberbezopasnosti-v-2018-godu).- 18.12.2017).***

***

«…**Positive Technologies подвела итоги уходящего года в контексте информационной безопасности и представила свои прогнозы на 2018 год…** Минувший год, по мнению экспертов Positive Technologies, запомнился следующими событиями и тенденциями:

Вирусы-вымогатели. Отсутствие актуальных обновлений и привычка жить с уязвимостями привели к остановке заводов Renault во Франции, Honda и Nissan в Японии; пострадали банки, школы, энергетические, телекоммуникационные компании.

Практическая безопасность. …Федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» не просто рекомендует, а обязывает защищаться государственные и коммерческие компании и вводит механизмы контроля эффективности защитных мер.

Уязвимости телекома стали использовать. Злоумышленники начали перехватывать коды для двухфакторной аутентификации с помощью уязвимостей сигнального протокола SS7. Первыми пострадали абоненты O2-Telefonica.

«Масштабируемые» атаки на банкоматы. …киберпреступники стали подключаться к локальной сети банка и удаленно контролировать множество АТМ…

Тайный майнинг. Весной 2017 года наши эксперты обнаружили сотни компьютеров в крупных компаниях, которые майнили криптовалюту для неизвестных взломщиков…

Войти через IoT. …с помощью незащищенных «умных» кофемашин стали останавливать нефтехимические заводы, а смарт-аквариумы использовать для атак на казино.

Биткоины и уязвимый веб. …хакеры сконцентрировали свое внимание на блокчейн-стартапах. Самая простая схема атаки — найти уязвимости на сайте ICO и подменить адрес кошелька для сбора инвестиций…

Эпидемия целевых атак. Число компаний, столкнувшихся в 2017 году с APT-атаками, увеличилось почти вдвое…

В числе прогнозов на 2018 год эксперты Positive Technologies отмечают следующие:

Ответом на усложнение атак стал рост интереса к построению центров мониторинга безопасности (SOC). Только в этом году около 10 компаний приступили к созданию своих SOC в той или иной форме. В 2018 году число SOC вырастет в три раза.

Система ГосСОПКА и требования закона N 187-ФЗ не гарантируют, что систему невозможно будет взломать, но выполнение этих требований и создание центров ГосСОПКА позволит отсечь 90% примитивных атак, позволив сконцентрироваться на высокоуровневых.

Продолжится рост логических атак на банкоматы… Банки, в свою очередь, станут еще активнее интересоваться реальными угрозами, грозящими финансовыми потерями, и оценивать риски.

Уязвимости мобильных сетей могут стоить человеческих жизней. С помощью мобильных сетей самоуправляемые автомобили обмениваются данными о скорости, расположении автомобилей на трассе и другими данными. DDoS-атаки могут оставить такой автомобиль буквально без «чувств и глаз»…

Внимание злоумышленников будет направлено на веб-кошельки — это хоть и удобно, но небезопасно, рано или поздно они будут взломаны. Мы прогнозируем также рост количества взломов веб-приложений блокчейн-проектов за счет фишинга…» ***(Итоги года и прогнозы от Positive Technologies // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/288913/).- 13.12.2017).***

***

«…Министерство обороны Сингапура объявило о запуске программы вознаграждения за поиск уязвимостей, в рамках которой эксперты в области кибербезопасности будут проверять online-ресурсы ведомства на предмет уязвимостей…

…За каждую найденную уязвимость эксперты получат вознаграждение в размере от 150 (порядка $111) до 20 тыс. ($14,8 тыс.) сингапурских долларов.

Программа продлится с 15 января до 4 февраля 2018 года и будет распространяться на 8 ресурсов минобороны…» ***(Минобороны Сингапура предложило хакерам найти уязвимости в системах ведомства // SecurityLab.ru (https://www.securitylab.ru/news/490223.php).- 12.12.2017).***

***

«В будущем году Gartner прогнозирует увеличение организациями расходов на информационную безопасность. Ожидается, что общемировые расходы увеличатся на 8% «YoY», до 96,3 млрд долл., тогда как по итогам нынешнего года выручка превысит 89,1 млрд долл…

Наиболее динамичный рост будет наблюдаться в сегментах защиты инфраструктуры и услуг безопасности, в частности по направлениям тестирования решений безопасности, ИТ-аутсоринга, управления информационной безопасностью и управления событиями безопасности (SIEM)» ***(Рост мирового рынка информационной безопасности достигнет 8% // «Компьютерное Обозрение»(http://ko.com.ua/rost_mirovogo_rynka_informacionnoj_bezopasnosti_dostignet_8_122725).- 11.12.2017).***

***

«Правительство Израиля 17 декабря утвердило предложение премьер-министра об объединении Национального киберштаба и Национального управления по киберзащите в единую Национальную систему кибербезопасности, которая будет отвечать за все аспекты киберзащиты в гражданской сфере…

Решение об объединении двух подразделений завершает выполнение национальной задачи о создании оптимальной системы защиты гражданского киберпространства, поставленной премьер-министром ещё в 2011 году» ***(Израиль: концентрация усилий по защите киберпространства // ISRAland Online Ltd. (http://www.isra.com/news/209166).- 18.12.2017).***

***

Сполучені Штати Америки

«…Президент США Дональд Трамп подписал законопроект, запрещающий американским государственным органам использовать программное обеспечение "Лаборатории Касперского". Документ является частью закона о финансировании национальной оборонной политики (NDAA), который был подписан… 12 декабря. Законопроект подкрепляет принятое в сентябре решение администрации Трампа, которое обязывает все гражданские госучреждения удалить софт Касперского из своих компьютерных систем. Теперь под это требование попадают и военные ведомства…

В "Лаборатории Касперского", в свою очередь, заявили, что принятие этого закона в США нанесет урон бизнесу компании, которая в данный момент изучает варианты последующих действий. Представители компании считают, что закон не

основан на исследовании имеющихся правил в отношении госзакупок программного обеспечения и никаким образом эти правила не улучшает, поэтому его принятие к снижению рисков в сфере кибербезопасности не приведет» ***(Трамп подписал закон о запрете софта Касперского в госучреждениях // Українська служба швидких новин (https://sumynews.online/tramp-podpisal-zakon-o-zaprete-softa-kasperskogo-v-gosuchrezhdeniyax/).- 13.12.2017).***

***

«Российская антивирусная компания "Лаборатория Касперского" подала в суд на Министерства внутренней безопасности США в связи с запретом на использование продуктов разработчика в госорганах сраны…

Е. Касперский заявил, что сведения, на которых основывается решение Министерства внутренней безопасности основано на сведениях из открытых источников, которые не предоставили достаточные доказательства…

Кроме того, по мнению отечественного разработчика, американское ведомство нарушило процедуру принятия решения и не подтвердило обоснованность своих обвинений…» ***("Лаборатория Касперского" подала иск против Министерства внутренней безопасности США // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120353).- 19.12.2017).***

***

«Білий Дім оприлюднив оновлену Стратегію національної безпеки США, що позначає глобальні загрози, найбільшими з яких визнано РФ та Китай. Документ опублікований на сайті Білого дому…

68-сторінковий документ, підписаний діючим президентом США Дональдом Трампом, включає чотири життєво важливих для національних інтересів США пункти: захист батьківщини, американського народу і американського стилю життя; розвиток американського добробуту; підтримання миру за допомогою сили і розширення американського впливу.

Серед глобальних загроз, що стоять перед США, перераховані Китай і Росія, регіональні диктатори (КНДР) і терористи-джихадісти (Ісламська держава і Аль-Каїда)…

Слід зазначити, що адміністрація Трампа також офіційно визнала наявність російської кіберзагрози…» ***(Самуїл Проскуряков. У новій стратегії Нацбезпеки США Російська Федерація визнана загрозою // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1705223-u-noviy-strategiyi-natsbezpeki-ssha-rosiyska-federatsiya-viznana-zagrozoyu).- 19.12.2017).***

***

«Колишній співробітник Агентства національної безпеки (АНБ) США Нгя Хоанг Фо визнав провину в незаконному зберіганні засекречених документів у себе вдома… які, як вважалося, пізніше були викрадені з його домашнього комп'ютера російськими хакерами…

У документах містилися відомості з питань національної оборони, у тому числі матеріали під грифами “цілком таємно” і “секретна інформація з особливим режимом зберігання”.

67-річний Нгя Хоанг Фо працював в особливому підрозділі АНБ, яке займалося зломом іноземних комп’ютерів, веденням розвідки в кіберпросторі та аналізом зібраних даних.

Підозрюваному загрожує до 10 років позбавлення волі…» (***Екс-співробітник АНБ США зізнався в зберіганні секретних документів у себе вдома // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1702032-eks-spivrobitnik-anb-ziznavsya-v-zberiganni-sekretnikh-dokumentiv-u-sebe-vdoma).- 02.12.2017).***

***

«…Власти США уверяют, что правительство может использовать свои юридические полномочия для того, чтобы тайно просить американскую компанию о технической помощи, к примеру, о внедрении бэкдора, то есть намеренного искажения алгоритма в продукт. В своих операциях по сбору разведывательных данных и наблюдению правительство США опирается на раздел 702 Закона о надзоре за внешней разведкой. В случае, если компания откажется выполнить просьбу, чиновники смогут обратиться в Суд… по надзору за внешней разведкой (FISC). В частности, FISC может утвердить ежегодную сертификацию, подтверждающую, что правительство требует помощи от технической компании США… Это дает правительству широкий круг полномочий издавать директивы без какого-либо дальнейшего утверждения или пересмотра.

Интересно, что в парламент США уже внесен законопроект, который будет требовать от правительства получать одобрение от FISC для каждого запроса о помощи…» ***(Устраивать слежку за гражданами с помощью бэкдоров власти США могут без решения суда // РосКомСвобода (https://roskomsvoboda.org/34103/).- 05.12.2017).***

***

«Палата представителей США приняла законопроект по созданию агентства кибербезопасности и безопасности инфраструктуры.

…Создание нового ведомства предполагает реорганизацию ряда подразделений министерства внутренней безопасности США для повышения устойчивости кибербезопасности США в случае чрезвычайных ситуаций и атак на объекты критической инфраструктуры…» ***(В США создадут государственное агентство по кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/490221.php).- 12.12.2017).***

***

«Компания ExpressVPN, один из крупнейших в США VPN-сервисов, представила данные проведенного ею опроса. Целью исследования было установить, насколько американцы обеспокоены тем, что их персональные данные могут оказаться в чужих руках.

…Так, лишь 28 процентов опрошенных согласились бы предоставить правительству доступ к своим персональным данным в ситуациях, когда того требуют интересы безопасности страны. 58 процентов участников категорически заявили, что доступ может предоставляться только на основании судебного ордера.

Респондентов также просили ответить, кого они более всего подозревают в просмотре своих сообщений электронной почты. На первом месте оказалось правительство США, вторую строчку заняла корпорация Google. Далее следуют интернет-провайдеры и работодатели (в случае с сообщениями, отправленными со служебных устройств)…» ***(Американцы не желают никому доверять свои персональные данные // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5457935-Amerikancy-ne-zhelayut-nikomu-dover.html#ixzz51E7SZne2).- 08.12.2017).***

***

«Согласно решению администрации президента США Дональда Трампа, у АНБ и ФБР есть законное право на реализацию своих программ слежения без судебного ордера, даже если Конгресс не успеет вовремя продлить срок действия соответствующих законов, истекающий в канун Нового года…

Учитывая риски, которые может повлечь за собой промедление со сроками, представители исполнительной власти пришли к выводу, что правительство может разрешить спецслужбам реализовывать программы слежения без ордера до апреля 2018 года даже в случае, если срок действия соответствующих актов не будет продлен.

Акт о негласном наблюдении в целях внешней разведки (Foreign Intelligence Surveillance Act, FISA) – федеральный закон США, описывающий процедуры физического и электронного наблюдения и сбора внешней разведывательной информации, передаваемой иностранными государствами и агентами иностранных государств. Агентами могут быть как иностранные, так и американские граждане и обладатели постоянного вида на жительство, подозреваемые в шпионаже и терроризме. Закон должен применяться исключительно на территории США…» ***(Спецслужбы США получили право без ордера следить за гражданами до апреля 2018 года // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120155).- 07.12.2017).***

***

«ИБ-эксперты из компании Pen Test Partners обнародовали отчет об уязвимостях в системах отопления школ и американских военных объектах…

В отчете указано, что неправильно установленные контроллеры отопительных систем зафиксированы в правительственных учреждениях, школах, офисах различных компаний и на военных базах. Эксперты потратили менее 10 секунд на то, чтобы обнаружить свыше 1000 уязвимых систем. Хакеры, используя майнеры, уже взломали некоторые системы отопления, хотя они технически непригодны для майнинга.

Уязвимые системы удалось найти посредством поисковой системы Shodan. Так, эксперты искали проблемное оборудование среди контроллеров IQ3 Excite и

IQ412 Excite производства Trend Controls. С помощью уязвимых устройств хакер может обходить процедуру аутентификации на встроенном веб-сервере, похищать пароли, а также перехватывать сессию через интернет…» ***(Хакеры могут воспользоваться уязвимостями в системах отопления школ и военных объектов // SecureNews (https://securenews.ru/heating/).- 14.12.2017).***

***

«…Армия США отправит в горячие точки команды киберсолдат.

…В течение шести месяцев киберсолдаты внедрялись в пехотные войска, и теперь они будут выполнять операции в соответствии с потребностями командования, сообщил полковник USCYBERCOM Уильям Хартман (William Hartman).

Последние три года в крупном центре на юге Калифорнии Армия США готовила специалистов для проведения подобных операций…

Кибернетическое командование США (United States Cyber Command, USCYBERCOM) – формирование вооруженных сил США, находящееся в подчинении стратегического командования США. Расположено на территории военной базы Форт-Мид (Мэриленд). Основными задачами командования являются централизованное проведение операций кибернетической войны (кибервойны), управление и защита военных компьютерных сетей США» ***(Армия США отправит в горячие точки киберсолдат // Internetua (http://internetua.com/armiya-ssha-otpravit-v-goryacsie-tocski-kibersoldat).- 17.12.2017).***

***

«Согласно результатам опроса, опубликованным аналитической компанией Accenture и Американской медицинской ассоциацией (AMA), с кибератаками уже столкнулись 83% предприятий медобслуживания в США…

В опросе, проведенном в июле — августе, приняли участие около 1,3 тыс. практикующих медиков…

В 64% медучреждений, переживших кибератаку, она повлекла до четырех часов простоя; в 12% случаев врачам пришлось прервать работу на 1-2 дня.

Наиболее распространенными угрозами в сфере здравоохранения США оказались фишинг, на который пожаловались 55% участников опроса, и вредоносное ПО (48%). Американским медикам также не в диковинку неавторизованный доступ к защищенным электронным документам (37%), взлом сети (12%) и кибервымогательство (9%). При этом вероятность атаки на крупный медицинский центр или клинику средней величины в два раза выше, чем на скромную частную практику…

Опрос также показал, что работники сферы здравоохранения зачастую доверяют защиту цифровых данных сторонним организациям. Тем не менее, около половины респондентов отметили, что в их клинике есть сотрудник, отвечающий за кибербезопасность. Остальные предпочитают нанимать для этого специалистов со стороны или пользоваться их услугами совместно с другим медучреждением» ***(Maxim Zaitsev. Какие киберугрозы знакомы американским врачам? // Threatpost***

(https://threatpost.ru/kakie-kiberugrozy-znakomy-amerikanskim-vracham/23743/).- 13.12.2017).

***

«Хакеры обнаружили критическую уязвимость в программном обеспечении Военно-воздушных сил США, благодаря которым они получили доступ к засекреченной сети Министерства обороны. Они сообщили об этом военным и получили награду в размере беспрецедентной суммы в $10 тыс.

Эксперты по кибербезопасности Бретт Буерхаус и Матиас Карлссон нашли эксплойт в рамках программы Hack the Air Force, которую запустило Минобороны США. Суть мероприятия в том, чтобы найти узвимости в системе раньше, чем это сделают злонамеренные хакеры, которые способны принести ущерб на миллиарды долларов или же украсть военные секреты…

За девять часов Буерхаус, Карлссон и еще несколько десятков контестантов обнаружили 55 уязвимостей в ПО ВВС США. Программа продлится до 1 января…» ***(Basil Naumov. Хакеры нашли уязвимость в ПО ВВС США // Game2Day.org (https://game2day.org/news/24703/hakery-nashli-uyazvimost-v-po-vvs-ssha).- 19.12.2017).***

***

«Група американських сенаторів від обох партій представила законопроект в сфері кібербезпеки, що має запобігти втручанню Росії та інших країн в майбутні вибори в країні…

Законопроект про безпечні вибори має перешкодити будь-яким майбутнім спробам іноземного втручання за рахунок надання допуску до секретних матеріалів представникам влади штатів, яких будуть оперативно інформувати про іноземне втручання.

Також передбачено обмін інформацією між федеральними розвідувальними органами і виборчими відомствами штатів…» ***(Саша Картер. У США представили законопроект про кіберзахист від російського втручання // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1705966-u-ssha-predstavili-zakonoproekt-pro-kiberzakhist-vid-rosiyskogo-vtruchannya).- 22.12.2017).***

***

Китай

«С начала 2015 года в Китае было закрыто более 13 000 сайтов из-за нарушения законов или других норм, и, как утверждает государственное информационное агентство Синьхуа, более 90 % опрошенных поддерживает усилия правительства по очистке киберпространства…

…63,5 % из опрошенных полагают, что в последние годы наблюдается очевидное сокращение вредного онлайн-контента, добавило Синьхуа.

Синьхуа также сообщило, что за последние пять лет в Китае более 10 миллионам человек, которые отказались зарегистрироваться с указанием своих настоящих данных, были заблокированы аккаунты…» ***(За три года в Китае закрыли более 13 000 сайтов // IGate (http://igate.com.ua/lenta/20833-za-tri-goda-v-kitae-zakryli-bolee-13-000-sajtov).- 27.12.2017).***

***

Країни ЄС

«Власти Германии готовят законопроект, обязывающий всех производителей электронных устройств встраивать в свои изделия бэкдоры для правоохранительных органов. Речь идет обо всех современных устройствах, от «умных» автомобилей до смартфонов и «интернета вещей».

Первое рассмотрение законопроекта намечено уже на эту неделю…

Министр внутренних дел ФРГ заявил, что у производителей электроники якобы есть «юридическое обязательство» оснащать свои разработки бэкдорами специально для правоохранительных органов. Он также выразил пожелание, чтобы ИТ-отрасль предоставила властям свои «программные протоколы» для дальнейшего анализа. В законопроекте есть соответствующее положение, и оно позволит властям Германии требовать, чтобы коммерческие компании раскрывали все подробности используемого ими шифрования.

Этим законопроект не ограничивается. Он также предполагает предоставить властям Германии право удаленно взламывать любой компьютер «в случае кризиса».

Эксперты, ознакомившиеся с текстом законопроекта, указывают, что отдельные его положения по сути предоставляют властям ФРГ право на перехват любого трафика в Сети…

Функционеры Евросоюза ранее говорили, что не дадут хода законопроектам о бэкдорах для шифрованных коммуникаций, однако в марте 2017 г. Еврокомиссия поддержала проект о предоставлении полиции и спецслужбам бэкдоров в сервисах мгновенного обмена сообщениями - WhatsApp, Telegram, Signal и других» ***(Немцы принимают закон о повсеместном внедрении бэкдоров для удобства полиции // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5457439-Nemcy-prinimayut-zakon-o-povsemestn.html#ixzz51E3Hsatl).- 06.12.2017).***

***

«В Великобритании подан коллективный иск против Google за незаконный сбор данных миллионов пользователей. Подобный иск в Великобритании подан впервые за всю историю…

…Согласно иску, Google обвиняется в незаконном сборе информации о 5,4 млн британцев в обход настроек безопасности на их iPhone…

Иск связан с использованием американским техногигантом файлов cookie. Как говорится в документе, в течение нескольких месяцев в 2011-2012 годах Google размещала файлы cookie для отслеживания рекламы на устройствах

пользователей Safari, где возможность использования таких cookie блокируется по умолчанию…» ***(Google обвиняется в незаконном сборе данных миллионов британцев // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120039).- 01.12.2017).***

***

«Согласно поправкам в Акт о полномочиях следствия (Investigatory Powers Act), также известным как "Хартия ищеек", высшие полицейские чины Великобритании потеряют право самостоятельно санкционировать доступ к личным телефонам и истории интернет-просмотров граждан. Изменения были внесены в рамках выполнения требований Европейского суда касательно полномочий британских правоохранительных органов.

Согласно документу, подготовленному Министерством внутренних дел Великобритании (Home Office), право подать запрос на доступ к данным о коммуникациях в будущем будет распространяться только на преступления, влекущие тюремное заключение сроком не менее шести месяцев.

По словам британских политиков, поправки в закон были внесены согласно решению Европейского суда, постановившему, что "общее и неизбирательное хранение" данных о персональных коммуникациях "не может считаться законным в демократическом обществе". Однако поправки не распространяются на деятельность организаций, занимающихся вопросами национальной безопасности, таких как Центр правительственной связи (GCHQ), MI6 и MI5, поскольку национальная безопасность находится вне юрисдикции ЕС…

В соответствии с принятыми поправками, запросы на получение доступа к данным о коммуникациях будут рассматриваться новым органом, Управлением по авторизации сбора данных о коммуникациях (Office for Communications Data Authorisation). Доступ к данным о коммуникациях будет предоставляться только в случае расследования серьезных преступлений, предусматривающих в качестве наказания не менее шести месяцев тюремного заключения. Помимо этого, требования по хранению и предоставлению доступа к данным о коммуникациях не распространяются на сферу здравоохранения, сбора налогов и регулирования финансовых рынков.

Под понятие данных о коммуникациях подпадает информация о том, кто, где, когда, каким образом и кому позвонил, отправил текстовое сообщение, электронное письмо или посетил web-страницу, однако оно не распространяется на содержимое разговоров и переписок.

Investigatory Powers Act (Акт о полномочиях следствия) – акт… наделяет ряд спецслужб широкими возможностями по слежке за гражданами, в том числе правом взламывать телефоны и компьютеры, массово собирать персональные данные и пр. В соответствии с данным законом все провайдеры страны должны с 2017 года собирать списки посещенных пользователями сайтов, хранить их на протяжении 12 месяцев и предоставлять полиции доступ к этим данным» ***(Британской полиции запретят санкционировать доступ к телефонам и компьютерам пользователей // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120060).- 01.12.2017).***

***

«Правительство Литвы обязало государственные структуры и компании в ближайшее время отказаться от программного обеспечения «Лаборатории Касперского», сочтя его потенциальной угрозой национальной безопасности, сообщили в минобороны Литвы…

Также отмечается, что соответствующим ведомствам поручено проанализировать риск использования программного обеспечения «Лаборатории Касперского» и в согласованные с Национальным центром кибербезопасности сроки заменить его. Сроки замены ПО не раскрываются.

По словам замминистра обороны Литвы Эдвинаса Кярза, решение правительства действует лишь в отношении критической инфраструктуры, в то время как «частные предприятия должны индивидуально оценить возможные риски использования ПО «Лаборатории Касперского».

В «Лаборатории Касперского» заявили, что разочарованы решением властей Литвы, однако отметили, что продолжат оказывать услуги частным клиентам в республике…» ***(Антон Касс. Власти Литвы отказались от антивируса Касперского // ООО «Деловая газета Взгляд» (https://vz.ru/news/2017/12/21/900804.html).- 21.12.2017).***

***

Російська Федерація

«…Российский Центр стратегических разработок (ЦСР) предложил поровну разделить риски по кибербезопасности между государством и частным сектором… Об этом сообщается в докладе ЦСР «Будущее информационной безопасности: глобальные трансформации и сценарии для России».

Доклад был подготовлен направлением «Внешняя политика и безопасность» совместно с ПИР-Центром с целью сделать наброски возможных путей развития ИБ в России. В частности специалистов интересует применение действующих норм международного права в отношении регулирования информационно-коммуникационных технологий…

…для выхода из сложившейся ситуации нужно сфокусироваться на трех основных направлениях. Во-первых, необходимо снизить риски использования информационных технологий в военно-политических целях и создать базу для создания международных норм ответственного поведения государств в киберпространстве.

Во-вторых, необходимо сосредоточиться на обеспечении безопасности, стабильности и отказоустойчивости интернета для российских пользователей. В-третьих, нужно обеспечивать поддержку российских интересов в сфере кибербезопасности…» ***(ЦСР предложил распределить риски по кибербезопасности между государством и частным сектором // SecurityLab.ru (https://www.securitylab.ru/news/490527.php).- 25.12.2017).***

***

«Вопросы кибербезопасности нужно включить в школьную программу в ближайшее время. Соответствующее письмо Минобрнауки направило в ответ на обращение вице-спикера Госдумы Ирины Яровой…

По её словам, соответствующие курсы с самого начала нужно было предусмотреть в таких дисциплинах, как информатика, ОБЖ и технологии…

Впервые предложение включить в школьную программу изучение кибербезопасности Яровая озвучила на заседании Координационного совета по реализации Национальной стратегии действий в интересах детей на 2012-2017 годы 15 ноября 2016 года.

Тогда решение поддержали Роскомнадзор, Следственный комитет, Генпрокуратура, МВД» ***(Алексей Велединский. Яровая предложила включить в школьную программу уроки по кибербезопасности // Парламентская газета (https://www.pnp.ru/politics/yarovaya-kiberbezopasnost-nuzhno-vklyuchit-v-shkolnuyu-programmu-v-blizhayshee-vremya.html).- 01.12.2017).***

***

«Федеральная служба по техническому и экспортному контролю (ФСТЭК России) вынесла на общественное обсуждение проект приказа «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»…

Согласно документу, системы безопасности создаются субъектами критической информационной инфраструктуры (КИИ) в рамках комплекса правовых, организационных, технических и иных мер, направленных на обеспечение информационной безопасности (защиты информации) информационных ресурсов субъектов КИИ. Системы безопасности включают силы обеспечения безопасности (подразделения субъекта КИИ, отвечающие за обеспечение безопасности, сопровождение, ремонт объектов КИИ и пр.) и средства обеспечения безопасности. К ним относятся программные и программно-аппаратные средства, применяемые для обеспечения безопасности.

В качестве задач систем безопасности указываются предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом КИИ, уничтожения таких данных, их модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации; недопущение воздействия на технические средства обработки информации, которое может привести к нарушению и/или прекращению функционированию объектов КИИ; обеспечение работы объектов КИИ в штатном режиме; восстановление функционирования объектов КИИ, в том числе за счет создания резервных копий необходимой для этого информации; непрерывное взаимодействие с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

…Кроме прочего, он предусматривает максимальные санкции за создание вредоносных программ для атак на КИИ в виде лишения свободы сроком до 10 лет.

Закон вступит в силу 1 января 2018 года» ***(ФСТЭК опубликовала проект приказа об утверждении требований к созданию систем безопасности объектов КИИ РФ // SecurityLab.ru (https://www.securitylab.ru/news/490015.php).- 02.12.2017).***

***

«…Россия позиционирует себя как сильный союзник Северной Кореи, стремясь обеспечить её выходом в интернет.

В конечном итоге Россия может придать храбрости Северной Корее, необходимой ей для того, чтобы запустить более разрушительные кибератаки. Более тесное сотрудничество между двумя странами — особенно в области кибератак — повышает вероятность того, что оно будет иметь разрушительный эффект для международного сообщества…

..Инвестируя понемногу в КНДР, Россия может включить её в свою геополитическую разрушительную повестку дня. У России, пострадавшей от санкций, которые привели к снижению ВВП, есть сильный стимул для международного партнёрства с КНДР. Снабжение северокорейских хакеров расширенной пропускной способностью и предоставление им возможности нападать на национальные банки и компании позволяет России финансировать киберпреступность. Более того, при поддержке России Северная Корея будет чувствовать себя готовой начать более разрушительные кибератаки.

…Очень возможно, что они уже проводили совместные кибератаки. Основываясь на предыдущих кибератаках, американское правительство и частные охранные компании назвали Россию и КНДР двумя основными угрозами для национальной безопасности…

…Крепкое партнёрство между Россией и Северной Кореей представляет собой серьёзнейшую киберугрозу. Если две страны будут сотрудничать с целью развязывания более агрессивных кибератак — а похоже, что именно об этом и идёт речь, — международному сообществу нужно лучше к этому подготовиться» ***(Россия и КНДР могут начать сотрудничество в сфере кибаратак // Инфомационное агентство «IP News» (https://www.ipnews.in.ua/news/world/141220-rossiya-i-kndr-mogut-nachat-sotrudnichestvo-v-sfere-kibaratak).- 05.12.2017).***

***

«Власти РФ к концу 2020 года планируют внести в международные организации проекты нормативно-правовых актов, запрещающих разработку, распространение и применение кибероружия. Помимо этого, разрабатываются методы обнаружения источника кибератак. …соответствующий документ разрабатывается в рамках программы «Цифровая экономика». …Эксперты утверждают, что вряд ли в скором времени получится создать универсальный алгоритм на международном уровне, все, что остается на данный момент — собирать лучшие практики и обмениваться ими» ***(Олег Иванов. Россия хочет запретить кибероружие на международном уровне // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2017-12-06-1447/25007).- 06.12.2017).***

***

«Роскомнадзор совместно со специалистами операторов связи разработал механизм, значительно ускоряющий процесс получения операторами выгрузки из Единого реестра запрещенной информации.

Новый механизм позволяет операторам еще до обновления всего массива данных в Реестре получать информацию только об IP-адресах, внесенных с момента последней выгрузки. Применение усовершенствованного алгоритма существенно сокращает время с момента добавления в Единый реестр запрещенного ресурса до его внесения в системы фильтрации операторов связи…

Применение нового механизма не носит обязательный характер. Он станет дополнительным инструментом повышения эффективности принимаемых операторами мер по ограничению доступа к противоправным ресурсам…

В настоящее время новый механизм внедряется на сетях более 60 операторов связи из всех федеральных округов. Подключение всех остальных операторов связи, желающих воспользоваться новым алгоритмом, запланировано на 2018 год» ***(Операторы связи смогут блокировать противоправные ресурсы быстрее // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5457974-Operatory-svyazi-smogut-blokirovat.html#ixzz51E94n5WN).- 08.12.2017).***

***

«Сегодня в России в среднестатистическом доме насчитывается 2 компьютера и 4 мобильных устройства. И все они имеют доступ к Интернету…

…«Лаборатория Касперского» спрогнозировала возможные угрозы, которые могут оказать самое непосредственное влияние на рядовых пользователей, их ежедневные дела и привычки.

В 2018 году, по мнению экспертов, злоумышленники могут выйти за границы привычных устройств и начать активнее атаковать новые подключенные к Интернету системы – например, автомобили или медицинские приборы…

Что касается подключаемых к Интернету медицинских приборов, то их число, по оценкам экспертов, в следующем году вырастет до 19 миллионов. Если добавить к этому еще более 100 миллионов фитнес-трекеров, которые также помогают людям следить за здоровьем, то можно представить, что злоумышленники вряд ли обойдут стороной столь широкий спектр подключенных к Сети устройств. Масштаб угрозы может варьироваться от кражи персональных данных о состоянии здоровья до опасной для жизни переустановки настроек на медицинских приборах, например, на дозаторах инсулина.

…41% пользователей в России заходит в системы онлайн-банкинга именно с мобильных устройств. В связи с этим значительные усилия злоумышленников в 2018 году будут направлены именно на смартфоны и планшеты…

Наконец, злоумышленники с высокой долей вероятности продолжат взламывать различные домашние гаджеты для создания на их основе больших ботнетов. Роутеры, веб-камеры, термостаты и прочие умные устройства в доме содержат немало уязвимостей, которыми, как показывает практика, умело пользуются киберпреступники. Для предотвращения подобного развития событий

эксперты рекомендует, по крайней мере, сменить пароли, установленные производителями этих устройств, а лучше выделить для них отдельную подсеть, чтобы хакеры не могли атаковать основные устройства в случае заражения…» ***(С какими угрозами могут столкнуться домашние пользователи в 2018 году // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5458178-S-kakimi-ugrozami-mogut-stolknutsya.html#ixzz51EBaGBc9).- 11.12.2017).***

***

«Больше половины (52%) банков и страховых компаний России и СНГ увеличили бюджет на инфобезопасность в 2016-17 г. в связи с ростом киберугроз и активности вредоносных программ…

Компания VMware представила результаты исследования крупнейших финансовых организаций, проведенного совместно с аналитическим центром TAdviser.

Исследование еще раз подтвердило, что за последний год количество угроз информационной безопасности для корпоративного сектора выросло значительно — это подтверждают 80% опрошенных финансовых организаций. Лишь 16% зафиксировали сохранение прежнего уровня киберпреступности… Поэтому в условиях роста киберугроз более половины (52%) компаний увеличили бюджет на средства защиты…

…среди наиболее распространенных угроз компании финансового сектора отметили DDoS-атаки (28%)… Среди других угроз респонденты отметили фишинг (26%) и атаки шифровальщиков (10%).

Цифровая трансформация банковского бизнеса также подразумевает перевод вычислений в облако. Например, по данным исследования VMware[i], в США 81% респондентов из банков с активами в 100 млрд долларов и более и 68% банков с активами от 15 до 100 миллиардов долларов в настоящее время осваивают облачные вычисления. Однако у финансовых компаний в России есть серьезные опасения в связи с облачной моделью. Так, более двух третей (70%) считают потеряю или хищение данных главными рисками при миграции в облачную среду. С большим отрывом респонденты отметили простои по вине провайдера (26%)…

…все чаще злоумышленники используют неизвестное вредоносное ПО. Это зловреды, которые не может отследить традиционный антивирус, потому что данных о них еще нет в базах ИБ-компаний. Эффективным ответом на эту новую угрозу является модель «нулевого доверия», которая стала возможной благодаря использованию программно-определяемых сетей (Software-Defined Networks, SDN) — она реализована в решении VMware NSX. Согласно опросу, половина банков (50%) и страховых компаний ориентируются на модель «нулевого доверия» при построении ИБ-систем…» ***(Киберугрозы служат развитию информатизации банков // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5458714-Kiberugrozy-sluzhat-razvitiyu-infor.html#ixzz51EdqoBM5).- 12.12.2017).***

***

«Сбербанк стал первым банком в России, чей центр управления кибербезопасностью (Security Operation Center – SOC) сертифицирован

Британским институтом стандартов (BSI) на соответствие международному стандарту…

Международный стандарт ISO/IEC 27001:2013 определяет требования к созданию, внедрению, обслуживанию и постоянному совершенствованию системы управления информационной безопасностью организации… Разработчиком стандарта является Международная организация по стандартизации (ISO), одним из аккредитованных органов по сертификации выступает BSI.

«…Сертификат подтверждает, что наши процессы мониторинга и реагирования на кибератаки соответствуют международным требованиям…», - отметил заместитель председателя правления Сбербанка Станислав Кузнецов» ***(Центр управления кибербезопасностью Сбербанка получил международный сертифікат // РАПСИ (http://rapsinews.ru/banking_law_news/20171214/281311143.html#ixzz51gwbnf00).- 14.12 2017).***

***

«…в период с 2013 по 2016 гг. число киберпреступлений в России выросло в шесть раз, а за первую половину 2017 года — еще на 30%. Эти цифры озвучил генпрокурор РФ Юрий Чайка, выступая на 15-м заседании генеральных прокуроров государств — членов ШОС (Шанхайской организации сотрудничества), состоявшемся на прошлой неделе в Петербурге.

По словам докладчика, ежегодно генпрокуратура РФ сталкивается с десятками тысяч противоправных деяний, совершаемых с использованием высоких технологий, и самые распространенные из них — кража денег через Интернет, пропаганда терроризма и экстремизма, кибершпионаж. Ответственность за такие преступления, как отметил Чайка, предусматривают 17 статей Уголовного кодекса РФ…

С нового года в России будут сурово карать за кибератаки на критическую инфраструктуру…

Согласно поправкам к УК РФ, вступающим в силу с января, создатель вредоносного ПО для проведения атак на подобные объекты может быть наказан лишением свободы на срок до пяти лет, взломщик компьютерных систем получит до шести лет со штрафом до 1 млн рублей. Если эти преступления совершены в составе преступной группы и повлекли тяжкие последствия, тюремный трок может быть увеличен до десяти лет…» ***(Maxim Zaitsev. Генпрокуратуру РФ беспокоит рост киберпреступности // Threatpost (https://threatpost.ru/russian-prosecutor-general-speaking-on-cybercrime-laws/23512/).- 04.12.2017).***

***

«В российском МИДе в четверг состоялась конференция по международной информационной безопасности. Ее участники признали: количество угроз в киберпространстве за минувший год существенно выросло, но государства не в состоянии объединить усилия для борьбы с ними — прежде всего из-за политических разногласий…

Директор ИПИБ, бывший глава ФАПСИ Владислав Шерстюк заявил, что сегодня уже более 60 стран активно развивают наступательные кибертехнологии, не говоря уже о негосударственных группировках и акторах… «В условиях, когда не решена проблема атрибуции кибератак, виновный может быть “назначен” исходя из политических соображений — и к нему могут быть применены не только санкции, но и силовые меры»,— отметил Владислав Шерстюк…

…представитель Главного оперативного управления Генштаба ВС РФ Константин Песчаненко представил новую российскую инициативу, направленную на предотвращение развития событий по худшему сценарию. По его словам, Москва выступает за подписание с Вашингтоном Соглашения о предотвращении опасной военной деятельности в киберпространстве… При этом Константин Песчаненко не уточнил, передала ли российская сторона свои предложения американской…

Андрей Крутских сообщил, что российские дипломаты намерены в 2018 году внести на Генассамблею ООН собственный свод правил поведения государств в киберпространстве — совместно со странами ШОС и, возможно, БРИКС….

Директор департамента по вопросам новых вызовов и угроз МИД РФ Илья Рогачев заявил об острой необходимости усовершенствовать международную правовую базу в области борьбы с киберпреступностью. Он напомнил о ранее уже озвученной инициативе Москвы по принятию на уровне ООН конвенции «О сотрудничестве в сфере противодействия информационной преступности». По задумке России этот документ должен прийти на смену Будапештской конвенции Совета Европы о компьютерных преступлениях 2001 года…

…вице-президент горно-металлургической компании «Норильский никель» Владислав Гасумянов анонсировал скорое открытие для подписания — в том числе и компаниями из других стран — Хартии информационной безопасности критических объектов промышленности…

Владислав Гасумянов сообщил, что идею подписания хартии уже поддержали другие крупные российские компании — «Северсталь», АЛРОСА, Новолипецкий металлургический комбинат, «Уралвагонзавод», «Евраз», ЛУКОЙЛ...

В хартии, в частности, говорится о недопустимости использования информационно-коммуникационных технологий в целях недобросовестной конкуренции и нанесения ущерба объектам промышленности; необходимости отказа от разработки и встраивания скрытых уязвимостей в информационно-коммуникационные системы критических объектов промышленности; осуждении деятельности, направленной на скрытое накопление информации об уязвимостях таких систем. В хартии приветствуются усилия международного сообщества по приданию опорным информационно-коммуникационным инфраструктурам, формирующим основу глобальной сети, «статуса демилитаризованной зоны, свободной от силового противоборства политических субъектов». И подчеркивается важность обмена лучшими практиками по обеспечению информационной безопасности объектов промышленности.

Впрочем, пока речь идет лишь о благих намерениях: Владислав Гасумянов уточнил, что «осознавая все деликатные особенности проблем информационной

безопасности на промышленных предприятиях», авторы хартии рассматривают ее «как рамочный этический документ, присоединение к которому не влечет юридических обязательств» ***(Елена Черненко. К кибербезопасности подошли с трех сторон. Российские дипломаты, военные и предприниматели представили инициативы по борьбе с киберугрозами // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3496533?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).- 15.12.2017).***

***

«Президент России Владимир Путин возложил на Федеральную службу безопасности обеспечение системы обнаружения, предупреждения и ликвидации последствий кибератак на информационные ресурсы РФ. Соответствующий указ опубликован на портале правовой информации…

Среди поставленных задач указаны прогнозирование ситуации в области обеспечения информационной безопасности, определение причин компьютерных инцидентов, обеспечение взаимодействия владельцев ресурсов, операторов связи и иных субъектов, осуществляющих лицензированную деятельность в области защиты информации и контроль защищённости информационных ресурсов от кибератак.

Указ вступает в силу с 1 января 2018 года» ***(Путин возложил на ФСБ обеспечение системы безопасности от кибератак // «Парламентская газета» (https://www.pnp.ru/social/putin-vozlozhil-na-fsb-obespechenie-sistemy-bezopasnosti-ot-kiberatak.html).- 22.12.2017).***

***

«…23 грудня Рамзан Кадиров повідомив, що його сторінки у Instagram та Facebook заблокували. За заявою міністра Чечні з національної політики Джамбулата Умарова, аккаунти Кадирова виявилися недоступним через "диверсійну кібератаку", що виконали за дорученням Державного департаменту США.

Згодом адміністрація соцмереж повідомила, що сторінки були заблоковані через санкції США проти чеченського ватажка…

Тим часом Кадиров повідомив, що досі веде свої сторінки у соціальній мережі Mylistory (чеченський аналог Instagram), "ВКонтакте" і канал у Telegram» ***(Facebook і Instagram заблокували сторінки Кадирова: згодом стало відомо, чому // Espreso.tv (https://espreso.tv/news/2017/12/27/instagram_ta_facebook_zablokuvaly_storinky_ramzana_kadyrova).- 27.12.2017).***

***

Республіка Таджикістан

«Обзор законодательства Республики Таджикистан в сфере информационной безопасности…

Базовым документом по информационной безопасности в Таджикистане является утвержденная Президентом страны, Концепция информационной безопасности Республики Таджикистан, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Республики Таджикистан. Под информационной безопасностью Республики Таджикистан понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства…

Выделяются четыре основные составляющие национальных интересов Республики Таджикистан в информационной сфере.

Первая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления республики, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны…

Вторая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя информационное обеспечение государственной политики, связанное с доведением до народа Таджикистана и международной общественности достоверной информации о государственной политике Республики Таджикистан, ее официальной позиции по социально значимым событиям Республики и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам…

Третья составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя применение современных информационных технологий, создание отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов…

Четвертая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории Республики Таджикистан…

Законодательство Таджикистан в сфере информационной безопасности развивается по следующим направлениям:

Закрепление общих положений о доступе к информации, о конфиденциальности и защите информации. Базовым актом здесь является Закон РТ “Об информации» и Закон РТ «О защите информации»…» ***(Обзор законодательства Республики Таджикистан в сфере информационной***

безопасности // Digital.Report (https://digital.report/zakonodatelstvo-tadzhikistana-v-sfere-informatsionnoy-bezopasnosti/).- 06.12.2017).

***

Міжнародне співробітництво у галузі кібербезпеки

«Заступник Міністра енергетики та вугільної промисловості України з питань європейської інтеграції Наталія Бойко зустрілася з делегацією корпорації MITRE (США)…

Наталія Бойко зазначила, що енергетична безпека є пріоритетним напрямком роботи Міненерговугілля. Реалізація політики кібербезпеки для підприємств електроенергетичної галузі включає, за її словами, цілий комплекс взаємоузгоджених комунікацій, скоординоване розгортання підрозділів кіберзахисту в паливно-енергетичному комплексі та організацію взаємодії зі спеціалізованими установами та міжнародною спільнотою.

Представники НЕК «Укренерго» поінформували про досвід компанії щодо ліквідації наслідків кібератак, які були раніше здійснені на комп'ютерні мережі деяких обленерго та НЕК «Укренерго». Зокрема, зазначено, що фахівцями компанії розроблено низку концепцій, спрямованих на запобігання загрозам енергетичній інфраструктурі… Крім того, фахівці компанії поінформували про створення в НЕК «Укренерго» відповідного центру реагування та розроблення плану відновлювальних робіт на випадок несанкціонованого втручання в роботу комп'ютерних мереж енергетичних підприємств.

Сторони обговорили можливості співпраці щодо забезпечення кібербезпеки, ефективного використання ресурсів та імплементації положень стратегії кібербезпеки, розробленої США, для зміцнення кібербезпеки енергосистеми України» ***(Міненерговугілля працює в напрямку зміцнення кібербезпеки об'єктів ПЕК // Кабінет Міністрів України (http://www.kmu.gov.ua/control/uk/publish/news_article?art_id=250483705&cat_id=244277212).- 07.12.2017).***

***

«Комітет у закордонних справах Палати представників США розглянув і рекомендував до схвалення проект "Закону 2017 про співпрацю з Україною з питань кібербезпеки"…

…законопроект визначає, що політикою США є надання допомоги Урядові України в удосконаленні власної стратегії кібер-безпеки.

Зокрема він діятиме в таких напрямах, як:

— встановлення найбільш сучасних безпекових оновлень на комп'ютерах органів державної влади;

— зменшення залежності України від російських технологій;

— сприяння розширенню участі України у програмах обміну інформацією, що пов'язана з проблематикою кібер-безпеки…» ***(Валентина Мартинюк. США підготували законопроект про допомогу Україні в сфері кібербезпеки // Інформаційне агентство «Українські Національні Новини»***

(http://www.unn.com.ua/uk/news/1704569-ssha-pidgotuvali-zakonoproekt-pro-dopomogu-ukrayini-v-sferi-kiberbezpeki).- 15.12.2017).

***

«НАТО завершило першу фазу надання допомоги Україні з кібербезпеки у межах трастового фонду і завершує планування другої фази. Про… сказав голова представництва НАТО в Україні Александер Вінніков під час круглого столу "Україна - НАТО. Рік зближення та інтеграції. Плани, очікування та підсумки взаємодії"…

Крім того, за словами голови представництва НАТО в Україні, трастовий фонд з питань медичної реабілітації продовжує надавати підтримку інституціям та окремим пацієнтам, фокусуючись на фізичній реабілітації та наданні протезів…» ***(Олександр Сивачук. НАТО незабаром розпочне реалізацію другої частини допомоги Україні з кібербезпеки // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1705096-nato-nezabarom-rozpochne-realizatsiyu-drugoyi-chastini-dopomogi-ukrayini-z-kiberbezpeki).- 18.12.2017).***

***

«…Комитет по иностранным делам Палаты представителей США рекомендовал нижней палате американского парламента принять законопроект о сотрудничестве с Украиной по вопросам кибербезопасности…

Этот законопроект определяет, что политикой США является оказание помощи правительству Украины в совершенствовании собственной стратегии кибербезопасности.

В частности, речь идет о таких направлениях, как установка более современных обновлений по безопасности на компьютерах органов государственной власти, в том числе систем программной защиты, направленных на защиту объектов критической инфраструктуры Украины; уменьшение зависимости Украины от российских технологий; содействие расширению участия Украины в программах обмена информацией, связанной с проблематикой кибербезопасности, и международных усилиях по противодействию киберугрозам, а также развитию нашей страной собственных возможностей в сфере кибербезопасности…» ***(Конгресс США порекомендовал украинскому парламенту принять закон о сотрудничестве в сфере кибербезопасности // E-NEWS.COM.UA. (http://e-news.com.ua/show/428192.html).- 15.12.2017).***

***

Кіберзахист критичної інфраструктури

«…Банки США объединились для запуска проекта Sheltered Harbor, призванного предотвратить крах финансовой системы в случае масштабной кибератаки на одну из кредитных организаций…

Проект предусматривает создание каждым банком резервной копии своих данных таким образом, чтобы другие участники могли получить к ним доступ, если работа банка будет нарушена. В настоящее время в проекте принимают участие крупнейшие банки и кредитные союзы США.

Данная инициатива направлена на минимизацию последствий при удалении или блокировке данных банка…

Для участия в проекте банки будут делать ежегодные взносы в размере от $250 до $25 тыс., в зависимости от размера кредитного учреждения. Участники должны следовать конкретным рекомендациям по форматированию данных, созданию резервного хранилища и предоставлению данных для аудита. Таким образом использовать резервную информацию пострадавшего учреждения можно будет в течение 48 часов после киберинцидента» ***(Банки США строят систему защиты от масштабных кибератак // SecurityLab.ru (https://www.securitylab.ru/news/490069.php).- 06.12.2017).***

***

«Специалисты советуют защищаться перед наступлением киберпреступности…

Специалисты уже создали специальную электронную карту, где показываются хакерские атаки. Этот процесс называется DDOSS, что является попыткой повлиять на работу в обслуживании систем. Например, искусственные перегрузки фейковыми звонками колл-центра полиции. Тогда реальный абонент не сможет позвонить правоохранителям и сообщить о какой-то опасности или преступлении.

"Поразило то, что у нас очень халатное отношение у многих государственных предприятиях, государственных органах власти по обеспечению безопасности своих собственных ресурсов. Они не могут защитить самих себя. Не говорю уже о тех данных, которые у них есть от граждан. То есть персональные данные граждан", - пояснил Егор Папишев, специалист по кибербезопасности.

Это касается данных от Госслужбы по чрезвычайным ситуациям, где разместили схемы коммуникаций кабелей связи; "Энергоатома", где выложили документы о доступе на территорию атомной электростанции; водоканала, где в свободном пространстве есть информация относительно удаленного управления подачи воды. Открытые данные нашли на ресурсах Херсонского облсовета, областной администрации, Донецкой военно-гражданской администрации и Государственного криминалистического центра, который занимается экспертизами преступлений.

Этот перечень, говорят активисты "Кибераль янса", которые как раз и объединились для обороны линии фронта в украинском киберпространстве, можно продолжать безконечно.

"Один из наших волонтеров обнаружил компьютер, который принадлежит Главному управлению Национальной полиции в Киевской области. Он пускает всех без пароля в сетевой диск "obmen Marina" с 150 гигабайтами информации областной полиции. Вместе с паролями, планами, протоколами, личными данными полицейских в свободном доступе", - сообщил специалист…

В октябре после сенсационной атаки на компьютерные системы вирусом Petya, который парализовал 90% инфраструктуры страны – от банков до аэропортов – в парламенте приняли закон "Об основных принципах обеспечения кибербезопасности Украины". Однако ситуация в стране так и не изменилась…» ***(Украина стала полигоном для киберпреступности, теряя данные и деньги // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/207407-ukraina_stala_poligonom_dlja_kiberprestupnosti_terjaja_dannye_i_denjgi).- 03.12.2017).***

***

«…Согласно сообщению департамента киберполиции Национальной полиции Украины, зафиксировано массовое распространение вируса-шифровальщика, известного как Scarab.

Этот вирус впервые был обнаружен специалистами по кибербезопасности в июне 2017 года. 24 ноября, было зафиксировано его распространения с помощью крупнейшей спам-ботнетсети «Necurs».

Специалисты по кибербезопасности установили, что с использованием «Necurs» было отправлено более 12,5 млн электронных писем в которых содержались файлы с новой версией Scarab ransomware…

За сутки в Департамент киберполиции Национальной полиции Украины не поступало обращений и заявлений по поводу поражения этим вирусом.

Для уменьшения риска заражения техники вирусом, специалисты по киберполиции рекомендуют пользователям тщательно и внимательно относиться ко всей электронной корреспонденции…» ***(Компьютеры украинцев атакует новый вирус-шифровальщик // PaySpaceMagazine «доступно о платежах» (https://psm7.com/news/kompyutery-ukraincev-atakuet-novyj-virus-shifrovalshhik.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29).- 04.12.2017).***

***

«Польша станет местом испытания программы по обеспечению киберзащиты авиационного сектора… После испытания данная система раннего оповещения об угрозах поможет сделать авиаперелеты более безопасными.

Сегодня специалисты авиационной сферы говорят о безопасности авиаперелетов и их защищенности от кибератак. Однако вместе с этим они признают, что вероятность таких атак есть, потому гражданская авиация должна быть готова противостоять современным угрозам…

Не стоит забывать и о самих воздушных судах. Развитие технологий предоставляет злоумышленникам новые возможности для нанесения большого ущерба…

Стоит отметить, что в 2015 г. польская авиакомпания LOT столкнулась с хакерской атакой, которая привела к приостановке деятельности компании на некоторое время. Были отменены многие рейсы, сотрудники варшавского аэропорта имени Фредерика Шопена в течение нескольких часов не могли

составить полетные планы. К счастью, проблема не затронула авиалайнеры, находившиеся в тот момент в воздухе. Представители авиакомпании назвали инцидент "первой атакой такого рода".

…Поэтому, полагает системный инженер Fortinet Андрей Терехов, гражданская авиация – одна из отраслей экономики, для которых обеспечение безопасности является наивысшим приоритетом» ***(Европейское агентство национальной безопасности (EASA) протестирует программу по обеспечению кибербезопасности для авиационного сектора // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120126).- 06.12.2017).***

***

«Национальный институт стандартов и технологий США (NIST) опубликовал вторую редакцию руководства по усилению кибербезопасности в критической инфраструктуре NIST Cybersecurity Framework…

Согласно заявлению NIST, вторая редакция версии 1.1 фокусируется на разъяснении, уточнении и расширении руководства, облегчая его использование, а также содержит обновленную "дорожную карту", в которой подробно описываются планы по дальнейшей разработке руководства.

Комментарии и отзывы по второй редакции могут быть отправлены в NIST до 19 января 2018 года. Изначально институт собирался опубликовать окончательный вариант руководства осенью текущего года, однако отстал от графика и теперь публикация запланирована на начало 2018 года…» ***(Национальный институт стандартов и технологий США опубликовал новую версию руководства по защите от киберугроз // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120211).- 11.12.2017).***

***

«В отчете, составленном экспертами FireEye, указано, что хакеры вмешались в работу объекта критической инфраструктуры. Используя специальную утилиту собственной разработки, кибергруппировка, вероятно, финансируемая властями одной из стран, пыталась перепрограммировать систему для мониторинга промышленных систем управления (ICS), спровоцировав неполадки в ее работе.

Эксперты не называют пострадавшее предприятие и его местоположение. Но в уведомлении от Symantec говорится, что был атакован объект в одной из стран Ближнего Востока (возможно, в Саудовской Аравии).

Злоумышленники пользовались вредоносной программой для того, чтобы манипулировать системами, которые позволяют внезапно завершать производственные процессы на предприятии. Утилита носит название TRITON, которая предназначается для вмешательства в работу системы Triconex Safety Instrumented System (SIS) производства Schneider Electric. Инструмент замаскирован под легитимное приложение, которое применяется для проверки логов.

В отчете FireEye утверждается, что хакеры заполучили доступ к рабочей станции Triconex SIS, которая функционирует под управлением Windows, и

установили вредоносную программу TRITON для перепрограммирования памяти приложений на контроллерах SIS. При перепрограммировании часть контроллеров SIS неудачно перешла в безопасный режим, что вызвало автоматическое завершение промышленных процессов.

Вероятно, хакеры не стремились к завершению работы процессов, которое происходит случайно. Злоумышленники хотели найти способ нанесения физический ущерба оборудованию через перепрограммирование контроллеров SIS…» ***(Выявлена новая вредоносная программа TRITON // SecureNews (https://securenews.ru/triton/).- 15.12.2017).***

***

«Основной угрозой кибербезопасности в банковской сфере является социальная инженерия, на которую приходится 80% всех атак на клиентов, сообщает «Интерфакс» со ссылкой на руководителя службы информационной безопасности Сбербанка Сергея Лебедя.

По словам Лебедя, Сбербанк ежедневно фиксирует около 2 тыс. обращений клиентов, связанных с мошенничеством, а за год в черные списки банка попадает около 50 тыс. мошенников, пытавшихся обмануть частных клиентов, и еще несколько тысяч, атаковавших юридических лиц.

Лебедь посетовал, что черные списки банка «не востребованы правоохранительной системой, все попытки передать эту информацию в ФСБ и МВД не находят понимания, что этим нужно заниматься».

Операторы связи также отмечают случаи банковского мошенничества, добавил Лебедь» ***(Сбербанк: главная киберугроза для клиентов — социальная инженерия // «Открытые системы» (https://www.computerworld.ru/news/Sberbank-glavnaya-kiberugroza-dlya-klientov--sotsialnaya-inzheneriya).- 11.12.2017).***

***

Кіберзлочинність та кібертерроризм

«…Аналитический центр компании InfoWatch представляет обзор крупнейших утечек, зарегистрированных в сентябре-ноябре 2017 года.

В начале осени стало известно о том, что хакеры украли данные более 28,7 млн учетных записей социального сервиса Taringa, воспользовавшись тем, что разработчики использовали устаревший алгоритм шифрования…

Крупнейшая утечка в истории Малайзии была раскрыта в октябре. По Интернету передавалась база, содержащая данные 46,2 млн абонентов операторов мобильной связи: номера, адреса клиентов, информация о SIM-картах. В краже информации обвинили хакеров из Нидерландов и Гонконга. Судя по всему, взлом операторских серверов произошел еще в 2014 году.

В ноябре компания Uber призналась, что с ее серверов еще прошлой осенью были похищены данные клиентов и таксистов – всего более 57 млн человек… Вместо своевременного оповещения регуляторов и оказания незамедлительной

поддержки пострадавшим представители Uber предпочитали вести переговоры с хакером, укравшим базу данным. Известно, что злоумышленник получил от компании выкуп в размере $100 тысяч.

Информацию о гигантской утечке раскрыло бюро кредитных историй Equifax. Несколько месяцев злоумышленники использовали уязвимость на сайте компании и успели похитить данные более 143 млн человек. Затронута личная информация клиентов Equifax в разных странах, но в основном потерянная информация касались граждан США….

Примерно половина населения пострадало и в Китае. Преступная группа в составе семи человек вступала в сговор с топ-менеджерами ряда крупных компаний и получала доступ к персональным данным. Всего было украдено более 700 млн записей, в том числе весьма чувствительные сведения. Более 80 млн записей злоумышленники успели продать через группы в соцсетях, выручив порядка $180 тысяч» ***(Топ-5 утечек осени-2017 // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5460292-Top5-utechek-oseni2017.html#ixzz51iAFgU5O).- 18.12.2017).***

***

«Влада КНДР руками хакерів атакує біржі криптовалюти, зокрема біткоінів…

Разом зі своїми колегами Ешлі Шен, дослідник кібербезпеки відстежувала атаки ймовірних угруповань хакерів з КНДР на фінансові інститути, в тому числі біржі біткоінів. За її словами, зломники мають намір заволодіти саме криптовалютою. Однак, додала експерт, поки їх спроби не мають успіху.

…якщо раніше хакери КНДР здійснювали атаки для того, щоб паралізувати суспільство, то тепер - щоб заволодіти коштами…» ***(Північнокорейські хакери обрали своєю ціллю біржі біткоїну // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1703646-pivnichnokoreyski-khakeri-obrali-svoyeyu-tsillyu-birzhi-bitkoyinu).- 11.12.2017).***

***

***«*…Хакерская атака на сайты и компьютерную сеть «Интерфакса», которая буквально «выключила» большинство новостных потоков более чем на сутки, была проведена «российской структурой, имеющей непосредственное отношение к разработке и распространению информации», — сообщила «Российская газета», ссылаясь на источник из агентства.**

Специалисты «Интерфакса» уверены: сам характер, интенсивность и степень координации вирусной атаки свидетельствуют о том, что настоящей целью ее авторов было не получение выкупа в несколько биткойнов, а демонстрация своих возможностей по разрушению коммуникаций крупных СМИ или попытка давления для достижения каких-то иных целей…

Исполнительный директор «Интерфакса» Владимир Герасимов подтвердил, что руководство информационного агентства готово поделиться своими подозрениями с правоохранительными органами.

«У нас есть определенные подозрения, кто бы это мог быть. Мы подали в связи с этой атакой заявление в УВД ЦАО и по нему возбуждено уголовное дело по статье 273 УК РФ», — сообщил он в интервью газете…

Кибератака на «Интерфакс» была проведена при помощи последней версии вируса-вымогателя Bad Rabbit, разработанного для ОС семейства Windows и обнаруженного 24 октября 2017 года… По предположениям аналитиков, программа имеет сходство отдельных фрагментов с вирусом NotPetya, ранее атаковавшим компьютерные сети на Украине, в Турции и Германии…» ***(Стало известно, кто стоял за атакой «плохого кролика» // Парламентская газета (https://www.pnp.ru/social/stalo-izvestno-kto-stoyal-za-atakoy-plokhogo-krolika.html).- 08.12.2017).***

***

«…В «Лаборатории Касперского», что в предстоящем году «атаковать будут… большие компании с надежной и многослойной киберзащитой». В таких случаях, как считают в «Лаборатории Касперского», проще использовать посредника, в роли которого может быть «производитель популярных программ, используемых в корпоративном сегменте»…

Также под угрозой взломов могут оказаться домашние роутеры и модемы. В связи с этим в компании рекомендуют юзерам сменить заводские пароли, а также по возможности выделить отдельную подсеть для домашних устройств.

В релизе «Лаборатории Касперского» отмечается, что роутеры и модемы «играют роль своеобразных «привратников», открывающих дверь в интернет, что делает их целью злоумышленников, когда те хотят незаметно закрепиться в сети»…» ***(Антон Касс. «Лаборатория Касперского» рассказала о мишенях кибератак в 2018 году // ООО «Деловая газета «Взгляд» (https://vz.ru/news/2017/12/6/898360.html).- 06.12.2017).***

***

«Полковник ФСБ Сергій Михайлов і ще троє обвинувачених у РФ у справі про державну зраду могли співпрацювати з американськими спецслужбами у справі про хакерські атаки перед виборами в США..

За даними журналістів The Bell, вони могли допомогти американським спецслужбам отримати докази причетності російських хакерів до злому серверів Демократичної партії США. Офіційних підтверджень цьому з американської сторони The Bell отримати не вдалося…

Американські спецслужби вважають, що саме в Головному розвідувальному управлінні організували хакерські атаки перед виборами. Сергій Михайлов працював у Центрі інформаційної безпеки ФСБ Росії. За даними журналістів, Михайлов співпрацював з ФБР…

Михайлова і ще трьох людей затримали у справі про держзраду наприкінці 2016 року. Їх звинувачують у передачі інформації іноземним спецслужбам. Справа слухається в закритому режимі.

ЗМІ повідомляли, що Федеральне бюро розслідувань США приховувало інформацію про російські хакерські атаки від офіційних осіб, пошту яких

намагалися зламати…» ***(Полковник ФСБ розкрив американцям докази російського втручання у вибори, - ЗМІ // Espreso.tv (https://espreso.tv/news/2017/12/05/polkovnyk_fsb_rozkryv_amerykancyam_dokazy_rosiyskogo_vtruchannya_u_vybory_zmi).- 05.12.2017).***

***

«Сбій системи сервісу покупки та продажу обчислювальних потужностей для створення нових криптовалют NiceHash привів до крадіжки Bitcoin, що становить понад $70 млн…

Керівник відділу маркетингу NiceHash Андрій Шкраба зазначив, що через кібератаку один із онлайн-гаманців втратив 4,7 тыс. Bitcoin. Співробітники сервісу нині працюють над тим, щоб відновити повноцінну роботу сервісу та усунути проблем….» ***(Викрали мільйони: хакери "взламали" біржу криптовалют // Народна Правда (https://narodna-pravda.ua/2017/12/08/vykraly-miljony-hakery-vzlamaly-birzhu-kryptovalyut/).- 08.12.2017).***

***

«Хакер з російського міста Єкатеринбург заявив про свою причетність до хакерських атак у США, зокрема, до зламу комітету Демократичної партії США…

Хакер на ім'я Костянтин Козловський є, одним з основних обвинувачених у справі групи Lurk — її учасників звинувачують в численних банківських зламах…

Видання The Bell повідомляє, у серпні 2017 року Козловський дав свідчення в Московському міському суді, з яких випливало, що він нібито багато років співпрацював з ФСБ і за дорученням її співробітників займався, в тому числі, зламами на території США.

Хакер на суді заявив, що «виконував різні завдання під керівництвом співробітників ФСБ, зокрема, «злам »Національного комітету Демократичної партії США та електронного листування Хілларі Клінтон», а також «зламував дуже серйозні військові підприємства США та інші організації»…

Суддя Московського суду підтвердила, що це засідання дійсно відбулось 15 серпня 2017 року…» ***(Російський хакер заявив про причетність до кібератак у США — ЗМІ // «Громадське радіо» (https://hromadskeradio.org/news/2017/12/11/rosiyskyy-haker-zayavyv-pro-prychetnist-do-kiberatak-u-ssha-zmi).- 12.12.2017).***

***

«Хакеры, связанные с иранским правительством, с 2014 года занимаются кибершпионажем в отношении ряда ближневосточных государств, сообщает… американская компания FireEye, которая специализируется на кибербезопасности…

В отчете компании содержится утверждение, что деятельность группы хакеров APT34… нацелена на государственные учреждения, частный сектор, включая финансы, энергетику, химпром и телекоммуникации» ***(Иран осуществляет кибершпионаж против ряда ближневосточных государств //***

Интерфакс-Украина (http://interfax.com.ua/news/general/468198.html).- 08.12.2017).

***

«Украинцам стоит готовится к массовым спам-рассылкам вирусов от интернет-магазинов под Новый год. Хакеры нашли новый способ забраться в кошельки покупателей. Они «ломают» веб-ресурсы украинских компаний через программу управления сайтами 1С-Битрикс.

Также интернет-площадки могут в дальнейшем использоваться как звено в цепи компьютеров, осуществляющих массированные ddos-атаки на другие предприятия…

«Использование платформ SMB (малый, средний бизнес) — это новый тренд. Начиная от вымогательства денег для восстановления работы сайта, и заканчивая скрытым проникновением через Битрикс и ее использованием для разного рода действий: спам-рассылок, массовой регистрации на почтовых сервисах, распространения бот-сетей и пр.», — рассказал член Комитета по кибербезопасности Ассоциации профессионалов корпоративной безопасности Украины (АПКБУ), R&D директор компании «IT Интегратор» Владимир Кург» ***(Хакеры всерьез взялись за украинские интернет-магазины // Вести-UA || Новости Украины | Новини України (https://vesti-ua.net/novosti/obschestvo/54370-hakery-vserez-vzyalis-za-ukrainskie-internet-magaziny.html).- 08.12.2017).***

***

«Тысячи британских компаний заплатили выкуп российским хакерам, которые устраивают сотни атак каждый день, требуя до 100 тыс. фунтов за возврат доступа к файлам.

По словам экспертов, "эпидемия" вирусов-вымогателей стала крупнейшей киберугрозой для страны и оказалась намного масштабнее майской атаки Wannacry, которая парализовала ИТ-системы десятков трастов NHS…

300 из 1500 британских компаний, опрошенных правительством в этом году, сообщили, что стали жертвами вымогателей, 120 организаций заявили, что атаки с целью получения выкупа стали причиной значительных нарушений в их работе. Согласно исследованию Malwarebytes, 43 процента компаний, ставших объектом кибератак до июля, заплатили выкуп.

Предполагается, что это могли сделать до 180 000 предприятий. Другие опросы показывают, что компании в Великобритании более охотно платят выкуп, чем находящиеся где-либо в другом месте.

Жертвами хакеров стали крупные компании, банки лондонского Сити, государственные организации и отдельные люди.

Хакеры обычно обманом вынуждаю жертв открывать электронные письма с вирусами, заражающими компьютеры и требующими выплаты от 350 до 100 тыс. фунтов в биткоинах за восстановление доступа к файлам.

Ущерб от атак для экономики, с учетом вынужденной остановки деятельности, потерянных доходов, информационно-технологических повреждений, уничтожения данных, судебной экспертизы и переподготовки

сотрудников, оценивается более чем в 1 млрд фунтов…» ***(The Times: Российские хакеры требуют выкуп у Британии // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/208371-the_times_rossijskie_hakery_trebujut_vykup_u_britanii).- 08.12.2017).***

***

«Масштабную кибератаку с помощью вируса-шифровальщика BadRabbit, в ходе которой пострадали многие организации по всему миру, спланировала российская структура. Об этом ссылаясь на источники, сообщает Российская газета.

Отмечается, что интенсивность и сам характер вирусной атаки доказывают, что ее целью было не получение выкупа, а демонстрация возможностей по разрушению коммуникаций крупных СМИ или в каких-либо других целях…

Как сообщалось, вирус Bad Rabbit который атаковал во вторник, 24 октября, Украину, зафиксировали также и в России, Турции и Германии. Для распространения вируса BadRabbit использовалось фейковое обновление Adobe Flash Player.

Глава киберполиции Украины Сергей Демедюк считает, что за кибератакой крылся более серьезный взлом» ***(За масштабной кибератакой BadRabbit стоит российская структура – СМИ // AllSvit (http://allsvit.net/allnews/za_masshtabnoy_kiberatakoy_badrabbit_stoit_rossiyskaya_struktura__smi/).- (08.12.2017).***

***

«…Германия подозревает китайских хакеров в кибершпионаже. Об этом 11 декабря сообщила пресс-служба Федерального ведомства по охране конституции по итогам многомесячного расследования. В частности, сообщается, что были зафиксированы попытки китайских хакеров при помощи "новых методов" проникнуть во внутренние сети различных ведомств и компаний.

Киберпреступники, говорится в сообщении, нападали на цели не впрямую, а через интернет-провайдера пытались получить доступ к интересующим их источникам информации и установить в сетях ведомств и компаний программы для "скачивания" секретных данных.

Помимо этого, внимание немецких спецслужб привлекла деятельность хакеров в социальных сетях, в частности, LinkedIn…

В Пекине отвергают обвинения. В частности, китайская сторона утверждает, что не использовала соцсети для взлома аккаунтов немецких политиков и бизнесменов…» ***(Григорий Аросев.ФРГ подозревает китайских хакеров в кибершпионаже // Deutsche Welle (http://www.dw.com/ru/%D1%84%D1%80%D0%B3-%D0%BF%D0%BE%D0%B4%D0%BE%D0%B7%D1%80%D0%B5%D0%B2%D0%B0%D0%B5%D1%82-%D0%BA%D0%B8%D1%82%D0%B0%D0%B9%D1%81%D0%BA%D0%B8%D1%85-%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D0%BE%D0%B2-%D0%B2-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%88%D0%BF%D0%B8%D0%B***

E%D0%BD%D0%B0%D0%B6%D0%B5/a-41744759?maca=rus-rss-MetaUA_rus_V_Mire-3045-xml-mrss).- 11.12.2107).

***

«Российская компания в сфере кибербезопасности Group-IB сообщила об изменении интереса хакеров, которые теперь в своей деятельности больше переключаются с банков на криптоиндустрию…

«Многие крупные преступные группы полностью переключились на криптоиндустрию», — сказал основатель компании Илья Сачков в ходе VIII международного форума по борьбе с мошенничеством в сфере высоких технологий AntiFraud Russia.

Основатель Group-IB пояснил, что в этом кроется практическая сторона вопроса — хакерам значительно проще обменять криптовалюту на фиатные деньги (доллары, евро и другие), которые позже можно перевести на банковские карты и обналичивать в любой стране» ***(Валерий Вискалин. Group-IB рассказала о переключении хакеров с банков на криптоиндустрию // Rusbase (https://rb.ru/news/group-ib-crypto/).- 06.12.2017).***

***

«Европол рапортует об успешном завершении международной операции по низвержению одного из крупнейших ботнетов, известного как Andromeda и Gamarue…

Вредоносное семейство Andromeda известно издавна, и прежде всего тем, что его представители зачастую используются для загрузки других зловредов…

Возможности Andromeda также с успехом использовала криминальная группировка Avalanche, обезвреженная год назад. Данные, собранные в ходе той совместной операции, помогли исследователям подготовить разгромную акцию против Andromeda.

Ныне совместными усилиями, как сообщает Европол, удалось выявить 1,5 тыс. доменов, ассоциированных с командной инфраструктурой Andromeda, и подменить по методу sinkhole семь ключевых серверов, которые злоумышленники использовали для управления 464 небольшими ботнетами, построенными на основе Andromeda. По данным некоммерческой организации Shadowserver Foundation, в течение первых двух суток с sinkhole-серверами пытались связаться около 2 млн уникальных IP-адресов (зараженных хостов), прописанных в 223 странах.

В ходе трансграничной операции был также произведен один арест: в Беларуси по наводке ФБР задержан житель Гомельской области, подозреваемый в принадлежности к ОПГ, стоящей за Andromeda. Федеральные агенты уличили его в торговле вредоносным ПО и оказании соответствующих услуг по техподдержке. В настоящее время задержанный находится под стражей, активно сотрудничает со следствием и дает признательные показания…» ***(Maxim Zaitsev. Долгожитель Andromeda повержен // Threatpost (https://threatpost.ru/andromeda-botnet-busted/23544/).- 05.12.2017).***

***

«Белорусское телеграфное агентство сообщает, что в одном из районных судов Минска огласили приговор по делу 21-летнего россиянина, совершившего ряд киберпреступлений.

Молодой человек занимался разработкой и распространением вирусных программ-вымогателей. С их помощью злоумышленник блокировал информацию на устройстве жертвы. При каждом последующем обращении к зараженным данным всплывало окно с требованием заплатить «штраф за просмотр и хранение запрещенных законом материалов».

Суд подтвердил виновность россиянина в преступлениях по нескольким статьям УК Беларуси: компьютерный саботаж, использование вредоносных программ и несанкционированный доступ к компьютерной информации. В качестве наказания злоумышленник проведет четыре года в колонии усиленного режима с конфискацией имущества.

По версии следствия, преступник действовал не в одиночку, а при поддержке сообщников, которые на данный момент разыскиваются. По оперативным данным, за два месяца зафиксировано более 600 удачных атак со стороны группы злоумышленников.

В 2016 году более 300 жителей Беларуси стали жертвами группы мошенников, которые вымогали деньги при помощи блокировщика экрана… Суммы взносов варьировались от 50 тысяч до 1 миллиона белорусских рублей. При этом зловред продолжал действовать даже после задержания предполагаемых преступников…» ***(Egor Nashilov. Вымогательство в сети: суд Минска признал россиянина виновным // Threatpost (https://threatpost.ru/minsk-court-finds-russian-cybercrook-guilty/23572/).- 06.12.2017).***

***

«Наиболее серьезной угрозой кибербезопасности «Сбербанк» считает не уязвимости в системах, приложениях или защитных программах, а человеческий фактор. Большинство атак — около 80% — становятся возможны из-за действий самого пользователя. Об этом на VIII международном форуме по борьбе с компьютерным мошенничеством Antifraud Russia сообщил руководитель службы информационной безопасности банка Сергей Лебедь…

Уязвимостями в данном случае становятся как сотрудники, которые открывают подозрительные файлы, так и администраторы, которые не обновляют вовремя систему. Сами клиенты тоже легко могут стать жертвами манипуляций и предоставить злоумышленникам пароли, PIN-коды или другую конфиденциальную информацию…

При помощи рассылок злоумышленники получают доступ к сети банка, затем закрепляются в ней и начинают изучать внутреннюю инфраструктуру, фиксируя активность сотрудников и анализируя работу банковских программ. Свои сообщения они искусно маскируют под деловую переписку…» ***(Egor Nashilov. Сбербанк считает мошенничество основной угрозой безопасности // Threatpost (https://threatpost.ru/sberbank-claims-social-engineering-is-the-main-threat/23652/).- 08.12.2017).***

***

«Серьезный скандал разразился вокруг компании Ai.Type – разработчика одноименного приложения, представляющего собой виртуальную клавиатуру для мобильных устройств. Выяснилось, что один из серверов компании не был защищен паролем. И доступ к базе данных общим объемом в 577 гигабайт мог получить буквально любой желающий.

Информация включает данные 31 миллиона пользователей и их устройств, в том числе имена, номера телефонов, адреса электронной почты, логины ассоциированных аккаунтов в социальных сетях, а также названия и модели устройств, IMEI-идентификаторы и т.д.

Неприятная находка была сделана специалистами компании Kromtech Security Center… Специалисты по кибербезопасности крайне встревожены инцидентом и призывают Федеральную комиссию по связи США (FCC), государственного регулятора отрасли, принять меры против Ai.Type, нарушившей свои обязательства» ***(В открытом доступе нашлись данные 31 миллиона пользователей Ai.Type // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5457564-V-otkrytom-dostupe-nashlis-dannye.html#ixzz51E52gjuF).- 07.12.2017).***

***

«Компания «Доктор Веб» уже рассказывала о троянце Linux.ProxyM, способном заражать «умные» устройства под управлением ОС Linux…

В сентябре аналитикам «Доктор Веб» стало известно, что злоумышленники рассылали с использованием Linux.ProxyM более 400 спам-сообщений в сутки с каждого инфицированного устройства. Письма рекламировали ресурсы «для взрослых» и сомнительные финансовые услуги. Вскоре киберпреступники стали использовать «Интернет вещей» для распространения фишинговых сообщений…

В декабре киберпреступники нашли новое применение зараженным Linux.ProxyM устройствам: используя реализованный в троянце прокси-сервер для сохранения анонимности, они стали предпринимать многочисленные попытки взлома веб-сайтов…

Специалисты «Доктор Веб» продолжают следить за активностью ботнета Linux.ProxyM…» ***(Злоумышленники взламывают сайты с помощью «Интернета вещей» // ООО "ИКС-МЕДИА"(http://www.iksmedia.ru/news/5457794-Zloumyshlenniki-vzlamyvayut-sajty.html#ixzz51E5qN5hv).- 07.12.2017).***

***

«Связанная с ДАИШ хакерская группировка Electronic Ghosts пригрозила масштабной кибератакой на правительства и военные ведомства по всему миру 8 декабря 2017 года…

По словам экспертов, нельзя точно сказать, насколько реальна данная угроза, однако можно с уверенностью заявить о низком профессионализме связанных с ДАИШ хакеров.

Хакерская группировка Electronic Ghosts - одна из четырех связанных с ДАИШ группировок, объединившихся в 2016 году для создания так называемого Объединенного Киберхалифата. До 24 ноября текущего года данное хакерское объединение бездействовало…» ***(Мусульманские хакеры пригрозили миру масштабной кибератакой 8 декабря // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120166).- 07.12.2017).***

***

«27-летний хакер из штата Мичиган (США) осуществил взлом правительственной компьютерной системы тюрьмы в округе Уоштено и теперь должен предстать перед судом…

В ходе заседания суда Конрадс Войтс признал свою вину за атаку компьютерной системы, принадлежащей правительству округа Уоштено, в начале этого года…

Войтсу удалось заполучить учетную информацию одного из сотрудников тюрьмы и воспользоваться ею для того, чтобы установить вредоносную программу в сеть округа и взломать систему XJail в марте этого года.

Войтс украл записи о заключенных, показания под присягой и конфиденциальную информацию свыше 1600 сотрудников тюрьмы. Кроме того, он скорректировал данные как минимум об одном заключенном, чтобы тот был досрочно освобожден.

Сотрудники тюрьмы заметили изменения в документах и сообщили о случившемся в ФБР. Правительство округа потратило свыше 235000 долларов на устранение последствий хакерской активность.

Через месяц после взлома хакер был арестован. Позже он признал свою вину. Злоумышленника могут приговорить к 10 годам лишения свободы и штрафу в размере до 250000 долларов» ***(Хакер взломал систему тюрьмы, чтобы досрочно освободить друга // SecureNews (https://securenews.ru/jail/).- 05.12.2017).***

***

«Как указано в отчете израильской ИБ-компании ClearSky Cybersecurity, иранец Бехзад Месри, обвиняемый во взломе телекомпании HBO, был членом кибергруппировки Charming Kitten.

Charming Kitten функционирует с 2013 года и, вероятно, сотрудничает с властями Ирана. Кроме того, эта кибергруппировка известна как Ajax Security Team, Flying Kitten, NewsBeef и Newscaster...

В официальном обвинительном заключении говорится, что Месри работал на иранскую армию и вместе с этим был вовлечен в хакерскую деятельность. Есть доказательства того, что Месри скомпрометировал сотни разных сайтов и, вероятнее всего, взломал компьютерные системы телеканала HBO. Эти действия он осуществил сам, не взаимодействуя с Charming Kitten, целью которой являются, прежде всего, иранские диссиденты…

Сейчас Месри находится в Иране. Иранские власти никак не прокомментировали обвинения американского правительства» ***(Хакер,***

атаковавший HBO, был участником кибергруппировки Charming Kitten // SecureNews (https://securenews.ru/hbo_3/).- 07.12.2017).

***

«Вьетнамский хакер Ле Дюк Хоанг Хай взломал компьютерные системы международного аэропорта в австралийском городе Перт и украл большое количество документов, включая информацию о системе безопасности и планы строительства…

Как утверждают власти Австралии, злоумышленник не смог нарушить работу систем, связанных с радарами и самолетами.

Сотрудники аэропорта выявили факт взлома и сообщили в Австралийский центр кибербезопасности, расположенный в Канберре, а также проинформировали о случившемся представителей Австралийской федеральной полиции. В ходе расследования удалось выяснить, что злоумышленник является жителем Вьетнама. Австралийские правоохранители сообщили об этом своим коллегам из Вьетнама, которые вскоре арестовали злоумышленника. Киберпреступник был приговорен вьетнамским военным судом к лишению свободы сроком в четыре года…» ***(Хакер из Вьетнама осуществил взлом систем международного аэропорта в Австралии // SecureNews (https://securenews.ru/vietnamese_hacker/).- 11.12.2017).***

***

«Експерти стежать за активністю нового троянця віддаленого доступу під назвою UBoatRAT, який зловмисники використовують проти організацій і співробітників зі зв'язками з Південною Кореєю або індустрією відеоігор.

…дослідники з підрозділу Unit 42 компанії Palo Alto Networks виявили, що UBoatRAT еволюціонує і стає все більш витонченим. Так, у вересневих зразках зловреда з'явилися нові методи маскування і закріплення в системі…

Перш за все BITS застосовується для розповсюдження оновлень Windows і стороннього ПО. У цієї служби багата історія по частині коректного використання, що тягнеться ще з 2007 року. Але навіть до цього дня BITS привертає хакерів, оскільки цей компонент Windows здатний отримувати або відправляти файли через додатки, яким довіряє мережевий екран комп'ютера…

Дослідники з'ясували, що творці UBoatRAT використовують інструмент командного рядка Bitsadmin.exe служби BITS, щоб створювати і відстежувати завдання BITS…» ***(Шпигунський троянець атакує Східну Азію через Google Диск // ООО "Центр інформаційної безпеки" (http://www.bezpeka.com/ua/news/2017/12/05/UBoatRAT.html).- 05.12.2017).***

***

«Ранее эксперты ESET уже сообщали о киберкампании по распространению шпионского ПО FinFisher (FinSpy). Данная операция проводилась в семи странах. Специалисты подозревали, что в кампании мог принять участие крупный интернет-провайдер. 21 сентября был опубликован отчет ESET, после чего киберкампания была остановлена.

Саму шпионскую программу FinFisher (FinSpy) создали сотрудники немецкой фирмы Gamma Group International, а за ее продажу отвечает дочерняя компания Gamma Group, чей офис расположен в Великобритании. Распространение FinFisher осуществляется среди правоохранительных органов разных государств…

Недавно эксперты ESET сообщили, что 8 октября в одной из стран, где за распространением FinFisher мог стоять интернет-провайдер, началась еще одна такая операция, в рамках которой применяется идентичная схема переадресации браузеров. Однако теперь осуществляется распространение не FinFisher, а новой шпионской программы – StrongPity2. В ESET изучили вредоносное ПО и нашли общие черты с шпионской программой, которая ранее, вероятно, использовалась хакерской группой StrongPity…

С 8 октября сотрудники ESET выявили свыше ста попыток атак с применением StrongPity2» ***(ESET вновь сообщает о шпионской киберкампании, в которой участвует интернет-провайдер // SecureNews (https://securenews.ru/strongpity2/).- 13.12.2017).***

***

«Американские власти «после тщательного расследования» официально возложили на КНДР ответственность за масштабную кибератаку, проведенную с использованием вируса WannaCry, сообщил помощник Дональда Трампа по вопросам внутренней безопасности Том Боссерт.

По его словам, обвинение в адрес Пхеньяна «основывается на доказательствах»…» ***(Ольга Никитина. США обвинили КНДР в распространении вируса WannaCry // ООО «Деловая газета Взгляд» (https://vz.ru/news/2017/12/19/900231.html).- 19.12.2017).***

***

«Киберпреступники начали использовать специальные программы для добычи криптовалюты на смартфонах без ведома пользователей устройств…

Ряд мобильных игр предлагают пользователям при запуске программы начать добывать криптовалюту для разработчика игры, в свою очередь пользователи за это получают вознаграждение игровой валютой…

Эксперт «Лаборатории Касперского» считает, что такие программы нельзя однозначного называть вредоносными, так как пользователи запускают их по своей воле…

Представитель Group-IB Сергей Никитин напоминает, что сейчас программы-майнеры запрещены в официальных магазинах приложений, поэтому их разработчики часто маскируют софт под развлекательные программы, чтобы добывать криптовалюту без ведома владельцев смартфонов…» ***(Валерий Вискалин. Хакеры научились «взламывать» смартфоны для майнинга криптовалюты // Rusbase (https://rb.ru/news/hacker-mining-gadget/).- 15.12.2017).***

***

«…15 декабря была зафиксирована успешная кибератака на один из российских банков, сообщили “Ъ” специалисты по информационной

безопасности и подтвердили в ЦБ. Особенность атаки в том, что денежные средства были выведены через SWIFT (международная межбанковская система передачи информации и совершения платежей), которую до сих пор хакеры в России не использовали. Название банка и размер ущерба не раскрываются.

…к атаке причастна группировка Cobalt. Проникновение в банк произошло через вредонос, который рассылался группировкой несколько недель назад по банкам, что характерно для Cobalt. В среднем промежуток от проникновения до вывода денег составляет три-четыре недели, средняя сумма хищения — 100 млн руб…

FinCERT, структурное подразделение ЦБ по информбезопасности, в своем отчете назвал группу Cobalt главной угрозой для кредитных организаций. …на счету группировки не менее 50 успешных атак на банки по всему миру…

Атака 15 декабря, по словам экспертов, отличается от уже привычных лишь способом вывода средств. Эксперты в области информационной безопасности до сих пор об использовании хакерами SWIFT при атаках на банки в РФ не слышали…

В SWIFT отказались комментировать «отдельных клиентов», но подчеркнули: «Мы очень серьезно относимся к кибербезопасности и изучаем все угрозы, принимая все соответствующие меры. Нет доказательств, что имел место какой-либо несанкционированный доступ к сетям SWIFT или ее службам обмена сообщениями». В российском случае SWIFT действительно не была именно объектом атаки…» ***(Вероника Горячева, Евгений Хвостик, Яна Рождественская. Хакеры прибежали на SWIFT. В России впервые атаковали банк через международную систему // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3501353?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).- 19.12.2017).***

***

«Компания Trend Micro рассказала об обнаружении двух новых видов вредоносного ПО для атак на банкоматы.

Один из вирусов активно распространяется сейчас, в том числе, на российских киберкриминальных ресурсах. Он носит название Cutlet Maker и используется для получения больших сумм наличных. Его особенность состоит в том, что вредоносное ПО технически не инфицирует систему банкомата, а запускается с внешнего USB-носителя.

…зловред, получивший название Prilex, …служит для похищения данных карт и пин-кодов клиентов. Вредоносное ПО подменяет экран для ввода пин-кода на свой собственный. Примечательно, что похищенные данные вскоре передаются на подконтрольный киберпреступникам сервер. По словам представителей Trend Micro, это едва ли не первый зловред, нацеленный на банкоматы, который предполагает интернет-соединение для передачи данных…» ***(Обнаружены два новых зловреда, атакующих банкоматы // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5460350-Obnaruzheny-dva-novyx-zlovreda-atak.html#ixzz51iBL8yIg).- 19.12.2017).***

***

«Специалисты ESET обнаружили новый банковский троян, которому удалось проникнуть в Google Play. Вредоносная программа маскируется под приложение для мониторинга курса криптовалют Crypto Monitor и StorySaver, инструмент для загрузки историй из Instagram.

Первое из вредоносных приложений – Crypto Monitor – было загружено в Google Play в ноябре разработчиком walltestudio. Второе – StorySaver от разработчика kirillsamsonov45 – появилось 29 ноября. Приложения набрали в общей сложности 1000–5000 загрузок и были удалены в начале декабря после предупреждения специалистов ESET.

Вредоносные приложения поддерживают заявленные функции, но, помимо этого, могут выводить на экран собственные сообщения, красть логины и пароли мобильного банка и перехватывать смс, используемые для двухфакторной аутентификации…» ***(В Google Play обнаружен новый банковский троян // ООО "ИКС-МЕДИА"(http://www.iksmedia.ru/news/5460468-ESET-nashla-novyj-bankovskij-troyan.html#ixzz51iBqUshc).- 19.12.2017).***

***

«…**25-летний Грант Уэст (Grant West) признался в совершении кибер-нападений** на компании Uber, Groupon, T Mobile, Just Eat, Ladbrokes, Asda, Argos, Nectar, Sainsburys, AO.com, Coral Betting, Vitality, RS Feva Class Association 2017, Британское сердечно-сосудистое общество, Mighty Deals Limited, Truly Experiences Ltd и MR Porter.

Следователи заявили, что кража учетных данных пользователей со страниц входа на сайты происходила с помощью Sentry MBA, программы атакующей методом подбора паролей.

Уэст позже использовал украденные данные для входа в учетные записи и сбора информации о пользователях.

Полиция утверждает, что Уэст открыл магазин в Dark Web, где в обмен на биткойны предлагал данные с 17 сайтов, которые ему удалось успешно атаковать…

Власти арестовали Уэста, и теперь он ожидает вынесения приговора, на прошлой неделе признав себя виновным» ***(Британский хакер признал себя виновным в нападениях на Uber, Groupon, T Mobile и другие компании // SecureNews (https://securenews.ru/hackercourvoisier/).- 18.12.2017).***

***

«Окружной суд штата Аляска заслушал заявления о признании вины в рамках трех уголовных дел о создании и противоправном использовании двух ботнетов. Парасу Джха (Paras Jha), проживающему в Нью-Джерси, Джосае Уайту (Josiah White) из Пенсильвании и Долтону Норману (Dalton Norman) из Луизианы инкриминируют преступный сговор и правонарушения, оговоренные в Законе о компьютерном мошенничестве и злоупотреблении (Computer Fraud & Abuse Act).

По версии следствия, за лето и осень прошлого года криминальное трио построило ботнет Mirai, массово захватывая контроль над роутерами, IP-камерами

и DVR. Злоумышленникам удалось инфицировать сотни тысяч IoT-устройств, которые они затем использовали для проведения мощнейших DDoS-атак…

Джха и Норман также признались, что с декабря 2016 года по февраль 2017-го они успешно заразили более 100 тыс. сетевых устройств с целью подзаработать на мошенническом показе рекламы…

Расследование деятельности молодых людей проводило ФБР; активную помощь федералам оказали британское Национальное управление по борьбе с преступностью (NCA), Главное управление внутренней безопасности Франции (DGSI), американская некоммерческая организация NCFTA (National Cyber-Forensics & Training Alliance), объединяющая специалистов по компьютерно-технической экспертизе, а также исследователи из Palo Alto Networks, Google, Cloudflare, Coinbase, Flashpoint, Yahoo и Akamai…»

(Maxim Zaitsev. На Аляске судят ботоводов Mirai // Threatpost (https://threatpost.ru/three-americans-plead-guilty-to-creating-mirai-botnet/23755/).- 14.12.2017).

***

«США займається серйозною політичною провокацією – Пхеньян не пов'язаний з якими-небудь кібератаками.

Про це заявив прес-секретар міністерства закордонних справ КНДР у відповідь на звинувачення США…

За його словами, звинувачення США було серйозною політичною провокацією проти Північної Кореї, яку Пхеньян ніколи не потерпить.

Нагадаємо, помічник президента США внутрішньої безпеки в Тому Боссерт заявив, що вірус WannaCry був створений в КНДР…» ***(В КНДР відкинули звинувачення США в причетності до кібератак // Західна інформаційна корпорація (http://zik.ua/news/2017/12/21/v_kndr_zvynuvachennya_ssha_v_prychetnosti_do_kiberatak_nazvaly_politychnoyu_1230621).- 21.12.2017).***

***

«По данным аналитического центра Национального агентства финансовых исследований, в 2017 году бизнес потерял из-за хакеров 115,97 млрд руб… Средняя сумма убытков одной российской компании составила 299,9 тыс. руб. Чаще всего кибератаки представляли собой заражение вирусами рабочих компьютеров сотрудников, в том числе с последующим вымогательством денег (20%), взломом почтовых ящиков (12%) и атаках на сайт компании (10%).

Предприниматели недооценивают последствия недостаточной информационной безопасности, сделали вывод в НАФИ. В большинстве российских компаний нет объективной оценки киберугроз, и это препятствует разработке планов действий на случай возможных атак, рассказали в агентстве. В основном бизнесмены ограничиваются установкой антивируса (88% опрошенных). Политика информационной безопасности есть в 47% организаций, ограничивают сотрудникам доступ в Интернет еще в 45% организаций. Регулярное обучение

информационной безопасности проводится в 29% предприятий, требование обязательной аттестации в этой сфере есть в 15% компаний.

Данные получены в результате опроса, проведенного в ноябре 2017 года среди 500 руководящих сотрудников предприятий в восьми федеральных округах России» ***(Российские компании в 2017 году потеряли 116 миллиардов рублей в результате кібератак // «Открытые системы» (https://www.computerworld.ru/news/Rossiyskie-kompanii-v-2017-godu-poteryali-116-milliardov-v-rezultate-kiberatak).- 20.12.2017).***

***

«…Российский хакер Константин Козловский, который недавно признался в причастности к взлому электронной почты Демократической партии (DNC), теперь заявляет, что оставил на ее серверах свои личные данные, которые могут доказать, что за кибератакой стоял глава Кремля Владимир Путин.

В комментарии телеканау «Дождь» хакер рассказал, что спрятал номер паспорта и визы на посещение острова Сен-Мартен в файле данных в системах DNC, чтобы позже подкрепить свои показания, сообщает Newsweek.

«Благодаря новой детали показания Козловского звучат правдоподобнее», – замечает издание…» ***(Кибератака на США: российский хакер оставил доказательства причастности Путина // ООО «Елисе Групп» (https://elise.com.ua/2017/12/29/kiberataka-na-ssha-rossijskij-haker-ostavil-dokazatelstva-prichastnosti-putina/).- 29.12.2017).***

***

«…Большинство специалистов по информационной безопасности (62%, согласно опросу компании Cylance), считают, что хакеры станут использовать ИИ как кибероружие уже в 2018 году. На Defcon 2017 датолог из Endgame (фирмы-распространителя систем безопасности) продемонстрировал работу автоматизированной программы, которая изучила среду OpenAI Gym и научилась прятать вредоносный файл от антивирусов. Еще несколько подобных инструментов и инноваций — и будет несложно представить себе, как ИИ поднимается еще на одну ступеньку вверх по эволюционной лестнице и создает системы, способные адаптироваться, выискивать компьютерные уязвимости и использовать их во вред человеку…» ***(Хакерские атаки 2018 года возглавит ИИ, — эксперты // 1news.info(https://www.1news.info/%d1%85%d0%b0%d0%ba%d0%b5%d1%80%d1%81%d0%ba%d0%b8%d0%b5-%d0%b0%d1%82%d0%b0%d0%ba%d0%b8-2018-%d0%b3%d0%be%d0%b4%d0%b0-%d0%b2%d0%be%d0%b7%d0%b3%d0%bb%d0%b0%d0%b2%d0%b8%d1%82-%d0%b8%d0%b8-406251).- 29.12.2017).***

***

«…20 декабря жертвой кибератаки хакеров, предположительно, из группировки Cobalt стали российские банки «Глобэкс» и «Севастопольский

морской банк». По версиям двух разных источников, сумма ущерба, причиненного севастопольскому банку, составила от 10 до 24 млн рублей…

«…По данному факту проводится проверка, по результатам которой будет принято процессуальное решение…», — сказали в пресс-службе УМВД.

При этом в УМВД не назвали точную сумму похищенных средств, она будет установлена в ходе проверки.

Ранее сообщалось, что, по мнению экспертов, ко взлому, скорее всего, причастна хакерская группировка Cobalt, использующая в том числе созданное для «мирного» тестирования систем киберзащиты одноименное программное обеспечение Cobalt Strike. Предположительно, она неделю назад похитила из банка «Глобэкс» порядка 80 млн рублей…» ***(Полиция проверяет обстоятельства кибератаки на банк в Севастополе // Меридиан Севастополь (http://meridian.in.ua/news/32088.html).- 29.12.2017).***

***

«Румынские хакеры вывели из строя две трети наружных камер наблюдения в округе Колумбия во время иннагурации президента Трампа.

От хакерских атак в январе пострадали 123 из 187 камер наружного наблюдения в полицейских участках округа, хакеры вывели их из строя на несколько дней. Двое граждан Румынии, которых сотрудники правоохранительных органов считают частью крупной организации, которая занимаются вымогательствами посредство взломов, находятся в федеральном суде округа Колумбия по обвинению в мошенничестве и киберпреступлениях…

25-летнего Михая Александра Исванка (Mihai Alexandru Isvanca) и 28-летнюю Эвелину Сисмару (Eveline Cismaru) арестовали в начале этого месяца. Трое других румынских хакеров, предстанут перед судом в Европе.

…В случае осуждения им грозит до 20 лет лишения свободы» ***(В США судят румынских хакеров за кибератаки во время иннагурации Трампа // Best Line (http://www.americaru.com/news/119953).- 29.12.2017).***

***

Протидія зовнішній кібернетичній агресії

«Украинские хакеры из "кибервойск" закрыли сайт террористов "ЛНР". Об этом сообщил руководитель проекта Евгений Докунин в Facebook.

"Закрыл сайт террористов путем отмены SSL сертификата. Позавчера утром обратился к компании Let's Encrypt и вчера утром они отозвали сертификат", - пишет он…» ***(Украинские кибервойска "убили" сайт террористов "ЛНР" // Internetua (http://internetua.com/ukrainskie-kibervoiska-ubili-sait-terroristov-lnr-).- 24.12.2017).***

***

«Служба безопасности Украины установила российское происхождение последних хакерских атак, которые были осуществлены осенью 2017 года на правительственные и инфраструктурные информационные системы…

…глава СБУ Василий Грицак напомнил, что осенью была массовая фишинговая рассылка на официальные электронные адреса центральных органов исполнительной власти, содержавшая вредоносное программное обеспечение, для похищения уязвимой информации.

"Сотрудники СБУ установили, что после открытия вредоносной программы реализовывался механизм полного удаленного управления пораженным компьютером. В частности, мы выяснили, что клиентская часть хакерского программного обеспечения "DarkTrack" после установки на компьютеры соединялась с серверным оборудованием с российскими IP-адресами. Фактически подконтрольные Кремлю российские хакеры могли получать возможность скрыто и удаленно администрировать украинские веб-ресурсы и получать с них информацию", - сказал В.Грицак.

Кроме того, по его словам, СБУ зафиксировала организованные спецслужбами РФ кибератаки двумя разновидностями вируса типа PSCrypt…» ***(Руку кремля увидели в хакерских атаках на инфраструктурные информсистемы в Украине // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/212200-ruku_kremlja_uvideli_v_hakerskih_atakah_na_infrastrukturnye_informsistemy_v_ukraine).- 29.12.2017).***

***

«В американский Конгресс внесли законопроект, который сулит Киеву защиту США от «российских кибератак»…

Комитет по иностранным делам палаты представителей Конгресса одобрил законопроект, согласно которому Соединенные Штаты должны помочь Украине укреплять ее кибербезопасность, а также бороться с «российской дезинформацией и пропагандой»…

…Госсекретарь США, согласно тексту, должен помочь Украине защитить ее правительственные компьютерные сети, в особенности те, что отвечают за защиту критически важной инфраструктуры. Помощь Вашингтона также направлена на снижение зависимости Киева «от российских информационных и телекоммуникационных технологий». Через 180 дней после вступления закона в силу шеф американской дипломатии представит профильным комитетам Конгресса отчет о проделанной работе…

«Поможет этот закон Украине или нет, в данном случае вопрос политический, потому как очевидно, что будут решаться только те задачи, которые интересуют Соединенные Штаты, а вовсе не безопасности в общем. Я бы скорее рассматривал это как формирование некоего нового института разведки, а именно безопасностью, полагаю, никто и заниматься не будет», – заявил газете ВЗГЛЯД эксперт по компьютерным технологиям, основатель группы компаний DZ Systems Дмитрий Завалишин.

«В финансовом плане, думаю, закон особенно много стоить не будет. Смысла в этом нет, да и платить Украине незачем», – отметил собеседник, добавив, что, скорее всего, американские айтишники просто помогут Киеву с установкой программных систем и системного оборудования…

Со времен прошлых атак кибербезопасность Украины «нисколько не укрепилась. На Украине сейчас дикое поле», заявил газете ВЗГЛЯД исполнительный директор «Лиги безопасного интернета» Денис Давыдов…

Заниматься решением украинских проблем американцы не будут. «Помогать Украине в чем-то никогда не было в интересах США. Это исключено. Просто какое-то время будут их использовать», – отметил Давыдов.

Давыдов уверен, что новый документ, если он будет принят, попросту поможет властям США узаконить виртуальную войну с Россией…» ***(Марина Балтачева, Никита Коваленко. США объявят России кибервойну в зоне ua // ООО «Деловая газета Взгляд» (https://vz.ru/world/2017/12/15/899731.html).- 15.12.2017).***

***

«…НАТО офіційно визнав кіберпростір операційним середовищем і таким чином прирівняв загрози, що там існують, до військових загроз. В Альянсі переглядають оборонну стратегію з огляду на нові загрози.

Для цього на початку листопада ухвалили рішення заснувати Центр кібероперацій і вже реформували командну структуру через російську загрозу.

Сполучені Штати, Велика Британія, Німеччина, Норвегія, Іспанія, Данія та Нідерланди розробляють механізми дій в умовах кібернетичної війни для своїх військових і сподіваються, що загальна доктрина кібербезпеки почне діяти в 2019 року.

Провідну роль у зміцненні європейського кіберзахисту відіграє Естонія. Маленька балтійська країна є чи не найбільш передовою в IT-сфері серед усіх країн континенту. Тут діють електронний уряд, електронне голосування на виборах, безліч послуг доступні онлайн…

Тож не дивно, що саме в Таллінні заснували Об'єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence), який сьогодні є флагманом європейської кібербезпеки.

Центр має акредитацію НАТО - формально не входячи до командної структури, він має величезний вплив на дії Альянсу в сфері кіберзахисту.

Центр заснували сім країн, а сьогодні він налічує 20 учасників – 17 членів НАТО та 3 країни-партнери…

Унікальність центру полягає в тому, що там разом працюють військові, цивільні, представники уряду. Робота центру сфокусована на трьох основних напрямках: дослідження, тренування та навчання…

На питання про найгірший тип кіберзагрози директорка центру Мерле Майгре відповідає однозначно: підтримувані на державному рівні атаки…

У Європі проблема використання кіберзброї є чутливим питанням, оскільки демократичні уряди не хочуть, щоб видавалося, ніби вони використовують ті самі прийоми, що й авторитарні режими. Поки що фахівці НАТО зосереджують свою

увагу на захисті мереж та блокуванні спроб викрадення або маніпулювання даними.

Однак окремі країни готуються не тільки оборонятися. Сполучені Штати, Британія, Нідерланди, Німеччина та Франція у складі своїх збройних сил вже створили кіберкомандування - спеціальні підрозділи для боротьби з кібернападами, які також здатні завдати удар у відповідь.

Естонія має намір запустити подібний підрозділ наступного року, розраховуючи, що до 2020 року він матиме і кіберзброю для контрзаходів…

Естонія також приділяє увагу співпраці у сфері кібербезпеки зі східними сусідами, зокрема, Україною та Грузією. Спільна робота переважно полягає у підготовці персоналу, технічних консультаціях та наданні обладнання…

Українські військові поки що не беруть участі у кібернавчаннях, проте в Естонії наголошують, що готові приймати нових учасників…» ***(Юрій Онищенко. Кіберудар у відповідь: як Естонія допомагає НАТО у боротьбі з хакерами // Європейська правда (http://www.eurointegration.com.ua/articles/2017/12/1/7074473/).- 13.12.2017).***

***

«Перед обличчям нових і старих загроз, породжених російською агресією, міжнародним тероризмом і кібератаками, країни-члени НАТО активно готуються до їх подолання і зміцнюють свою обороноздатність…

…наразі шість з 29 держав-членів Альянсу - Сполучені Штати, Велика Британія, Греція, Естонія, Румунія та Польща - виділяють на потреби оборони не менше 2% ВВП. Низка держав близька до досягнення цієї мети….

Держсекретар США Рекс Тіллерсон… дав високу оцінку прогресу, досягнутому у виконанні поставленої мети Албанією, Хорватією, Францією, Угорщиною та Румунією.

…на власну оборону і захист союзників США витрачають 683 млрд доларів, або майже 3,6% від ВВП. Ця цифра в два з половиною рази перевищує витрати всіх інших членів НАТО (середні витрати становлять менше 1,5 відсотка).

22 відсотка консолідованого бюджету НАТО фінансується США, 15 - Німеччиною, 11 - Францією, 10 - Великою Британією і 8 відсотків - Італією. Більше інших союзників в розрахунку на душу населення виділяють на оборону США - 1887 доларів, на другому місці Норвегія - 1421 долар…» ***(Юлія Шрамко. Країни ЄС підвищують витрати на оборону // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1702757-krayini-yes-pidvischuyut-vitrati-na-oboronu).- 06.12.2017).***

***

«Національний центр кібербезпеки (NCSC) при Центрі урядового зв'язку Великобританії направив до усіх урядових установ припис не використовувати російського антивірусного програмного забезпечення в системах, пов'язаних з національною безпекою…

Агентство з кібербезпеки Великобританії побоюється, що антивірусне програмне забезпечення може бути використане російським урядом. Чиновники

кажуть, що рішення Національного центру кібербезпеки Великобританії засноване скоріше на аналізах можливих ризиків, ніж на будь-яких свідченнях того, що були такого роду спроби шпигунства…» ***(Британським відомствам наказали не послуговуватися російськими антивірусами // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1702026-britanskim-vidomstvam-nakazali-ne-poslugovuvatisya-rosiyskimi-antivirusami).- 02.12.2017).***

***

«Компания "Лаборатория Касперского" находится в конструктивном диалоге с британским Центром национальной кибербезопасности (NCSC) для выработки механизма, который бы помог осуществить независимую верификацию безопасности ее продуктов и сервисов…

Ранее стало известно, что NCSC, входящий в Центр правительственной связи (ЦПС, аналог Агентства национальной безопасности США), запретил использование продуктов "Лаборатории Касперского" в государственных учреждениях, ответственных за национальную безопасность…

"Мы в настоящий момент не видим оснований распространять данные рекомендации (об отказе использовать продукцию компании - прим. ТАСС) на весь госсектор, а также на бизнес и частных пользователей", - отметили в NCSC»

("Касперский" ведет диалог с британской госслужбой после запрета продуктов компании для органов нацбезопасности // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=120092).- 04.12.2017).

***

«Советник премьер-министра Великобритании по национальной безопасности Марк Седвилл заявил, что если Россия проведет кибератаку против британских объектов, то ответ будет несимметричным. По словам Седвилла, сказанным во время выступления в Комитете по стратегии национальной безопасности британского парламента в Лондоне, правительство страны, вероятно, отреагирует, используя оружие на свое усмотрение…

Седвилл в своей речи …отметил, что преимущество Британии перед Россией, у которой нет союзников, заключается в возможности заключить военный союз с Францией и другими западными державами…

…По его словам, которые приводит «Голос Америки», Россия представляет собой растущую угрозу и готова использовать пропаганду, подрывную деятельность и кибератаки для нанесения ущерба Великобритании и другим странам Европы.

Как отметил советник премьер-министра, угрозы со стороны России включают как нетрадиционные инструменты ведения войны, например кампании по дезинформации, так и наращивание ее военного потенциала в Северной Атлантике и в Восточной Европе…» ***(Британия готова несимметрично ответить Росси на кибератаки // Elise Journal (https://elise.com.ua/2017/12/19/britaniya-gotova-nesimetrichno-otvetit-rossi-na-kiberataki/).- 19.12.2017).***

Освіта та підвищення цифрової обізнанності населення у галузі кібербезпеки

«У Львові юрист Європейського суду, ІТ-бізнесмени та інженери, фахівці з комунікації та розвитку технологій створили підручник, що буде корисний для тих, хто велику частину своєї роботи проводить через онлайн комунікацію. Посібник «Що повинні знати НДО аби захистити себе в інформаційному колі», видали Львівська бізнес-школа УКУ (LvBS) та Громадська спілка «Форум НДО в Україні» у партнерстві зі Школою права Українського католицького університету у межах проекту «Інформаційна безпека для НДО».

…Складається він з 16 параграфів, присвячених інструментам доступу до публічної інформації, практичним аспектам дотримання правових стандартів захисту персональних даних, а також, питанням конфіденційності кореспонденції та збереження інформації. Також підручник містить актуальний для сучасних користувачів Інтернету питання кібербезпеки.

На сторінках видання читачі знайдуть практичні поради і лайфхаки щодо використання механізмів інформаційної безпеки у своїй діяльності, зможуть пройти тест на рівень безпеки їхньої організації та напрацювати плани її посилення…» ***(Лілія Кузік. LvBS презентувала посібник з інформаційної безпеки для НДО // Львівська міська рада (http://city-adm.lviv.ua/news/city/lviv-changes/244503-lvbs-prezentuvala-posibnyk-z-informatsiinoi-bezpeky-dlia-ndo).- 12.12.2017).***

***

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

Актуальні проблеми правоохоронної діяльності : зб. матеріалів Всеукр. наук.-практ. Інтернет-конф. (23 груд. 2016 р.). - Сєвєродонецьк : РВВ ЛДУВС ім. Е. О. Дідоренка, 2017. - 421 с.

Зі змісту:

Лизогубенко Є.В. DDOS-атака як один з інструментів вчинення кіберзлочинів;

Меленті Є.О., Абрамов К.А. Адаптація сектору безпеки і оборони України у сфері забезпечення кібербезпеки.

Шифр зберігання НБУВ: ВА814076.

***

Вергун А.О. Окремі аспекти міжнародної інформаційної безпеки / Вергун А.О. // Актуальні проблеми вітчизняної юриспруденції. - 2017. – Спец. вип.- Ч. 2.- С. 98-101.

Досліджено роль міжнародних норм та права як регулятора інформаційних відносин.

Шифр зберігання НБУВ: Ж74269.

***

Гончар С. Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури / С. Гончар, Г. Леоненко // Information Technology and Security. - 2016. - Vol. 4, № 2. - С. 262-268.

Розглянуто складові частини системи кіберзахисту інформаційних систем об'єктів критичної інфраструктури. Приведено модель взаємодії елементів інформаційної системи об'єкту критичної інфраструктури. Здійснено аналіз їх впливу на стан кібербезпеки даної системи. Розглянуто питання нормативно-правового забещпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Шифр зберігання НБУВ: Ж74190.

***

Грицун О. О. Міжнародно-правове забезпечення міжнародної інформаційної безпеки : автореф. дис. ... канд. юрид. наук : 12.00.11 / Грицун Ольга Олександрівна ; Київ. нац. ун-т ім. Тараса Шевченка. - Київ, 2017. - 20 с.

Узагальнено міжнародно-правові концептуальні підходи до розуміння міжнародної інформаційної безпеки у міжнародному праві та її окремих аспектах. Запропоновано авторське визначення поняття міжнародної інформаційної безпеки. Визначено місце інституту міжнародної інформаційної безпеки у системі сучасного міжнародного права. Запропоновано авторську періодизацію етапів становлення та розвитку інституту міжнародної інформаційної безпеки та визначено принципи його регулювання. Проаналізовано формування міжнародно-правових основ військового-політичного, антитерористичного та кримінально-правового аспектів міжнародної інформаційної безпеки.

Шифр зберігання НБУВ: РА431656.

***

Дзьобань О. П. Інформаційна безпека: екзистенційні аспекти і мережеві практики / О. П. Дзьобань, Є. М. Мануйлов // Вісник Національного університету "Юридична академія України імені Ярослава Мудрого" . Серія : Політологія. - 2017. - № 2. - С. 42-54.

Доведено, що інформаційна безпека – це і захист інформації, і захист від інформації, а її забезпечення включає в себе взаємодію з різними експертними системами, делокалізацію дій, мінімізацію ризиків.

Шифр зберігання НБУВ: Ж73716.

***

Діордіна І.В. Поняття та зміст системи забезпечення кібербезпеки / Діордіна І.В. // Актуальні проблеми вітчизняної юриспруденції. - 2017. - Вип. 2. – Том 1.- С. 62-68.

Акцентовано увагу на відсутності унвфікованого визначення системи забезпечення кібербезпеки та запропоновано авторське розуміння. Приділено увагу суб'єктам та об'єктам системи забезпечення кібербезпеки.

Шифр зберігання НБУВ: Ж74269.

***

Зінюк А. В. Особливості забезпечення інформаційної безпеки в електронному навчанні / А. В. Зінюк, Л. М. Змій // Вісник Одеського національного університету. Соціологія і політичні науки. - 2016. - Т. 21, Вип. 3. - С. 33-40.

Розглянуто проблеми інформаційної безпеки та об'єкти, які потребують особливого захисту. Досліджено погляди на проблеми конфіденційності інформації в електронному навчанні. Продемонстровано ключові характерні риси встановлення системи інформаційної безпеки для учасників електронної освіти.

Шифр зберігання НБУВ: Ж69659.

***

Камінський І.І. Концепція державного суверенітету в контексті застосування кіберсили / Камінський І.І. // Альманах міжнародного права. - 2017. - Вип. 16. - С. 3-10.

Досліджено питання здійснення державами своїх суверенних прав у кіберпросторі. Встановлено правову природу кіберпростору. Розглянуто принцип невтручання, який тісно пов'язаний із концепцією державного суверенітету, як міжнародно-правової підстави заборони застосування кібербезпеки.

Шифр зберігання НБУВ: Ж73864.

***

Курченюк П.В. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу / Курченюк П.В., Довгаль А.О. // Electronics and communications. - 2017. - Т. 22, № 2. - С. 79-84.

Засобами регресійного аналізу з використанням багаторівневої класифікації загроз, яка базується на моделі OSI, розроблено математичну модель загроз безпеці інформаційно-комунікаційних систем. Розглянуто постановку задачі та показано, як з теоретичної моделі отримати апроксимаційне рівняння регресії, яке може бути використано для подальшого прогнозування впливу можливих атак на стан мережі.

Шифр зберігання НБУВ: Ж69367.

***

Нізовцев Ю.Ю. Щодо нормативно-правового регулювання у сфері протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем / Ю.Ю. Нізовцев // Криміналістичний вісник. - 2017. - № 1. - С. 54-61.

Проаналізовано та висвітлено прогалини в нормативно-правовму регулюванні у сфері протидії несанкціонованим втручанням у роботу інформаційно-телекомунікаційних систем. Проведено огляд нормативно

закріпленого понятійного апарату, що використовується під час проведення судових комп'ютерно-технічних і телекомунікаційних експертиз.

Шифр зберігання НБУВ: Ж70560.

***

Петров В. В. Особливості логістичного забезпечення національної системи кібербезпеки України в сучасних усовах / В.В.Петров, А.В.Тарасенко // Держава і право. Юридичні науки. - 2017. - Вип. 76. - С. 88-101.

Проаналізовано наукові джерела та нормативні акти, які стосуються логістичного забезпечення національної системи кібербезпеки України. Охарактеризовано проблеми логістичного забезпечення національної системи кібербезпеки України, що впливають на діяльність органів державної влади та об'єктів критичної інфраструктури.

Шифр зберігання НБУВ: Ж28079/юр.

***

Храпенко В.С. Протидія нотаріусів кіберзлочинам, що вчиняються в процесі державної реєстрації прав на нерухоме майно / Храпенко В.С. // Актуальні проблеми вітчизняної юриспруденції. - 2017. – Спец. вип.- Ч. 2.- С. 205-208.

Розглянуто проблеми інформаційної безпеки та незаконного доступу до закритих даних, що виникають під час здійснення нотаріусами функцій державного реєстратора.

Шифр зберігання НБУВ: Ж74269.

***

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.