Федеральная служба по техническому и экспортному контролю

ФЕДЕРАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ГОСУДАРСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ
ИНСТИТУТ ПРОБЛЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ»
(ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)

ГРНТИ 81.93.29
УДК 002:004.056

Экз. № 97

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ СБОРНИК

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(по материалам из открытых источников)

ВЫПУСК 3 (57)

Воронеж
2019

Сборник подготовлен с использованием открытых публикаций и информационных ресурсов, размещенных в сети Интернет

СОДЕРЖАНИЕ

1. Сведения о развитии и реализации новых технологий в сфере ответственности ФСТЭК России

1.1. Противодействие техническим разведкам

Американские спутники проявляют подозрительную активность в космосе

По информации сайта anna-news.info, американские военные спутники-шпионы ведут подозрительную активность в космосе. Фонд «Secure World Foundation» представил доклад, из которого следует, что эти американские аппараты осуществляют тайное сближение с гражданскими космическими объектами, принадлежащими России и Китаю.

Сейчас у США четыре таких шпионских спутника GSSAP, участвующих в программе осведомления на геостационарной орбите и работающих в интересах военно-воздушных сил (ВВС) США. Сближение с китайскими и российскими спутниками американские аппараты осуществляют под покровом тени Земли, где возможности наблюдающих телескопов ограничены. При этом, американские военные не предоставляют никаких публичных данных о местоположении или маневрах спутников GSSAP, но все равно их большая активность фиксируется другими средствами слежения.

Источник: http://www.anna-news.info/amerikanskie-sputniki-proyavlyay-ut-podozritelnuyu-aktivnost-v-kosmose/ (дата размещения материала 06.04.2019).

Запущен космический аппарат «PRISMA»

Как сообщает сайт space.skyrocket.de, система «PRISMA» представляет собой космический аппарат наблюдения Земли итальянского космического агентства, оснащенный оптико-электронным прибором, который сочетает гиперспектральную камеру с панхроматической камерой среднего разрешения. Аппаратура спутника имеет пространственное разрешение 20-30 метров (в гиперспектральном режиме съемки) и 2,5-5 метров (в панхроматическом режиме съемки) с шириной полосы съемки 30-60 километров.

Преимущества данной комбинации камер заключаются в том, что в дополнение к обычному способу наблюдения, который основан на распознавании формы и размера объекта, гиперспектральная камера определяет химико-физический состав интересующего объекта. Это предлагает пользователям множество областей применения данного космического аппарата, в том числе в области национальной безопасности и разведки.

Источник: https://www.space.skyrocket.de/doc_sdat/prisma_asi.htm (дата размещения материала 22.03.2019).

Запущено 20 спутников типа «Flock»

По данным сайта space.skyrocket.de, система космических аппаратов «Flock» («Стая») не имеет строгой орбитальной структуры и телевизионная съемка осуществляется только в надир на всей освещенной поверхности Земли.

Большинство запущенных аппаратов оснащаются многоспектральными оптико-электронными средствами съемки земной поверхности, работающими в трех спектральных полосах видимого диапазона: 0,42-0,53, 0,5-0,59, 0,61-0,7 микрометра, а некоторые – в четырех спектральных полосах: 0,455-0,515, 0,5-0,59, 0,59-0,67, 0,78-0,86 микрометра.

Начиная с третьего поколения спутников, используются матрицы размером 29 мегапикселей, что обеспечивает разрешение около 3 метров с высоты 400 километров и не хуже 5 метров с высоты 500 километров. Часть данных, получаемых с указанных спутников, закупается национальным управлением геопространственной разведки министерства обороны США.

Источник: https://www.space.skyrocket.de/doc_sdat/flock-1.htm (дата размещения материала 01.04.2019).

Ракета-носитель PSLV вывела на орбиту разведывательный спутник «Emisat»

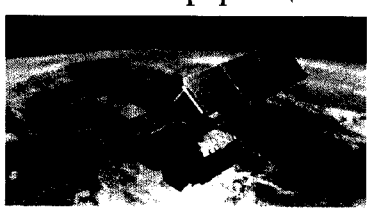
Как сообщается на сайте avianews.info со ссылкой на телеканал «NDTV», индийская организация космических исследований ISRO 1 апреля вывела на

орбиту разработанный оборонно-исследовательской организацией DRDO разведывательный спутник «Emisat», который будет определять местоположение радиолокационных станций (РЛС) противника. Спутник выведен на орбиту высотой 753,6 километра. Кроме этого, ракета-носитель PS4 вывела на орбиту 28 иностранных спутников, принадлежащих США, Литве, Испании и Швейцарии.

Источник: https://www.avianews.info/raketa-nositel-pslv-vyvela-na-orbi-tu-razvedyvatelnyj-sputnik-emisat/ (дата размещения материала 01.04.2019).

Китай запустил сразу два новейших спутника ДЗЗ «Tian Hui-2-01»

По информации сайта sovzond.ru, Китай успешно запустил на орбиту два



спутника «Tian Hui-2-01». Спутники проведут ряд научных экспериментов, включая исследование наземных ресурсов, а также географические и картографические исследования.

Спутники семейства «Tian Hui» используются

для дистанционного зондирования Земли (ДЗЗ), они оснащены мультиспектральными стереоскопическими камерами разрешением 10 метров, благодаря которым удается получить трехмерное изображение.

Источник: https://www.sovzond.ru/press-center/news/dzz/5732/ (дата размещения материала 30.04.2019).

В Норвегию привезли американские радары для слежки за Россией

По информации, размещенной на сайте b-port.com, из США в порт норвежского города Вардё поступил специальный транспорт с частями военного радара разведывательной системы «Глобус». Здание для размещения радара вместе с подземными уровнями составляет порядка 15 этажей, что является одним из самых высоких сооружений в Финнмарке. Система «Глобус» отправляет разведывательные данные в стратегическое командование США, которое отвечает за применение ядерного оружия и военные операции.

Объекты системы «Глобус» находятся в 28 километрах от границы с Россией. В нескольких милях от них расположены атомные подводные лодки Северного флота – главная военная сила России.

Как отмечают СМИ, норвежские власти не дают никакой информации о перевозке нового американского разведывательного радара в Вардё.

Источник: https://www.b-port.com/news/item/225812.html (дата размещения материала 25.03.2019).

Пентагон подтверждает развертывание новой пассивной РЛС[1]

Согласно данным сайта defence-blog.com, Пентагон подтвердил создание экспериментальных пассивных сенсорных систем для повышения эффективности обнаружения воздушных целей. Специалисты включили пассивный датчик ALPS в интегрированную систему боевого управления противовоздушной (ПВО) и противоракетной (ПРО) обороны, обеспечивающей непрерывное наблюдение за самолетами, беспилотными летательными аппаратами (БПЛА) и крылатыми ракетами.

Новая система ALPS – одна из самых засекреченных систем наблюдения армии США. Характеристики этой системы не раскрываются. Нет информации даже о ее внешнем виде.

Считается, что база данных в ALPS может хранить в памяти около семисот различных типов воздушных целей, включая российские крылатые ракеты, которые были использованы в ходе военной операции в Сирии.

---

[1] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

Источник: https://www.defence-blog.com/army/pentagon-confirms-deploying-new-passive-sensor-against-cruise-missiles-aircraft-drones.html (дата размещения материала 15.04.2019).

Швейцария заключила контракт с компанией «Thales» на поставку системы IMINT/GEOINT[2]

Как информирует сайт janes.com, швейцарские вооруженные силы заключили контракт с компанией «Thales» на поставку элементов центра видовой и геопространственной разведки IMINT/GEOINT.

Контракт был подписан в конце марта 2019 года, поставки элементов системы должны начаться в начале 2020 года.

Новый центр будет базироваться на основе системы обработки и передачи информации видовой разведки MINDS компании «Thales». Она может вести визуальную разведку, а также получать информацию от оптико-электронных и инфракрасных датчиков, РЛС с синтезированной апертурой, осуществлять индикацию движущихся целей и проводить полномасштабную видеозапись происходящего. Система MINDS обладает гибкой архитектурой, которая может применяться как в стратегическом, так и в тактическом звене.

Источник: https://www.janes.com/article/87851/swiss-armed-forces-contract-thales-for-new-imint-geoint-system (дата размещения материала 11.04.2019).

Бундесвер разрабатывает радар для обнаружения стелс-истребителей

По данным сайта topwar.ru со ссылкой на издание «Defense News», ВВС Германии разработали официальную дорожную карту получения технологий пассивного зондирования, присоединившись к программе разработки РЛС, способных засекать современные малозаметные истребители. Информация о статусе программы появилась после того, как в ноябре прошлого года стало известно об острой заинтересованности в разработке пассивного радара.

Министерство обороны Германии организовало недельную «замерочную» кампанию, направленную на визуализацию воздушного движения всего региона через пассивную радиолокационную систему «Twinvis» компании «Hensoldt».

Руководство ВВС Германии заявляет, что заинтересовано в пассивном радаре для повышения эффективности наблюдения за регулярным воздушным сообщением над Германией, хотя разработчики системы утверждают, что технология способна на гораздо большее. Пассивная РЛС сама не излучает сигналов, она занимается только их приемом и обработкой. Система работает с лю-

[2] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

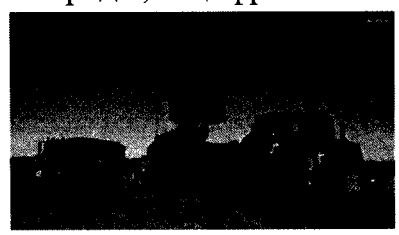
бым типом сигнала, присутствующим в зоне ее приема, включая радио- или телевизионные передачи, а также сигналы станций мобильной связи. Традиционный радар, напротив, работает, излучая радиолокационные волны, а затем отслеживая их путь.

Такая система, по существу, скрыта, то есть пилоты, входящие в контролируемую зону, могут не знать, что их отслеживают. Данная схема может работать даже в случае с малозаметными самолетами «стелс», такими, как F-35, хотя пока нет общедоступных данных, подтверждающих эффективность действия пассивного радара против «стелсов» и их радиопоглощающих покрытий.

Источник: https://www.topwar.ru/155971-bundesver-razrabatyvaet-radar-dlja-lovli-malozametnyh-istrebitelej.html (дата размещения материала 25.03.2019).

На Украине смогли создать соперника российскому комплексу «Зоопарк-1М»

По информации сайта vpk.name, на Украине сообщили о завершении государственных испытаний комплекса контрбатарейной борьбы 1Л220УК, который предназначен для разведки позиций артиллерии противника. Его РЛС работает в микроволновом диапазоне и обнаруживает снаряды, а цифровая система определяет траектории их полетов. Это позволяет установить местонахождение пушек, гаубиц, минометов, реактивных систем залпового огня, а также ракетных комплексов ПВО и тактических ракет противника.



Мощность цифровой фазированной антенной решетки 1Л220УК дает возможность разместить контрбатарейный радар в нескольких десятках километров от линии фронта и наблюдать за полем боя в секторе до 180 градусов.

В пресс-релизе не указываются более точные характеристики данного комплекса, но, по мнению военных экспертов, он является продолжением еще советских разработок. Предполагается, что его будут позиционировать как конкурента российскому комплексу 1Л260-Е «Зоопарк-1М».

Источник: https://www.vpk.name/news/269853_na_ukraine_smogli_sozdat_sopernika_rossiiskomu_kompleksu_zoopark1m_.html (дата размещения материала 10.04.2019).

Новый заказ на самолеты ДРЛО E-2D «Advanced Hawkeye»

Согласно данным сайта forum.militaryparitet.com, военно-морские силы (ВМС) США подписали с компанией «Northrop Grumman» контракт на производство 24 палубных самолетов дальнего радиолокационного обнаружения (ДРЛО) E-2D «Advanced Hawkeye». Поставки планируется завершить в августе 2026 года.

Особенностями самолета этой версии является

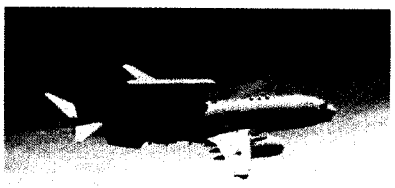
наличие мощного радара с механическим и электронным типами сканирования, полностью интегрированная «стеклянная кабина» экипажа, новый бортовой компьютер, модернизированная линия связи и передачи данных.

Установка нового радара позволит увеличить возможности самолета E-2D по ведению разведки и наблюдения и сократить время между передачей первых данных и активными действиями боевых сил.

Источник: http://www.forum.militaryparitet.com/viewtopic.php?id=24233 (дата размещения материала 11.04.2019).

Великобритания закупила пять самолетов ДРЛОиУ E-7

Как сообщает ряд источников, Великобритания подписала контракт на поставку пяти самолетов дальнего радиолокационного обнаружения и управления (ДРЛОиУ) E-7/E-737 производства компании «Boeing».



E-7 закупаются для замены шести самолетов ДРЛО E-3D «Sentry», состоящих на вооружении британских ВВС. Они не прошли вовремя усовершенствование до стандарта «блок-40/45» аналогично самолетам ВВС США и становятся все более непригодными для эксплуатации. Поставки новых самолетов начнутся с начала 2020 года.

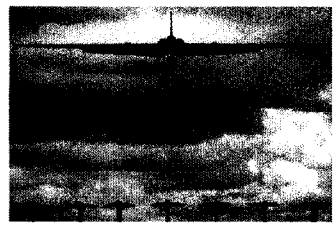
Аналогично многоцелевому самолету базовой патрульной авиации P-8A «Poseidon», E-7 создан на базе авиалайнера «Boeing-737» и уже состоит на вооружении Австралии в количестве шести единиц под названием «Wedgetail», Южной Кореи – в количестве четырех единиц под названием «Peace Eye» и Турции – в количестве четырех единиц под названием «Peace Eagle».

В отличие от РЛС с антенной с механическим сканированием, установленной на самолете E-3D «Sentry», E-7 оснащен многоцелевой РЛС с антенной решеткой с электронным сканированием, которая обеспечивает круговой обзор на дальности, превышающей 322 километра для воздушных целей и 241 километр для наземных целей типа патрульного катера. Эти параметры могут быть существенно увеличены, если мощность радара сконцентрировать в определенном направлении, а не по всей зоне обзора. Многоцелевая РЛС с электронным сканированием компании «Northrop Grumman» обеспечивает самолету E-7 зону обзора в 4 млн. квадратных километров при его продолжительности полета в 10 часов.

Источники: Военно-техническое сотрудничество, 2019, № 13, с. 5; https://www.bestlj.ru/133774-Velikobritanija-priobretaet-pjat-samoletov-DRLO-i-upravlenija-E-7.html (дата размещения материала 25.03.2019); http://www.nevskii-bastion.ru/boeing-737aewc/.

США перебросили в Европу стратегические высотные разведчики U-2

По данным сайта vpk.name, два американских стратегических высотных разведывательных самолета U-2S «Dragon Lady» после трансатлантического перелета с континентальной части США совершили посадку на передовой авиабазе Фэрфорд в Великобритании. До последнего времени авиабаза Фэрфорд использовалась для переброски самолетов U-2S, способных выполнять задания на высотах более 21 тыс. метров, на Ближний Восток.



В целях проведения разведки у границ России Пентагон в настоящее время в основном использует самолеты ВВС США RC-135 «Rivet Joint» в различных модификациях, дальние беспилотники RQ-4B «Global Hawk», а также патрульные противолодочные самолеты P-8A «Poseidon», размещенные в Европе.

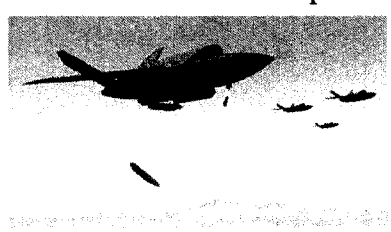
Ранее в Интернет-издании «Nplus1» появилась информация о том, что в США закончены испытания разработанной компанией «Raytheon» новой РЛС «ASARS-2B» с синтезированной апертурой для оснащения высотных самолетов-разведчиков U-2 «Dragon Lady».

Источник: https://www.vpk.name/news/275287_ssha_perebrosili_v_evropu_strategicheskie_vyisotnyie_razvedchiki_u2.html (дата размещения материала 25.04.2019).

Опытный БПЛА XQ-58A «Valkyrie»

По сообщению сайта topwar.ru, американская компания «Kratos Unmanned Aerial Systems» провела первый полет перспективного БПЛА XQ-58A «Valkyrie». В будущем эта машина может стать универсальной платформой для строительства БПЛА разного назначения.

Согласно техническому заданию, XQ-58A «Valkyrie» должен представлять собой малозаметный дозвуковой летательный аппарат. В проекте XQ-58A особый интерес представляет бортовое радиоэлектронное оборудование. Прежде всего, беспилотник должен иметь систему дистанционного управления и автопилот. Также должны использоваться оптико-электронные или радиолокационные средства наблюдения. Ожидается, что XQ-58A вместе с некоторыми другими перспективными БПЛА в будущем сможет взаимодействовать с самолетами тактической авиации последних поколений. Они станут ведомыми пилотируемых истребителей или бомбардировщиков. На БПЛА предлагается возложить ведение разведки с передачей данных ведущему. Кроме того, беспилотники смогут нести различное вооружение.



Расчетная максимальная скорость аппарата – 1050 километров в час. Дальность пока определяется на уровне 3500-4000 километров. Практический потолок – 13700 метров.

Источник: https://www.topwar.ru/155327-opytnyj-bpla-kratos-xq-58a-valkyrie-ssha.html (дата размещения материала 23.03.2019).

В Турции начались летные испытания нового разведывательно-ударного дрона

По информации сайта vpk.name, в Турции начались летные испытания разработанного турецкой компанией «TAI» перспективного средневысотного беспилотника большой продолжительности полета YFYK.

Новый беспилотник YFYK или «Anka-Aksungur» выполнен по двухбалочной схеме и оснащен двумя турбированными дизельными двигателями. Аппарат рассчитан на полеты на высоте до 7,6 тыс. метров продолжительностью до 24 часов.

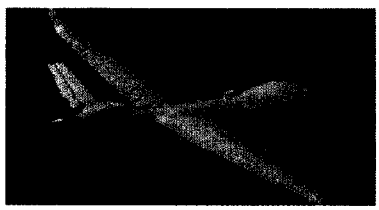
Основное предназначение нового дрона – ведение разведки и наблюдения, однако он также может применяться и для нанесения ударов. «Anka-Aksungur» оснащен спутниковой системой связи, на нем планируется установить оптико-электронную систему наблюдения, камеру с объективом с широким углом обзора и РЛС с режимом синтезированной апертуры.

Источник: https://www.vpk.name/news/274703_v_turcii_nachalis_letnyie_ispyitaniya_novogo_udarnorazvedyivatelnogo_drona.html (дата размещения материала 23.04.2019).

США одобрили продажу БПЛА «SkyGuardian» Бельгии

Согласно информации журнала «Военно-техническое сотрудничество», госдепартамент США одобрил продажу Бельгии четырех средневысотных БПЛА большой продолжительности полета MQ-9B «SkyGuardian».

Бельгия планирует использовать аппараты для выполнения задач наблюдения, разведки, обнаружения целей и сбора информации в рамках поддержки операций, выполняемых национальными вооруженными силами, войсками НАТО, а также миссий, санкционированных ООН.



Максимальная рабочая высота полета «SkyGuardian» составляет 13700 метров, максимальная продолжительность полета – 40 часов, максимальная скорость 370 километров в час.

В случае реализации контракта Бельгия станет второй после Великобритании страной, которая приобрела БПЛА «SkyGuardian». Этот беспилотник является самой современной версией MO-9 «Reaper» и сертифицирован для полетов в гражданском воздушном пространстве.

Источник: Военно-техническое сотрудничество, 2019, № 14, с. 28-29.

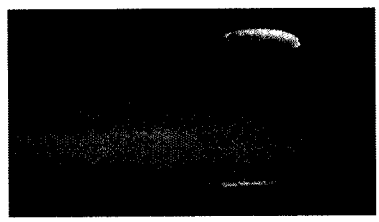
Шершень-наблюдатель

Как собобщает сайт unian.net, военный дрон-разведчик «Черный шершень» стал самой миниатюрной в мире разведывательной системой. Беспилотник весит около 16 грамм при длине 10 сантиметров и хорошо помещается в кармане. Военный дрон-разведчик оснащен камерой и системой навигации, может находиться в воздухе до 25 минут без подзарядки. В 2013 году дроны использовались британскими военными в Афганистане. Уже в 2017 году компания «Flir Systems» оснастила аппараты системой ночного видения. Сейчас мини-разведчики находятся на вооружении армий Франции, Германии, Австралии, Норвегии, Нидерландов и Индии.

Источник: https://www.unian.net/world/10502154-shershen-nablyudatel-kak-rabotaet-samaya-miniatyurnaya-v-mire-razvedyvatelnaya-sistema-video.html (дата размещения материала 02.04.2019).

Компания «RT LTA Systems Ltd.» представила аэростат «SkyStar 110»[3]

По данным сайта uasweekly.com, израильская компания «RT LTA Systems Ltd.» на выставке, посвященной обеспечению безопасности границ, представила свой аэростат «SkyStar 110», который является идеальным для использования в военных целях и ведения пограничного контроля, обеспечивает непрерывное наблюдение в течение длительного времени при минимальной стоимости. Серия аэростатов «SkyStar» также включает в себя «SkyStar 180», «SkyStar 120» и «SkyStar 330».



«SkyStar 110» – это аэростатная система, предназначенная обеспечивать войсковых командиров разведывательной информацией в режиме реального времени. Система компактна и надежна, ее могут транспортировать, собрать, запустить и обслуживать всего два человека. Аэростат может быть собран и запущен за 15 минут, при этом он может работать в экстремальных погодных условиях.

В Израиле аэростаты «SkyStar» развернуты на границе с сектором Газа и используются в рамках антитеррористической операции.

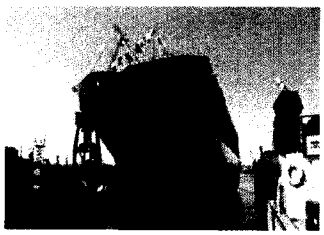
Источник: https://www.uasweekly.com/2019/03/25/border-security-expo-2019-rt-to-present-the-skystar-110-aerostat/ (дата размещения материала 25.03.2019).

[3] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

В Польше спустили на воду корабль разведки для ВМС Швеции

Как сообщает сайт arms-expo.ru, в Польше на верфях «Stocznia Remontowa Nauta S.A.» состоялась церемония спуска на воду первого специализированного корабля радио- и радиотехнической разведок («SIGINT») для ВМС Швеции. Корабль получил название «Artemis».

После спуска на воду корабль будет достроен на польской верфи, пройдет швартовные и ходовые испытания, после чего отправится на судостроительное предприятие «Saab», где на нем будет установлена аппаратура радио- и радиотехнической разведок, там же пройдут приемочные испытания корабля. Планируется, что ввод корабля в состав ВМС Швеции пройдет в 2020 году. Технические характеристики проекта не раскрываются.



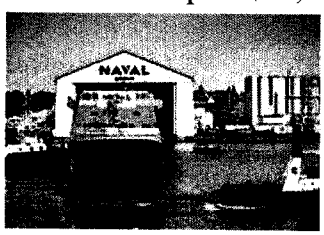
Новый корабль будет применяться для обнаружения излучений станций радиосвязи, их пеленгации, перехвата и анализа передаваемых сообщений в Балтийском регионе. В составе ВМС Швеции он заменит корабль A201 «Orion» такого же класса, введенный в строй еще в середине 80-х годов прошлого века и не раз уже модернизированный.

Источник: http://www.arms-expo.ru/053049049048124051052056056053.html (дата размещения материала 19.04.2019).

Состоялся спуск на воду седьмого фрегата класса «FREMM» для ВМС Франции

По данным сайта factmil.com, французская компания «Naval Group» объявила о состоявшейся церемонии спуска на воду многоцелевого фрегата «Alsace» класса «FREMM», предназначенного для ВМС Франции.

«Alsace» является девятым многоцелевым фрегатом «FREMM», строящимся во Франции, и седьмым, который будет передан французским ВМС по контракту, подписанному с Европейским управлением по закупкам вооружений. Корабль станет первым из двух фрегатов, которые будут построены в версии ПВО при сохранении возможностей борьбы с подводными лодками противника.

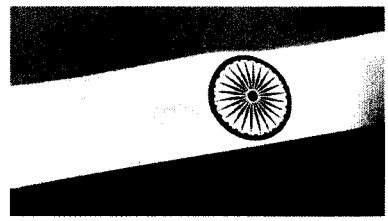


Для соответствия последним требованиям военных в конструкцию фрегата были внесены изменения, которые коснулись, в первую очередь, боевых систем. В частности, корабль оборудован более мощной многофункциональной РЛС, расширенным комплектом средств связи, получил три дополнительные консоли боевой информационно-управляющей системы «SETIS» в центре анализа боевой информации CIC, зенитный ракетный комплекс с зенитными управляемыми ракетами «Астер-15» и «Астер-30». Через несколько дней «Alsace» также получит новую мачту, позволяющую повысить эффективность обнаружения воздушных и надводных целей.

Источник: http://www.factmil.com/news/18_04_2019_na_verfi_v_lorjane_sostojalsja_spusk_na_vodu_sedmogo_fregata_klassa_fremm_dlja_vms_francii/2019-04-18-8874 (дата размещения материала 18.04.2019).

Компания «GRSE» поставит ВМС Индии противолодочные корабли

Согласно информации сайта armstrade.org, минобороны Индии объявило о заключении с национальной компанией «GRSE» контракта на постройку восьми противолодочных кораблей для мелководного фарватера «ASWSWC».



В рамках проекта компания «GRSE» поставит ВМС Индии корабли водоизмещением 750 тонн, способные развивать скорость до 25 узлов. Они будут применяться для противолодочной борьбы в прибрежных водах, ведения разведки, постановки мин, проведения поисково-спасательных операций. Первый корабль должен быть поставлен заказчику в течение 42 месяцев с даты подписания контракта. Далее планируется принимать на вооружение по два судна в год.

Компания «GRSE» в настоящее время уже реализует ряд крупных программ, включая поставку ВМС Индии трех малозаметных фрегатов «Проект 17А», противолодочных корветов «ASW», многоцелевых десантных катеров «Mk.4» и четырех гидрографических судов.

Источник: http://www.armstrade.org/includes/periodics/news/2019/0506/121552234/detail.shtml (дата размещения материала 06.05.2019).

На Украине спустили на воду средний корабль-разведчик

По информации ряда сайтов, ВМС Украины в скором времени получат на вооружение разведывательный корабль собственного производства. На судостроительном заводе «Кузня» на Рыбальском состоялся торжественный спуск на воду первого среднего разведывательного корабля. Корабль-разведчик построен для нужд ВМС Украины по заказу минобороны в рамках государственной целевой оборонной программы развития вооружения и военной техники на период до 2020 года.

Корабли этого класса предназначены для радиоперехвата каналов связи на различных частотах, ведения телеметрической, радиотехнической разведки, ретрансляции закрытых каналов. По всей видимости, задачей экипажа станет прослушивание переговоров моряков Черноморского флота России. Вот только поможет ли новый корабль, передвигающийся со скоростью 11,6 узлов и разработанный почти полвека назад повысить эффективность ВМС Украины?

Разведывательный корабль строится путем переделки траулера проекта 502ЭМ «Эгет», пять готовых корпусов для постройки которых находились на

стапелях завода в разной степени готовности. Когда будет закончена достройка корабля и какое разведывательное оборудование на него установят не сообщается.

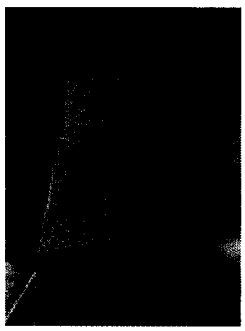
Источники: https://www.vpk.name/news/275135_na_ukraine_spustili_na_vodu_srednii_korablrazvedchik.html (дата размещения материала 24.04.2019); https://www.utro.ru/army/2019/04/24/1398099.shtml; https://www.bmpd.live-journal.com/ 36 21573.html.

США меняют радары на эсминцах

Как сообщается на ряде сайтов, американский флот готовится провести масштабную модернизацию эсминцев «Arleigh Burke». Модернизация должна стать ответом на усилившиеся угрозы со стороны Китая и России.

ВМС планируют приобрести особую версию радара ПВО компании «Raytheon» AN/SPY-6. Она должна сменить установленный на эсминцах «Arleigh Burke» серии IIA радар AN/SPY-1D. Такая модернизация должна дать существенный эффект в повышении чувствительности и дальности действия радара.

В 2020 году ВМС США начнут закупку 24 комплектов радаров AN/SPY-6 в комплекте с радиолокационным модулем RMA и связанными с ними радиоэлектронными системами. Монтаж оборудования запланирован на 2025 год.



Модернизированный радар для эсминцев этого класса третьей серии будет иметь 37 так называемых радиолокационных модульных элементов, которые представляют собой небольшие коробки линейной размерности около 60 сантиметров, в которых используется технология нитрида галлия для направления радиолокационного излучения на воздушные цели. Более старые эсминцы серии Flight IIA имеют 24 модуля RMA.

Новый радар будет чрезвычайно энергоемким. Ожидается, что для его нормальной работы потребуется десятимегаваттная мощность, что, в свою очередь, должно повлечь монтаж новой генераторной системы, смены всей электрической сети корабля, а также повышение напряжения бортовой сети. Это, в свою очередь, повлечет проблемы с электробезопасностью.

Несмотря на определенные трудности при монтаже и эксплуатации, AN/SPY-6 будет гораздо проще обслуживать, чем стоящий на вооружении AN/SPY-1D. В компании «Raytheon» утверждают, что модульность конструкции позволит без труда менять элементы RMA на новые.

Источники: https://www.vpk.name/news/263108_ssha_menyayut_radaryi_na_esmincah_na_fone_riska_snizheniya_elektrobezopasnosti.html (дата размещения материала 22.03.2019); http://www.arms-expo.ru/053049049048124051052056056053.html.

Американские беспилотные тральщики оснастят новейшими гидролокаторами

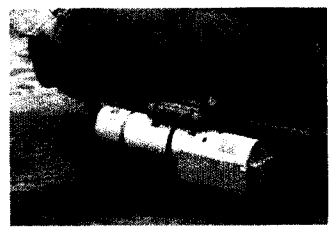
По данным сайта vpk.name, ВМС США завершили опытные испытания буксируемого противоминного гидролокатора Q-20C (AN/AQS-20C), предназначенного для оснащения безэкипажных катеров. Q-20C обладает расширенными возможностями акустического и оптико-электронного зондирования, которые позволяют обнаруживать и классифицировать морские мины различных типов.

Улучшения, внедренные в Q-20C, позволяют установить гидролокатор на беспилотный противоминный катер типа «MCM USV» уже в 2020 году.

Источник: https://www.vpk.name/news/270123_amerikanskie_bespilotnyie_tralshiki_osnastyat_noveishimi_gidrolokatorami.html (дата размещения материала 10.04.2019).

Подвесная лазерная система обнаружения мин

По информации, размещенной на сайте nevskii-bastion.ru, компания «Northrop Grumman» получила от ВМС США контракт на производство бортовой подвесной лазерной системы обнаружения мин AN/AES-1 ALMDS. Контейнер с датчиками ALMDS обнаруживает, классифицирует и опознает подповерхностные, якорные морские мины, им оснащаются вертолеты MH-60S «Knight Hawk», чтобы обеспечить быструю широкомасштабную разведку и оценку минных угроз в прибрежных зонах, узких проливах, районах действий амфибийных судов. Управление работой AN/AES-1 осуществляется с приборной доски в кабине вертолета MH-60S, туда же на многофункциональные индикаторы выводятся результаты сканирования водного пространства. Ожидается, что работы будут завершены к августу 2021 года.



Компания «Northrop Grumman», помимо ALMDS, разработала еще две противоминные системы. Первая из них, получившая обозначение RAMCS, предназначена для уничтожения надводных и подводных мин при помощи устанавливаемой на вертолеты MH-60S 30-миллиметровой пушки и специальных снарядов. В настоящее время она проходит наземные испытания. Вторая разработка – ASTAMIDS – представляет собой интегрированный комплект датчиков воздушного базирования, который может устанавливаться на БПЛА вертолетного типа «Fire Scout» для обнаружения и определения координат наземных мин.

Источник: http://www.nevskii-bastion.ru/system-almds-usa/ (дата размещения материала 30.04.2019).

США применили дроны в роли минных тральщиков

Как сообщается на сайте vpk.name, в марте 2019 года ВМС США и королевский флот Великобритании провели совместные учения в Карибском море по отработке минно-тральной тактики с использованием беспилотных надводных (БНА) и подводных аппаратов (БПА).

Учения проходили в соответствии с утвержденной концепцией UUV «Master Plan» (генеральным планом по БПА), которая предусматривала использование БНА и БПА для противоминной и противолодочной борьбы, ведения разведки, сбора информации и решения океанографических задач в интересах ВМС США.

В качестве мобильного подразделения, предназначенного для обезвреживания морских мин, было выбрано вспомогательное судно королевского флота «Mounts Bay», переоборудованное в корабль-носитель БНА и БПА.

На «Mounts Bay» были размещены посты управления БПА «Knifefish» и БНА «CUSV». БПА «Knifefish» оснащен гидролокатором с синтезированной апертурой, который позволяет обнаруживать мины на глубинах свыше 100 метров. На нем размещена аппаратура, которая может находить и классифицировать подозрительные объекты, передавать информацию оператору для дальнейшего анализа и принятия решения на их нейтрализацию.

БНА «CUSV» – беспилотный катер, который может управляться либо оператором, либо через спутник. В стандартные задачи этого БНА входит патрулирование, разведка и проведение ударных операций, а для отработки минно-тральных задач БНА оснащается беспилотной системой минного траления UISS.

Источник: https://www.vpk.name/news/270835_strategiya_lataniya_dyir_ssha_primenili_dronyi_v_roli_minnyih_tralshikov.html (дата размещения материала 12.04.2019).

Система «XLUUV» как возможный британский ответ «Лошарику»

По информации сайта vpk.name, британское минобороны изучает варианты разработки сверхбольшого беспилотного подводного корабля «XLUUV», предназначенного для выполнения секретных операций на расстояниях до 3000 морских миль. Автономность плавания нового изделия должна составить три месяца. Учитывая функциональное назначение «XLUUV», можно предположить, что новая система станет возможным ответом на российский вариант атомной подводной лодки АС-12 «Лошарик».

В перечень оборудования, предназначенного для установки на «XLUUV», входят оптико-электронная система, средства радиоэлектронной борьбы, а также акустические или неакустические системы наблюдения для ведения «надежной противолодочной борьбы на больших расстояниях». Благодаря дан-

ному оснащению «XLUUV» сможет выполнять три основные миссии: сбор разведывательных данных, создание противолодочного барьера, а также развертывание и возврат оборудования.

«XLUUV» после выхода из дока в автономном режиме переместится до места назначения, задержится на глубине перископа или ниже и будет контролировать проходящие суда сроком до трех месяцев. При этом система может располагаться на морском дне, используя для наблюдения выдвижное оборудование. При обнаружении объекта, вызывающего интерес, «XLUUV» сообщает об этом оператору и продолжает мониторинг.

С целью создания противолодочного барьера, «XLUUV» приходит в контрольную точку и патрулирует заранее определенную область в течение трех месяцев. «XLUUV» распознает акустическую подпись интересующей цели, идентифицирует ее как враждебную, сообщает о происшествии и продолжает патрулирование.

Для размещения оборудования «XLUUV» погружается на рабочую глубину, перемещается в необходимую зону и сбрасывает полезную нагрузку, за которой впоследствии возвращается.

Источник: https://www.vpk.name/news/273451_sistema_xluuv_kak_vozmozhnyii_britanskii_otvet_loshariku.html (дата размещения материала 19.04.2019).

Индонезийские рыбаки поймали китайский подводный беспилотник

Как сообщается на ряде сайтов, индонезийские рыбаки выловили в Южно-Китайском море подводный аппарат, позже идентифицированный как беспилотник-глайдер «Haiyi-7000», принадлежащий ВМС Китая.

Задача автономного глубоководного дрона «Haiyi-7000» – исследование дна и мониторинг заданных районов на предмет обнаружения подводных лодок противника. За месяц глайдер, используя попутные течения, способен пройти до тысячи километров.

Во время испытания в 2017 году подводный беспилотник погрузился в Марианскую впадину до отметки 6329 метров, установив мировой рекорд. В августе того же года НОАК запустила в Южно-Китайское море на опытное дежурство 12 аппаратов. Возможно, пойманный у берегов Бинтана дрон, является одним из аппаратов.

Источники: https://www.vpk.name/news/264247_indoneziiskie_ryibaki_poimali_kitaiskii_podvodnyii_bespilotnik.html (дата размещения материала 26.03.2019); http://www.arms-expo.ru/053049049048124051052056056053.html.

Британский корабль-разведчик
пришвартовался в Одессе

Как сообщает сайт riafan.ru, разведывательный корабль королевского военно-морского флота Великобритании HMS «Echo» H87 прибыл в Одессу 6 мая.

Британский корабль вошел в Черное море еще 20 апреля. Пять дней HMS «Echo» H87 провел в румынском порту Констанца, а затем с 30 апреля по 3 мая находился в грузинском Батуми. Согласно договору о режиме черноморских проливов, корабль покинет Черное море 9 мая.

Многоцелевое гидрографическое судно HMS «Echo» H87 предназначено для проведения геодезических работ в интересах подводного флота и планирования десантных операций. Также оно может использоваться как противоминный корабль для поиска мин и других подводных объектов.

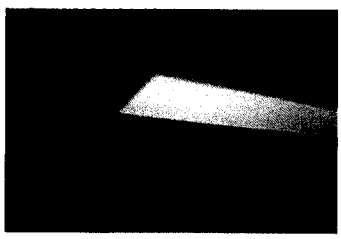
Источник: https://www.riafan.ru/1176113-britanskii-korabl-razvedchik-prishvartovalsya-v-odesse (дата размещения материала 06.05.2019).

1.2. Техническая защита информации

Президент Российской Федерации
подписал закон о суверенном Рунете

По информации сайта securitylab.ru, Президент Российской Федерации В.Путин подписал закон об изоляции Рунета, призванный обеспечить стабильную работу российского сегмента Интернета в случае отключения от всемирной сети или скоординированных атак.

Согласно положениям закона, в случае возникновения угроз устойчивой, безопасной и целостной работе Рунета на территории Российской Федерации и сети связи общего пользования Роскомнадзор сможет осуществлять централизованное управление трафиком согласно порядку, установленному российским правительством. При этом кабинет министров будет утверждать порядок такого управления, определять виды угроз и меры по их устранению.



Кроме того, правительство будет определять «случаи управления техническими средствами противодействия угрозам и передачи обязательных к выполнению указаний», а также определять условия и случаи, при которых операторы связи получат право не направлять трафик через технические средства противодействия угрозам. Такие средства будут предоставляться Роскомнадзором. Операторы, установившие такие технические средства, освобождаются от обязанности ограничивать доступ к сайтам с запрещенной информацией. Согласно действующему законодательству, сейчас они должны сами блокировать такой контент.

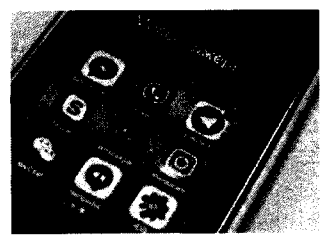
Закон также предусматривает создание национальной системы доменных имен. Порядок ее создания, требования к ней и правила ее использования установит Роскомнадзор. Ведомство также установит список групп доменных имен, составляющих российскую национальную доменную зону. Координировать деятельность по формированию доменных имен будет некоммерческая организация, одним из учредителей которой будет Российская Федерация.

Закон вступит в силу с 1 ноября 2019 года, за исключением ряда положений, в частности о криптографической защите и национальной системе доменных имен, которые начнут действовать с 1 января 2021 года.

Источник: https://www.securitylab.ru/news/498984.php (дата размещения материала 03.05.2019).

Новые правила идентификации в мессенджерах вступили в силу

Как сообщает сайт gazeta.ru со ссылкой на РИА «Новости», новые правила идентификации пользователя в мессенджерах начали действовать в России с 5 мая. Теперь сервисы обмена сообщениями должны взаимодействовать с операторами сотовой связи. Администраторы мессенджера будут нести ответственность за проверку корректности телефонного номера клиента.



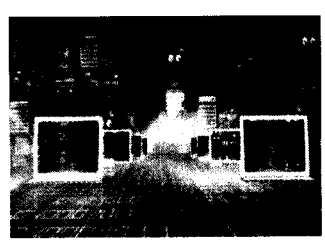
При регистрации нового пользователя мессенджер должен запросить данные клиента у мобильного оператора, причем ответ должен быть дан в течение 20 минут. Если данные совпадают, то пользователь может продолжить авторизацию, получив в SMS уникальный код. Операторы теперь будут пополнять свои базы данных сведениями о том, какие приложения люди используют для обмена сообщениями.

При отказе следовать новым правилам компанию-владельца мессенджера ожидает денежный штраф до 1 млн. рублей и блокировка на российской территории.

Источник: https://www.gazeta.ru/tech/2019/05/05_a_12339505.shtml (дата размещения материала 05.05.2019).

В реестр отечественного ПО будут допускаться только решения с российской технической поддержкой

По информации сайта iso27000.ru, Правительство Российской Федерации добавило новый пункт в правила формирования Единого реестра российского программного обеспечения (ПО), согласно которому гарантийным обслуживанием, технической поддержкой и модернизацией включенного в перечень ПО могут заниматься только российские коммерческие или некоммерческие организации без преобладающего иностранного участия либо граждане России.



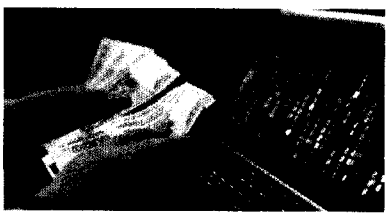
Аналогично, в реестр евразийского ПО включаются сведения о ПО, гарантийное обслуживание, техническая поддержка и модернизация ПО которого осуществляются коммерческой или некоммерческой организацией Евразийского экономического союза (ЕАЭС) без преобладающего иностранного участия либо гражданином страны-участницы ЕАЭС.

Изменения также коснулись пункта, разрешающего внесение ПО в реестр при условии, что ПО правомерно введено в гражданский оборот на территории России, его экземпляры либо права использования свободно реализуются на всей территории страны, отсутствуют ограничения, установленные в том числе иностранными государствами и препятствующие распространению или иному использованию программ на территории Российской Федерации или ее отдельных субъектов. Теперь указывается, что на всей территории России должны также свободно реализовываться услуги по предоставлению доступа к данному ПО.

Источник: http://www.iso27000.ru/novosti-i-sobytiya/v-reestr-otechest-vennogo-po-budut-dopuskatsya-tolko-resheniya-s-rossiiskoi-tehpodderzhkoi (дата размещения материала 04.04.2019).

Государство заставит российских ИБ-вендоров потратиться, а «варягов» уйти

Как сообщается на ряде сайтов, утвержденные приказом ФСТЭК России от 30 июля 2018 г. № 131 Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, вступают в силу с 1 июня 2019 года и касаются разработчиков и производителей программных и программно-аппаратных средств защиты информации (СЗИ), заявителей на осуществление сертификации, а также для испытательных лабораторий и органов, выполняющих работы по сертификации средств защиты на соответствие требованиям по безопасности информации. В отношении СЗИ должны быть проведены испытания по выявлению уязвимостей и недекларированных возможностей («закладок», «бэкдоров») в соответствии с методикой, разработанной и утвержденной ФСТЭК России в феврале 2019 года.



ФСТЭК России рекомендует разработчикам и производителям СЗИ провести оценку соответствия своих решений новым требованиям и представить результаты в ФСТЭК России для переоформления сертификатов соответствия до 1 января 2020 года, в противном случае действие сертификатов может быть приостановлено.

В связи с принятием новых требований, по мнению участников рынка решений в сфере информационной безопасности, бизнесу потребуются значительные инвестиции в разработку и сопровождение продуктов. С другой стороны, ужесточение требований позволит отсеять недобросовестных участников рынка. Одно из ключевых требований проверки недекларируемых возможно-

стей – передача исходного кода решений с описанием каждой функции и механизма работы. Иностранные разработчики решений в области информационной безопасности предоставлять исходные коды откажутся, что естественно снизит количество СЗИ зарубежных вендоров в госструктурах. Это, в свою очередь, выгодно отечественным поставщикам ИБ-решений, которые смогут занять освободившуюся нишу.

Источники: http://www.safe.cnews.ru/news/top/2019-04-09_gosudarstvo_zastavit_rossijskih_ibvendorov_potratitsya (дата размещения материала 09.04.2019); https://www.hitech.newsru.com/article/09apr2019/sec_po.

Иностранным компаниям без российского юридического лица могут закрыть доступ к данным россиян

По данным сайта securitylab.ru, автономная некоммерческая организация «Цифровая экономика», занимающаяся реализацией одноименного проекта, предложила запретить иностранным компаниям без российского юридического лица использовать данные россиян. Автором идеи является Ассоциация участников рынка больших данных, в которую входят Mail.Ru Group, «МегаФон», «Ростелеком» и другие компании.

В настоящее время подготовкой концепции управления данными занимается центр компетенций «Сколково». Рабочая версия концепции предлагает ввести единые требования для российских и иностранных компаний, использующих персональные данные россиян и осуществляющих свою деятельность на территории Российской Федерации.

Отечественные и зарубежные компании должны конкурировать между собой, но на них должны распространяться одни и те же требования. Нельзя при равных условиях предъявлять к российским компаниям более жесткие требования.

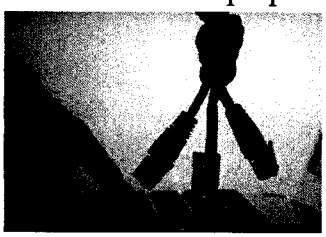
Некоторые иностранные компании обещали открыть российское представительство или отдельное юридическое лицо, но так этого и не сделали. Такие компании обязаны соблюдать российское законодательство, в противном случае доступ к данным россиян для них будет закрыт.

Согласно проекту, у иностранных компаний, не соблюдающих требования законодательства Российской Федерации по ограничению доступа к данным, не должно быть более выгодного положения по отношению к законопослушным отечественным компаниям.

Источник: https://www.securitylab.ru/news/498645.php (дата размещения материала 05.04.2019).

Глава Роскомнадзора призвал не сравнивать закон о суверенном Рунете с опытом Китая

Как сообщается на сайте securitylab.ru, закон об устойчивом Рунете не имеет отношения к опыту Китая в данной сфере. Об этом заявил руководитель Роскомнадзора А.Жаров.



В КНР профильные ведомства работают по принципу «белого списка» (запрещено все, что не разрешено), в России же ограничительные меры будут реализовываться по принципу «черного списка» – запрещено только то, что нарушает российские законы. Закон не скажется на работе операторов связи, однако Роскомнадзор так или иначе стремится избежать вероятных сбоев.

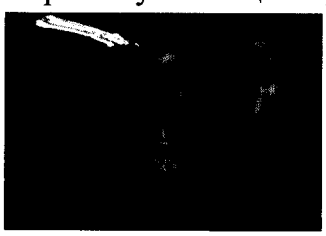
Как предполагается, новый закон позволит создать систему, которая обеспечит работу российского сегмента Интернета при отключении от инфраструктуры глобальной сети.

Источник: https://www.securitylab.ru/news/498891.php (дата размещения материала 23.04.2019).

Директор ФСБ России призвал мировое сообщество предоставить спецслужбам доступ к переписке

По информации, размещенной на сайте securitylab.ru со ссылкой на заявление главы ФСБ России А.Бортникова, Интернет должен работать согласно единым международным правилам, а у спецслужб должен быть доступ к зашифрованным сообщениям в защищенных мессенджерах.

Как отметил директор ФСБ России, размещение террористических ресурсов на иностранных серверах фактически обеспечивает им неуязвимость. Если мировому сообществу удастся договориться и ввести единые правила и стандарты в Интернете, террористы лишатся львиной доли ресурсов. В частности, у них будут сильно ограничены возможности для вербовки, пропаганды, финансирования, связи и управления.



Директор ФСБ России отдельно отметил проблему применения шифрования в сервисах для общения. Из-за повсеместного использования криптографической защиты эффективность оперативно-технических мероприятий по противодействию терроризму снизилась. Помочь в данном вопросе может разработанная российскими специалистами инициатива. Документ предусматривает создание доверенной и прозрачной для контроля системы депонирования ключей шифрования, генерируемых мобильными приложениями. Реализация концепции на международном уровне создаст правовые и технологические возможности для получения законного доступа к зашифрованным данным, передаваемым террористами с мобильных устройств.

Источник: https://www.securitylab.ru/news/498863.php (дата размещения материала 10.04.2019).

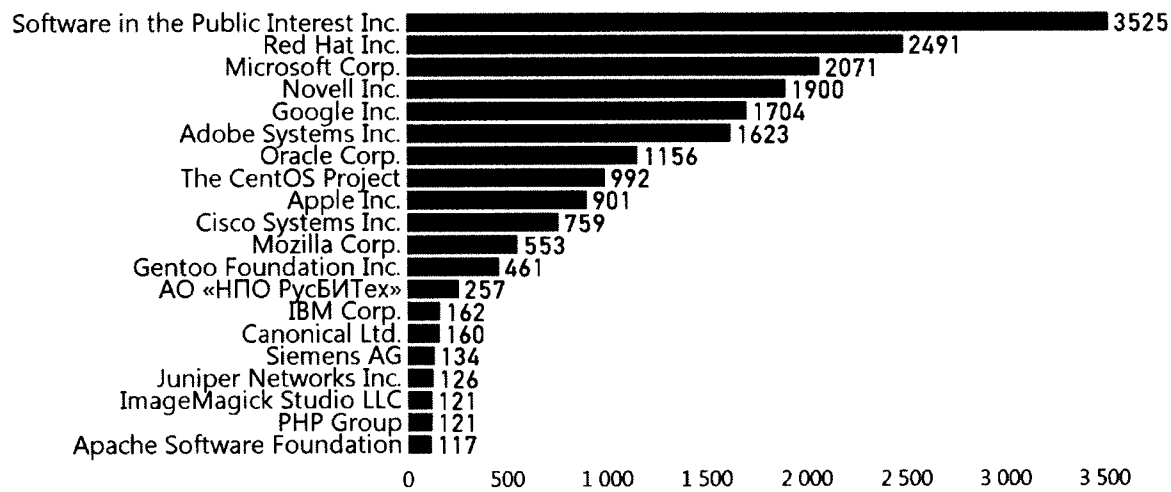
Банк данных угроз безопасности информации ФСТЭК России

На сайте ФСТЭК России bdu.fstec.ru размещен и поддерживается в актуальном состоянии банк данных угроз безопасности информации. Доступ к нему возможен также через официальный сайт ФСТЭК России fstec.ru (раздел «Техническая защита информации», подраздел «Банк данных угроз»).

По состоянию на 13 мая текущего года сайт банка данных угроз безопасности информации ФСТЭК России содержит 21279 записи об уязвимостях ПО и 213 записей об угрозах безопасности информации, наиболее характерных для государственных информационных систем, информационных систем персональных данных и автоматизированных систем управления технологическими процессами (АСУ ТП) на критически важных объектах (по каждой уязвимости дается описание по 20 полям).

В период с 26 марта по 13 мая 2019 года произведено 10 обновлений базы данных сайта, в результате которых внесены сведения о 595 уязвимостях в 322 видах ПО.

Основные статистические данные по уязвимостям ПО и угрозам безопасности информации:



Распределение уязвимостей по основным разработчикам программного обеспечения

Распределение уязвимостей по степени критичности

Распределение угроз безопасности информации по объектам воздействия

В БДУ ФСТЭК России реализован функционал в части предоставления сервисов для автоматизации процессов оценки уязвимости программного обеспечения и определения актуальных угроз для информационных (автоматизированных) систем. Примерами реализаций таких сервисов являются наличие на сайте БДУ безопасности информации ФСТЭК России программы ScanOVAL для автоматизированного определения уязвимостей в ПО (bdu.fstec.ru/site/scanoval), а также наличие классификации угроз безопасности информации (bdu.fstec.ru/cltthreat), позволяющие выбрать актуальные угрозы безопасности информации в соответствии с классификационными признаками (инцидентом, объектом воздействия, способом реализации угрозы, источником), учитывающими структурно-функциональные характеристики исследуемых информационных систем и характерные для них возможные угрозы безопасности информации.

Источники: http://www.bdu.fstec.ru; http://www.fstec.ru; http://www.twitter.com/gniiiptzi.

Исследователи научились скрывать от искусственного интеллекта истинную суть сказанного

По данным сайта securitylab.ru, специалисты компаний «IBM», «Amazon» и Техасского университета разработали атаку на алгоритмы обработки естественного языка NLP, с помощью которой им удалось изменить поведение модели искусственного интеллекта. Суть атаки, названной исследователями «атакой перефразирования», заключается в изменении вводимого текста таким образом, чтобы при сохранении первоначального смысла искусственный интеллект воспринимал его по-другому.

К примеру, существует алгоритм искусственного интеллекта, анализирующий содержимое электронных писем и обозначающий их как «спам» или «не спам». Злоумышленник может так модифицировать текст спам-сообщения, чтобы искусственный интеллект классифицировал его как «не спам». В то же время для человека смысл сообщения останется без изменений.

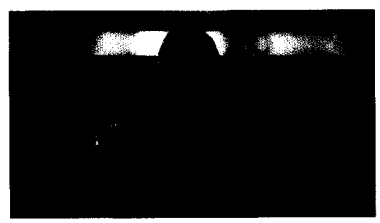
Предыдущие варианты атак на текстовые модели предполагали изменение одного слова в предложениях. Такое модифицирование текста действительно позволяло «обмануть» алгоритм, однако сами предложения при этом звучали неестественно. Исследователи решили не менять слова в предложениях, а перефразировать их полностью, сохраняя при этом читабельность.

Исследователи также создали алгоритм для поиска оптимальных изменений в предложениях, которые позволили бы манипулировать поведением модели NLP.

Источник: https://www.securitylab.ru/news/498602.php (дата размещения материала 02.04.2019).

«Лаборатория Касперского» нашла в Windows новую опасную уязвимость

Согласно данным сайта profile.ru, эксперты «Лаборатории Касперского» обнаружили новую уязвимость в операционной системе (ОС) Microsoft Windows. Брешь позволяет хакерам получить контроль над зараженным устройством. Злоумышленники использовали так называемый бэкдор – особый тип вредоносного ПО, с помощью которого можно получить удаленный доступ к компьютеру пользователя, запустить exe-файл и установить программу. Она, в свою очередь, запускала бэкдор, написанный на PowerShell. Это легитимный компонент Windows, благодаря которому хакерам удалось обойти стандартные механизмы защиты ОС.



Ранее издание «Профиль» писало о том, что «Microsoft обрушила» производительность миллионов компьютеров по всему миру очередным обновлением Windows 10.

Источник: https://www.profile.ru/news/scitech/gadgets/laboratoriya-kas-perskogo-nashla-v-windows-novuyu-opasnuyu-uyazvimost-137896 (дата размещения материала 16.04.2019).

Истребители F-35 уязвимы к кибератакам

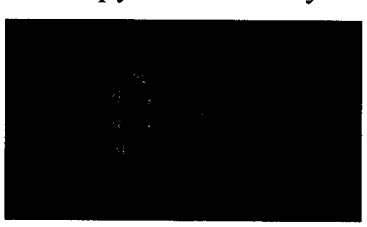
По информации сайта knews.kg, истребители F-35 совершенно не защищены от кибератак. К такому выводу пришли специалисты американской организации «Проект государственного надзора». F-35 считается самой дорогостоящей военной системой в истории, однако перед вредоносным ПО истребитель абсолютно беспомощен.

Кибербезопасность в F-35 играет чрезвычайно важную роль, поскольку его работа во многом зависит от сети автоматизированных систем. Из-за полностью интегрированной природы всех систем в F-35 кибербезопасность для него имеет гораздо большее значение, чем для других самолетов. Взаимосвязанная природа компьютерных систем F-35 уже сама по себе является серьезной уязвимостью. Все отдельные подсистемы самолета, такие как радары, система распределенной апертуры и система связи, навигации и идентификации, обмениваются данными между собой, то есть скомпрометировав лишь одну из них, злоумышленники смогут получить доступ ко всем остальным.

Источник: https://www.knews.kg/2019/03/30/istrebiteli-f-35-uyazvimy-k-kiberatakam/ (дата размещения материала 30.03.2019).

Киберпреступники активно эксплуатируют уязвимость в WinRAR

По данным, размещенным на сайте securitylab.ru, компания «Microsoft» опубликовала_подробности о мартовских атаках на компьютеры под управлением ОС Windows, использующиеся в телекоммуникационных компаниях. «Необычные техники» указывают на возможную причастность к инцидентам APT-группы «MuddyWater».



В ходе атак злоумышленники эксплуатировали известную уязвимость в WinRAR, получившую популярность в последнее время у киберпреступных и APT-групп. Преступники вооружились ею сразу после публикации компании «Check Point» в феврале. Исследователи продемонстрировали, как через уязвимость можно выполнить произвольный код на системе с помощью особым образом сконфигурированного файла ACE (формат компрессированных файлов).

Новая, исправленная версия WinRAR вышла за месяц до публикации Check Point, но даже в марте Microsoft по-прежнему детектировала атаки с использованием CVE-2018-20250.

В ходе мартовской кампании злоумышленники рассылали фишинговые письма якобы от министерства внутренних дел Афганистана. Используемые ими методы социальной инженерии были продуманы до мелочей с целью обеспечения полной удаленной компрометации системы в рамках ограниченной уязвимости в WinRAR. Фишинговые письма содержали документ Microsoft Word со ссылкой на другой документ на OneDrive. Никаких вредоносных макросов в нем не было, вероятно для того, чтобы избежать обнаружения атаки. Зато документ, загружаемый с OneDrive, содержал вредоносные макросы, после активации которых на систему жертвы загружалось вредоносное ПО.

В документе также была кнопка «Next page», отображающая поддельное уведомление об отсутствии нужного файла DLL и необходимости перезагрузки компьютера. Этот трюк был нужен, так как уязвимость позволяет вредоносному ПО только записывать файлы в определенную папку, но не запускать их сразу же. Поэтому идеальным вариантом являлся запуск вредоноса в папке «Автозагрузка», запускаемой сразу после перезагрузки компьютера. После перезагрузки на зараженной системе запускался бэкдор PowerShell, предоставляющий злоумышленникам полный контроль над ней.

Источник: https://www.securitylab.ru/news/498767.php (дата размещения материала 12.04.2019).

ИБ-эксперты заставили медицинское оборудование выдавать ложные результаты

Согласно данным сайта securitylab.ru, киберпреступники могут взломать современное медицинское оборудование, которое хранит критически важную информацию о пациентах, и модифицировать изображения, полученные в результате 3D-сканирования. Специалисты национального научно-исследовательского центра кибербезопасности при университете имени Бен-Гуриона продемонстрировали, как злоумышленник может ввести в заблуждение врачей, скомпрометировав компьютерный томограф и изменив результаты диагностики.

Эксперты, используя созданное ими устройство, тайно подключились к рабочей станции медицинского учреждения и перехватили управление томографом. Затем с помощью алгоритмов на основе искусственного интеллекта они модифицировали снимки, добавив на них злокачественные образования. Примечательно, что в 99% случаев врачи-радиологи не распознали обман и поставили ошибочный диагноз здоровым пациентам. Даже когда медикам рассказали об эксперименте, в большинстве случаев они не смогли отличить фальшивые снимки от настоящих.

Теоретически подобные атаки могут иметь масштабные последствия, вплоть до изменения хода политических выборов. Кроме того, они могут повлечь за собой смерть пациентов из-за неправильной постановки диагноза или использоваться в мошеннических схемах для обмана страховых компаний. Подобными атаками могут воспользоваться и вымогатели, например, модифицировав несколько сканов и затем требуя деньги за информацию.

Источник: https://www.securitylab.ru/news/498630.php (дата размещения материала 04.04.2019).

File Cabinet от «Google» содержит вредоносные загрузки[4]

По информации, размещенной на сайте darkreading.com, исследователям удалось обнаружить новый вид атаки «drive-by download» («скрытая загрузка»), в рамках которой шаблон file cabinet от «Google Sites» является средством доставки вредоносного ПО.

Специалисты исследовательской лаборатории «Netskope Threat» заметили, что шаблон file cabinet используется для доставки банковского трояна «LoadPCBanker» жертвам, которые либо говорят на португальском языке, либо являются жителями Бразилии.

«Google Sites» – это платформа для построения простых веб-сайтов. Для загрузки файлов на веб-сайт используется отдельная функция Google File Cabinet, которой пользуются злоумышленники для загрузки своего вредоносного ПО на веб-сайты и отправки фишинговых писем. Жертвам достаточно нажать на ссылку, которая отображается как Google URL, и вредоносное ПО перенаправляет их на веб-сайт злоумышленника. Там происходит загрузка вредоносного исполняемого файла, который замаскирован под PDF-файл.

Исследователи полагают, что такое распространение данный тип атаки получил потому, что пользователи практически безоговорочно доверяют всем сервисам от «Google».

Источник: https://www.darkreading.com/endpoint/google-file-cabinet-plays-host-to-malware-payloads/d/d-id/1334513 (дата размещения материала 23.04.2019).

Обнаружена недокументированная технология в микросхемах «Intel»

Как сообщает сайт ptsecurity.com, эксперты «Positive Technologies» представили исследование, посвященное неизвестной ранее технологии в чипсетах и процессорах «Intel». Она позволяет считывать данные из памяти и перехватывать сигналы периферийных

POSITIVE TECHNOLOGIES

[4] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

устройств. Исследователи обнаружили, что микросхемы PCH, установленные на материнских платах современных компьютеров на базе процессоров «Intel», содержат полноценный логический анализатор сигналов, который называется «Intel Visualization of Internal Signals Architecture» (VISA). Эта технология дает возможность отслеживать состояние внутренних линий и шин системы в режиме реального времени. Аналогичный анализатор реализован также в современных процессорах «Intel». Несмотря на то, что «Intel VISA» по умолчанию отключена на коммерческих системах, эксперты нашли несколько способов ее активации.

Через микросхему PCH, которую исследовали эксперты, осуществляется взаимодействие процессора с периферийными устройствами, поэтому этот чип имеет доступ практически ко всем данным компьютера. Исследователи предполагают, что «Intel VISA» используется для проверки наличия брака при производстве чипов «Intel». Вместе с тем, благодаря огромному количеству параметров, эта технология позволяет создавать собственные правила для захвата и анализа сигналов, которые могут быть использованы злоумышленниками для получения доступа к критически важной информации.

Проанализировать технологию позволила ранее выявленная экспертами «Positive Technologies» уязвимость INTEL-SA-00086 в подсистеме «Intel Management Engine» (IME), которая также интегрирована в микросхему PCH. Это дает злоумышленникам возможность атаковать компьютеры, например, устанавливать шпионское ПО в код данной подсистемы. Для устранения этой проблемы недостаточно обновления ОС, необходима установка исправленной версии прошивки.

Источник: https://www.ptsecurity.com/ru-ru/about/news/obnaruzhena-nedokumentirovannaya-tehnologiya-v-mikroshemah-intel/ (дата размещения материала 28.03.2019).

Сканер отпечатка пальца «SAMSUNG GALAXY s10» не гарантирует 100% защиту от взлома

Согласно информации, размещенной на сайте securitylab.ru, исследователь безопасности смог обмануть ультразвуковой датчик с помощью трехмерного отпечатка пальца. Речь идет об ультразвуковом сканере отпечатков пальцев, который, по заверению «Samsung», обеспечивает высокий уровень защиты устройства. Однако оказалось, что датчик легко обмануть. Исследователю удалось обойти систему защиты при помощи трехмерной модели отпечатка пальца.

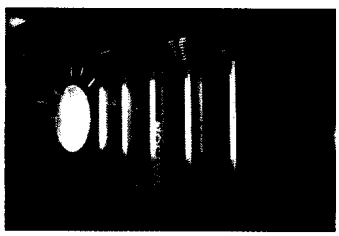
Для эксперимента он сфотографировал отпечаток своего пальца на бокале на смартфон, а затем отредактировал снимок, изменив насыщенность и контрастность, чтобы отпечаток лучше выделялся на общем фоне. Далее эксперт придал объем изображению с помощью программы 3ds Max для 3D моделирования и распечатал готовый объект на 3D-принтере. Используя созданный от-

печаток, пользователю удалось без проблем разблокировать сканер «Samsung Galaxy s10».

Источник: https://www.securitylab.ru/news/498653.php (дата размещения материала 06.04.2019).

Система аналитики «Watson» позволяет захватывать устройства и красть данные

Как сообщает сайт safe.cnews.ru, корпорация «IBM» выпустила предупреждение о нескольких серьезных уязвимостях, выявленных в ее аналитической системе «Watson» и уже исправленных в последнем обновлении. Все эти уязвимости так или иначе связаны с использованием Java.



Наиболее серьезной из них является CVE-2018-2633, которая позволяет злоумышленнику захватывать контроль над целевым устройством при наличии доступа к локальной сети, в котором оно расположено. Эксплуатировать данную уязвимость весьма непросто. Но учитывая ценность устройств, на которых запускается «Watson», для потенциальных злоумышленников уязвимость рекомендуется исправить как можно скорее. При успешной атаке злоумышленник может получить контроль над локальными приложениями JavaSE, JavaSEEmbedded и JRockit в OracleJavaSE.

Другая уязвимость – CVE-2018-2603 – позволяет вызвать «падение» системы, на которой запущен «Watson», с помощью DDoS-атаки. К сожалению, «IBM» не стала раскрывать подробности об этой уязвимости, ограничившись лишь констатацией, что эксплуатация этого бага проще, чем у CVE-2018-2633.

Три оставшиеся уязвимости – CVE-2018-2579, CVE-2018-2588 и CVE-2018-2602 – могут приводить к несанкционированному раскрытию конфиденциальной информации. Никаких подробностей о способах их эксплуатации не приводится.

Источник: http://www.safe.cnews.ru/news/top/2019-04-01_znamenitaya_sistema_analitiki_ibm_watson_pozvolyaet (дата размещения материала 01.04.2019).

«Huawei P30» превращает пользователей в потенциальных шпионов

Согласно информации сайта securitylab.ru, новая модель смартфона от компании «Huawei» позволяет тайно следить за людьми и записывать нажатия кнопок на банкоматах. С помощью пятидесятикратного цифрового зума в последних моделях смартфонов «Huawei» можно читать надписи и делать снимки небольших объектов на расстоянии сотен метров. Несмотря на удобство этой функции, по мнению ИБ-экспертов она представляет собой серьезную угрозу конфиденциальности данных. К примеру, с ее помощью, находясь на приличном расстоянии, злоумыш-

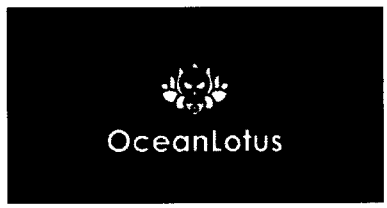
ленники смогут незаметно снимать, как пользователи вводят свои PIN-коды на банкоматах.

Безусловно, профессиональные фотоаппараты и телескопы также обладают подобным функционалом, но в отличие от смартфонов они не так доступны и не умещаются в карман. Когда человек с телескопом попытается снять банкомат, то сразу же привлечет к себе внимание. Чего не скажешь о стоящем через дорогу человеке с телефоном в руках – его легко принять за безобидного прохожего или туриста.

Источник: https://www.securitylab.ru/news/498820.php (дата размещения материала 17.04.2019).

Группа «OceanLotus» начала использовать новый бэкдор для macOS

По данным сайта itsec.ru, компания «ESET» обнаружила новую версию вредоносного ПО киберпреступной группировки «OceanLotus». Угроза представляет собой бэкдор для платформы macOS. Файл бэкдора зашифрован и обработан при помощи UPX-упаковщика, что затрудняет его обнаружение рядом антивирусных решений. Однако многие пользователи macOS игнорируют продукты для безопасности, поэтому защита бэкдора от обнаружения имеет второстепенное значение.



При запуске вредоносная программа проверяет принадлежность устройства к семейству Mac (MacBook Pro, MacBook Air). Информация, которую бэкдор отправляет на командный C&C-сервер, содержит сведения о процессоре, памяти, серийном номере устройства и MAC-адресах сетевого интерфейса.

Уверенные в безопасности macOS пользователи часто игнорируют антивирусное ПО. При этом аналитики фиксируют стремительный рост числа вредоносных программ для компьютеров «Apple».

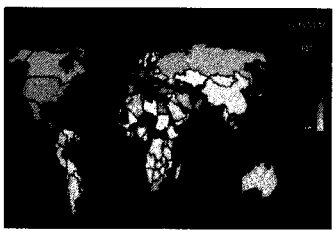
Источник: http://www.itsec.ru/news/gruppa-oceanlotus-nachala-ispol-zovat-novuy-backdoor-dlia-macos (дата размещения материала 17.04.2019).

Руткит «Scranos» вышел за пределы Китая и теперь распространяется по всему миру

Как сообщается на сайте webver.ru, операторы многофункционального руткита «Scranos» расширили поле деятельности за границы Китая и теперь атакуют пользователей по всему миру. По данным специалистов компании «Bitdefender», наибольшее число случаев инфицирования зафиксировано в Румынии, Франции, Италии, Индии, Бразилии и Индонезии.

«Scranos» сочетает в себе функции бэкдора, инфостилера и рекламного ПО и может работать на всех версиях Windows. В основном вредонос распространяется через взломанное ПО, поэтому в особой зоне риска находятся пользователи, имеющие привычку загружать и устанавливать именно такое ПО. Заразив устройство, «Scranos» получает полный контроль над ним.

Пока «Scranos» находится на стадии разработки, но даже в таком виде вредонос очень опасен. Он обладает модульной структурой, благодаря которой может выполнять различные функции, в том числе: извлекать cookie-файлы и учетные данные из браузеров Google Chrome, Chromium, Mozilla Firefox, Opera, Microsoft Edge, Internet Explorer, Baidu и Яндекс; загружать и выполнять любую

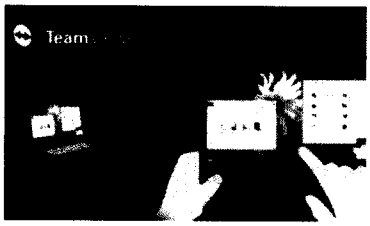


полезную нагрузку; похищать платежные данные с принадлежащих жертве аккаунтов в «Facebook», «Amazon» или «Airbnb»; от имени жертвы отправлять запросы на добавление в друзья в «Facebook»; отправлять фишинговые сообщения друзьям пользователя в «Facebook», содержащие вредоносные APK файлы (для заражения устройств на Android); красть учетные данные для авторизации в Steam; внедрять рекламное ПО в Internet Explorer; устанавливать расширения для Chrome/Opera для внедрения рекламного ПО; подписывать жертву на YouTube-каналы и пр. Специалисты «Bitdefender» выявили несколько случаев, когда «Scranos» использовался для установки «левых» расширений в браузеры и подписи тысяч пользователей на определенные каналы на YouTube.

Источник: http://www.webver.ru/news/security/ (дата размещения материала 17.04.2019).

Атаки «TeamViewer» под личиной государственного департамента США[5]

В атаках, использующих электронную почту и нацеленных на сотрудников посольства и правительственные финансовые органы, используется вредоносное вложение, замаскированное под документ с грифом «совершенно секретно». Это осуществляет «Team Viewer» – популярное ПО с удаленным доступом, для получения полного контроля над зараженным компьютером.



Атака начинается с электронного письма с информацией о «Военной программе финансирования» от государственного департамента США. Отличительной особенностью вложения файла является то, что имя вложения написано кириллицей.

Потенциальные жертвы получают подсказку задействовать макрокоманду, и как только они это делают, запускается легальная команда AutoHotkeyU32.exe наряду со скриптом AHK, который вызывает три дополнительных скрипта AHK URL из сервера управления и контроля.

Эти скрипты делают скриншоты компьютера жертвы, перехватывают имя пользователя и информацию о компьютере и отправляют полученные данные на сервер управления и контроля. Третий скрипт также загружает вредоносную версию «TeamViewer».

Обнаруженные жертвы атаки находятся в разных странах – это Бермудские острова, Гайана, Италия, Кения, Ливан, Либерия и Непал.

---

[5] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

Источник: https://www.threatpost.com/teamviewer-attacks-state-department/144014/ (дата размещения материала 22.04.2019).

Хакеры начали заражать компьютеры через старую переписку

По данным сайта lenta.ru, новая волна массовых заражений вредоносным ПО «Emotet» захлестнула пользователей сети в начале апреля 2019 года. На этот раз хакеры используют новую тактику, основываясь на данных, полученных в ходе своих предыдущих взломов.

Пользователи получают на электронную почту письмо от одного из предыдущих собеседников, которое на самом деле отправлено с сервера «Emotet». Письмо обычно начинается со слов: «Во вложении конфиденциальные документы». Далее следует ссылка, перейдя по которой пользователь скачивает вредоносное ПО.

Сейчас удар «Emotet» на себе испытывают в основном англоязычные пользователи, однако эксперты считают, что скоро под угрозой могут оказаться и немецкоговорящие страны. Пока хакеры используют учетные записи, которые они взломали до ноября 2018 года, но вскоре, как считают специалисты, перейдут и к другим пользователям.

«Emotet» – одно из самых опасных вредоносных ПО в мире в настоящее время. Оно появилось в 2014 году и изначально использовалось для получения данных банковских карт. С тех пор «Emotet» развился и теперь используется для заражения корпоративных сетей и распространения других вредоносных программ.

Источник: https://www.lenta.ru/news/2019/04/15/emotet/ (дата размещения материала 15.04.2019).

Системные администраторы готовятся к «Дню 768 тысяч»

Согласно информации сайта securitylab.ru, Интернет неумолимо приближается к рубежу, известному как «День 768 тысяч», и системные администраторы начинают подготовку к возможным отключениям из-за устаревшего оборудования.

Термин «День 768 тысяч» происходит от «День 512 тысяч», который пришелся на 12 августа 2014 года. В этот день тысячи интернет-провайдеров по всему миру столкнулись с массовым отключением Интернета. Причиной глобального отключения стал тот факт, что

у устаревших маршрутизаторов закончилась память для хранения глобальной таблицы маршрутизации BGP (файла, в котором хранятся адреса IPv4 всех известных подключенных к Интернету сетей). В то время огромная часть интернет-трафика маршрутизировалась через устройства с троичной ассоциативной

памятью (TCAM), выделенной области которой хватало не более чем на 512 тыс. маршрутизаторов.

12 августа 2014 года телекоммуникационная компания «Verizon» добавила 15 тыс. новых BGP-маршрутизаторов, в результате чего количество строк в таблице маршрутизации BGP превысило 512 тысяч. Это привело к переполнению выделенной памяти на старых моделях маршрутизаторов, и при каждой попытке обращения к таблице устройства выходили из строя.

Многие маршрутизаторы получили экстренные обновления, позволяющие системным администраторам расширить область выделенной памяти для хранения таблицы маршрутизации BGP. Большинство системных администраторов последовали рекомендациям и повысили лимит до 768 тысяч.

Как сообщают специалисты компании «AAGICo Berlin», «День 768 тысяч» наступит уже в следующем месяце. Однако ожидать массового отключения Интернета как в 2014 году не стоит. Крупные компании уже обновили свое оборудование, и переполнения памяти не предвидится.

Источник: https://www.securitylab.ru/news/498858.php (дата размещения материала 19.04.2019).

«Facebook» вступит в борьбу за контроль над подводными каналами связи

По данным сайта securitylab.ru со ссылкой на издание «The Wall Street Journal», китайская компания «Huawei» прокладывает по дну Индийского океана в направлении Африки оптоволоконный кабель, чем всерьез обеспокоены власти США. По мнению американского правительства, контроль за подводными кабелями может дать китайской компании возможность осуществлять шпионаж в пользу КНР.

Теперь же о планах проложить вокруг Африки подводный кабель сообщила компания «Facebook». Проект получил название «Simba».

В настоящее время проект находится на стадии обсуждения и о точном маршруте прокладывания подводного кабеля говорить пока рано. Тем не менее, в случае реализации проекта «Simba» привлечет к «Facebook» огромное количество новых пользователей на быстрорастущем африканском рынке, где некоторые сервисы компании уже успели завоевать популярность.

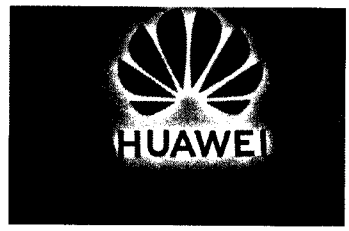
В прошлом «Facebook» уже участвовала в подобных проектах, но только в качестве партнера. Как правило, компания выступала в роли инвестора совместно с телекоммуникационными компаниями, у которых не было достаточно средств для самостоятельного прокладывания оптоволоконных трасс. Поскольку большая часть трафика исходит от пользователей «Facebook», компании было бы выгоднее иметь собственные кабели без участия посредников. Другие американские компании также заинтересованы в контроле над подводными каналами связи. К примеру, компания «Alphabet», которой принадлежит

«Google», в рамках проекта «Equiano» ведет работы по прокладыванию оптоволоконного кабеля вдоль западного побережья африканского материка.

Источник: https://www.securitylab.ru/news/498665.php (дата размещения материала 08.04.2019).

ЦРУ сообщило о финансировании «Huawei» китайским правительством

Как информирует сайт securitylab.ru со ссылкой на издание «The Times», власти США нашли очередное доказательство связи компании «Huawei» с китайским правительством. По данным издания, компания финансировалась национальной комиссией по безопасности КНР, народно-освободительной армией Китая и одним из подразделений государственной разведки. ЦРУ уведомило об этом своих союзников из разведывательного альянса «Пять глаз», куда, помимо США и Великобритании, также входят Австралия, Канада и Новая Зеландия.



В настоящее время Вашингтон активно призывает своих союзников отказаться от использования оборудования производства «Huawei» из-за возможного наличия в нем закладок. В частности, американские власти просят не использовать продукцию китайской компании при строительстве сетей 5G.

Источник: https://www.securitylab.ru/news/498884.php (дата размещения материала 22.04.2019).

Сотрудники ФБР проходят переобучение в связи с ростом киберугроз

По данным сайта securitylab.ru, ФБР проводит масштабное переобучение своих спецагентов в связи с растущим числом финансируемых противниками кибератак, угрожающих экономическим и политическим интересам США. В последний раз бюро проводило переквалификацию сотрудников таких масштабов в 2001 году после террористической атаки 11 сентября.

Эволюция угроз требует изменений в работе ФБР. По данным международной исследовательской организации «Third Way», правоохранители предпринимают шаги по отношению лишь к 1% киберинцидентов и расследуют только наиболее значительные из них, такие как кибератаки, финансируемые правительствами зарубежных стран, или сложные транснациональные преступные схемы.

Как отметил исполнительный директор программы по развитию кибербезопасности и технологий Аспенского Института Г.Графф, с точки зрения киберресурсов бюро находится на порядок или два ниже, чем требуется. Несмотря на очевидный прогресс в последнее время, только четыре или пять ре-

гиональных управлений ФБР имеют достаточно ресурсов и обладают соответствующими знаниями для противодействия сложным киберпреступлениям.

Источник: https://www.securitylab.ru/news/498569.php (дата размещения материала 01.04.2019).

В Эстонии начались ежегодные киберучения НАТО

Как сообщается на сайте securitylab.ru, 8 апреля в Эстонии стартовали ежегодные киберучения НАТО «Locked Shields 2019», которые являются крупнейшими и самыми передовыми международными военными киберучениями в мире. Специалисты стран НАТО примут участие в технико-стратегической игре, в ходе которой смогут испытать всю цепочку командования на случай серьезного киберинцидента, начиная от стратегического уровня и заканчивая оперативным, с привлечением как гражданских, так и военных ресурсов.

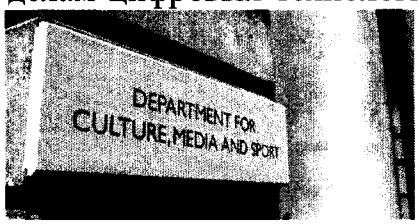
Согласно сценарию игры, выдуманная островная страна Берилия столкнулась с ухудшением ситуации с кибербезопасностью накануне выборов. Из-за координированных кибератак происходят сбои в работе систем очистки воды, электросетей, мобильной связи и других ключевых компонентов критической инфраструктуры. Инциденты также влияют на реакцию общественности на результаты выборов, из-за чего в стране происходят волнения.

Участники учений выступят в качестве национальных групп быстрого реагирования, брошенные на помощь Берилии. С технической стороны задачей участников является поддержание работы различных систем под сильным давлением. Со стратегической стороны они должны понимать принятые в стране механизмы координации, принцип действий правоохранительных органов и работу стратегических каналов связи.

Источник: https://www.securitylab.ru/news/498681.php (дата размещения материала 09.04.2019).

Великобритания обзаведется собственным Роскомнадзором

По информации, размещенной на сайте securitylab.ru, министерство по делам цифровых технологий, культуры, СМИ и спорта Великобритании предложило создать в стране независимое ведомство, которое займется регулированием контента в Интернете. Совместно с Хоум-офисом министерство разработало проект документа под названием «Online Harms White Paper».



Авторы документа предлагают создать независимое ведомство, которое разработало бы свод правил для технологических компаний, и наделить его правом взимать штрафы за их нарушение. Документ

также допускает возможность введения штрафов для руководства провинившихся компаний и блокировки сайтов-нарушителей.

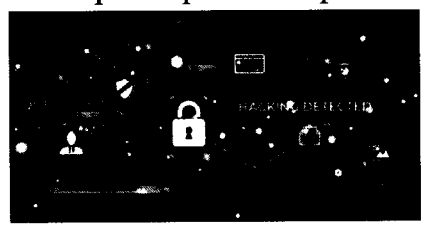
Согласно документу, новое ведомство займется сайтами, распространяющими нелегальный контент и занимающимися продажей незаконных товаров. Под пристальным взглядом регулятора также окажутся сайты, вовлеченные в кибербуллинг, троллинг и распространение фейковых новостей.

Источник: https://www.securitylab.ru/news/498672.php (дата размещения материала 08.04.2019).

Мировой рейтинг кибербезопасности

Как сообщается на сайте aussiedlerbote.de, ежегодно эстонская академия электронного управления составляет мировой рейтинг национальной кибербезопасности «National Cyber Security Index». В этом году самой защищенной страной назвали Чехию, которая немного опередила прошлогоднего лидера – Эстонию.

Исследователи оценили 130 стран мира по таким параметрам: конфиденциальность и сохранение целостности данных, законодательство в сфере информационных технологий и др., всего – 46 показателей.



Топ-10 «National Cyber Security Index 2019» выглядит так: Чехия (90,91 балла), Эстония (90,81), Испания (89,61), Литва (88,31), Франция (83,12), Дания (81,82), Германия (80,52), Сингапур (80,52), Словакия (79,22) и Финляндия (79,22).

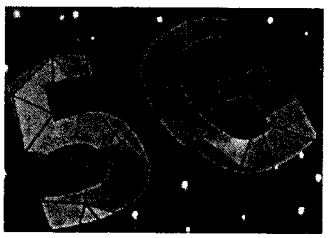
Параллельно был составлен рейтинг уровня развития цифровых технологий. В этом списке на первом месте оказалась Швейцария (85,13 балла), на втором и третьем месте Южная Корея (84,25) и Исландия (84,19). Германия по уровню диджитализации занимает 14 место с результатом 81,95 балла.

Источник: https://www.aussiedlerbote.de/2019/04/mirovoj-rejting-kiber-bezopasnosti-germaniya-na-7-meste/ (дата размещения материала 12.04.2019).

ЕС разработает стандарты безопасности для сетей 5G

По данным сайта iso27000.ru со ссылкой на издание «Bloomberg», Европейский Союз (ЕС) намерен призвать европейские правительства к обмену информацией для управления рисками безопасности беспроводных сетей 5G. ЕС опубликует рекомендации, согласно которым странам-участницам будет дано несколько месяцев на выявление и сообщение ЕС потенциальных угроз безопасности сетей 5G на их рынках. На базе этой информации будут разработаны минимальные стандарты безопасности, действительные на всей территории ЕС.

Данный шаг направлен на координацию европейского подхода к управлению киберрисками на фоне обвинений в шпионаже, выдвинутых правительством США против компании «Huawei» и других китайских технологических компаний. В настоящее время Вашингтон активно призывает своих союзников отказаться от услуг «Huawei» по строительству сетей 5G. Американские власти даже угрожают Германии прекратить сотрудничество в обмене разведданными, если она будет иметь дело с китайской компанией.



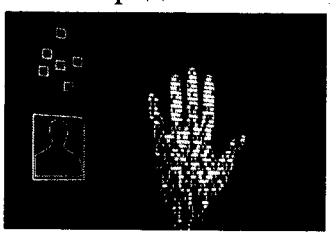
Тем не менее, ЕС готовит гораздо более мягкие меры, чем хотелось бы США. Европейские страны пытаются найти баланс между обеспечением кибербезопасности на фоне растущего влияния Китая и выгодным сотрудничеством со вторым крупнейшим торговым партнером на этом рынке. Германия и Франция предлагают не отказываться от сотрудничества с «Huawei», а ужесточить требования для сетей передачи данных.

Источник: http://www.iso27000.ru/novosti-i-sobytiya/es-razrabotaet-standarty-bezopasnosti-dlya-setei-5g/ (дата размещения материала 26.03.2019).

ЕС намерен создать огромную биометрическую базу данных

По информации сайта securitylab.ru, Европейский парламент проголосовал за создание единой базы данных, объединяющей ряд систем пограничного контроля, миграции и правоохранительных органов. Новая база под названием «Common Identity Repository» (CIR) будет доступна для поиска и позволит отслеживать биометрические данные граждан стран ЕС и не входящих в союз государств.

Предполагается, что CIR будет объединять идентификационные записи (имена, даты рождения, номера паспортов и другую идентифицирующую информацию) и биометрические данные (отпечатки пальцев, сканы лиц). Доступ к сведениям смогут получать все пограничные и правоохранительные органы. Основное предназначение базы данных заключается в упрощении работы пограничников и сотрудников органов правопорядка ЕС, которые смогут быстрее осуществлять поиск в единой системе, а не в разрозненных базах данных.



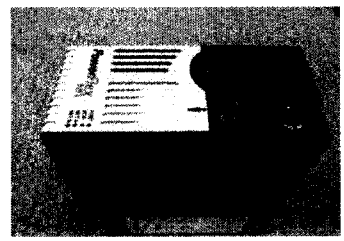
После запуска CIR пополнит число крупнейших отслеживающих баз данных мира наряду с базой данных китайского правительства и индийской биометрической системой «Aadhar». В свою очередь, Европейский парламент и ЕС пообещали реализовать надлежащие меры для защиты конфиденциальности граждан и контроля доступа к данным правоохранительных органов.

Источник: https://www.securitylab.ru/news/498876.php (дата размещения материала 19.04.2019).

1.3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры

В преобразователях частоты «Rockwell Automation» обнаружена опасная уязвимость

По информации сайта securitylab.ru, преобразователи частоты компании «Rockwell Automation» «Allen Bradley PowerFlex 525» содержат опасную уязвимость, позволяющую вызвать отказ в обслуживании и перехватить контроль над уязвимым устройством.



Эксплуатируя уязвимость атакующий может вызвать сбой в работе ПО, используемого для управления и конфигурации устройства. Для этого потребуется отправить специально сформированные UDP-пакеты, которые приведут к сбою стека CIP.

В результате ПО перестанет работать, а пользователи будут заблокированы. Однако злоумышленник сможет отправлять команды на систему. Таким образом он сможет выполнять различные команды, например, изменить скорость работы устройства или запустить/отключить его. Единственное решение проблемы – жесткая перезагрузка устройства.

По словам экспертов, баг вызывает нарушения в работе CIP демона, в результате устройство возвращает ряд некорректных значений, а установка нового соединения блокируется. Одна из проблем заключается в том, что управляющее ПО постоянно отслеживает все нужные значения и при получении неожиданного значения пытается переустановить соединение, в конечном итоге это приводит к блокировке. В то же время, используя простенький скрипт, атакующий может инициировать соединение и продолжить отправлять команды и запросы. После закрытия соединения для установки новых подключений требуется жесткая перезагрузка устройства.

Указанная уязвимость была выявлена в версии «PowerFlex 525 5.001», но эксперты полагают, что она может затрагивать и более ранние версии.

Источник: https://www.securitylab.ru/news/498559.php (дата размещения материала 29.03.2019).

Уязвимость в ПЛК «Rockwell Automation» позволяет переадресацию на вредоносные сайты

По информации, размещенной на сайте securitylab.ru, в ряде программируемых логических контроллеров (ПЛК) производства компании «Rockwell Automation» обнаружена опасная уязвимость, воспользовавшись которой злоумышленники могут перенаправить пользователей на вредоносные сайты. Уязвимость затрагивает контроллеры серий «MicroLogix 1100» и «MicroLogix 1400», а также «CompactLogix 5370» (L1, L2 и L3). Степень опасности бага оценена в 7,1 балла по шкале CVSS v3.

Проблема представляет собой уязвимость открытого редиректа, которая связана с реализованным в устройствах web-сервером. Сервер принимает входные данные с web-интерфейса ПЛК, чем может воспользоваться неавторизованный атакующий для внедрения вредоносной ссылки, переадресовывающей пользователей на подконтрольный злоумышленнику сайт, содержащий вредоносное ПО.

Производитель уже выпустил обновление, устраняющее проблему. Если возможность установить обновление отсутствует, пользователям рекомендуется отключить web-сервер и реализовать меры для предотвращения потенциальных атак.

Источник: https://www.securitylab.ru/news/498933.php (дата размещения материала 26.04.2019).

Сетевые DDoS-атаки на ПЛК могут привести к сбою физических процессов

Как сообщается на сайте securitylab.ru, исследователи продемонстрировала интересный вид DDoS-атаки на ПЛК, позволяющий нарушить физические процессы, контролируемые устройством.

Уровень опасности данной уязвимость оценивается в 7,5 балла по шкале CVSSv3. В отличие от ИТ-систем в промышленной среде именно уязвимости отказа в обслуживании представляют большую угрозу.

Атака направлена на время цикла ПЛК. Рабочий цикл контроллера включает несколько фаз: начало цикла, чтение состояния входов (датчиков), выполнение кода программы пользователя, выполнение задач по диагностике и коммуникации, запись состояния выходов. Как правило, цикл занимает от 1 до 10 миллисекунд.

Исследователи продемонстрировали, как специально сформированный сетевой трафик, направленный на ПЛК, может повлиять на время цикла, что приведет к сбою контролируемых устройством физических процессов. По их словам, атака может быть осуществлена либо из Интернета (если целевое устройство подключено к Интернету), либо со скомпрометированного устройства в той же сети, что и ПЛК. При этом атакующему не нужно знать, какие процессы контролирует ПЛК или какая программа на нем работает.

Атака была протестирована на 16 устройствах от шести различных производителей, в частности, «ABB», «Phoenix Contact», «Schneider Electric», «Siemens» и «WAGO». По мере возможности она производилась на ПЛК с установленными по умолчанию настройками.

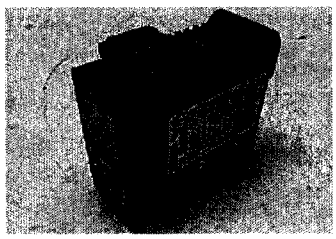
Только одно из протестированных устройств оказалось не подвержено атаке данного типа. Патчи, устраняющие данную уязвимость, выпустил только один вендор из шести. Компания «Schneider Electric» выпустила соответствующие обновления для решений «Modicon M221» и «EcoStruxure Machine Expert».

В «ABB» заявили, что атака затрагивает только устройства с установленными по умолчанию настройками. По словам представителей «Phoenix Contact», проблема касается только устаревших устройств и не затрагивает новые версии продуктов. Как сообщили в «Siemens», ее продукты уязвимости не подвержены, а в «WAGO» заявили, что проблема довольно старая и порекомендовали использовать ПЛК в закрытых сетях либо защитить их межсетевым экраном, а также установить ограничение сетевого трафика.

Источник: https://www.securitylab.ru/news/498862.php (дата размещения материала 19.04.2019).

В точках доступа «RAD-80211-XD» обнаружена опасная уязвимость

По данным сайта infocost.ru, в беспроводных модулях «RAD-80211-XD» производства немецкой компании «Phoenix Contact» обнаружена серьезная уязвимость. По шкале CVSS v3 она получила оценку 9,9 балла из максимальных 10.С ее помощью любой авторизованный пользователь может воспользоваться утилитой WebHMI и выполнить на сервере произвольные команды ОС. Для осуществления атаки особые знания не требуются. Поскольку эти продукты являются устаревшими и больше не поддерживаются производителем, обновления безопасности для них выпущены не будут.

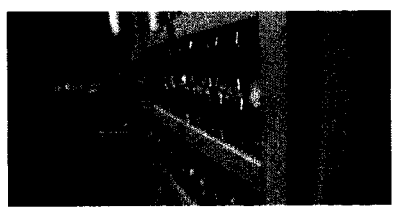


Беспроводные модули «RAD-80211-XD» используются в организациях, связанных с телекоммуникациями, информационными технологиями и производством. В качестве мер защиты от возможной эксплуатации уязвимости злоумышленниками рекомендуется использовать модули в закрытых сетях или сетях, защищенных надежными межсетевыми экранами. Производитель также настоятельно рекомендует перейти на использование актуальных версий модулей.

Источник: https://www.infocost.ru/2019/03/28/v-tochkah-dostupa-rad-80211-xd-obnaruzhena-opasnaya-uyazvimost/ (дата размещения материала 28.03.2019).

ФСТЭК России планирует ввести административную ответственность за несоблюдение требований к безопасности объектов КИИ

По информации сайта kommersant.ru, ФСТЭК России планирует с 2020 года ввести административную ответственность за несоблюдение требований к безопасности объектов критической информационной инфраструктуры (КИИ). Сейчас Федеральный закон № 187-ФЗ «О безопасности критической информационной структуры Российской Федерации», вступивший в силу в прошлом году, все еще работает неполноценно, признают участники рынка. Это связано с тем, что нет четких сроков по завершению процессов категорирова-



ния. Многие организации оттягивают этот процесс и, следовательно, не занимаются обеспечением безопасности. В то же время в регионах уже начинают требовать его соблюдения.

По закону владельцы значимых объектов уже обязаны соблюдать требования к их безопасности, но при этом ответственности за несоблюдение этой нормы нет, если оно не повлекло неправомерного воздействия на КИИ. За само неправомерное воздействие на КИИ закон предусматривает уголовную ответственность.

По словам независимого эксперта по кибербезопасности А.Лукацкого в Кодексе об административных правонарушениях уже есть статья «Нарушение правил защиты информации», но в ФСТЭК России всегда говорили, что она не работает для КИИ. По сути планируется ввести аналогичную статью, но под критическую инфраструктуру.

Также по словам эксперта, ФСТЭК России уже инициировала внесение изменений, согласно которым завершить категорирование объектов КИИ нужно будет к 1 июня 2019 года. Кроме того, речь может идти и о введении административной ответственности за неправильное категорирование объектов.

Источник: https://www.kommersant.ru/doc/3924986 (дата размещения материала 28.03.2019).

2. Сведения о перспективах развития и достижениях в создании способов и средств защиты информации

СУБД «Microsoft SQL Server 2017» получила сертификат ФСТЭК России

На сайте servernews.ru компания «Сертифицированные информационные системы» сообщила о сертификации ФСТЭК России системы управления базами данных (СУБД) «Microsoft SQL Server 2017». В рамках сертификации СУБД прошла проверку на соответствие требованиям безопасности и техническим условиям, а также на предмет отсутствия недекларированных разработчиком возможностей.

Выданный ФСТЭК России сертификат удостоверяет, что «Microsoft SQL Server 2017» в редакциях «Enterprise», «Standard», «Developer», «Web», «Express with Advanced Services» является СУБД со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям по безопасности информации, установленным в ТУ 5021-003-29176085-2018. Продукт может применяться для защиты информации в ГИС до 3 класса защищенности включительно, а также в информационных системах персональных данных (ИСПДн) до 3-го класса защищенности включительно для актуальных угроз безопасности информации 3-го типа.

Источник: https://www.servernews.ru/984858 (дата размещения материала 27.03.2019).

ОС «Astra Linux» сертифицирована ФСБ России и ФСТЭК России

По информации сайта spbit.ru, ОС «Astra Linux Special Edition» (релиз «Ленинград»), разработанная в 2018 году для вычислительных комплексов с процессорной архитектурой «Эльбрус», успешно прошла сертификацию по требованиям безопасности информации ФСТЭК России к ОС типа А 2-го класса защиты и требованиям безопасности информации ФСБ России к средствам защиты информации. ОС «Astra Linux Special Edition» может применяться в автоматизированных системах в защищенном исполнении.

В 2018 году Минобороны России, Генеральным штабом Вооруженных Сил Российской Федерации и АО «НПО «РусБИТех» был подписан регламент устранения уязвимостей в ОС «Astra Linux». Теперь все обновления ОС, решающие задачу обеспечения определенного уровня защищенности и информационной безопасности, оперативно доводятся до операторов и пользователей автоматизированных систем органов военного управления.

Источник: https://www.spbit.ru/news/n168176/ (дата размещения материала 10.04.2019).

Специальное программное обеспечение «Аккорд-KVM»

Согласно данным сайта accord.ru сообщается, что компания «ОКБ САПР» разработала специальное программное обеспечение (СПО) «Аккорд-KVM», которое является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну.

Новое решение представляет собой элемент системы защиты информации информационных систем и предназначено для защиты среды виртуализации, построенной на базе технологии KVM с применением библиотеки виртуализации libvirt.

Сертификат ФСТЭК России подтверждает соответствие СПО «Аккорд-KVM» требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по четвертому уровню контроля и технических условий ТУ 501410-073-37222406-2018 при выполнении указаний по эксплуатации, приведенных в документации, что позволяет применять его для средств виртуализации, обрабатывающих сведения конфиденциального характера.

Источник: http://www.accord.ru/ (дата размещения материала 01.04.2019).

Вышла обновленная версия «Гарда БД»

По данным сайта itweek.ru, компания «Гарда Технологии» представила обновленную версию системы защиты баз данных и веб-приложений «Гарда БД». Решение представляет собой аппаратно-программный комплекс для аудита сетевого доступа к базам данных и веб-приложениям. Система непрерывно контролирует легитимность доступа всех пользователей к базам данных, выявляет подозрительную активность, информирует об инцидентах в режиме реального времени.

В новой версии большое внимание уделено автоматизации работы системы и удобству работы с кластеризованными и географически распределенными системами. В продукте появилась возможность автоматически ставить вновь обнаруженные базы данных на контроль. В результате сокращаются временные промежутки, когда мониторинг доступа не ведется. Администрато-

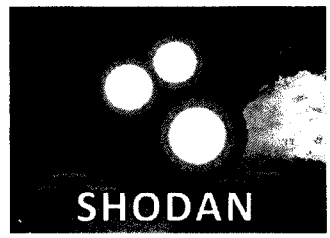
ру системы теперь не нужно постоянно следить за целостностью и полнотой подпадающих под аудит данных.

Одним из ключевых обновлений системы «Гарда БД» стала значимая переработка агентских решений по мониторингу доступа к СУБД. Расширен список поддерживаемых ОС, доступных для установки агентов.

Источник: https://www.itweek.ru/security/news-company/detail.php?ID=206963 (дата размещения материала 23.04.2019).

«Shodan» запустил сервис, помогающий определить поверхность атаки

Как сообщает сайт anti-malware.ru, знаменитый в кругах специалистов поисковик «Shodan» запустил новый сервис под названием «Shodan Monitor», который способен помочь организациям отслеживать подключенные к Интернету системы. В итоге «Shodan Monitor» может стать для организаций отличным инструментом, который поможет определить поверхность атаки за счет оценки систем, подключенных к Интернету. Новый сервис позволяет пользователям запускать сканирование и получать уведомления о детектировании нового обнаруженного устройства в режиме реального времени.

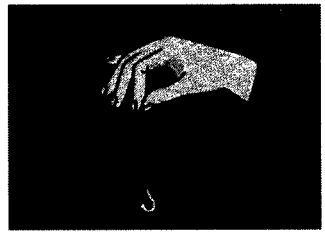


Источник: https://www.anti-malware.ru/news/2019-03-29-1447/29301 (дата размещения материала 29.03.2019).

«Google» реализует новую меру защиты от фишинговых атак

Согласно информации, размещенной на сайте allnokia.ru, с целью обеспечения лучшей защиты от атак типа «человек посередине» компания «Google» будет блокировать попытки авторизации, инициированные из встроенных фреймворков для web-браузинга, которые нередко используются в фишинговых атаках.

Речь идет о «Chromium Embedded Framework» (CEF), «XULRunner» и тому подобных инструментах. Встроенные фреймворки браузеров позволяют разработчикам добавлять в приложения функции браузера. К примеру, CEF предоставляет возможность встраивать в приложения браузерный движок Chromium.



Фишеры могут использовать такие фреймворки для выполнения скрипта JavaScript на web-странице и автоматизации пользовательской активности. В рамках атаки «человек посередине» злоумышленник, владеющий учетными данными и кодами двухфакторной аутентификации, может автоматизировать авторизацию в действующих сервисах «Google».

Подобные атаки сложно обнаружить, и блокировка попыток авторизации с этих платформ должна решить проблему. Данная мера коснется разработчи-

ков, которым придется изъять такие фреймворки из своих приложений. Им «Google» рекомендует перейти на использование Oauth-аутентификации.

Источник: https://www.allnokia.ru/news/324588/ (дата размещения материала 19.04.2019).

«Apple» обновила «XProtect», чтобы бороться с вредоносными файлами Windows

По данным, размещенным на сайте anti-malware.ru, компания «Apple» усовершенствовала свое защитное ПО «XProtect». Теперь оно в состоянии детектировать файлы Windows, которые могут представлять угрозу для пользователей macOS. Эксперты в области безопасности утверждают, что обновленная версия «XProtect» может детектировать файлы Windows Portable Executable (PE).

«XProtect» представляет собой защитную систему, основанную на использовании сигнатур. Она связана со встроенным в систему macOS антивирусом «Gatekeeper». Для защиты и уведомления пользователей об обнаруженных подозрительных и вредоносных файлах «Gatekeeper» использует систему карантина файлов, схожую с той, что используется в Windows. Если антивирус в macOS обнаруживает подозрительный файл, его сверяют с базой сигнатур «XProtect». При этом «XProtect» работает на основе правил Yara и черных списков. Вышедший недавно апдейт дополнил «XProtect» базой MACOS.d1e06b8, содержащей сигнатуры файлов PE. Причиной такого шага стал вредонос «TrojanSpy.MacOS.Winplyer», разработанный для заражения macOS-компьютеров.

Источник: https://www.anti-malware.ru/news/2019-04-25-1447/29540 (дата размещения материала 25.04.2019).

«Kaspersky ASAP» обучит сотрудников основам защиты от киберугроз

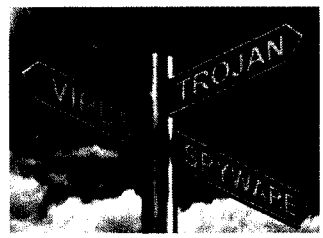
По информации сайта anti-malware.ru, компания «Лаборатория Касперского» анонсировала новую автоматизированную платформу «Kaspersky Automated Security Awareness Platform (ASAP)». «Kaspersky ASAP» способна предложить новый подход к организации тренингов по защите от киберугроз. В сущности, новая разработка представляет собой онлайн-инструмент, позволяющий сформировать и закрепить у сотрудников навыки безопасной работы в цифровом пространстве. Эксперты «Лаборатории Касперского» еще раз напомнили, что человек является самым слабым звеном в цепочке информационной защиты организации. Антивирусная компания провела исследование, согласно которому 52% компаний рассматривают сотрудников в качестве одной из самых серьезных угроз корпоративной безопасности.

И здесь на помощь приходит платформа «Kaspersky ASAP». Новая разработка позволит оценить текущие знания каждого отдельного сотрудника по части кибербезопасности. Более того, на основе полученных данных «Kaspersky ASAP» подберет индивидуальный график программы для каждого работника. При построении графика будут учитываться рабочие обязанности, профиль риска и набор навыков, необходимый сотруднику. При этом «Kaspersky ASAP» принимает во внимание человеческую память – каждый урок длится не более 10 минут, а также на ключевых сообщениях несколько раз делается акцент. Сотрудникам будут предложены: интерактивный модуль, видеоролики, упражнения на закрепление полученного материала и его проверку.

Источник: https://www.anti-malware.ru/news/2019-04-01-1447/29314 (дата размещения материала 01.04.2019).

NCSC создал онлайн-инструмент для тестирования защищенности организаций

Как сообщает сайт anti-malware.ru, новый бесплатный инструмент, разработанный центром правительственной связи (NCSC) Великобритании, позволит организациям проверить свои возможности по части отражения кибератак. Это поможет компаниям подготовиться к фишинговым атакам, вредоносным программам и другой злонамеренной активности. Специалисты NCSC разработали этот онлайн-инструмент, получивший название «Exercise in a Box», чтобы организации смогли проверить степень своей защиты в сценариях, основанных на реальных атаках. Этот новый онлайн-инструмент может сыграть ключевую роль в укреплении киберзащиты малого бизнеса, ряда местных властей и организаций из других важных секторов.



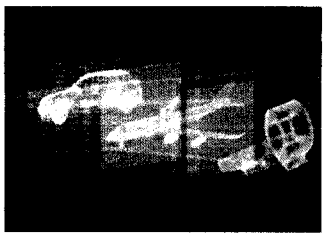
«Exercise in a Box» предоставляет пользователю определенный набор различных сценариев, которые берут за основу реальные киберугрозы. Следовательно, организации могут попрактиковаться в противодействии реальным атакам. Компании, желающие опробовать инструмент в действии, могут зарегистрироваться для использования «Exercise in a Box» на сайте NCSC.

Источник: https://www.anti-malware.ru/news/2019-04-26-1447/29548 (дата размещения материала 26.04.2019).

NIST обновил инструмент для поиска ошибок в критически важном ПО

По информации сайта securitylab.ru, национальный институт стандартов и технологий (NIST) США выпустил обновление исследовательского набора инструментов ACTS, призванное помочь разработчикам сложных критически важных с точки зрения безопасности приложений выявлять потенциально опасные ошибки в своем ПО.

Решение ACTS позволяет разработчикам удостовериться, что их продукты не содержат «одновременные комбинации входных значений», которые могут вызвать серьезную ошибку. В случае критически важных с точки зрения безопасности приложений, реализованных на ядерных объектах, в самолетах, автомобилях и т.п., подобные ошибки могут привести к серьезным последствиям.



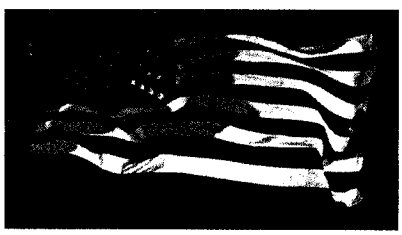
Кроме этого, исследователи из NIST разработали инструмент под названием «Combinatorial Coverage Measurement» (CCM), позволяющий тестировать ПО с тысячами входных переменных. Новое решение позволит не только улучшить безопасность, но и снизить расходы на разработку ПО. Инструмент CCM уже добавлен в состав набора ACTS.

Источник: https://www.securitylab.ru/news/498931.php (дата размещения материала 26.04.2019).

Министерство энергетики США рассматривает блокчейн для предотвращения кибератак на электростанциях

Согласно данным сайта bitjournal.media, министерство энергетики США исследует технологию блокчейна как линию защиты от кибератак на электростанциях. Подразделение национальной лаборатории энергетических технологий объявило о начале второго этапа проекта по обеспечению безопасности электросетей в сотрудничестве с децентрализованным стартапом по кибербезопасности «Taekion».

В рамках второго этапа проекта стартап будет изучать, как можно использовать технологию блокчейна для обеспечения безопасности электростанции. Система может быть взломана так, что она будет выглядеть работоспособной, в то время, когда она фактически была закрыта хакерами, потенциально «оставляя миллионы людей без электропитания».



«Taekion» планирует работать и над другими приложениями, которые помогут защитить данные о транзакциях электроэнергии, повысить надежность энергосистемы и интегрировать энергетическую инфраструктуру. Этот проект является частью программы управления энергетических датчиков и контроля ископаемых источников энергии департамента и финансируется в рамках программы исследований инноваций в малом бизнесе.

Источник: https://www.bitjournal.media/11-04-2019/ministerstvo-jener-getiki-ssha-rassmatrivaet-blokchejn-dlja-predotvrashhenija-kiberatak-na-jelekt-rostancijah/ (дата размещения материала 11.04.2019).

Разведка США поддержала стартап, который предсказывает кибератаки

По информации сайта knews.kg со ссылкой на издание «Forbes», еще в 2015 году агентство передовых исследований в сфере разведки IARPA начало

поиск технологий, которые бы не просто предсказывали кибератаки, но и заранее предоставляли подробности о них: например, какие слабые места окажутся под ударом и какое цифровое оружие будет использовано. В марте 2019 года проект «Среда для нестандартных автоматизированных детекторов кибератак» (CAUSE) был завершен.

Разработанный в рамках данного проекта инструмент «Omnisense», управляемый из «материнского» датацентра, постоянно наблюдает за Интернетом. Его «прослушивающие серверы» разбросаны по всей планете. Они отслеживают интернет-трафик и пытаются вычислить IP-адрес каждого сервера, выполняющего определенные действия, такие как поиск уязвимостей или попытки угадывать пароли компьютеров методом перебора на устройствах, подключенных к Интернету. Как только «Omnisense» находит заслуживающий интерес сервер, он проводит «глубокую проверку» в поиске всех программ, запущенных на хосте, и любых доменных имен, связанных с этим IP-адресом, прежде чем выставить оценку уровню угрозы.

На основе всех этих данных исследователи ежедневно готовят прогноз возможных угроз в Интернете. Службы безопасности могут пользоваться им, чтобы блокировать источники угрозы до того, как они становятся заметны в Интернете, или предпринимать другие подходящие профилактические меры.

Источник: https://www.knews.kg/2019/04/02/razvedka-ssha-podderzhala-startap-kotoryj-predskazyvaet-kiberataki/ (дата размещения материала 02.04.2019).

Япония создаст кибероружие в форме бэкдоров для самообороны

Как сообщает сайт anti-malware.ru, Япония планирует создать и поддерживать специальное кибероружие в форме вредоносных программ различных видов. Это оружие будут использовать для обороны страны в случае нападения агрессоров в киберпространстве. В эту связку войдут трояны, бэкдоры и прочие вредоносные программы. В случае реализации идеи Япония обзаведется своим первым в истории кибероружием. Ожидается, что Страна восходящего солнца осуществит задуманное к концу текущего года. К разработке вредоносных программ будут привлечены подрядчики, а также негосударственные служащие.

На сегодняшний день никакие технические детали, а также принцип работы самого кибероружия и отдельных программ, входящих в его состав, не разглашаются. Также в секрете держится информация о том, как Япония планирует использовать новинку. Как сообщают японские СМИ, новое оружие будет применяться в случае атак на государственные учреждения Японии, только против самих атакующих.

Источник: https://www.anti-malware.ru/news/2019-05-06-1447/29578 (дата размещения материала 06.05.2019).

«Linxdatacenter» запускает защищенное облако

По данным сайта comnews.ru, компания «Linxdatacenter» разработала новый продукт «Защищенное облако 152-ФЗ» – сервис по аренде виртуальной инфраструктуры для компаний, работающих с персональными данными граждан Российской Федерации. В новом сервисе реализованы меры защиты информации, отвечающие требованиям Федерального закона № 152-ФЗ «О персональных данных». Он входит в реестр операторов персональных данных, обладающих лицензией ФСТЭК России на деятельность по технической защите информации, а используемые программные средства защиты информации сертифицированы ФСТЭК России и ФСБ России.

Сервис предназначен для компаний, регулярно работающих с персональными данными. Защищенное облако помогает бизнесу соблюдать требования законодательства Российской Федерации, без необходимости самим компаниям становиться операторами персональных данных. Услуга может быть адаптирована под нужды клиента с помощью гибридных решений и интегрирована в существующую ИТ-инфраструктуру. Отличительными особенностями являются быстрота запуска системы и легкое масштабирование ресурсов в случае необходимости наращивания мощности.

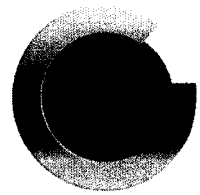
Сервис доступен в двух конфигурациях. Типовое решение предлагает серверные средства защиты информации, достаточные для обеспечения защиты персональных данных в информационных системах IV и III уровней защищенности. Для компаний, обрабатывающих большие объемы персональных данных и нуждающихся в комплексных мерах по защите информации, предусмотрены индивидуальные решения. В рамках такого сервиса клиент получает систему для хранения персональных данных до II уровня защищенности и полный комплект документов, подтверждающих соответствие решения требованиям законодательства Российской Федерации.

Источник: https://www.comnews.ru/digital-economy/content/118952/news/2019-04-08/linxdatacenter-zapuskaet-zashchishchennoe-oblako (дата размещения материала 08.04.2019).

«G-Protec» – сервис защиты от DDoS-атак на основе технологии интеллектуальной фильтрации трафика

Как сообщает сайт itweek.ru, компания «G-Core Labs» представила инновационную защиту от DDoS-атак для веб-приложений – сервис «G-Protect». Наряду с услугами CDN, хостинга и видеостриминга, защита от DDoS-атак станет еще одним необходимым сервисом для компаний любых отраслей, развивающих свой бизнес в онлайне.

Уникальная технология, комбинирующая анализ статистических, сигнатурных, технических и поведенческих факторов, позволяет нейтрализовать низкочастотные атаки («low and slow») на уровне приложения и отсекать даже единичные запросы ботов. Благодаря этому, помимо купирования DDoS-атак, сервис позволяет защитить сайт или API клиента от парсинга, автоматического подбора паролей и любой другой вредоносной активности ботов.



G·CORE LABS

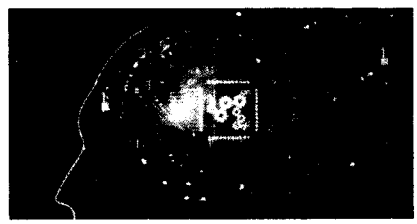
Новый сервис «G-Protect» позволяет защитить вебсайт, API или мобильное приложение от DDoS-атак любой сложности и объема, а благодаря быстрой интеграции может начать отражать атаку в течение нескольких минут.

Среди преимуществ «G-Protect» можно отметить: экономию на инфраструктуре; быструю интеграцию с сайтом благодаря возможности настройки сервиса через личный кабинет; статистику в режиме реального времени; уникальную защиту от ботов на уровне приложения.

Источник: https://www.itweek.ru/security/news-company/detail.php?ID=207010 (дата размещения материала 25.04.2019).

Чат-бот на базе искусственного интеллекта помогает жертвам мошенничества

По данным сайта securitylab.ru, официальный портал правительства США USA.gov запустил созданного на базе искусственного интеллекта чат-бота по имени Сэм, помогающего пользователям находить информацию о мошенничестве. Бот был запущен в феврале 2019 года, и за месяц его услугами воспользовалось порядка 4 тыс. человек. 78% из них успешно задали Сэму вопросы и получили ответы.



Бот был создан с целью автоматизации процесса предоставления пользователям доступа ко всей информации и базам данных, хранящимся на правительственном портале. Сэм специализируется на теме мошенничества, ведь именно вопросы о мошенничестве являются одними из наиболее часто задаваемых на сайте.

Перед запуском бота специалисты USA.gov опросили более 30 пользователей, столкнувшихся с мошенниками. Они не только рассказали о самих инцидентах, но также поделились эмоциями и пояснили, почему решили сообщить о них властям. Анализ ответов помог разработчикам выявить основные проблемы, с которыми сталкиваются граждане при поиске нужной информации на правительственном портале. На основании этой информации создатели бота разработали навигационную схему, с помощью которой Сэм направляет пользователей на искомый ответ. При общении с пользователями бот выражает сочувствие, а его ответы исполнены дружелюбия.

Источник: https://www.securitylab.ru/news/498660.php (дата размещения материала 07.04.2019).

Представлен бесплатный инструмент для проверки безопасности web-сайтов

Как информирует сайт itsec.ru, швейцарская компания «ImmuniWeb» выпустила бесплатное решение «Website Security Test», предназначенное для проверки безопасности сайтов и соответствия стандартам PCI DSS. Инструмент позволяет проводить анализ систем управления контентом (CMS), web-серверов, политик безопасности, а также выявлять проблемы, связанные с конфиденциальностью.

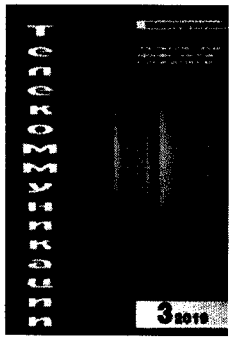
В частности, «Website Security Test» проверяет наличие защитного экрана уровня приложений (WAF), актуальность версий CMS и их компонентов, актуальность компонентов JavaScript, корректность настроек cookie-файлов, активность каталогов web-сервера, а также наличие ПО для майнинга криптовалют. Также инструмент проводит проверку на предмет наличия уязвимостей в ПО.

Кроме того, инструмент анализирует HTTP-заголовки, связанные с безопасностью, шифрованием и конфиденциальностью, и политики защиты контента, призванные обеспечить защиту от XSS-, CSRF-атак, атак с использованием вымогательского ПО и программ для добычи криптовалюты.

Источник: http://www.itsec.ru/news/predstavlen-besplatniy-instrument-dlia-proverki-bezopasnosti-web-saitov (дата размещения материала 30.04.2019).

Функциональные аспекты моделирования процесса перехвата информативных сигналов побочных электромагнитных излучений и наводок на объектах информатизации

Статья, размещенная в журнале «Телекоммуникации», открывает серию публикаций, посвященных представлению процесса перехвата информативных сигналов электромагнитных полей, излучаемых основными техническими средствами и системами и вспомогательными техническими средствами и системами объектов информатизации, а также съема сигналов, наводимых на токопроводящие линии, выходящие за пределы контролируемой зоны.



Приводятся основные положения теории функционального моделирования применительно к решению важной и актуальной для методологии обеспечения информационной безопасности проблемы разработки функциональных моделей угроз утечки информации по каналам побочных электромагнитных излучений и наводок.

Представлен общий механизм декомпозиции целевой функции «Перехват сигналов информативных сигналов побочных электромагнитных

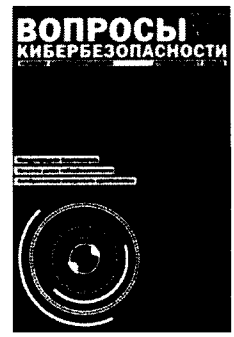
излучений и наводок на объектах информатизации». Приводятся результаты ее детализации на отдельные этапы.

Источник: Телекоммуникации, 2019, № 3, с. 35-41.

К вопросу об оценке эффективности защиты информации в системах электронного документооборота

В статье, размещенной в журнале «Вопросы кибербезопасности», предложен новый показатель оценки эффективности защиты электронных документов, направленный на сравнение вероятностно-временных характеристик процессов реализации угроз в системах электронного документооборота в условиях применения мер защиты и процессов обработки электронных документов. Это позволяет учесть время обработки документов в оценке эффективности их защиты.

На основе аппарата сетей Петри-Маркова разработана математическая модель и получены аналитические соотношения для расчета предложенного показателя на примере жизненного цикла входящих электронных документов с учетом времени выполнения типовых процедур и функций их обработки, времени реализации угроз, таких как несанкционированная замена физических адресов сетевых адаптеров компьютеров в составе системы электронного документооборота, а также применения мер защиты – использования специальных программ обнаружения фактов подмены физических адресов. Разработанная модель позволяет не только оценивать эффективность предпринимаемых мер защиты электронных документов от конкретных угроз, но и обосновывать на количественной основе требования к времени обработки электронных документов в зависимости от вероятностно-временных характеристик реализации угроз, выявлять слабые места в системах электронного документооборота, которые могут быть использованы для реализации угроз, и условия, при которых такие угрозы реализуются.



Источник: Вопросы кибербезопасности, 2019, № 1, с. 25-33.

3. Сведения о новых документах, регламентирующих вопросы в области защиты информации

3.1. Документы ФСТЭК России

Информационное сообщение ФСТЭК России от 29 марта 2019 г. № 240/24/1428 «О порядке предоставления Перечня средств измерений, испытательного оборудования, программно-аппаратных средств и Перечня нормативных правовых актов, методических документов и национальных стандартов, необходимых для выполнения работ по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну»

ФСТЭК России утвержден Перечень средств измерений, испытательного оборудования, программных (программно-аппаратных) средств и Перечень нормативных правовых актов, методических документов и национальных стандартов, необходимых для выполнения работ по аттестации объектов информатизации, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну (далее – Перечни). Перечни предназначены для органов по аттестации, а также для организаций, претендующих на получение аккредитации в качестве органов по аттестации.

Рассылку Перечней в аккредитованные органы по аттестации осуществляют управления ФСТЭК России по федеральным округам.

Предоставление Перечней организациям, претендующим на аккредитацию в качестве органов по аттестации, осуществляется управлениями ФСТЭК России по федеральным округам на основании заявки на получение Перечней, в которой указываются наименование организации, юридический и фактический адреса, адреса секретной и несекретной переписки. К заявке прилагается копия действующей лицензии ФСБ России на проведение работ с использованием сведений, составляющих государственную тайну.

Заявка на получение Перечней направляется в соответствующее управление ФСТЭК России по федеральному округу.

Источник: система Консультант-Плюс.

Информационное сообщение ФСТЭК России от 29 марта 2019 г. № 240/24/1525 «О требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

Утверждены Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (далее – Требования).

Требования предназначены для разработчиков и производителей программных и программно-технических (программно-аппаратных) средств защиты информации, средств обеспечения безопасности информационных технологий, включая защищенные средства обработки информации, заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации СЗИ на соответствие требованиям по безопасности информации.

Выполнение Требований является обязательным при проведении работ по сертификации средств защиты информации, организуемых ФСТЭК России в пределах своих полномочий.

Требования к уровню доверия подлежат применению при сертификации СЗИ с 1 июня 2019 г.

Разработчикам и производителям сертифицированных СЗИ рекомендуется с привлечением испытательных лабораторий провести оценку их соответствия Требованиям и представить результаты в ФСТЭК России для переоформления соответствующих сертификатов соответствия. Действие сертификатов соответствия СЗИ, в отношении которых указанная оценка соответствия не будет проведена до 1 января 2020 г., может быть приостановлено.

Обеспечение федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций Требованиями и Методикой выявления уязвимостей и недекларированных возможностей в программном обеспечении (далее – Методика) производится в соответствии с Порядком обеспечения органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации, органов местного самоуправления и организаций документами ФСТЭК России. Организации, имеющие лицензии ФСТЭК России на разработку и (или) производство СЗИ, а также аккредитованные ФСТЭК России в качестве органов по сертификации или испытательных лабораторий, могут получить Требования и Методику, изданные типографским способом в ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Источник: система Консультант-Плюс.

Информационное сообщение ФСТЭК России
от 8 мая 2019 г.

С 7 мая 2019 г. запрещено применение генератор-излучателя акустических и виброакустических помех «Шторм» (сертификат соответствия от 9 марта 2010 г. № 2052) для защиты информации, обрабатываемой на объектах информатизации, в связи с прекращением заявителем ЗАО «Орбита» технической поддержки. Необходимо заменить указанное средство защиты информации на аналогичное сертифицированное средство защиты информации.

Источник: система Консультант-Плюс.

3.2. Национальные стандарты

ГОСТ Р XXXX-20XX «Защита информации. Идентификация и аутентификация. *Общие положения» (проект, окончательная редакция)*

Стандарт устанавливает единообразную организацию процессов идентификации и аутентификации в средствах защиты информации, в том числе реализующих криптографическую защиту, средствах вычислительной техники и автоматизированных (информационных) системах, а также определяет общие правила применения методов идентификации и аутентификации, обеспечивающих необходимую уверенность в результатах.

Положения стандарта не исключают применение криптографических методов (алгоритмов) при идентификации и аутентификации, но не устанавливают требования по их реализации.

Стандарт определяет состав участников и основное содержание процессов идентификации и аутентификации, рекомендуемое к реализации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом. Положения стандарта могут использоваться при управлении доступом к информационным ресурсам, вычислительным ресурсам средств вычислительной техники, ресурсам автоматизированных (информационных) систем, средствам вычислительной техники и автоматизированным (информационным) системам в целом.

Источник: http://www.fstec.ru.

3.3. Патентные документы

Пат. 2 686 552 Российская Федерация, МПК G06F 21/53 (2013.01). Системы и способы предоставления результата текущей команды процессора при выходе из виртуальной машины / ЛУКАКС Сандор, ЛУТАС Андрей-Влад; патентообладатель: БИТДЕФЕНДЕР АйПиАр МЕНЕДЖМЕНТ ЛТД – 2017104752, заявл. 11.08.2015, опубл. 29.04.2019.

Изобретение относится к области компьютерной безопасности. Техническим результатом является обеспечение компьютерной безопасности виртуальной машины.

Пат. 2 683 152 Российская Федерация, МПК G06F 21/55 (2013.01). Системы и способы отслеживания вредоносного поведения по множеству объектов программных средств / ХАЖМАСАН Георге-Флорин, ПОРТАСЕ Раду-Марьян; патентообладатель: БИТДЕФЕНДЕР АйПиАр МЕНЕДЖМЕНТ ЛТД – 2018105765, заявл. 04.07.2016, опубл. 26.03.2019.

Изобретение относится к области вычислительной техники. Техническим результатом является определение атаки вредоносных программ на основе организации совокупности отслеживаемых исполняемых объектов во множество групп объектов.

Пат. 2 684 483 Российская Федерация, МПК G06F 21/34 (2013.01). Устройство для защиты от несанкционированного доступа к данным, хранимым на компьютере / Пушкин О.В.; патентообладатель: Пушкин О.В. – 2018118978, заявл. 23.05.2018, опубл. 09.04.2019.

Изобретение относится к области защиты информации от несанкционированного доступа. Технический результат заключается в повышении надежности защиты компьютера и информации от несанкционированного доступа.

Пат. 2 684 575 Российская Федерация, МПК G06F 21/00 (2013.01). Способ управления потоками данных распределенной информационной системы при DDOS атаках / Бухарин В.В., Карайчев С.Ю., Казачкин А.В., Шалагинов В.А., Богданов С.П.; патентообладатель: Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» – 2018117653, заявл. 14.05.2018, опубл. 09.04.2019.

Изобретение относится к способу управления потоками данных распределенной информационной системы при DDoS-атаках. Техническим результатом является повышение защищенности распределенных информационных систем за счет блокирования нелегитимных потоков данных, исходящих потоков данных, осуществляющих реализацию DDoS-атак путем формирования и дальнейшего анализа проверочных данных.

Пат. 2 685 989 Российская Федерация, МПК H04L 29/06 (2006.01). Способ снижения ущерба, наносимого сетевыми атаками серверу виртуальной частной сети / Гречишников Е.В., Закалкин П.В., Добрышин М.М., Стародубцев Ю.И., Петухова Ю.А.; патентообладатель: Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» – 2018103850, заявл. 31.01.2018, опубл. 23.04.2019.

Изобретение относится к области телекоммуникаций. Техническим результатом является обеспечение услугами связи узлов VPN, использующих ресурсы сервера VPN, за счет своевременного и организованного перевода узлов VPN с основного на дополнительный сервер VPN.

Пат. 2 685 994 Российская Федерация, МПК H04L 29/06 (2006.01). Способ оценки сетевой атаки, способ безопасной передачи данных сети и соответствующее устройство / ЛИНЬ, Юйфэй; патентообладатель: ГУАНЧЖОУ УКВЕБ КОМПЬЮТЕР ТЕКНОЛОДЖИ КО., ЛТД. – 2017114862, заявл. 08.04.2016, опубл. 23.04.2019.

Изобретение относится к способам, устройствам, системе и носителю информации для определения сетевой атаки. Технический результат заключается в обеспечении определения сетевой атаки.

Пат. 2 686 023 Российская Федерация, МПК. G06F 21/55 (2013.01), H04L 29/06 (2006.01). Способ защиты вычислительных сетей / Гаврилов А.Л., Катунцев С.Л., Максимов Р.В., Орехов Д.Н., Пряхин В.П., Тимашенко Д.В., Соколовский С.П., Тимашенко В.К.; патентообладатель: Федеральное государ-

ственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное училище имени генерала армии С.М. Штеменко» – 2018120288, заявл. 31.05.2018, опубл. 23.04.2019.

Изобретение относится к области защиты вычислительных сетей. Техническим результатом является повышение результативности защиты и введение в заблуждение нарушителя относительно структуры вычислительной сети.

Пат. 2 684 584 Российская Федерация, МПК G06F 21/42 (2013.01), G06F 21/31 (2013.01), G06F 21/62 (2013.01). Устройство для хранения информации и способ его работы / ЧОУ Хун-Чиэнь; патентообладатель: ЧОУ Хун-Чиэнь – 2018114504, заявл. 19.04.2018, опубл. 09.04.2019.

Изобретение относится к области хранения информации. Техническим результатом является предотвращение несанкционированного доступа к устройству для хранения информации.

4. Статистические данные по анализу защищенности информационных систем

«Ростелеком» сообщает о росте числа и мощности DDoS-атак на российские компании в 2018 году

Как сообщается на сайте rt-solar.ru, компания «Ростелеком» провела исследование DDoS-атак, осуществлявшихся на российский сегмент Интернета в 2018 году. Как свидетельствует отчет, в 2018 году произошел резкий рост не только количества DDoS-атак, но и их мощности.

По сравнению с 2017 годом количество атак выросло почти в два раза – на 95%. Аналитики полагают, что во многом это связано с их дешевизной и эффективностью. При этом мощность DDoS-атак также резко возросла. Самая серьезная атака, зафиксированная «Ростелекомом» в 2018 году, осуществлялась на телеком-оператора «Dtel.ru». Ее интенсивность достигала 450 гигабит в секунду, тогда как рекорд 2017 года – всего 54 гигабит в секунду. Самая продолжительная DDoS-атака длилась 280 часов. Для сравнения, в среднем такие атаки длятся 1,5-2 часа.

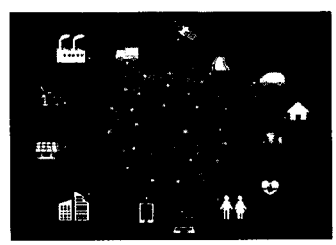
Чаще всего злоумышленники атакуют компании, относящиеся к сферам игровой индустрии и электронной коммерции. Доля атак на игровые серверы составила 64%. Предприятия электронной коммерции стабильно удерживают второе место (16%). Доля DDoS-атак на телекоммуникационные компании выросла с 5% до 10%, а доля образовательных учреждений, напротив, резко сократилась – с 10% до 1%. Рост среднего числа атак на одного клиента составил 45% для игрового сегмента и 19% – для игровой коммерции.

Наиболее популярным методом DDoS-атак является UDP-флуд – почти 38% всех атак осуществляются именно этим способом. Также отмечается резкий рост доли атак с амплификацией и атак типа SYN-флуд.

Источник: https://www.rt-solar.ru/events/news/1588/ (дата размещения материала 27.03.2019).

Более 45% компьютеров АСУ ТП в России хотя бы раз подвергались заражению вредоносным ПО

По данным сайта securitylab.ru со ссылкой на отчет «Лаборатории Касперского», во втором полугодии 2018 года практически каждый второй (45,3%) компьютер АСУ ТП в России подвергался атакам вредоносного ПО.



В указанный период было обнаружено более 19,1 тыс. модификаций вредоносных программ из 2,7 тыс. различных семейств. При этом большинство случаев попыток заражения компьютеров АСУ ТП носят случайный характер, а основными источниками угроз по-прежнему являются Интернет (26,1%), съемные носители (8%) и электронная почта (4,9%).

Во второй половине 2018 года трояны также оставались актуальными угрозами для АСУ ТП. Программы такого класса были выявлены на 27,1% компьютеров АСУ ТП, эксплоиты – на 3,2% устройств, бэкдоры – на 3,2%, а атакам вымогательского ПО подверглись 2% компьютеров.

Источником более 30% атак на компьютеры АСУ ТП в России стал Интернет. По данному показателю Россия вошла в список стран, технологические компьютеры в которых чаще всего подвергались web-атакам. Эксперты также отмечают рост атак с использованием вредоносной электронной почты. Доля таких атак в мире составила почти 5%, в России – 2,6% (однако за 6 месяцев показатель вырос в 1,5 раза).

Как минимум 4,3% компьютеров АСУ ТП в мире были заражены троянами, бэкдорами и кейлоггерами, распространяемыми через фишинговые письма. В большинстве случаев целью злоумышленников было хищение конфиденциальной информации, в том числе для доступа к бухгалтерским системам, позволяющей вывести деньги со счетов атакуемых предприятий.

Источник: https://www.securitylab.ru/news/498525.php (дата размещения материала 27.03.2019).

Количество уязвимостей в АСУ ТП выросло на 30%

По информации, размещенной на сайте news.rambler.ru, в России в 4,5 раза увеличилось число компонентов АСУ ТП, доступных из Интернета, что легко позволяет злоумышленникам обнаруживать составляющие промышленных систем. Согласно исследованию «Positive Technologies», число новых уязвимостей АСУ ТП по сравнению с предыдущим годом увеличилось на 30%, причем доля недостатков критического и высокого уровня риска выросла на 17%. Россия показала один из наиболее высоких темпов роста числа компонентов АСУ ТП, доступных из Интернета, переместившись с 28 на 12 место. Если

в 2017 году в Интернете были обнаружены IP-адреса 892 компонентов АСУ ТП, то в 2018 году исследователи зафиксировали уже 3993 устройства.

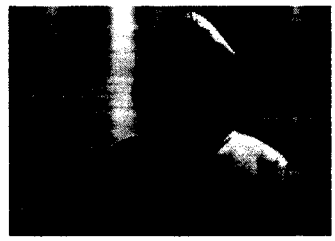
Общее количество компонентов АСУ ТП, доступных в Интернете, с прошлого года выросло на 27% и теперь составляет более 220 тысяч. Наибольшее число таких систем находится в США (95661), Германии (21449), Китае (12262), Франции (11 007), Италии (9918) и Канаде (9580). Вновь наиболее распространенными стали устройства компании «Honeywell», которых было обнаружено около 30 тысяч.

Эксперты «Positive Technologies» не раз сообщали об опасности доступности в Интернете сетевых устройств, например таких, как коммутаторы или конвертеры интерфейсов для технологического процесса. За два года доля доступных из Интернета сетевых устройств выросла с 5% до 19%.

Источник: https://www.news.rambler.ru/other/42022837-kolichestvo-uyazvimostey-v-asu-tp-vo-vsem-mire-vyroslo-na-30/ (дата размещения материала 11.04.2019).

В 2018 году в России зафиксирован почти двухкратный рост кибератак

По данным сайта itsec.ru, в прошлом году в России было осуществлено около 765 тыс. виртуальных атак, что почти вдвое превышает показатели предыдущего периода.



Учитывались как хакерские атаки (заражение вредоносным софтом, эксплуатация уязвимостей, фишинг, DDoS-атаки) на отечественные компании, так и мошенничества со стороны собственных сотрудников или подрядчиков (утечки конфиденциальных данных, незаконный доступ к внутренним ресурсам, использование вредоносных приложений).

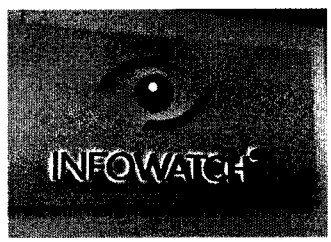
Около 75% кибератак приходится на кредитно-финансовые организации, электронную коммерцию и игровые ресурсы. Кроме того, участились нападения на объекты критической информационной инфраструктуры.

Источник: http://www.itsec.ru/news/rostelekom-v-2018-godu-v-rossii-zafiksirovan-pochti-2-kratniy-rost-kiberatak (дата размещения материала 18.04.2019).

Утечек через незащищенные серверы стало больше на 43%

Как сообщает сайт itweek.ru со ссылкой на результаты исследования аналитического центра компании «InfoWatch», в 2018 году было зафиксировано в СМИ и других открытых источниках 70 утечек конфиденциальных данных через облачные серверы и другие незащищенные хранилища информации с доступом через Интернет. Это в полтора раза больше, чем годом ранее. Более 40% инцидентов в минувшем году произошло из облачных хранилищ, принадлежащих компаниям сферы высоких технологий.

Самые масштабные по числу скомпрометированных записей персональных данных инциденты зафиксированы в 2017 году. Тогда из незащищенных серверов утекло более 1,7 млрд. записей или около 13% всего объема данных, украденных и потерянных за год.



В распределении инцидентов по типу данных преобладают персональные данные – 80% случаев. В равной доле, по 9,2% случаев – это утечки платежной информации, а также коммерческих секретов и производственных ноу-хау.

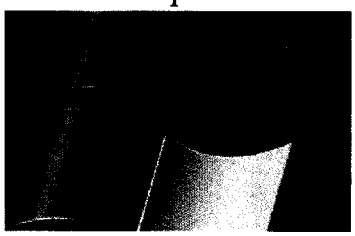
Более четверти всех известных случаев утечек данных из облаков в 2018 году пришлось на объектные хранилища «Amazon S3». В прошлом году резко возросло число утечек с серверов «Mongo DB». Кроме того, отмечено большое число случаев компрометации данных, хранящихся на платформах

«Elasticsearch» и «Apache», а также при использовании файлового хостинга «Google Drive». Доля утечек в процессе резервного копирования сократилась примерно втрое, а при работе с репозиториями «GitHub» – в семь раз.

Источник: https://www.itweek.ru/security/news-company/detail.php?ID=207008 (дата размещения материала 25.04.2019).

81% критических уязвимостей в продуктах «Microsoft» решаются отключением прав администратора

По информации сайта zen.yandex.ru, за период с 2013 по 2018 годы количество уязвимостей в решениях компании «Microsoft» выросло на 110%. В общей сложности в 2018 году в продуктах техногиганта было выявлено более 700 проблем. За прошедшие шесть лет число уязвимостей, классифицированных как «критические», также возросло – на 29%. Основная доля проблем, обнаруженных в 2018 году, приходится на баги удаленного выполнения кода (292 уязвимости), еще 197 уязвимостей охарактеризованы как критические (61%).



В минувшем году в платформах Windows Vista, Windows 7, Windows RT, Windows 8/8.1 и Windows 10 в общей сложности было обнаружено 499 уязвимостей, из них 169 критические (34%). Аналогичное число проблем было выявлено и в Windows Server (30% составляют критические уязвимости).

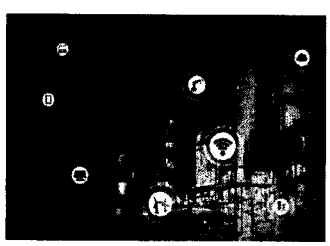
Несмотря на сравнительную новизну браузера Microsoft Edge, число обнаруженных в нем уязвимостей (112) в три раза превышает показатель Internet Explorer (39). За два года количество обнаруженных в Microsoft Edge багов увеличилось в шесть раз. Кроме того, за шесть лет возросло и число уязвимостей в пакете Microsoft Office (на 121%).

По итогам анализа эксперты пришли к выводу, что 81% критических уязвимостей из официальных бюллетеней безопасности Microsoft за 2019 год можно устранить, просто отключив права администратора.

Источник: https://www.zen.yandex.ru/media/securitylab.ru/81-kritiche-skih-uiazvimostei-v-produktah-microsoft-reshaiutsia-otkliucheniem-prav-admi-nistratora-5cc71dadc9bd6400b307ff6e (дата размещения материала 30.04.2019).

Самые распространенные угрозы для промышленных предприятий

По данным сайта ib-bank.ru, с целью повышения эффективности производства промышленные предприятия все чаще полагаются на сочетание цифровых и физических систем, однако повсеместное применение различных технологий и концепций значительно увеличивают поверхность атак.



Промышленные предприятия чаще по сравнению с другими сферами используют устаревшее оборудование и ОС. В частности, почти 5% из 150 тыс. промышленных компьютеров работают на базе Windows XP (в других секторах показатель составляет 3%), 60,2% –

под управлением Windows 7 и 28,9% – Windows 10. Как полагают эксперты, такая ситуация, скорее всего, связана с длительными сроками службы специализированного оборудования и тем, что многие компании придерживаются принципа «не трогать рабочую систему».

Что касается вредоносного ПО, чаще всего промышленные организации сталкиваются с червями, хакерскими программами, майнерами криптовалюты и вымогательским ПО. Одними из наиболее распространенных угроз являются вредоносные программы WannaCry, Downad, AutoKMS, Coinminer и MalXMR. Вредоносы, распространяемые через USB-накопители, часто эксплуатируют файлы autorun.inf, используемые для автоматического запуска приложений в Windows. По числу таких файлов промышленный сектор (25%) значительно опережает другие сферы, в том числе правительственную (13%), сферы образования (12%), здравоохранения (11%) и технологический сектор (5%).

Источник: https://www.ib-bank.ru/news/10962 (дата размещения материала 04.04.2019).

Кто чаще всего становится жертвой кибератак?[6]

Согласно информации сайта darkreading.com со ссылкой на результаты исследования компании «Proofpoint», в настоящее время злоумышленники меняют свои тактики и выбор жертв. Теперь даже сотрудники компаний, занимающие низшие должности, не защищены от фишинговых атак. Теперь инженерно-технический персонал чаще становится целью атакующих, чем сотрудники других подразделений, а инженеры и разработчики чаще подвергаются атакам, чем руководство.

Самая быстрорастущая категория атакуемых адресов – это функциональные аккаунты типа «sales@xyz.com» или «inquiries@xyz.com». Именно на такой тип адресов приходится до 30% всех атак на электронную почту, зарегистрированных в четвертом квартале 2018 года.

При этом злоумышленники не ограничивают себя только атаками на электронную почту. За I квартал текущего года количество атак с использованием методов социальной инженерии выросло на 150%, а за прошедший год фишинговые атаки с использованием поддельных аккаунтов поддержки социальных сетей взлетели до 442%.

Источник: https://www.darkreading.com/vulnerabilities---threats/who-gets-targeted-most-in-cyberattack-campaigns/d/d-id/1334494 (дата размещения материала 22.04.2019).

---

[6] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

5. Сведения об инцидентах информационной безопасности

Сетевые торговые площадки выкладывают в открытый доступ данные россиян

По данным ряда сайтов, не менее 2,24 млн. записей с паспортными данными, номерами СНИЛС и сведениями о трудоустройстве россиян находится в открытом доступе.

В рамках исследования была проанализиована информация электронных торговых площадок в России. В частности, проверены 562 тыс. записей закупочного модуля ZakazRF, 550 тыс. записей «РТС-тендер», а также записи Росэлторга «Национальной электронной площадки», ЭТП РАД и «Сбербанк АСТ» (468 тыс., 142 тыс.,18 тыс., 500 тыс. соответственно). Установлено, что найти личную информацию участников аукционов можно на каждой из этих площадок. Механизм скачивания документов с персональными данными на них совпадает: информация содержится в хранящихся на площадках решениях об одобрении открытых аукционов.

Ранее компания «DeviceLock» изучила более 1,9 тыс. серверов в российском сегменте Интернета, использующих облачные базы данных «MongoDB», «Elasticsearch» и «Yandex ClickHouse». Более половины из них (52%) предоставляли возможность неавторизованного доступа.

Источники: https://www.kommersant.ru/doc/3960232 (дата размещения материала 29.04.2019); https://www.news.rambler.ru/community/42111375-postradali-milliony-pochemu-dannye-rossiyan-okazalis-v-otkrytom-dostupe/.

Украинские хакеры украли базу данных российской скорой помощи и выложили в Интернет

Как сообщается на сайте cnews.ru, в свободном доступе оказалась база данных подмосковных пациентов скорой помощи. Объем утечки еще предстоит оценить, но файл с базой данных имеет объем почти 18 гигабайт и содержит при этом лишь текстовую информацию. Ответственные за кражу пока не найдены, но под подозрение экспертов попала украинская группа хакеров «THack3forU».

Специалисты компании «Group-IB» сообщили, что утекшая база данных была построена на СУБД «MongoDB». Злоумышленники нашли эту базу, воспользовавшись специализированными поисковыми системами для обнаружения доступных баз данных, к которым можно подключиться без логина и пароля. База данных, содержащая в себе столь обширное количество личной информации, может привлечь внимание других злоумышленников.

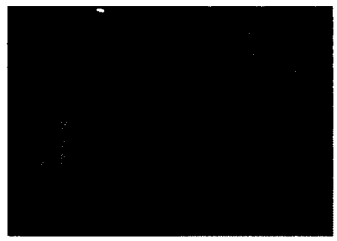
Утекший файл содержал в себе значительное количество личных данных. В их число входит имя вызвавшего скорую помощь, телефон, описание состоя-

ния пациента по прибытию врачей, дата и время вызова, а также адрес, на который был произведен выезд скорой помощи. База содержит данные подстанций скорой помощи в городах Дмитрове, Балашихе, Мытищах и Королеве.

Источник: http://www.cnews.ru/news/top/2019-04-09_ukrainskie_hakery_ukrali_bazu_dannyh_rossijskoj (дата размещения материала 09.04.2019).

Неизвестные подменяют IP-адреса крупных американских банков

По информации сайта news.rambler.ru, в последнее время эксперты фиксируют странный всплеск трафика, имитирующего IP-адреса крупных американских банков, в том числе «Bank of America», «JPMorgan Chase» и «SunTrust». Как считают исследователи из компании «GreyNoise Intelligence», занимающейся отслеживанием интернет-трафика, таким образом организаторы кампании пытаются нарушить работу защитных решений, блокирующих вредоносный трафик.



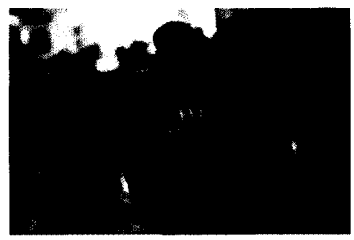
По словам экспертов, злоумышленники создают видимость масштабного сканирования Интернета, заставляя людей думать, будто данные IP-адреса являются вредоносными. Как отмечают исследователи, объем трафика слишком маленький для DDoS-атаки. По всей видимости, злоумышленники пытаются заставить межсетевые экраны и другие защитные продукты блокировать трафик, исходящий с банковских IP-адресов, расценивая его как вредоносный.

В настоящее время неизвестно, кто стоит за данной кампанией. В целом инцидент может оказаться полезным для производителей решений в области безопасности, поскольку может помочь им выявить ложные срабатывания.

Источник: https://www.news.rambler.ru/other/42096680-neizvestnye-podmenyayut-ip-adresa-krupnyh-amerikanskih-bankov/ (дата размещения материала 25.04.2019).

Хакеры опубликовали личные данные примерно 4000 полицейских и федеральных агентов США

По сообщению сайта ixbt.com, хакеры взломали несколько web-сайтов, связанных с ФБР, и опубликовали похищенные данные, включая информацию примерно о 4000 федеральных агентов и сотрудников правоохранительных органов. Данные, похищенные с серверов, включают имена, персональные и служебные адреса электронной почты, названия должностей, телефонные номера и их почтовые адреса.



Всего было взломано более 1000 сайтов, в том числе содержащих огромное количество данных о госслужащих. После структурирования данных они могут быть проданы.

Источник: https://www.ixbt.com/news/2019/04/14/hakery-opublikovali-lichnye-dannye-primerno-4000-policejskih-i-federalnyh-agentov-ssha.html (дата размещения материала 14.04.2019).

Данные американских домохозяйств
оказались в открытом доступе

По информации сайта computerworld.ru, специалисты компании «vpnMentor» обнаружили на сервере в облачной системе «Microsoft» незащищенную базу данных, в которой содержалась информация примерно о 80 млн. американских домохозяйств. В нее включены полные почтовые адреса домов, географическая широта и долгота, полные имена проживающих, их возраст и дата рождения. Кроме того, условными кодами обозначены пол, семейное положение, доход и некоторые другие данные домовладельцев и членов семей.

Хотя в базе данных нет финансовых данных – номеров кредитных карт или социального страхования, опасность, по мнению специалистов, все-таки существует. Мошенники могут использовать эти данные для проведения различных целевых кибератак, вымогательства и фишинга. Даты рождения и почтовые индексы часто используются людьми в качестве паролей и ответов на вопросы безопасности, а знание адреса позволит преступникам следить за домом.

По всей видимости, база данных принадлежит какой-то страховой, медицинской или ипотечной компании.

Источник: https://www.computerworld.ru/news/Dannye-na-80-millionov-amerikanskih-domohozyaystv-okazalis-v-otkrytom-dostupe(дата размещения материала 30.04.2019).

МИД Бельгии сообщил о попытке
взлома своей сети хакерами

Как сообщается на сайте ria.ru, хакеры предприняли попытку взлома компьютерной сети МИД Бельгии. По информации чиновника внешнеполитического ведомства, была установлена попытка вторжения во внешнеполитическую сеть и для ее предотвращения принято решение изолировать сеть и приступить к перезапуску системы. Компьютерная сеть бельгийского МИД была отключена во всех странах, хакерам не удалось проникнуть к отдельным серверам. Для восстановления работы сети, которую в том числе используют бельгийские консульства, потребуется около 72 часов.

В МИД Бельгии отказались сообщить, откуда может происходить хакерская атака.

Источник: https://www.ria.ru/20190416/1552746157.html (дата размещения материала16.04.2019).

Киберпреступники атаковали крупную фармацевтическую компанию «BAYER»

По информации ряда сайтов со ссылкой на информационное агентство «Reuters», крупнейшая фармацевтическая компания Германии «Bayer» сообщила об обнаружении кибератаки на свои компьютерные системы. В начале прошлого года специалисты выявили в сетях компании вредоносное ПО из арсенала киберпреступной группировки «Winnti» и до недавнего времени тайно наблюдали за его активностью, после чего вредонос был удален.

Никаких свидетельств компрометации данных исследователи не обнаружили, однако оценка общего ущерба пока что не окончена.

С начала текущего года используемое «Winnti» вредоносное ПО было обнаружено еще в трех немецких компаниях. В 2016 году группировка также атаковала сети немецкого промышленного концерна «ThyssenKrupp».

Группировка «Winnti», также известная как «Axiom», связывается ИБ-специалистами с Китаем. Со временем инфраструктуру и инструменты «Winnti» стали использовать и другие группировки, работающие на китайское правительство.

Источник: https://www.securitylab.ru/news/498632.php (дата размещения материала 04.04.2019); https://www.securitylab.ru/news/4930 82.php.

«Toyota» сообщила о возможной утечке данных клиентов

Как сообщает сайт rbc.ru, персональные данные нескольких миллионов клиентов автопроизводителя «Toyota» могли быть похищены в результате взлома серверов и несанкционированного доступа к базам данных дилерских центров автоконцерна на территории Японии.

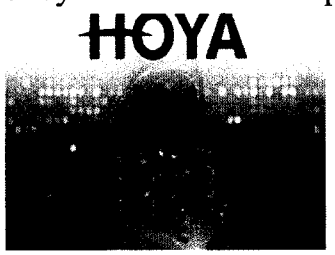
В руках злоумышленников могли оказаться данные более чем 3 млн. владельцев автомобилей «Toyota» и «Lexus». Автопроизводитель не раскрыл, какие именно данные могли быть украдены, но отметил, что финансовая информация клиентов не пострадала. В настоящее время ведется расследование инцидента.

Источник: https://www.rbc.ru/rbcfreenews/5c9fbebe9a79473cabfb43b0 (дата размещения материала 01.04.2019).

Кибератака на три дня остановила работу завода «HOYA» в Таиланде

Согласно информации сайта securitylab.ru со ссылкой на издание «Kyodo News», японский производитель оптического оборудования «HOYA» был вынужден на три дня приостановить работу своего завода в Таиланде из-за кибератаки.

Злоумышленники заразили порядка сотни компьютеров вредоносным ПО, предназначенным для хищения учетных данных и внедрения майнера криптовалюты. Атака была обнаружена после того, как специалисты компании заметили существенную нагрузку на сетевой сервер. Работу криптомайнера удалось заблокировать, однако кибератака привела к снижению производительности завода примерно на 40%.



Инцидент затронул не только серверы в Таиланде, но и подключенные к сети компьютеры в штаб-квартире «HOYA» в Японии, в результате чего сотрудники компании не смогли выписывать счета-фактуры. Как отмечается, признаков утечки данных не обнаружено.

Источник: https://www.securitylab.ru/news/498685.php (дата размещения материала 09.04.2019).

Иранские кибершпионы атакуют компании в США и Саудовской Аравии

По информации сайта news.rambler.ru, в течение последних трех лет кибершпионская группировка «Elfin», предположительно финансируемая правительством Ирана, активно атакует организации в США и Саудовской Аравии. Помимо правительственного сектора, «Elfin» также интересуют производственные, инженерные и химические предприятия, исследовательские организации, консалтинговые фирмы, финансовые и телекоммуникационные компании.

За последние три года жертвами «Elfin» стали 18 организаций в США, в том числе компании из списка «Fortune 500». Некоторые из них были атакованы с целью осуществления дальнейших атак на цепочку поставок.

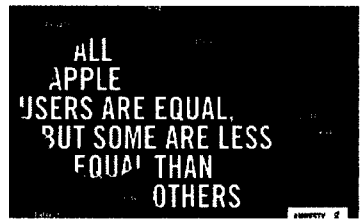
Последняя волна атак была зафиксирована в феврале нынешнего года. Для их осуществления злоумышленники пытались эксплуатировать известную уязвимость в утилите WinRAR, позволяющую устанавливать файлы и выполнять код в системе. Эксплоит попал на компьютеры двух сотрудников атакуемой организации через фишинговое письмо со вложенным вредоносным файлом JobDetails.rar. После его открытия на систему загружался эксплоит.

Источник: https://www.news.rambler.ru/other/41943197-iranskie-kibershpiony-atakuyut-kompanii-v-ssha-i-saudovskoy-aravii/ (дата размещения материала 28.03.2019).

Китайское отделение «Amnesty International» в течение нескольких лет находилось под кибератакой

По данным сайта itsec.ru со ссылкой на издание «Agence France-Press», гонконгский офис правозащитной организации «Amnesty International» в тече-

ние нескольких лет находился под атакой хакеров, предположительно работающих на правительство Китая. Впервые признаки взлома были обнаружены 15 марта текущего года в процессе миграции ИТ-инфраструктуры в более защищенные сети в рамках планового обновления. Заподозрив неладное, организация обратилась за помощью к ИБ-экспертам.



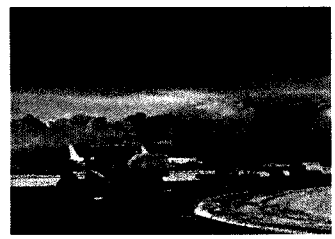
В ходе расследования специалисты выявили связь между инфраструктурой, использовавшейся для атак на «Amnesty International», и предыдущими операциями APT-группы, связываемой исследователями с китайским правительством. Как отметили ИБ-эксперты, за атаками стоит «известная APT-группа, чьи тактики, техники и процедуры указывают на хорошо подготовленного противника». Поскольку расследование все еще продолжается, точное название группировки не раскрывается.

Источник: http://www.itsec.ru/news/kitayskoye-otdeleniye-amnesty-in-ternational-v-techenii-neskolkih-let-nahodilos-pod-kiberatakoy (дата размещения материала 26.04.2019).

Крупнейший производитель спецтехники
«Aebi Schmidt» стал жертвой вымогательского ПО

По информации сайта securitylab.ru со ссылкой на издание «TechCrunch», швейцарский производитель спецтехники для содержания территорий аэропортов и уборки улиц компания «Aebi Schmidt» была вынуждена приостановить операции из-за кибератаки с использованием вымогательского ПО. В результате атаки была нарушена работа компьютеров во внутренней сети компании. Кроме того, вышли из строя несколько систем по всему миру, подключенных к данной сети. Нерабочими оказались системы, отвечающие за производственные процессы, а также электронная почта компании. В настоящее время неясно, о какой программе-вымогателе идет речь.

Представитель «Aebi Schmidt» подтвердил факт атаки и заявил, что компания уже восстановила работу части своих систем, однако корпоративная Windows-сеть «пострадала от вируса» и некоторые системы отключены в качестве меры предосторожности.



«Aebi Schmidt» пополнила список компаний, пострадавших от вымогательского ПО в последние несколько месяцев. В частности, в марте один из крупнейших мировых производителей алюминия компания «Norsk Hydro» была вынуждена приостановить операции из-за хакерской атаки, а в конце апреля кибератака прервала вещание телеканала «The Weather Channel».

Источник: https://www.securitylab.ru/news/498919.php (дата размещения материала 25.04.2019).

Хакеры пытались получить доступ к военным разработкам Испании

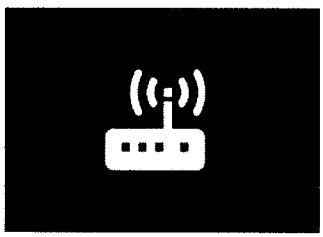
Как сообщает сайт vpk.name со ссылкой на газету «El Pais», министерство обороны Испании заявило, что хакерская атака неназванной «иностранной державы» на компьютерную сеть ведомства в первой половине марта предположительно была совершена с целью получить доступ к секретным сведениям в сфере военной промышленности.

Ранее минобороны объявило о «возможном вторжении в сеть общего назначения». Расследование, которое ведет прокуратура, свидетельствует о том, что хакерская атака оказалась серьезнее, чем предполагалось изначально. Вероятно, киберпреступники хотели получить доступ к секретным сведениям военной промышленности.

Источник: https://www.vpk.name/news/264840_hakeryi_pyitalis_poluchit_dostup_k_voennyim_razrabotkam_ispanii.html (дата размещения материала 27.03.2019).

Android-приложение для поиска точек доступа Wi-Fi раскрывало пароли 2 млн. сетей

По данным сайта allnokia.ru со ссылкой на издание «TechCrunch», приложение «WiFi Finder», загруженное из «Google Play Store» тысячами пользователей, позволяет находить поблизости доступные сети Wi-Fi. Пользователи также могут загружать пароли для доступа к беспроводным сетям со своих устройств в базу данных приложения, чтобы ими могли пользоваться другие. Однако эта база данных находилась в открытом доступе, и покопаться в ней мог любой желающий.



Исследователи безопасности обнаружили базу данных и сообщили о ней журналистам издания. В течение более двух недель они общими усилиями пытались связаться с разработчиком приложения, предположительно находящимся в Китае, но безуспешно. В итоге журналисты обратились к хостинг-провайдеру «DigitalOcean», который в тот же день отключил незащищенную базу данных.

Каждая запись в базе данных содержала имя сети Wi-Fi, ее точное местоположение, идентификатор BSSID и пароль в незашифрованном виде. Хотя, по словам разработчика, приложение предоставляет пароли только для доступа к общественным беспроводным сетям, в БД содержатся данные множества домашних сетей.

Приложение не требует, чтобы пользователи получали разрешение от владельца сети Wi-Fi, тем самым подвергая ее угрозе несанкционированного доступа. Имея доступ к сети, злоумышленник может изменить настройки маршрутизатора таким образом, чтобы ничего не подозревающие пользователи попадали на вредоносные сайты. Находясь в сети, преступник также может

просматривать проходящий через беспроводную сеть незашифрованный трафик и похищать конфиденциальные данные.

Источник: https://www.allnokia.ru/news/324813/ (дата размещения материала 23.04.2019).

Кибератака «выбила» канал о погоде из эфира[7]

Согласно информации, опубликованной на сайте infosecurity-magazine.com, на один из каналов о погоде была совершена кибератака, в результате чего на 90 минут была парализована работа канала. После возобновления работы руководство канала заявило, что на канал была совершена атака с использованием вредоносного ПО.

Несмотря на то, что атаки на телесети не часто попадают в новости, их жертвами стали многие страны. Например, в феврале 2018 года кибератака на Олимпийские игры в Пхёнчхане заблокировала работу официального сайта игр на 12 часов и нарушила работу Wi-Fi и телевещания на Олимпийском стадионе Пхёнчхана.

Источник: https://www.infosecurity-magazine.com/news/cyber-attack-knocks-the-weather/ (дата размещения материала 19.04.2019).

[7] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.