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

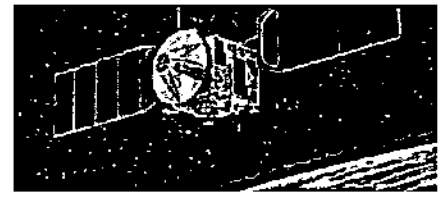
СОДЕРЖАНИЕ

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

1.1. Противодействие техническим разведкам

Группировка спутников ДЗЗ EarthNow будет вести непрерывную видеосъемку

Как сообщает сайт sovzond.ru, компания «EarthNow LLC» объявила о намерении развернуть большую группировку усовершенствованных спутников дистанционного зондирования Земли (ДЗЗ), способных поставлять непрерывное видео в реальном масштабе времени почти всей поверхности Земли. В настоящее время группировка спутников EarthNow планирует получать более качественные данные по сравнению с другими спутниковыми системами ДЗЗ, которые поставляют потребителям снимки, а иногда и видеоклипы. При использовании существующих систем пользователи могут видеть только то, что случилось в прошлом. С помощью спутниковой группировки EarthNow можно наблюдать, как разворачиваются события в реальном масштабе времени.



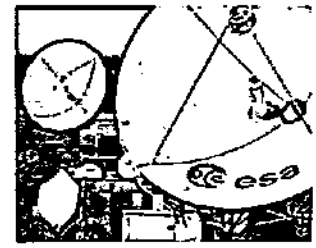
EarthNow использует преимущества модернизированной версии спутниковой платформы, первоначально разработанной для телекоммуникационных сервисов OneWeb. Каждый спутник будет оснащен большим количеством бортовых средств обработки данных, включая более мощный центральный процессор по сравнению с другими коммерческими спутниками.

Источник: https://www.sovzond.ru/press-center/news/corporate/4098/ (дата размещения материала 24.04.2018).

Европейское космическое агентство испытает новый радарный спутник

По данным сайта tass.ru, европейское космическое агентство совместно с финской компанией «Iceye» испытает новый космический радарный спутник, который по замыслу конструкторов должен быть в разы дешевле и компактнее своих современных аналогов.

Новый радар построен на базе технологии радиолокационной синтезированной апертуры, что позволяет ему получать изображение поверхности планет и различных объектов независимо от уровня естественного освещения, климатических и погодных условий. Установлен он будет на космическом аппарате, габариты которого составляют всего 80×60×50 см, что намного меньше всех современных радарных спутников. Отправляемая в космос разработка будет также оснащена раздвижной антенной, которая после выхода на орбиту развертывается и достигает 3,5 метров в длину.



Радар будет испытан в рамках программы мониторинга окружающей среды «Copernicus». Всего компания «Iceye» в перспективе планирует запуск еще

порядка двух десятков подобных аппаратов. Первый был уже запущен в январе. Следующий планируют отправить на орбиту предстоящим летом.

Источник: http://www.tass.ru/kosmos/5069935 (дата размещения материала 27.03.2018).

Китай успешно запустил три оптических спутника

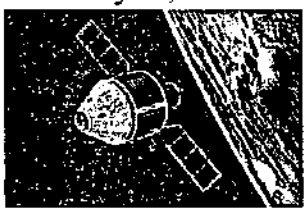
По информации, размещенной на ряде сайтов, Китай вывел на орбиту три оптических спутника. Аппараты созданы на базе введенного в эксплуатацию в апреле 2013 года спутника ДЗЗ высокого разрешения «Gaofen-1». Установленная на них оптика позволяет производить цветную съемку с разрешением в 2 метра. В числе прочего спутники будут собирать данные о природных ресурсах.

Утверждается, что это первая группировка спутников, запущенных Китаем исключительно для гражданских нужд.

Источники: https://www.ren.tv/novosti/2018-03-31/kitay-uspeshno-zapustil-tri-opticheskih-sputnika (дата размещения материала 31.03.2018); http://www.novosti-kosmonavtiki.ru/news/35945/.

Китай запустил группу спутников ДЗЗ «Yaogan-31»

Как сообщает ряд сайтов со ссылкой на информационное агентство «Синьхуа», Китай успешно осуществил запуск группы спутников ДЗЗ «Yaogan-31». Аппараты выведены на орбиту при помощи ракеты-носителя «Чанчжэн-4С». Международные наблюдатели считают, что спутниковая серия «Yaogan» предназначена для целей разведки НОАК Китая.



Вместе со спутниками «Yaogan-31» на орбиту выведен также экспериментальный наноспутник. Аппараты будут использоваться для изучения электромагнитных полей и проведения других технических экспериментов.

Источники: https://www.vpk.name/news/211939_smi_kitai_zapustil_gruppu_sputnikov_distancionnogo_zondirovaniya_zemli_yaogan31.html (дата размещения материала 11.04.2018); http://www.agat-roscosmos.ru/novosti-otechestvennih-smi/v-kitae-zapustili-pervuyu-gruppu-ka-yaogan-31/; http://www.avianews.info/neozhi-dannyj-zapusk-tryoh-razvedyvatelnyh-sputnikov-yaogan-31/; http://www.tass.ru/kosmos/5109339.

С космодрома Танегасима запущен спутник «Gaofen-5»

По данным сайта ecoruspace.me, космический аппарат «Gaofen-5» – это спутник ДЗЗ, который оснащен шестью типами полезных нагрузок. Спутник имеет срок активного существования восемь лет и построен на основе спутни-

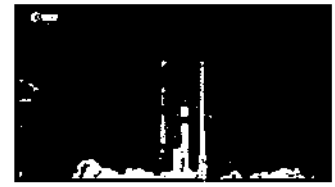
ковой платформы SAST-5000B. В качестве аппаратуры на спутнике установлены: улучшенный гиперспектральный сенсор AHSI; оптический и инфракрасный многоспектральный сенсор VIMS; инструмент для измерения парниковых газов GMI; ультраспектральный инфракрасный атмосферный сенсор AIUS; инструмент для слежения за окружающей средой EMI; направленная поляризационная камера DPC.

Источник: https://www.ecoruspace.me (дата размещения материала 08.05.2018).

Ракета «Рокот» вывела европейский спутник «Sentinel-3B» на орбиту

По информации ряда сайтов 25 апреля с космодрома Плесецк успешно осуществлен пуск ракеты-носителя легкого класса «Рокот» с космическим аппаратом «Sentinel-3B».

Спутник «Sentinel-3B» предназначен для решения задач программы мониторинга окружающей среды «Copernicus». Аппарат будет использоваться для сбора данных о состоянии океанов, морских льдов и прибрежных зон. Этот спутник станет третьим из аппаратов серии «Sentinel», запущенных на ракете «Рокот» в рамках контрактов, заключенных Европейским космическим агентством с компанией «Eurockot».



Источники: http://www.spacenews.com/eurockot-conducts-final-rockot-mission-with-sentinel-3b-satellite/ (дата размещения материала 25.04.2018)[1]; http://www.infoespacial.com/es/2018/04/26/noticia-sentinel3b-reune-tecnologia-hasta-empresas-espanolas.html[2].

Заработала космическая лазерная оптическая линия связи

По данным, размещенным на ряде сайтов со ссылкой на информационное агентство «РИА Новости», европейская космическая система «SpaceDataHighway» успешно введена в эксплуатацию и начала получать информацию со всех четырех спутников Sentinel по программе «Copernicus». Первые две пары спутников – «Sentinel-1A» и «Sentinel-1B», а также «Sentinel-2A» и «Sentinel-2B» – присоединились к системе «SpaceDataHighway» в рамках соглашения между Европейским союзом, Европейским космическим агентством и компанией «Airbus», которая владеет «SpaceDataHighway» и осуществляет ее коммерческую эксплуатацию.

«SpaceDataHighway» – это космическая лазерная оптическая линия связи, созданная с помощью передовых лазерных технологий. На геостационарной

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

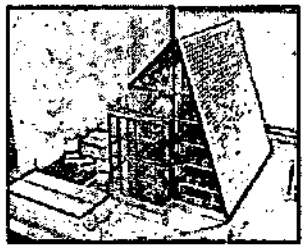
орбите уже находится первый спутник-ретранслятор «EDRS-A», который возглавит группировку спутников, работающих с наземными станциями наблюдения. Ежедневно он может передавать до 40 Тбайт данных, полученных со спутников наблюдения, беспилотных летательных аппаратов (БПЛА) и пилотируемых летательных аппаратов.

Спутники-ретрансляторы предназначены для обслуживания низкоорбитальных спутников с помощью лазера и сбора данных, которые они получили в ходе исследования планеты. Затем «SpaceDataHighway» со своей геостационарной орбиты отправляет собранные данные в европейский центр на Земле. Таким образом, спутник-ретранслятор выступает в качестве промежуточного звена при передаче данных. Этот процесс позволяет спутникам, находящимся на более низких орбитах, непрерывно передавать получаемую информацию вместо того, чтобы хранить ее до момента связи с наземной станцией. Таким образом, спутники могут отправлять больше данных за меньшее время.

Источники: https://www.sovzond.ru/press-center/news/dzz/3883/ (дата размещения материала 27.03.2018); https://www.m24.ru/news/tehnologii/27 0320 18/28627.

Франция учится смотреть за горизонт

Как сообщается на сайте vpk.name, в ближайшие годы Франция может вооружиться загоризонтным радаром. Французский центр аэрокосмических исследований «ONERA» приступил к испытаниям прототипа загоризонтной радиолокационной станции (РЛС), способной отслеживать пуски баллистических ракет с расстояния в несколько тысяч километров.



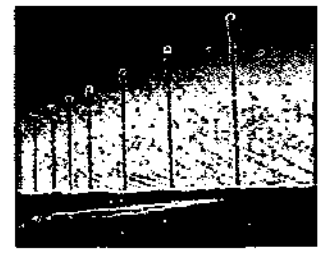
Минобороны Франции подписало контракт на разработку прототипа загоризонтного радара DRTLP в 2011 году. Разработкой РЛС занимаются компания «Thales» и французский центр аэрокосмических исследований «ONERA». Согласно условиям контракта, загоризонтный радар должен иметь возможность отслеживать пуски баллистических ракет с расстояния до 3000 километров. Кроме того, разработчики намерены протестировать установку на возможность обнаружения и отслеживания космических аппаратов. По завершении испытаний минобороны Франции примет решение о дальнейшем финансировании программы разработки DRTLP.

Источник: https://www.vpk.name/news/210172_franciya_uchitsya_smotret_za_gorizont.html (дата размещения материала 26.03.2018).

Австралийский загоризонтный радар получит «ночное зрение» к 2024 году

По информации сайта nplus1.ru со ссылкой на издание «Aviation Week», австралийское подразделение британской компании «BAE Systems» в апреле 2018 года приступило к модернизации загоризонтной РЛС JORN. Благодаря

проведенным работам РЛС сможет обнаруживать малоразмерные объекты в ночное время.

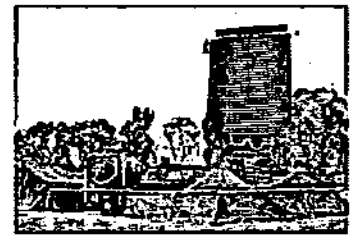


Австралийский загоризонтный радар JORN, помимо двух основных комплексов, включает в себя контрольную станцию на авиабазе ВВС «Эдинбург» в Южной Австралии, 12 вертикальных ионозондов, установленных в разных точках Австралии, и семь приемо-передающих станций. У последних принимающие и передающие установки разнесены друг от друга на существенные расстояния, чтобы избежать самовозбуждения. В настоящее время JORN работает на уменьшенной мощности и способен «видеть» на дальность до четырех тысяч километров. На полной мощности дальность обзора может достигать 5,5 тысячи километров, что позволяет «видеть» воздушные цели над частью территории Китая.

Источник: https://www.nplus1.ru/news/2018/04/21/night (дата размещения материала 21.04.2018).

Литва покупает у Израиля РЛС

Как информирует сайт kompravda.eu, Литва закупает у Израиля пять радаров для наблюдения за воздушным пространством ближнего радиуса действия. Эти РЛС для перекрытия «мертвых зон» могут быть размещены в Варенском, Швянченском, Вильнюсском, Юрбаркском и Пагегяйском районах. Закупаемые радары планируется интегрировать в общую систему противовоздушной обороны (ПВО) Литвы и начать их эксплуатацию до конца 2019 года.



Как сообщило минобороны Литвы, два из пяти радаров приобретаются для снижения негативного влияния ветряных парков в Шилутском и Таурагском районах на способность РЛС ПВО обнаруживать и сопровождать воздушные цели.

Источник: https://www.kompravda.eu/online/news/3070314/ (дата размещения материала 05.04.2018).

Начато создание квантового радара, от которого не спасут стелс-технологии

Как сообщает сайт dailytechinfo.org, исследователи из канадского университета Ватерлоо приступили к разработке квантовой радарной системы, способной работать в условиях присутствия высокого уровня фоновых шумов, что, в свою очередь, позволит этому радару безошибочно находить и сопровождать самолеты и ракеты, оборудованные самыми современными стелс-технологиями, в том числе и активными.

Технология, лежащая в основе работы квантового радара, основана на так называемом «квантовом освещении». Только в данном случае для освещения

пространства используется не обычный свет, а свет, состоящий из «запутанных» на квантовом уровне фотонов. Когда состояние одного из «запутанных» фотонов изменяется из-за столкновения с поверхностью самолета-невидимки, к примеру, состояние второго фотона также моментально изменяется, невзирая на разделяющее их расстояние.

Один из фотонов «запутанной» пары отправляется квантовой радарной установкой в пространство, а второй остается на месте, будучи удерживаемым в специальной фотонной ловушке. Радарная система анализирует лишь состояние фотонов, сохранивших «запутанность» со вторым фотоном. Те фотоны, которые потеряли «запутанность» в результате воздействия явления декогеренции, т.е. влияния естественных шумов окружающей среды, отбрасываются и все это позволяет во много раз увеличить значение соотношения сигнал/шум в определенных ситуациях.

Однако, для того, чтобы создать реально работающий квантовый радар, требуется создание быстрого и надежного источника «запутанных» фотонов. Канадские ученые уже имеют в своем распоряжении такой лабораторный источник, который был использован для лабораторных испытаний технологии квантового освещения. Теперь ученые работают над созданием полностью работоспособного опытного образца квантового радара.

Источник: https://www.dailytechinfo.org/military/10179-nachato-sozda-nie-kvantovogo-radara-ot-kotorogo-ne-spasut-nikakie-stels-tehnologii.html (дата размещения материала 27.04.2018).

Разработка плана сохранения на вооружении самолетов E-8C JSTARS до 2030 года

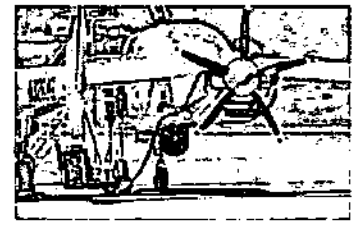
По данным издания «Авиационные системы/Экспресс-информация», «Northrop Grumman» и ВВС США разрабатывают план сохранения на вооружении до 2030 года 16 самолетов объединенной радиолокационной системы наблюдения E-8C JSTARS за счет их модернизации. Компания планирует заменить или модернизировать имеющиеся на борту самолетов E-8C центральные (главные) компьютеры, максимально используя новейшие технологии, что позволит в будущем осуществлять их замену с меньшими затратами. ВВС также поручили компании добавить в JSTARS функцию обнаружения малоразмерных целей, одновременно продолжая работу по повышению способности РЛС самолета обнаруживать новейшие боевые средства противника.

Кроме этого, специалисты работают и над повышением эффективности действий оператора, пользующегося средствами вычислительной техники для принятия решения, в условиях возникающих киберугроз.

Источник: Авиационные системы/Экспресс-информация, 2018, № 12, с. 3.

Таинственный самолет-шпион
компании «Northrop Grumman»[3]

На сайте thedrive.com размещена информация о появлении снимков нового пилотируемого высотного разведывательного самолета компании «Northrop Grumman» под названием H03. Его внешний вид и конструкция позволяют предположить, что самолет предназначен для полета с малой скоростью на большой высоте.



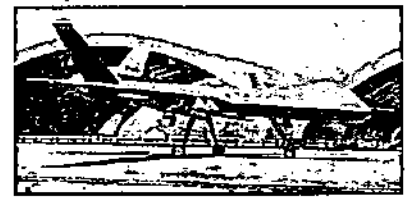
Весьма вероятно, что H03 сделан из легких композитных материалов, которые могут уменьшить эффективную площадь рассеивания. У самолета имеется большая турель, смонтированная под фюзеляжем, где могут размещаться оптико-электронные, инфракрасные или многоспектральные видеокамеры, а также лазерные дальномеры или целеуказатели. Все это свидетельствует о разведывательной функции самолета.

Хотя до сих пор неизвестно для кого «Northrop Grumman» сделала этот самолет, но очевидно, что существует спрос на подобные самолеты. Кроме того, из-за низкой стоимости H03 может заменить другие пилотируемые и беспилотные высотные разведывательные самолеты, такие как U-2 «Dragon Lady», RQ-4 «Global Hawk» или даже RQ-170 «Sentinel».

Источник: http://www.thedrive.com/the-war-zone/19898/mysterious-northrop-grumman-spy-plane-emerges-at-the-mojave-air-and-space-port (дата размещения материала 04.04.2018).

США разместят беспилотники MQ-9 «Reaper»
у города Лариса

Как сообщается на сайте rua.gr со ссылкой на греческую газету «To Vima», уже в мае этого года американские беспилотники начнут использовать базу греческих ВВС в центральной части страны у города Лариса. Основной задачей дронов станет сбор разведывательной информации в стратегически важном регионе юго-востока Европы.



Если исходить из дальности полета БПЛА данного типа (почти 2000 километров), то эти аппараты вполне могут быть использованы для ведения разведки не только в Средиземном, но и в Черном море, в том числе у берегов Крыма.

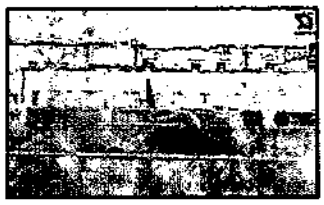
Источник: https://www.rua.gr/news/gospol/25510-ssha-razmestyat-boe-vye-bespilotniki-mq-9-reaper-u-goroda-larisa.html (дата размещения материала 26.03.2018).

---

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

Китай разместил БПЛА «Xianglong» на авиабазе ВМС НОАК на острове Хайнань

По информации ряда сайтов со ссылкой на издание «Jane's Defence Weekly», Китай расширяет свои возможности по ведению воздушной разведки в районе острова Хайнань, который является стратегически важной точкой в Южно-Китайском море.



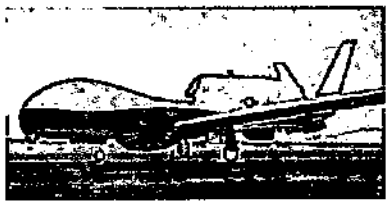
Два многоцелевых высотных БПЛА большой продолжительности полета «Xianglong» были размещены на авиабазе ВМС НОАК в северо-восточном Китае. По данным издания, крейсерская скорость «Xianglong» составляет около 830 километров в час, высота полета – 18000 метров, максимальная дальность полета – 3780 морских миль.

Данный проект является попыткой обеспечить НОАК аппаратами с возможностями, близкими к БПЛА RQ-4 «Global Hawk».

Источники: https://www.vpk.name/news/210144_kitai_razmestil_bla_syanlun_na_aviabaze_vms_noak_linshui_na_ostrove_hainan.html (дата размещения материала 26.03.2018); http://www.legacy.paukpress.ru/app/article/1254252//.

Германия намерена приобрести у США беспилотники «Triton»

По данным ряда сайтов, Германия намерена закупить у США четыре БПЛА MQ-4C «Triton», предназначенных для морского патрулирования.

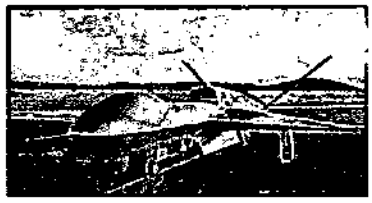


Разведывательный беспилотник «Тритон» разработан корпорацией «Northrop Grumman» специально для ВМС. Он оборудован реактивным двигателем, который позволяет ему подниматься на высоту до 20 километров и находиться в полете около 30 часов. Высокая точность сбора информации и большая зона покрытия беспилотника обеспечивается комплектом инфракрасных сенсоров и мощным радаром.

Источники: http://www.tass.ru/mezhdunarodnaya-panorama/5100104 (дата размещения материала 06.04.2018); https://www.kommersant.ru/ doc/3594483.

Рекорд «Avenger ER» по продолжительности полета

По информации сайта absrf.ru, БПЛА увеличенной дальности «Avenger Extended Range» (ER) производства компании «General Atomics Aeronautical Systems, Inc.» установил новый рекорд по продолжительности полета.



В январе этого года БПЛА «Avenger ER» в конфигурации разведчика провел в воздухе 23,4 часа, имитируя выполнение разведывательных задач в реальном масштабе времени. Робототехническая автоматизация обеспечивает долговременный режим работы и возможности высокоточного удара, что достигается и поддерживается широким спек-

тром датчиков и полезных нагрузок для выполнения задач разведки, наблюдения и рекогносцировки, а также авиационной поддержки наземных сил.

Линейка беспилотных самолетов «Avenger» способна нести такие полезные нагрузки, как мультирежимный радар GA-ASI Lynx и оптико-электронный и инфракрасный датчик MS-177.

Источник: http://www.absrf.ru/ru/technology/1523973473.htm (дата размещения материала 17.04.2018).

Турецкий ударный беспилотник научился вести радиоэлектронную разведку

Как сообщает сайт nplus1.ru со ссылкой на издание «Aviation Analysis Wing», турецкая компания «TAI» приступила к испытаниям новой версии средневысотного БПЛА «Anka» («Феникс»), предназначенной для ведения радиоэлектронной разведки. Разработка этой версии ударного беспилотника прежде держалась в секрете.

Новая версия аппарата получила конформные отсеки с системами радиоэлектронной разведки, расположенные ближе к носовой части по сторонам фюзеляжа, а также набор антенн, позволяющих принимать сигналы в широком диапазоне частот. Аппарат также оснащен системой передачи разведывательных данных на пункт управления в режиме реального времени.

Летные испытания БПЛА проводятся на авиабазе к северо-западу от Анкары. Предположительно, во время испытаний аппарат совершил по меньшей мере один разведывательный вылет в Сирию.

Источник: https://www.nplus1.ru/news/2018/03/29/intelligence (дата размещения материала 29.03.2018).

«Boeing» приступил к сборке сотого самолета P-8A «Poseidon»

Как сообщает сайт arms-expo.ru, в настоящее время корпорация «Boeing» приступила к сборке сотого самолета P-8A «Poseidon», который предназначен для ВМС США. Всего на текущий момент компания получила заказы почти на 150 самолетов, из которых 108 предназначены для американской армии, а остальные будут переданы Великобритании, Индии и Австралии. Кроме того, в прошлом году пять самолетов заказала Норвегия. Всего же «Boeing» планирует продать порядка 200 самолетов этого типа. В частности, планы на расширение заказа уже озвучили в минобороны США. Кроме того, потенциальным заказчиком является и Южная Корея.

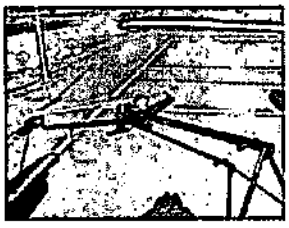
P-8A «Poseidon» – патрульный противолодочный самолет нового поколения, оснащен бортовой РЛС AN/APS-137D(V)5 или РЛС AN/APY-10. Во внутреннем отсеке вооружения размещаются гидроакустические буи, предназна-

ченные для обнаружения субмарин на больших глубинах, свободнопадающие и глубинные бомбы, а также торпеды Mark 54.

Источник: http://www.arms-expo.ru/news/vooruzhenie_inostrannykh_armiy/patrolnyy_protivolodochnyy_samolyet_p_8_poseidon_popularmechanics_com/ (дата размещения материала 13.04.2018).

Компании «Mahindra Defense» и «Aeronautics» достигли договоренности о производстве морских БПЛА

По информации ряда сайтов со ссылкой на издание «Jane's Defence Weekly», индийская «Mahindra Defense» и израильская «Aeronautics Ltd.» подписали соглашение по вопросу организации лицензионного производства морской версии БПЛА «Orbiter-4», в случае его закупки для ВМС Индии. Аппарат может эксплуатироваться с бортов небольших военных кораблей, необорудованных вертолетной палубой.

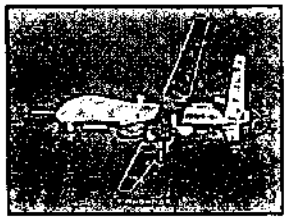


Продолжительность полета «Orbiter-4» составляет 24 часа, практический потолок – 5485 метров. Беспилотник способен одновременно нести две полезные нагрузки, включая морскую РЛС, аппаратуру перехвата сотовой связи, средства спутниковой связи, РЛС с синтезированной апертурой, систему автоматической идентификации объектов и различные оптико-электронные и инфракрасные камеры.

Источники: http://www.armstrade.org/includes/periodics/news/2018/0416/1-52546347/detail.shtml (дата размещения материала 16.04.2018); http://www.vestnik-glonass.ru/news/corp/drony-dlya-voennomorskikh-sil/.

Южнокорейский беспилотный летательный аппарат большой дальности

По данным ряда сайтов, в Южной Корее проходят летные испытания первого прототипа национального разведывательно-ударного БПЛА большой дальности, известного под обозначением KUS-FS.



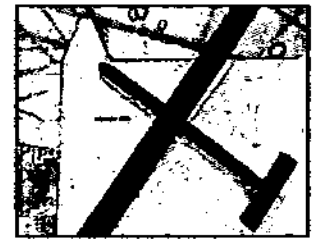
БПЛА штатно оснащается комплектом оборудования разведки, наблюдения и целеуказания, включая РЛС с синтезированной апертурой разработки компании «LIG Nex1» и круглосуточную оптико-электронную станцию компании «HanwhaSystem», а также аппаратуру радио- и радиотехнической разведок. Также возможно оснащение БПЛА аппаратурой радиоэлектронной борьбы и другими типами РЛС.

Крейсерская скорость полета аппарата составляет около 250 километров в час, продолжительность полета – от 24 до 32 часов, высота – до 15500 метров.

Источники: https://www.bmpd.livejournal.com/3131840.html (дата размещения материала 23.03.2018); http://www.arms-expo.ru/news/inostrannye_razrabotki/yuzhnokoreyskiy_bespilotnyy_letatelnyy_apparat_bolshoy_dalnosti/; http://www.firstnewz.ru/news/31116-yuzhnokoreyskiy-bespilotnyy-letatel-nyy-apparat-bolshoy-dalnosti.html.

Компания «Укрспецсистемс» разработала версию БПЛА PD-1 с вертикальным взлетом и посадкой

Как сообщает журнал «Военно-техническое сотрудничество», украинская компания «Укрспецсистемс» представила на индийской выставке «Дефэкспо-2018» версию своего БПЛА PD-1 с вертикальными взлетом и посадкой. Продолжительность полета аппарата превышает 10 часов; рабочая высота полета составляет 3000 метров, дальность – более 500 километров.



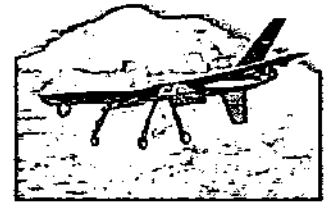
Беспилотник способен вести наблюдение на дальности до 100 км и может быть оснащен комплектом полезной нагрузки, включая видеокамеры высокого разрешения и лазерные дальномеры. Данные этих датчиков могут передаваться оператору в реальном времени.

PD-1 может применяться пограничниками и береговой охраной для проведения операций на море, сбора разведывательных данных и ведения наблюдения.

Источник: Военно-техническое сотрудничество, 2018, № 16, с. 26-27.

Украина применит американские беспилотники против России

По данным сайта lenta.ru, украинские военные научились получать информацию с американских разведывательно-ударных БПЛА MQ-9 «Reaper». Во время проведения курсов слушатели получили теоретические знания и практические навыки по планированию специальных операций по стандартам и процедурам НАТО.



В настоящее время у Украины нет собственных средних и крупных военных беспилотников. Полеты над территорией страны осуществляются американскими дронами, главным образом в районе Донбасса. Также американские дроны неоднократно были замечены в районе Крыма. Одной из наиболее вероятных причин полетов беспилотников считается разведка позиций, находящихся на российской территории.

Разведывательно-ударный БПЛА MQ-9 «Reaper» в зависимости от поставленных задач способен проводить съемку в видимом и инфракрасном диапазонах, а также может оснащаться лазерным дальномером-целеуказателем.

Источник: https://www.lenta.ru/news/2018/04/10/mq9reape (дата размещения материала 10.04.2018).

Новая версия программы UASMaster для обработки данных БПЛА

Как сообщается на сайте sovzond.ru, компания «Trimble Geospatial» выпустила новую версию программы UASMaster 9.0, которая предназначена для фотограмметрической обработки данных, полученных с любых современных типов БПЛА.

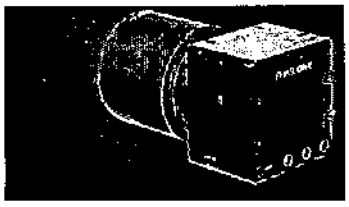
UASMaster 9.0 включает в себя два новых независимых рабочих процесса, каждый из которых оптимизирован для конкретных требований к обработке: рабочий процесс «Area Mapping» («Площадное картографирование») предназначен для проектов, съемка которых велась близко к надиру с классическими прямыми линиями полета и новый рабочий процесс «Close Range 3D» («3D малой дальности»), оптимизированный для обработки нелинейной наклонной съемки мультикоптеров, например, съемки вокруг зданий и сооружений. Также «Close Range 3D» используется для проектов, съемка которых велась наземно обычными камерами или даже смартфонами.

Эта новая возможность в UASMaster позволяет создавать полные 3D-модели объектов, таких как здания, опоры линий электропередач и т.п., а также формировать правильное представление вертикальных структур в горных районах.

Источник: https://www.sovzond.ru/press-center/news/corporate/3989/ (дата размещения материала 09.04.2018).

«Phase One Industrial» выпускает камеру для аэрофотосъемки на датчике среднего формата разрешением 100 мегапикселей

По данным сайта ixbt.com компания «Phase One Industrial» освоила выпуск камеры iXM 100 MP, которая дополнена сменными объективами и рассчитана на установку на БПЛА. По словам производителя, камера позволяет вести высококачественную аэрофотосъемку в интересах разнообразных картографических, геодезических и инспекционных приложений. Диапазон ее светочувствительности равен ISO50-6400. Камера способна снимать со скоростью 3 кадра в секунду.

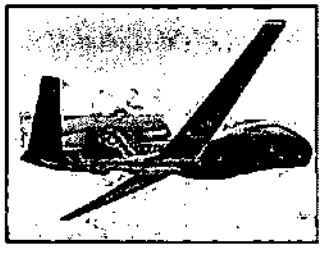


Список объективов, рассчитанных на новый датчик с размерами активной области 33×44 мм, включает две модели с фиксированной фокусировкой (с фокусным расстоянием 35 мм и 80 мм) и две модели с приводом фокусировки (с фокусным расстоянием 80 мм и 150 мм).

Источник: https://www.ixbt.com/news/2018/05/02/phase-one-industrial-100.html (дата размещения материала 02.05.2018).

Американский беспилотник провел разведку вблизи находящихся в Сирии российских баз

По данным сайта vpk-news.ru со ссылкой на информационное агентство «Интерфакс-АВН», стратегический беспилотник ВВС США RQ-4B «Global Hawk» провел 24-часовой полет вблизи Сирии и расположенных на ее побережье российской авиабазы Хмеймим и базы материально-технического обеспечения ВМФ России в порту Тартус.



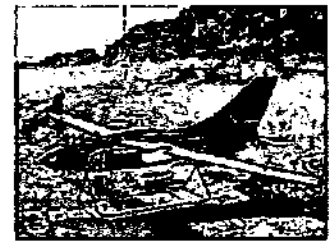
Беспилотник с бортовым номером 10-2043, выле-

тевший с авиабазы Сигонелла на итальянском острове Сицилия, курсировал над международными водами Средиземного моря вблизи границ Ливана и Сирии на высоте около 16 тыс. метров. С учетом возможностей ведения разведки на глубину до 450 км, он мог наблюдать за всей контролируемой Дамаском территорией Сирии, а также российскими базами.

Источник: https://www.vpk-news.ru/news/42224 (дата размещения материала 16.04.2018).

Украинский беспилотник проинспектировал Крым

Как сообщает ряд сайтов со ссылкой на «Укроборонпром», украинский беспилотник «Spectator-M» начал «патрулировать административные границы с временно оккупированным Крымом». Дрон представляет собой модернизированный беспилотник «Spectator» с улучшенными эксплуатационными характеристиками, большей грузоподъемностью и дальностью полета.



«Spectator-M» оснащен видео- и тепловизионной камерой, позволяющей вести разведку на глубину до 50 километров на высоте до двух километров.

Источники: https://www.lenta.ru/news/2018/04/18/drone/ (дата размещения материала 18.04.2018); https://www.news.rambler.ru/weapon/3961 8105-zapuschennyy-rogatkoy-ukrainskiy-dron-poletel-nad-krymom/.

США намерены применять в Арктике робототехнику

Как информирует сайт sovzond.ru, США намерены в ближайшем будущем приступить к применению в Арктике трех основных видов робототехники для изучения местности. Об этом заявил командующий американской береговой охраны адмирал П.Зукунфт.

По его словам, речь идет о БПЛА, более крупных БПЛА, которые способны находиться в воздухе значительно дольше, а также необитаемых подводных аппаратах. Есть и другие технологии, включая автономные корабли, которые могут быть использованы как платформы для ведения разведки.

Командующий уточнил, что в настоящее время картографировано всего около 5% Арктики в соответствии со стандартами XXI века. Поэтому, чтобы не заниматься этой работой в чрезвычайно суровых условиях, эту задачу могут решать необитаемые аппараты.

Источник: https://www.sovzond.ru/press-center/news/bpla/4014/ (дата размещения материала 12.04.2018).

В США создали рой подводных беспилотников

По данным ряда источников, американская компания «Aquabotix» представила робота SwarmDiver, способного образовывать с десятками таких же

устройств рой, который управляется как единый объект. Робот имеет несколько встроенных датчиков, а также интерфейсы для их добавления. Устройство умеет перемещаться в надводном положении и нырять на глубину до 50 метров.

Разработчики позиционируют робота как инструмент для мониторинга водоемов в гражданских или военных целях.

Внешне SwarmDiver представляют собой желтые трубки с пропеллером, внутри которых находятся датчики. Данные устройства способны двигаться со скоростью 2,2 метра в секунду и работать на глубине до 50 метров. Испытания показали, что аппарат способен выполнять задачи и на глубинах более 100 метров. Батареи хватает на 2,5 часа работы, за это время робот может проплыть не менее семи километров. В настоящее время аппарат оснащен датчиками для сбора данных об окружающей среде. Аппараты в составе роя могут быть оснащены и другими датчиками в зависимости от выполняемых задач.

Источники: https://www.topwar.ru/139783-v-ssha-sozdali-roy-bespilotnikov-teper-podvodnyh.html (дата размещения материала 16.04.2018); http://www.super-orujie.ru/blog/43801816973/V-SSHA-sozdali-roy-bespilotnikov.-Teper-podvodnyih; Военно-техническое сотрудничество, 2018, № 16, с. 27.

Турция разработала подводного робота-ската

По информации сайта vpk-news.ru, в скором времени любой корабль может оказаться абсолютно незащищенным перед новой угрозой. Турецкая компания «Albayraklar Group» анонсировала выпуск принципиально нового типа подводных дронов. Новая разработка получила название WATTOZZ («морской

скат»). Роботизированный подводный дрон внешне почти неотличим от настоящего ската. Благодаря используемым материалам его невозможно обнаружить с помощью сонаров и других систем отслеживания подводных целей.

При этом группа дронов, прикрепившись ко дну корабля с помощью электронных магнитов, может легко потопить его при активации встроенной боевой части. Еще одно назначение подводных аппаратов – наблюдение и разведка. Для этого WATTOZZ оснащен двумя камерами, а также системами самозащиты от морских обитателей. Аппараты управляются с помощью гидроакустических сигналов, аналогичных тем, которые издают подводные млекопитающие. Встроенного аккумулятора хватает на 12 часов работы, в движение дрон приводится с помощью трех специальных двигателей. При необходимости WATTOZZ может впадать в «спячку», а затем атаковать корабли и субмарины противника, получив соответствующий сигнал. Официальная презентация робота-ската намечена на 20 июня текущего года.

Источник: https://www.vpk-news.ru/news/42274 (дата размещения материала 17.04.2018).

Пентагон заказал разработку
БПЛА для субмарин

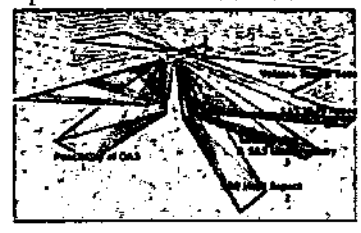
Как сообщает сайт vpk.name со ссылкой на издание «Warspot», экспериментальное управление оборонных инноваций «DIUx» минобороны США объявило тендер на разработку нового разведывательного дрона для подводных лодок. В настоящее время некоторые субмарины ВМС США имеют в своем оснащении беспилотники «Blackwing», которые используются как центры связи, а также могут выполнять некоторые разведывательные задачи для координации ударов. Теперь же минобороны США заявило, что подводный флот нуждается в специализированных разведывательных беспилотниках.

По требованиям военного ведомства, новый аппарат будет базироваться в специальных пусковых установках, и при необходимости подлодка сможет его выпустить, не всплывая на поверхность. Таким образом, беспилотник должен уметь преодолевать путь на поверхность сквозь толщу воды, после чего взлетать и находиться в воздухе не менее часа. Дроны должны иметь возможность летать как под управлением оператора, так и в полностью автоматическом режиме. Радиус полета должен достигать 50 километров. Беспилотники подводного базирования будут оснащаться оптическим модулем, а также разведывательным оборудованием.

Источник: https://www.vpk.name/news/210026_pentagon_zakazal_razrabotku_bpla_dlya_submarin.html (дата размещения материала 26.03.2018).

Гидроакустические станции
миноискания ВМС Франции

В статье, размещенной в журнале «Зарубежное военное обозрение», приведено описание новой гидроакустической системы (ГАС) SAMDIS ВМС Франции, предназначенной для обнаружения мин и отображения подводной обстановки. Благодаря своей компактности и модульности, система может быть размещена как на необитаемом подводном аппарате, так и на буксируемом аппарате.



Новая разработка позволяет решать в реальном масштабе времени широкий круг задач по получению высококачественных изображений поверхности дна и расположенных на нем объектов. В ее состав входит широкополосная интерферометрическая ГАС бокового обзора с синтезированной апертурой. Для работы интерферометрического режима с каждого борта носителя устанавливается дополнительная приемная антенна.

В системе SAMDIS реализован многоаспектный обзор, при этом интерферометрическая обработка осуществляется только для траверзного направления. Для устранения влияния многолучевого распространения на мелководье формируются узкие в вертикальной плоскости характеристики

направленности ГАС.

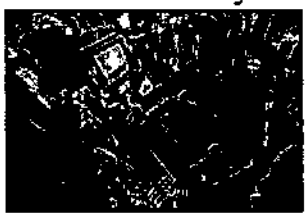
В результате сочетания многоаспектного обзора и интерферометрической обработки сигналов улучшаются возможности по интерпретации обстановки, обнаружению, классификации и определению координат потенциально опасных объектов.

ВМС Франции продолжают работы по совершенствованию ГАС миноискания. Ожидается, что классификационные возможности этих ГАС будут улучшены за счет применения более широкополосных сигналов, алгоритма синтезирования апертуры при обработке принятых сигналов, многоаспектного обзора и интерферометрической обработки. В ряде случаев они смогут опознавать цели.

Источник: Зарубежное военное обозрение, 2018, № 4, с. 73-77.

В США готовятся следить за российскими подлодками в Атлантике

По данным ряда сайтов, американские эксперты заявили, что российские многоцелевые субмарины могут стать большой проблемой для кораблей ВМС США. Поэтому главной задачей воссозданного в США второго флота станет



противодействие российским подлодкам в Атлантике. Одной из главных задач этого оперативного соединения станет противостояние угрозе со стороны атомных подводных лодок ВМФ России, таких как АПЛ «Северодвинск» проекта 885 «Ясень».

Помимо противолодочных кораблей и патрульных самолетов США и страны НАТО привлекут к работе в Атлантике целый ряд вспомогательных средств – акустические системы и средства контроля на больших глубинах.

Источники: https://www.life.ru/t/%D0%B0%D1%80%D0%BC%D0%B8%D1%8F/1114390/v_ssha_ghotoviatsia_sliedit_za_rossiiskimi_podlodkami_v_atlantikie (дата размещения материала 07.05.2018); http://www.rosbalt.ru/world/2018/05/07/1701339.html.

1.2. Техническая защита информации

Процессоры Intel уязвимы к новой атаке BranchScope

По информации сайта securitylab.ru, исследователи обнаружили новый тип атаки по сторонним каналам, который может быть запущен на устройствах

с процессорами Intel. Атака получила название BranchScope. Подобно атакам с использованием Meltdown и Spectre, BranchScope может быть проведена злоумышленником для получения потенциально важной информации, которую нельзя получить напрямую. Злоумышленник должен иметь доступ к целевой системе, а также у него должна быть возможность выполнять произвольный код.

Как полагают исследователи, требования к данной атаке вполне реалистичны, что делает ее серьезной угрозой для современных компьютеров «наравне с другими атаками по сторонним каналам». Атака BranchScope была продемонстрирована на устройствах с тремя типами процессоров Intel i5 и i7 на основе микроархитектуры Skylake, Haswell и Sandy Bridge. Атака работает, даже если целевое приложение запущено внутри анклава Intel SGX. Технология Intel SGX представляет собой набор процессорных инструкций, которые могут быть использованы приложениями для организации защищенных регионов кода и данных (анклавов).

Как и атаки с использованием Spectre, метод BranchScope направлен на модуль предсказания переходов BPU. Данные устройства используются для повышения производительности конвейерных процессоров путем угадывания пути выполнения инструкций перехода. Однако, когда два процесса выполняются на одном и том же физическом ядре процессора, они совместно используют BPU, что потенциально позволяет вредоносному процессу манипулировать направлением команды перехода, выполняемой целевым приложением. BPU имеет два компонента: буфер предсказания переходов BTB и предсказатель ответвлений. Управление любым из них может быть использовано для получения важных данных из памяти.

Исследователи предложили серию контрмер, которые включают как программные, так и аппаратные решения.

Источник: https://www.securitylab.ru/news/492321.php (дата размещения материала 27.03.2018).

Корпорация «Intel» объявила, что далеко не все процессоры с уязвимостями Meltdown и Spectre получат обновления

Как сообщает сайт itsec.ru, корпорация «Intel» не планирует выпускать обновления против уязвимостей Meltdown и Spectre для некоторых семейств своих центральных процессоров. В компании признали, что в некоторых устройствах присутствует вариант уязвимости Spectre, исправить которую слишком сложно или невозможно вовсе. Причин тому называется несколько.

Первая – это микроархитектурные характеристики, препятствующие практической реализации функций, исправляющих второй вариант уязвимости Spectre. Вторая – ограниченная доступность поддерживаемых систем. Третья – использование процессоров в изолированных от внешней сети системах, где вероятность эксплуатации уязвимости стремится к нулю.

Обновления не получат процессоры семейств Bloomfield, Bloomfield Xeon, Clarksfield, Gulftown, Harpertown Xeon C0 и E0, Jasper Forest, Penryn/QC, SoFIA 3GR, Wolfdale, Wolfdale Xeon, Yorkfield и Yorkfield Xeon. Большая часть этих процессоров поступила в продажу между 2007 и 2011 годами, так что, вероятно, лишь некоторая их часть остается в активном использовании. Какие именно из этих процессоров невозможно исправить с помощью патчей, «Intel» не уточняет. В свою

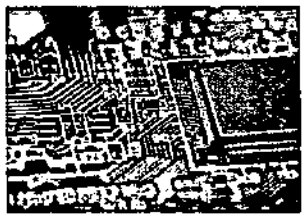
очередь, патчи для процессоров серий Arrandale, Clarkdale, Lynnfield, Nehalem и Westmere уже разработаны.

Источник: http://www.itsec.ru/newstext.php?news_id=122347 (дата размещения материала 05.04.2018).

«Intel» патчит уязвимость в SPI Flash, через которую можно удалить или подменить BIOS/UEFI

Как сообщает сайт huaweiclub.ru, в начале текущего месяца разработчики «Intel» представили исправления для уязвимости CVE-2017-5703, получившей 7,9 балла по шкале CVSS:3.0. Баг был найден самими специалистами компании и позволяет влиять на работу SPI Flash, что чревато крайне неприятными последствиями.

По словам специалистов «Lenovo», которые уже распространяют исправления «Intel» для своих продуктов, уязвимость позволяет локальному атакующему отключить обновления BIOS/UEFI на уязвимом устройстве или выборочно повредить или стереть определенные части прошивки. Второй вариант эксплуатации уязвимости, наиболее вероятно, приведет к сбою и возникновению неисправности, однако в некоторых случаях таким способом можно добиться выполнения произвольного кода, то есть прошивка может стать вредоносной.

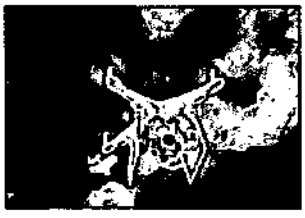


«Intel» сообщает, что уже предоставила исправления в распоряжение производителей персональных компьютеров и материнских плат.

Источник: http://www.huaweiclub.ru/2018/04/16/25535/ (дата размещения материала 16.04.2018).

Найден простой способ обнаружить факт видеосъемки с беспилотника

Как информирует сайт secnews.ru, в зашифрованном потоке данных, исходящих из беспилотника, можно находить признаки того, что он производит фотографирование. Как это делать, придумали ученые из израильского университета Бен-Гуриона. Разработка израильских специалистов обнаруживает факт видеосъемки, но не сам беспилотник, и никак не воздействует на сам выявленный аппарат. Она будет полезна для частного пользователя или небольшой фирмы, у которых нет собственных средств поиска беспилотников.



Для обнаружения факта видеотрансляции с беспилотника необходимо, прежде всего, улавливать трафик, идущий от него к оператору. Исследователи использовали для этого параболическую антенну, подключенную к ноутбуку. Суть метода состоит в использовании мерцающего источника яркого света. В случае защиты дома от слежки с беспилотника для этого используются полоски из светодиодов, вывешиваемые на окно. Мерцание этих светодиодов дает резкие колебания яркости света, который попадает в объектив камеры, установленной на беспилотнике. Если съемка ве-

дется, то мерцание светодиода вызывает резкое изменение распределения яркости в кадре камеры беспилотника и, следовательно, рост битрейта в трафике радиосигнала, который передается от него оператору. Антенна улавливает такое возрастание битрейта. Если оно коррелирует по времени со вспышками светодиодов, то можно считать установленным, что извне ведется съемка дома. Таким образом, дешифровка передаваемого сигнала в данном случае не нужна. Для обнаружения слежки с дрона за человеком на улице полоска из светодиодов прикрепляется к его одежде.

Данный метод может быть реализован с помощью любого ноутбука, работающего на операционной системе (ОС) Linux. Пользователю не нужно иметь знания по вопросам защиты информации.

Источник: http://www.secnews.ru/foreign/23665.htm#axzz5AqvkPuIX (дата размещения материала 31.03.2018).

Представлен способ хищения данных через кабель питания компьютера

По информации, размещенной на сайте securitylab.ru, исследователи из университета имени Бен-Гуриона (Израиль) опубликовали доклад под названием «PowerHammer: эксфильтрация данных с физически изолированных компьютеров через электрическую сеть». В нем описан способ установки вредоносного программного обеспечения (ПО), регулирующего использование центрального процессора и создающего колебания электрического тока, способные модулировать и кодировать данные.

В зависимости от использованного атакующим подхода данные могут быть извлечены со скоростью от 10 до 1 тыс. бит в секунду. Скорость будет выше, если злоумышленнику удастся получить доступ к кабелю питания компьютера и ниже, если атакующий сможет подключиться только к электрической сети здания.

Разработанная исследователями вредоносная программа PowerHammer увеличивает загрузку процессора, выбирая ядра, которые в настоящее время не используются пользовательскими операциями (для избежания обнаружения). Для модуляции данных специалисты использовали метод частотной манипуляции, позволяющий передавать частоты с определенной амплитудой колебаний в качестве 1 и 0. Данные модулируются, кодируются и передаются поверх текущих колебаний тока, а затем перенаправляются и распространяются через линии электропередач. Этот феномен известен под названием «наведение помех».

Источник: https://www.securitylab.ru/news/492621.php (дата размещения материала 12.04.2018).

На GitHub опубликовано краткое пособие по взлому сетей Wi-Fi

По данным сайта anti-malware.ru, участник сообщества GitHub опубликовал краткое пособие, в котором рассматривается способ взлома сетей Wi-Fi, которые защищены слабыми паролями. Автор утверждает, что опубликованная информация поможет пользователям проверить безопасность собственных сетей. Описанная атака полностью пассивна, поэтому невозможно определить, что вы именно взламываете пароль, а не просто используете его для подключения. Также эксперт для ускорения процесса предлагает дополнительную атаку деаутентификации, описанную в конце опубликованного материала. Специалист призывает использовать его руководство исключительно в ознакомительных целях, либо же для проверки безопасности собственных сетей. За любое незаконное использование его метода автор не готов отвечать.

Источник: https://www.anti-malware.ru/news/2018-04-02-1447/25886 (дата размещения материала 02.04.2018).

Новые вредоносы в Google Play

Как информирует сайт news.rambler.ru, специалисты «Symantec» обнаружили 38 вредоносов в Google Play Store, замаскированных под игры и учебные приложения. Они скрывают свое существование на зараженных устройствах, удаляя свои значки с экрана и перенаправляют жертвы для установки другого приложения из Google Play Store, которое отображает рекламные объявления, и имеет минимальные дополнительные возможности. Вредоносные приложения были опубликованы в Play Store в декабре 2017 года.

Когда приложение установлено на устройстве, у него есть поддельное имя «Помощник». После запуска приложения оно немедленно вызывает API setComponentEnabledSettings, чтобы его значок удалялся с главного экрана, в то время как само приложение все еще активно работает в фоновом режиме. После запуска вредонос принудительно перенаправляет жертвы для установки другого приложения из Play Store. Расширенное приложение называется «Change my voice», имя пакета com.ModifySound.VoiceChanger, и разработано TopTech. Кроме того, что оно имеет простую функциональность для изменения голоса, оно также отображает большое количество рекламных объявлений.

Источник: https://www.news.rambler.ru/internet/39821442-novye-vredonosy-v-google-play/ (дата размещения материала 11.05.2018).

Вымогатель научился удалять антивирусы с компьютеров жертв

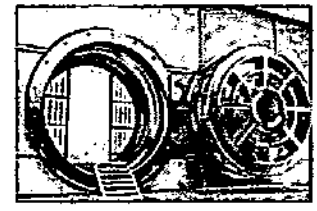
По данным, размещенным на сайте ursa-tm.ru со ссылкой на издание «Bleeping Computer», эксперты из «MalwareHunterTeam» обнаружили программу-вымогатель AVCrypt, которая блокирует работу установленных на компьютере антивирусов до того, как вся информация на устройстве будет зашифрована. AVCrypt удаляет службы ПО Windows Defender и Malwarebytes. Затем вымогатель запрашивает у системы информацию о других антивирусах, зарегистрированных в Центре обеспечения безопасности Windows, после чего пытается избавиться и от них через командную строку. При этом данный способ почему-то не работает с программой Emsisoft.

Исследователи отмечают, что никогда раньше не фиксировали деятельность вымогателей такого рода. Они предположили, что вирус может являться программой-вайпером, то есть создан для уничтожения информации на устройстве жертвы.

Источник: http://www.ursa-tm.ru/forum/index.php?/topic/272013-vymogatel-nauchilsya-udalyat-antivirusy-s%C2%A0kompyuterov-zhertv/ (дата размещения материала 28.03.2018).

Шпионский троян атакует российские банки

Согласно данным сайта threatpost.ru, центр по борьбе с киберугрозами Центробанка России предупредил финансово-кредитные организации страны об атаке трояна Dimnie, нацеленной на кражу денег и конфиденциальной информации. Dimnie известен с 2014 года и с тех пор несколько раз модернизировался, осваивая новые методы проникновения и кражи данных. На данный момент это многофункциональный шпионский троян с функциями удаленного администрирования и практически не оставляющий следов. Новый виток распространения трояна может привести к масштабным потерям – теоретически киберпреступники способны похищать средства банка через систему SWIFT или рабочее место клиента Банка России.



Программа использует бесфайловый метод заражения и плохо детектируется обычными антивирусами. Dimnie проникает на компьютер через спам-рассылку. Далее троян скачивает на устройство несколько дополнительных скриптов и начинает охоту за конфиденциальной информацией. Зловред собирает учетные данные пользователя, используя встроенный кейлоггер.

Пока злоумышленники не конвертировали полученную информацию в реальный ущерб. Центробанк России не располагает сведениями о выводе денег со счетов кредитных учреждений, однако угроза более чем реальна – интенсивность рассылок, содержащих троян, возрастает.

Источник: https://www.threatpost.ru/trojan-dimnie-attacks-russian-banks/25710/ (дата размещения материала 20.04.2018).

Новый вредонос устанавливает троян в загрузчик[4]

На сайте darkreading.com опубликована информация об обнаружении нового варианта известного вредоносного загрузчика VBScript, который позволяет удаленно контролировать жертву.

VBScript уже давно является вектором атаки, который устанавливает вредоносное ПО на зараженную машину. В рамках недавно обнаруженной кампании VBScript позволяет PHP-приложению получить контроль над компьютером и превратить его в часть ботнета. Новый ARS VBS Loader, описанный специалистами «Flashpoint», выполняет загрузку вредоносного ПО и обеспечивает удаленный доступ к контроллеру ботнета, что позволяет ARS VBS Loader являться одновременно загрузчиком вредоносного ПО и трояном.

Специалисты также отмечают уникальность механизма сохранения присутствия вредоноса на зараженной машине. Он передает данные об успешном внедрении на C&C-сервер и может загружать дополнительное вредоносное ПО с этого сервера. В результате злоумышленник может оперативно осуществлять изменение вектора атаки, профилей и т.д.

Источник: https://www.darkreading.com/attacks-breaches/new-malware-adds-rat-to-a-persistent-loader/d/d-id/1331559 (дата размещения материала 17.04.2018).

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 10 мая текущего года сайт банка данных угроз безопасности информации ФСТЭК России содержит 18485 (по каждой уязвимости дается описание по 20 полям) записей об уязвимостях ПО и 208 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.

---

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

В период с 24 марта по 10 мая 2018 года произведено семь обновлений базы данных сайта, в результате которых внесены сведения об одной угрозе безопасности информации и о 207 уязвимостях в 130 видах ПО.

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

Программа Scrcpy поможет управлять смартфоном на Android с компьютера

Как информирует сайт vistanews.ru, разработчик Р.Вимонт создал программу Scrcpy, с помощью которой можно управлять смартфоном с компьютера. Для удаленного управления необходимо иметь любое Android-устройство, и компьютер под управлением Windows, macOS или Linux. Для работы Scrcpy не нужно устанавливать на гаджет никаких посторонних программ. Вся работа производится через инструмент для отладки Android под названием Android Debug Brodge(ADB), который встроен в ОС.

В процессе работы Scrcpy создается небольшой сервер, который работает с получением и отправлением данных. Все действия мышки на компьютере транслируются в смартфон, и им можно удаленно управлять. Scrcpy не создает большой нагрузки на систему и поддерживает хорошую скорость трансляции данных. После завершения работы, Android Debug Brodge(ADB) не оставляет после себя никаких посторонних файлов, которые могут занимать свободное место.

Источник: https://www.vistanews.ru/computers/219116 (дата размещения материала 10.03.2018).

Опубликована седьмая версия рекомендаций CIS CONTROLS

По информации, размещенной на сайте securitylab.ru, представлена новая версия руководства по кибербезопасности CIS Controls Version 7, включающая в себя 20 рекомендаций по защите информационных технологий.

В новую версию руководства были внесены некоторые изменения. В частности, был изменен приоритет некоторых рекомендаций (рекомендации в руководстве отсортированы по степени важности) для того, чтобы лучше отражать текущую ситуацию в мире киберугроз. Помимо этого, все рекомендации в CIS Controls V7 были разделены на три категории: базовые, основополагающие и организационные.

В категории «Базовые» (CIS Controls 1-6) содержатся рекомендации по ключевым элементам управления, которые должны быть реализованы в каждой организации для обеспечения необходимой киберзащиты. В категорию «Основополагающих» (CIS Controls 7-16) попали меры по кибербезопасности, обеспечивающие четкие преимущества в области защиты от киберугроз для различных организаций. Категория «Организационные» (CIS Controls 17-20) ориентирована, в основном, на людей и процессы, связанные с

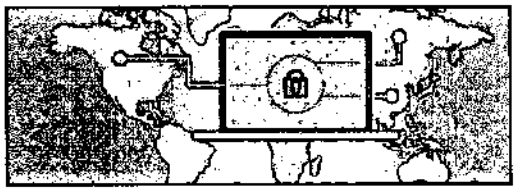
кибербезопасностью. В ней описаны такие меры по обеспечению безопасности, как правильная работа с персоналом и рекомендации по реагированию на инциденты.

Рекомендации CIS Controls обеспечивают четкое, приоритетное руководство, помогающее организациям решать самые распространенные проблемы в сфере киберугроз.

Источник: https://www.securitylab.ru/news/492247.php (дата размещения материала 04.04.2018).

МАИ и «HackerU» создали две образовательные программы по информационной безопасности

Как сообщается на сайте tproger.ru, Московский авиационный институт (МАИ) и автономная некоммерческая организация дополнительного профессионального образования «ВышТех», представляющая в России израильскую высшую школу информационной безопасности «HackerU», запускают совместные образовательные программы по подготовке специалистов в области кибербезопасности и программирования.



В конце апреля 2018 года на базе IT-центра МАИ стартовал курс «Профессиональный пентестинг». Его главные направления: этичный взлом, поиск уязвимостей, безопасность приложений и сетей, защита от DDoS-атак, повышение привилегий и постэксплуатации в Linux и в Windows.

Осенью 2018 года обещают запустить магистерскую программу «Кибербезопасность и инфокоммуникации». Она содержит расширенные курсы в области пентестинга и компьютерной криминалистики, четверть из которых являются практическими. Студенты, завершившие обучение, получат дипломы МАИ и международные сертификаты «HackerU». Самым успешным представится возможность попасть на прохождение стажировки в крупной IT-компании и последующее трудоустройство.

Источник: https://www.tproger.ru/news/hackeru-mai-safety/ (дата размещения материала 04.04.2018).

Национальный институт стандартов и технологий выпустил версию 1.1 руководства по защите от киберугроз[5]

На официальном сайте национального института стандартов и технологий NIST США nist.gov опубликована новая версия 1.1 популярного руководства Cybersecurity Framework. Новая версия сфокусирована на сферах, жизненно важных для обеспечения национальной и экономической безопасности, включая энергетику, банковское дело, телекоммуникации и оборону. В новой версии обновлены рекомендации в отношении аутентификации

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

и идентичности, самостоятельной оценки рисков кибербезопасности, обеспечения кибербезопасности в цепочках поставок, а также раскрытия информации об уязвимостях.

Источник: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework (дата размещения материала 16.04.2018).

Британский центр кибербезопасности заявил об опасности китайского сетевого оборудования

Как сообщает ряд сайтов, британский центр национальной кибербезопасности NCSC заявил о возможном риске, который несет интеграция оборудования китайской компании «ZTE» в сетевую инфраструктуру страны.

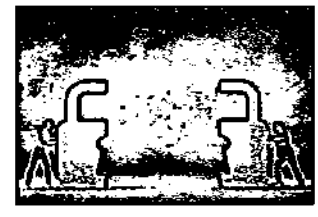
NCSC считает, что смягчить угрозы национальной безопасности, возникающие в связи с использованием оборудования или услуг компании «ZTE», невозможно в рамках существующей телекоммуникационной инфраструктуры Британии. Письма с соответствующим предупреждением уже направлены в британские телекоммуникационные компании. Какие именно угрозы несут в себе устройства «ZTE», не сообщается.

Ранее министерство торговли США объявило о лишении компании «ZTE» привилегий при поставках своей продукции в страну и вывозе оборудования за рубеж из-за многократных ложных заявлений, в том числе связанных с предоставлением профильных услуг в Иране и Северной Корее.

Источники: http://www.inforos.ru/ru/?module=news&action=view&id=65943 (дата размещения материала 16.04.2018); https://www.interfax.com.ua/news/telecom/499248.html.

Центробанк представил стандарт по аутсорсингу информационной безопасности финансовой системы

По информации сайта d-russia.ru, Банк России совместно с профессиональным сообществом разработал стандарт, который определяет процесс обеспечения информационной безопасности для финансовых организаций при использовании услуг аутсорсинга. Стандарт предназначен для банков, субъектов национальной платежной системы и других участников финансового рынка. Его положения имеют особое значение для деятельности малых и средних организаций, которым необходимо формировать и поддерживать на приемлемом уровне систему обеспечения информационной безопасности в условиях дефицита финансовых и кадровых ресурсов.



Стандарт определяет факторы риска нарушения информационной безопасности при аутсорсинге, устанавливает требования к управлению такими рисками, контролю за ними и их оценке. Кроме того, стандарт определяет зону ответственности и задачи руководства финансовых организаций при аутсорсинге услуг по обеспечению информационной безопасности, устанавливает

критерии оценки поставщика услуг и требования к содержанию соглашений об аутсорсинге.

Стандарт вступает в силу с 1 июля 2018 года. Он носит рекомендательный характер. В дальнейшем при необходимости может быть рассмотрен вопрос об его обязательном применении.

Источник: http://www.d-russia.ru/tsentrobank-predstavil-standart-po-autsorsingu-informatsionnoj-bezopasnosti-finansovoj-sistemy.html (дата размещения материала 30.03.2018).

В России учреждена Национальная ассоциация международной информбезопасности

По данным ряда сайтов, в России учреждена Национальная ассоциация международной информационной безопасности (НАМИБ). В ее задачи будет входить контроль соблюдения национальных интересов Российской Федерации

в информационной сфере, а также координация и содействие реализации государственной политики России в области кибербезопасности. В качестве учредителей новой ассоциации выступили МГУ им. Ломоносова, МГИМО, Дипломатическая академия МИД России, РАНХиГС, а также дочернее предприятие компании «Норникель».

Причиной создания НАМИБ стало прежде всего отсутствие четкого свода правил и практик, который бы позволил эффективно противостоять киберпреступности. Учитывая, что количество кибератак неуклонно растет, крайне важно оперативно реагировать и быстро ликвидировать угрозы. В настоящее время атаки с использованием эффективных вредоносных программ происходят по всему миру, злоумышленники практически никогда не ограничиваются одной страной, это еще один повод действовать сообща в противостоянии киберпреступникам. НАБИМ будет представлять собой некий центр научных и методических компетенций в сфере информационной безопасности, который будет вырабатывать соответствующие научные и экспертные рекомендации для органов принятия решений. При этом будут учитываться интересы как общества, так и бизнеса, и, разумеется, государства.

Источники: https://www.anti-malware.ru/news/2018-04-12-1447/25984 (дата размещения материала 12.04.2018); http://www.tass.ru/obschestvo/5111643.

Агентство национальной безопасности объясняет, как борется с уязвимостями нулевого дня[6]

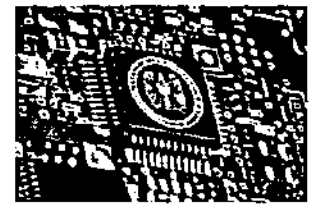
По информации сайта muyseguridad.net, на конференции в Сан-Франциско технический директор АНБ США выступил с докладом, посвященным анализу лучших практик защиты информации, которые они используют внутри своего ведомства. По его словам, при обнаружении каждой новой уязвимости или эксплойта у агентства есть самое большее 24 часа для разработки

---

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

и выпуска патча. У частных компаний для принятия защитных мер иногда уходят недели, а то и месяцы.

Большинство атак против АНБ – это фишинг и атаки на системы с неустраненными уязвимостями. Поэтому лучшая защита – это обновление используемого ПО. Дисциплинированность в этом вопросе позволила последние 24 месяца не страдать от эксплуатации уязвимостей нулевого дня. В 2017 году 93% уязвимостей были предотвращены посредством своевременного обновления всего ПО.



Источник: https://www.muyseguridad.net/2018/04/20/nsa-combate-vulnerabilidades-zero-day/ (дата размещения материала 20.04.2018).

Кибернетическое командование США пересматривает свои позиции[7]

Как сообщается на сайте militaryaerospace.com, кибернетическое командование США выпустило новую стратегию, целью которой является достижение и поддержание превосходства в киберпространстве. Стратегия имеет пять основных постулатов, один из которых заключается в исследовании новейших технологий для обеспечения превосходства над возможностями вероятного противника. Другие четыре постулата требуют: обеспечения киберпревосходства для реализации операций во всех пространствах; развития информационного преимущества для поддержки операционных результатов путем расширения вариантов ведения информационной войны; обеспечения гибкости и скорости при ведении кибероперациий в инвестиционной и политической областях, а также расширения партнерских отношений с частным сектором, другими учреждениями и союзниками.

Источник: http://www.militaryaerospace.com/articles/pt/2018/03/u-s-cyber-command-revamps-its-vision-aims-to-maintain-superiority-in-cyber-security.html (дата размещения материала 27.03.2018).

В Нью-Йорке будут реализованы инструменты общественной кибербезопасности

По информации сайта anti-malware.ru, мэр Нью-Йорка Б.Де Блазио объявил, что в городе реализованы меры кибербезопасности, которые помогут защитить жителей от вредоносной активности, особенно это касается мобильных устройств. Уже летом этого года жители города смогут воспользоваться нововведениями, для этого надо будет загрузить бесплатное приложение под названием NYC Secure. Приложение будет предупреждать пользователей смартфонов о потенциальных угрозах, которые могут находить-

---

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

ся на устройстве, а также давать некие советы по обеспечению безопасности. Среди подобных советов будут рекомендации отключиться от известной вредоносной сети Wi-Fi, закрыть страницы вредоносного сайта и удалить вредоносные приложения. Само приложение при этом не будет предпринимать никаких действий самостоятельно. Кроме того, NYC Secure не будет собирать и передавать конфиденциальную информацию пользователей. Также в Нью-Йорке реализуют безопасность общедоступных сетей Wi-Fi, которые любят использовать злоумышленники для перехвата трафика по незашифрованным каналам.

Источник: https://www.anti-malware.ru/news/2018-03-30-1447/25869 (дата размещения материала 30.03.2018).

Британия готова атаковать российские компьютерные сети

Согласно информации, размещенной на сайте vpk-news.ru со ссылкой на газету «Sunday Times», британские спецслужбы готовы атаковать российские компьютерные сети в ответ на возможные «агрессивные» действия Москвы в киберпространстве. В разработке ответных мер принимают участие центр правительственной связи и министерство обороны.

По данным газеты, Лондон ожидает кибератаки на ключевые объекты инфраструктуры страны, в частности на учреждения системы здравоохранения. Кроме того, британская разведка полагает, что Россия может распространить в Интернете компромат на членов британского кабинета министров, парламентариев и других высокопоставленных лиц. Предупреждение разведслужб получила лично премьер-министр Т.Мэй.

Источник: https://www.vpk-news.ru/news/42206 (дата размещения материала 15.04.2018).

Правительство Франции планирует перейти на отечественный защищенный мессенджер уже к лету

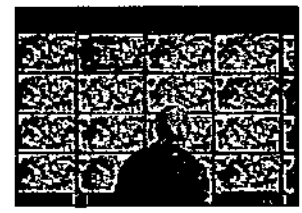
Как сообщается на сайте d-russia.ru со ссылкой на агентство «Reuters», правительство Франции разрабатывает собственную зашифрованную службу обмена сообщений, чтобы минимизировать возможность доступа иностранных организаций к переписке высших должностных лиц государства. Беспокойство французских должностных лиц вызывает то, что ни один из популярных мессенджеров (в частности WhatsApp и Telegram, которым активно пользуется президент Макрон) не хранит информацию пользователей на серверах во Франции. Планируется, что использование нового мессенджера станет обязательным для всего правительства к лету.

Ранее в этом году на телефоны французских чиновников было установлено специализированное ПО, препятствующее использованию WhatsApp и Telegram.

Источник: http://www.d-russia.ru/pravitelstvo-frantsii-planiruet-perejti-na-otechestvennyj-zashhishhennyj-messendzher-uzhe-k-letu.html (дата размещения материала 17.04.2018).

В Эстонии прошли киберучения НАТО

По информации ряда сайтов, масштабные международные киберучения «Locked Shields» («Закрытые щиты»), в которых приняли участие почти тысяча человек из 30 стран, прошли с 23 по 27 апреля в Эстонии. Учения проводились с целью тренировки специалистов в области защиты информационных систем и критической инфраструктуры от кибератак. В соответствии со сценарием учений, вымышленная страна «Берилия» сталкивается с ухудшением ситуации в области безопасности, которая сопровождается серией враждебных действий и скоординированными кибератаками против гражданского интернет-провайдера и военной авиабазы. Атаки вызывают серьезные сбои в работе электросети, сетей общественной безопасности, других важных компонентов инфраструктуры.



Locked Shields – одни из крупнейших киберучений в мире, они проводятся с 2010 года. Североатлантический совет НАТО в 2008 году утвердил аккредитацию центра кибербезопасности НАТО в Таллине и присвоил ему статус международной военной организации. Сейчас в работе центра участвуют 20 государств: США, Эстония, Германия, Франция, Великобритания, Бельгия, Словакия, Италия, Литва, Латвия, Испания, Венгрия, Чехия, Польша, Голландия, Греция, Турция. Не входящие в НАТО Австрия, Финляндия и Швеция являются странами-партнерами центра.

Источники: https://www.ghall.com.ua/2018/04/24/v-estonii-startovali-kiberucheniya-nato/ (дата размещения материала 24.04.2018); https://www.securitylab.ru/news/492895.php.

В Токио создали единый центр
борьбы с киберпреступностью

Как сообщает ряд сайтов со ссылкой на информационное агентство «Kyodo», единый центр борьбы с киберпреступностью в составе 500 следователей и аналитиков открыт в японской столице. Он будет действовать в рамках токийского полицейского управления.

Ранее специалисты по преступлениям в виртуальном пространстве были разбросаны по различным подразделениям полиции и других служб безопасности. Теперь их решено собрать вместе для активизации борьбы с нарастающим количеством правонарушений в киберпространстве.

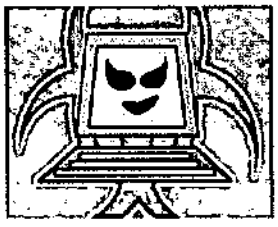
Источники: http://www.tass.ru/ekonomika/5086403 (дата размещения материала 02.04.2018); https://www.360tv.ru/news/nauka_i_tehnologiya/edinyj-tsentr-borby-s-kiberprestupnostju-pojavilsja-v-tokio/.

1.3. Обеспечение безопасности значимых объектов критической информационной инфраструктуры

«Positive Technologies» обнаружила опасные уязвимости в оборудовании «Siemens» для электроподстанций

По данным сайта ptsecurity.com, эксперты «Positive Technologies» выявили уязвимости высокого уровня риска в устройствах релейной защиты и автоматики (РЗиА) производства «Siemens», которые используются для управления и защиты силового оборудования на электроэнергетических объектах. «Siemens» уже устранила уязвимости и выпустила соответствующие рекомендации.

Обнаруженным уязвимостям могут быть подвержены устройства SIPROTEC 4, SIPROTEC Compact и Reyrolle, использующие коммуникационный модуль EN100 и ПО DIGSI 4. Эксплуатируя эти уязвимости, злоумышленник мог удаленно внести изменения в конфигурацию отдельно взятых устройств РЗиА, что могло привести к отказу функции защиты силового оборудования или отключению потребителей.

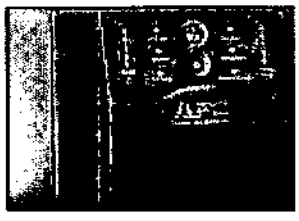


Наибольшая опасность связана с уязвимостью CVE-2018-4840, которая может эксплуатироваться удаленно, при этом от злоумышленников не требуется высокий уровень квалификации. Механизм работы позволяет неаутентифицированному удаленному пользователю загружать модифицированную конфигурацию устройства посредством перезаписи авторизационных паролей доступа. Вторая уязвимость (CVE-2018-4839) дает возможность атакующему получить полный доступ к устройству. Нарушитель может, перехватив сетевой трафик или получив данные от устройства, восстановить пароли авторизации доступа к устройствам. Третья уязвимость (CVE-2018-4838) позволяет злоумышленнику удаленно загрузить более старую версию прошивки с известными недостатками безопасности и тем самым дает возможность выполнения кода на целевой системе.

Источник: https://www.ptsecurity.com/ru-ru/about/news/291869/ (дата размещения материала 10.04.2018).

«Positive Technologies» выявила критически опасные уязвимости в источниках бесперебойного питания APC

Как сообщает сайт ptsecurity.com, эксперты «Positive Technologies» обнаружили четыре уязвимости в модулях управления сетевыми источниками бесперебойного питания APC компании «Schneider Electric», которые используются в промышленности, медицине, нефтегазовом секторе, центрах обработки данных, системах управления зданиями и в других сферах. Две уязвимости получили оценку в 10 баллов по шкале CVSS v. 3, что соответствует наивысшему уровню опасности.



Проблемы безопасности выявлены в модулях управления APC MGE SNMP/Web Card Transverse 66074, установленных в источниках бесперебойного питания Galaxy 5000/6000/9000, EPS 7000/8000/6000, Comet UPS/3000, Galaxy PW/3000/4000, STS (Upsilon и Epsilon).

Первая уязвимость CVE-2018-7243 (оценка 10) во встроенном веб-сервере (порт 80/443/TCP) позволяет удаленному злоумышленнику в обход системы аутентификации получить полный доступ к управлению бесперебойником, что представляет угрозу непрерывности работы подключенного к электросети оборудования. Вторая уязвимость встроенного веб-сервера (порт 80/443/TCP) заключается в возможности получения «чувствительной информации» об источнике бесперебойного питания (оценка 5,3). Эксплуатация третьей уязвимости (оценка 7,3) позволяет злоумышленнику без авторизации изменить различные параметры устройства, в том числе параметры отключения.

Четвертая уязвимость (оценка 10) дает удаленному злоумышленнику возможность перехватить данные учетной записи администратора. Если на устройстве не активирован SSL, при запросе страницы контроля доступа данные аккаунта будут отправлены в открытом виде.

Источник: https://www.ptsecurity.com/ru-ru/about/news/292101/ (дата размещения материала 20.04.2018).

В приложении «Siemens» для промышленных систем обнаружена опасная уязвимость

Как сообщает сайт itsec.ru, в мобильном приложении Siemens SIMATIC WinCC OA Operator для iOS, предназначенном для управления промышленными системами, обнаружена опасная уязвимость. CVE-2018-4847 представляет собой уязвимость раскрытия информации в файлах и каталогах. Ее успешная эксплуатация может позволить злоумышленнику с физическим доступом прочитать конфиденциальные данные, находящиеся в каталоге приложения.

«Siemens» опубликовала ряд рекомендаций для предотвращения эксплуатации уязвимости. Пользователям рекомендуется отказаться от сохранения пароля при входе в систему и выходить из системы после каждого рабочего сеанса.

Simatic WinCC OA Operator – бесплатное приложение для iOS, позволяющее контролировать и управлять промышленными объектами с помощью мобильного устройства. Программа обменивается данными через HTTPS-сервер с использованием интерфейса SSL-RPC.

Источник: http://www.itsec.ru/newstext.php?news_id=122659 (дата размещения материала 23.04.2018).

В промышленном ПО Omron CX-One обнаружены опасные уязвимости

По данным сайта securitylab.ru, в ПО для конфигурации промышленного оборудования Omron CX-One обнаружено три опасных уязвимости, позволяю-

щие злоумышленнику вызвать переполнение буфера и получить несанкционированный доступ (НСД) к определенным объектам. Совместная эксплуатация данных уязвимостей может привести к удаленному выполнению произвольного кода.

Первая уязвимость представляет собой проблему парсинга файлов проекта и может вызвать переполнение буфера в куче. Вторая уязвимость аналогична первой, однако может вызвать переполнение буфера в стеке. Третья уязвимость является проблемой анализа недоработанных файлов проекта и может позволить указателю вызвать неправильный объект, что приведет к доступу к ресурсу с использованием несовместимого типа.

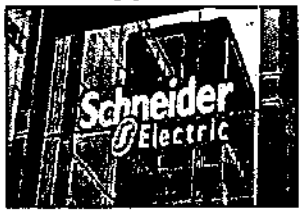
Компания-производитель уже выпустила соответствующие исправления.

Источник: https://www.securitylab.ru/news/492596.php (дата размещения материала 11.04.2018).

Критическая уязвимость ставит под угрозу безопасность электростанций

Как информирует сайт anti-malware.ru, исследователи из компании «Tenable» обнаружили баг в ПО компании «Schneider Electric», которое широко используется в промышленности. Уязвимость обнаружена в ПО InduSoft Web Studio и InTouch Machine Edition, которые служат промежуточным звеном между промышленным оборудованием и оператором.

По мнению исследователей, с помощью этого бага злоумышленник может нарушить или полностью прекратить работу электростанций или других критически важных объектов промышленности. Киберпреступник может без авторизации отправить вредоносный пакет данных и вызвать переполнение буфера. После этого злоумышленник получает возможность выполнить произвольный код в уязвимой системе. Использовать атаку можно разными способами. Злоумышленник может использовать уязвимость для DDoS-атаки и взломать удаленное управление операционного центра. Также баг можно использовать, чтобы закрепиться в сети для доступа к другим объектам производства. В этом случае злоумышленник может отправить команды в некоторые физические центры управления электростанцией или промышленного комплекса.



Метод относительно прост потому, что требуется только интерпретатор командной строки и доступ к Интернету. «Schneider Electric» уже выпустила обновления безопасности, которые минимизируют потенциальные угрозы проникновения в систему.

Источник: https://www.anti-malware.ru/news/2018-05-04-107504/26162 (дата размещения материала 04.05.2018).

Как защитить промышленные системы управления от хакеров, финансируемых государствами[8]

Согласно информации сайта darkreading.com, американская группа реагирования на киберинциденты US-CERT выпустила предупреждение в отношении деятельности российских хакеров против секторов критической инфраструктуры, включая энергетику, авиацию и критическое производства. Атаки, в которых подозреваются российские хакеры, не бессистемные, они хорошо спланированы, состоят их нескольких этапов и предназначены для того, чтобы закрепиться в критических областях для последующей реализации еще более масштабных атак.

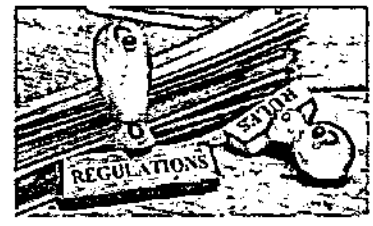
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Единственным путем обеспечения безопасности значимых объектов критической информационной инфраструктуры является использование методов анализа сетевых данных. Эти методы менее уязвимы по сравнению с другими инструментами обеспечения безопасности к взлому и стиранию информации атакующими и не требуют полномасштабных обновлений или установки современного ПО на существующие системы.

Источник: https://www.darkreading.com/attacks-breaches/how-to-protect-industrial-control-systems-from-state-sponsored-hackers/a/d-id/1331529 (дата размещения материала 19.04.2018).

Новый стандарт безопасности для промышленных АСУ

Как сообщает сайт threatpost.ru, семейство стандартов ISA/IEC 62443, посвященных безопасности промышленных автоматизированных систем управления (АСУ), пополнилось новым документом. Регламент ISA/IEC 62443-4-1-2018 определяет требования к обеспечению жизненного цикла продукта. Он затрагивает все этапы разработки АСУ.



Новый стандарт касается прежде всего деятельности разработчиков систем. Положения документа включают базовую терминологию в сфере безопасности, определяют требования к дизайну, дают рекомендации по написанию исходного кода и устанавливают принципы тестирования, а также подходы к управлению дефектами. Регламент не затрагивает эксплуатацию конечного продукта с точки зрения пользователя или системного интегратора, а фокусируется на создании поставщиком безопасной инфраструктуры для работы АСУ. Одним из важнейших разделов документа является блок «Управление исправлениями безопасности», описывающий процедуру выпуска патчей для промышленных систем управления.

Серия стандартов ISA/IEC 62443 разрабатывается комитетом ISA99 для использования в качестве национальных стандартов США и одобрена Международной электротехнической комиссией IEC.

---

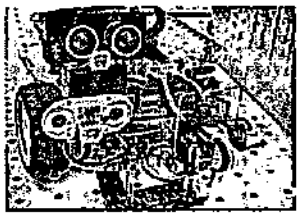
[8] Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

Источник: https://www.threatpost.ru/new-isaiec-security-standard-for-automated-control-systems-issued/25381/ (дата размещения материала 30.03.2018).

Робот «HoneyBot» призван защищать промышленную автоматику, отвлекая хакеров на себя

По информации сайта xakep.ru, группа специалистов из технологического института Джорджии создала небольшого робота «HoneyBot», который призван защищать промышленную автоматику, отвлекая внимание хакеров на себя.

К примеру, атака на АСУ ТП, в теории, может заставить конвейер крупной фабрики остановиться, что повлечет за собой огромные убытки; хуже того, неполадки в работе промышленного манипулятора могут стоить жизни людям. Подобные сценарии атак на промышленных и домашних роботов ранее уже описывали и демонстрировали эксперты в области информационной безопасности.



Задача «HoneyBot» крайне проста. Робот представляет собой идеальную приманку для потенциальных злоумышленников. Взломав робота, они получат возможность убедиться, что имеют дело с настоящей машиной, например, смогут манипулировать показателями сенсоров и удостовериться, что контролируют происходящее. В свою очередь, обнаружив атаку, «HoneyBot» немедленно поднимет тревогу и уведомит о происходящем своих операторов.

Источник: https://www.xakep.ru/2018/04/03/honeybot/ (дата размещения материала 03.04.2018).

Обеспечение безопасности АСУ ТП в соответствии с современными стандартами

Как информирует журнал «ИСУП», вышла в свет новая книга для специалистов в области безопасности техногенных систем «Обеспечение безопасности АСУ ТП в соответствии с современными стандартами».

Подробно рассмотрены требования к безопасности АСУ ТП международного стандарта МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью», дана их интерпретация для практического воплощения. Последовательно раскрыты конкретные шаги, необходимые для получения сертификата соответствия МЭК 61508. Особое внимание уделено подготовке к сертификации, в том числе определению объекта сертификации, проектной инфраструктуры, плана и сметы затрат на выполнение работ. Рассмотрены требования стандарта, относящиеся к управлению безопасностью, предложены методы ее количественного оценивания и меры по ее обеспечению. Дан набор упражнений для закрепления навыков в области обеспечения и оценивания функциональной безопасности.

Источник: ИСУП, 2018, № 1, с. 27.

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

ПАК средств защиты от несанкционированного доступа «Аккорд-АМДЗ»

Как сообщается на сайте accord.ru, программно-аппаратный комплекс (ПАК) средств зашиты информации от НСД «Аккорд-АМДЗ», разработанный компанией ОКБ «САПР», представляет собой аппаратный модуль доверенной загрузки для IBM-совместимых компьютеров – серверов и рабочих станций локальной вычислительной сети, обеспечивающий защиту устройств и информационных ресурсов от НСД.

Комплекс начинает работу сразу после выполнения системного кода BIOS компьютера – до загрузки ОС. Контроллеры семейства «Аккорд-АМДЗ» обеспечивают доверенную загрузку ОС, поддерживающих наиболее распространенные файловые системы.

Соответствие изделия методическому документу ФСТЭК России «Требования к средствам доверенной загрузки» и профилю защиты ИТ.СДЗ.ПР4.ПЗ подтверждается сертификатом № 3879.

Источник: http://www.accord.ru/amdz.html (дата размещения материала 03.04.2018).

Универсальный шлюз безопасности «UserGate UTM»

Как информирует сайт entensys.com, компании «еСЛ Девелопмент» и «Юзергейт» выпустили универсальный шлюз безопасности «UserGate UTM», который объединяет межсетевой экран нового поколения, систему обнаружения вторжений, защиту от вредоносных программ и вирусов, систему контент-фильтрации, серверный антиспам, VPN-сервер и другие функции в едином решении, удобном для установки и администрирования. В продукте также реализованы всевозможные функции, более востребованные крупными организациями. К ним относятся контроль доступа, основанный на идентификации пользователя, балансировка нагрузки, управление полосой пропускания, предотвращение угроз, анализ SSL, распознавание приложений и другие.

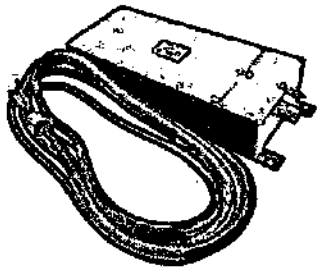
«UserGate UTM» позволяет обеспечить безопасность корпоративной сети от внешних интернет-угроз, обеспечить управление трафиком и шириной канала, контролировать политики доступа в Интернет и использование интернет-приложений, а также обеспечивать безопасность электронной почты.

Шлюз доступен в различных аппаратных исполнениях, предназначенных для широкого диапазона объектов – от малых предприятий до центров обработки данных и объектов со сложными природными и климатическими условиями.

Источник: http://www.entensys.com/ru/products/usergate-utm/overview (дата размещения материала 03.05.2018).

Фильтр сетевой помехоподавляющий «ФП-6МА»

По информации сайта filtr-fp.ru, компания «Специальное и профессиональное оборудование» разработало фильтр сетевой помехоподавляющий «ФП-6МА», который предотвращает утечки информации по цепям электропитания, а также защищает средства оргтехники от внешних помех. Фильтр ослабляет любые сигналы в диапазоне 0,02-10 ГГц и, соответственно, не пропускает информативные сигналы, возникающие при работе оргтехники.



Изделие соответствует требованиям методического документа «Требования к пассивным средствам защиты информации от утечки за счет побочных электромагнитных излучений и наводок на линии электропитания», что подтверждается сертификатом соответствия ФСТЭК России.

Фильтр «ФП-6МА» может использоваться для защиты сведений, составляющих государственную тайну, и устанавливаться в выделенных помещениях до 1 категории.

Источник: http://www.filtr-fp.ru/produktsiya/filtr-fp-6ma-40a-detail (дата размещения материала 03.05.2018).

Мобильный телефон для закрытой правительственной связи разработали в Белоруссии

Мобильный телефон для закрытой правительственной связи, имеющий высокую степень защиты информации, разработали в Белоруссии. Новинку продемонстрировал председатель Комитета госбезопасности республики В.Вакульчик.

По его словам, данная модель телефона позволяет вести разговоры «с высокой степенью защищенности от прослушиваний и перехвата». Также «телефон защищен от проникновения злоумышленников». Если будет попытка вскрытия, предусматривается «самоуничтожение» содержимого аппарата.

Источники: http://tass.ru/mezhdunarodnaya-panorama/5172863 (дата размещения материала 01.05.2018); https://tvzvezda.ru/news/vstrane_i_mire/content/201805030101-o02n.htm.

Программное изделие «Kaspersky Anti Targeted Attack Platform»

Как сообщает сайт kaspersky.ru, программное изделие «Kaspersky Anti Targeted Attack Platform», созданное АО «Лаборатория Касперского», предназначено для защиты ИТ-инфраструктуры организации путем обнаружения угроз, таких как атаки «нулевого дня» и целевые атаки при

помощи анализа сетевого взаимодействия информационной системы и внешних сетей.

Изделие «Kaspersky Anti Targeted Attack Platform» реализует следующие функции безопасности: аудит безопасности; идентификация и аутентификация; управление безопасностью; защита данных; анализ собранных данных; сбор данных о событиях и активности в контролируемой информационной системе; реагирование на вторжения и нарушения безопасности; обновление базы решающих правил и базы данных признаков вредоносных компьютерных программ (вирусов).

Изделие соответствует требованиям методического документа ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 4 уровню контроля, что подтверждается сертификатом № 3854.

Источник: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform (дата размещения материала 03.04.2018).

Вышла новая версия межсетевого экрана «Traffic Inspector»

На сайте servernews.ru компания «Смарт-Софт» сообщила о выпуске новой версии программного решения «Traffic Inspector 3.0.2», которое представляет собой шлюз безопасности с межсетевым экраном для контроля и защиты интернет-доступа в корпоративных компьютерных сетях. Решение обеспечивает защищенное подключение всех рабочих станций организации к ресурсам глобальной сети и антивирусную защиту, предотвращает доступ в корпоративную сеть извне, блокирует вредоносные сайты, в том числе по критерию недопустимого контента, ведет учет сетевого трафика. Продукт рассчитан на использование в среде ОС Windows и устанавливается на выполняющем функции шлюза для LAN-сети сервере. Администрирование выполняется в графическом режиме через оснастку Microsoft Management Console.

В новой версии «Traffic Inspector» доработкам подверглись ядро программного комплекса, планировщик, средства мониторинга и формирования отчетов. Были расширены возможности SMS-идентификации пользователей, добавлена функция редиректа для HTTPS-ресурсов, обновлен SDK Traffic Inspector Antivirus Powered by Kaspersky и исправлены ошибки в различных модулях продукта. Шлюз безопасности теперь не поддерживает ОС Windows с версией ядра ниже 6.0.

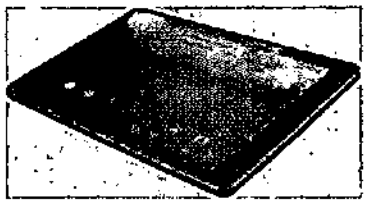
Программный комплекс «Traffic Inspector» сертифицирован ФСТЭК России и может быть использован как в государственных информационных системах (ГИС), так и для защиты информации в информационных системах персо-

нальных данных (ИСПДн) в организациях здравоохранения, образования, коммерческих компаниях.

Источник: https://www.servernews.ru/967598 (дата размещения материала 27.03.2018).

Планшет «AtPAD»

Как информирует журнал «InformationSecurity», ОКБ САПР разработало планшет «AtPAD», который позволяет мобильно обрабатывать информацию с высоким уровнем защищенности. Изделие может поставляться с ОС Windows или Linux.



В планшете установлено средство доверенной загрузки «Аккорд-АМДЗ» на базе контроллера «Аккорд-СХМ2™», соответствующее сертификату ФСБ России, что обеспечивает среду функционирования криптографии для сертифицированного средства защиты конфиденциальной информации, требующего наличия аппаратно-программного модуля доверенной загрузки класса 1Б.

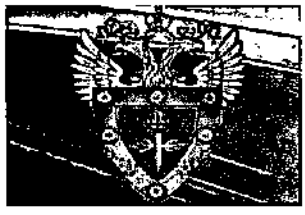
На российском рынке планшет появится во втором полугодии 2018 года.

Источник: InformationSecurity, 2018, № 1, с. 48.

О получении сертификата ФСТЭК России на новую линейку решений «UserGate»

На сайте ib-bank.ru компания «UserGate» сообщает о получении сертификата ФСТЭК России на универсальный шлюз безопасности «UserGate UTM». Сертификация была пройдена по требованиям к межсетевым экранам (4-й класс, профили А и Б) и по требованиям к системам обнаружения вторжений (4-й класс) для программно-аппаратных (модели UserGate C, D, D+, E, E+, F, X1) и виртуальных платформ «UserGate».

«UserGate» может использоваться в составе автоматизированных систем до класса защищенности 1Г и в ИСПДн и ГИС до 1 класса (уровня) защищенности включительно.

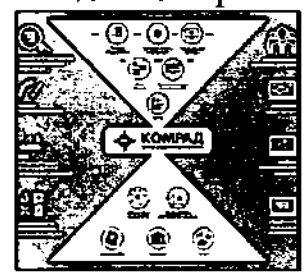


«UserGate» является комплексным решением по обеспечению безопасности компьютерных сетей любого размера. В его основе лежит ОС UG OS, обеспечивающая всестороннюю защиту, а также специально адаптированная и оптимизированная аппаратная часть. С 2016 года данное решение успешно используется как в органах власти, так и на предприятиях финансовой, энергетической, производственной, агропромышленной сфер, в образовании и здравоохранении. Во многих проектах «UserGate» успешно замещает ранее использовавшиеся зарубежные аналоги.

Источник: https://www.ib-bank.ru/news/9085 (дата размещения материала 30.03.2018).

Минобороны России сертифицировало систему управления событиями ИБ «Комрад»

Как сообщает сайт servernews.ru, НПО «Эшелон» сообщило об успешном прохождении сертификационных испытаний на соответствие стандартам Минобороны России программного комплекса «Комрад», совместимого с отечественными средствами защиты информации и предназначенного для централизованного управления событиями информационной безопасности (ИБ).



Система «Комрад» позволяет IT-службам осуществлять централизованный мониторинг событий ИБ, выявлять инциденты ИБ, оперативно реагировать на возникающие угрозы, а также выполнять требования, предъявляемые регуляторами к защите персональных данных, в том числе, к обеспечению безопасности ГИС.

Выданным ведомством сертификат подтверждает соответствие системы «Комрад» требованиям Минобороны России по 2 уровню контроля отсутствия недекларированных возможностей.

Источник: https://www.servernews.ru/967536 (дата размещения материала 26.03.2018).

«JaCarta Management System» прошла инспекционный контроль во ФСТЭК России

На ряде сайтов компания «Аладдин Р.Д.» сообщила о том, что актуальная версия корпоративной системы управления жизненным циклом средств аутентификации и электронной подписи «JaCarta Management System» (JMS) версии 3.3 прошла инспекционный контроль во ФСТЭК России. Результаты проверки гарантируют, что система создана с учетом требований к обеспечению ИБ и надежности работы, предъявляемым крупными государственными и корпоративными заказчиками.

Обновленный сертификат ФСТЭК России удостоверяет, что JMS является программным средством управления средствами аутентификации, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям руководящих документов ФСТЭК России. Это позволяет использовать JMS в ИСПДн до 1 уровня защищенности включительно и ГИС до 1 класса защищенности включительно, а также при создании автоматизированных информационных систем до класса защищенности 1Г включительно.

Источники: http://www.safe.cnews.ru/news/line/2018-03-26_jacarta_manage-ment_system_33_proshla_inspektsionnyj (дата размещения материала 26.03.2018); https://www.servernews.ru/967534.

«Positive Technologies» представила технологическую платформу для построения центров ГосСОПКА

На своем сайте ptsecurity.com компания «Positive Technologies» сообщила о выпуске решения «PT Platform 187», предназначенного для создания корпоративных и ведомственных центров ГосСОПКА. «PT Platform 187» включает набор технических средств, необходимых для взаимодействия с Национальным координационным центром компьютерных инцидентов (НКЦКИ) и построения

эффективной системы безопасности объектов критической информационной инфраструктуры (КИИ) в рамках федерального закона № 187-ФЗ.

Решение позволит: получать данные о событиях информационной безопасности из различных источников, автоматически их анализировать и выявлять инциденты; обнаруживать уязвимости и контролировать их устранение; проводить ретроспективный анализ при расследовании инцидентов; инвентаризировать информационные ресурсы и поддерживать сведения об инфраструктуре в актуальном состоянии; контролировать процессы реагирования на инциденты, ликвидации их последствий и взаимодействовать с НКЦКИ.

В первую очередь, решение будет интересно региональным органам власти, госучреждениям, обеспечивающим информационную безопасность госструктур, дочерним организациям крупных предприятий с отдельной ИТ-инфраструктурой, которые являются субъектами значимых объектов.

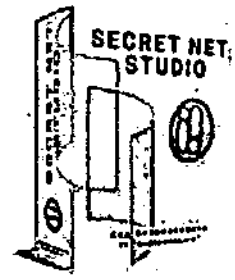
В «PT Platform 187» объединены 5 продуктов собственной разработки «Positive Technologies»: система контроля защищенности «MaxPatrol 8», система мониторинга событий и выявления инцидентов ИБ «MaxPatrol SIEM», система комплексного анализа сетевого трафика «PT Network Attack Discovery», система выявления вредоносного контента «PT MultiScanner» и «ПТ Ведомственный центр» – система управления инцидентами и взаимодействия с НКЦКИ. Продукты могут использоваться для выполнения методических рекомендаций
ФСБ России по построению центров ГосСОПКА, требований ФСТЭК России к системам безопасности значимых объектов КИИ и к обеспечению их безопасности, а также требований проекта приказа ФСБ России к техническим средствам ГосСОПКА.

Источник: https://www.ptsecurity.com/ru-ru/about/news/292165/ (дата размещения материала 24.04.2018).

Вышел «Secret Net Studio 8.4» с централизованным управлением «Secret Net LSP»

На сайте itweek.ru компания «Код безопасности» объявила о выходе новой версии продукта «Secret Net Studio», предназначенного для комплексной защиты рабочих станций и серверов от внешних и внутренних угроз. В «Secret Net Studio» версии 8.4 увеличена производительность ряда механизмов продукта, а также повышено удобство инструментов управления и мониторинга. Од-

ним из главных функциональных новшеств версии 8.4 является возможность централизованного управления клиентами под ОС Linux с установленным средством защиты информации «Secret Net LSP» версии 1.7.



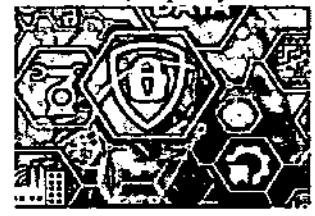
«Secret Net Studio 8.4» выпускается в двух редакциях: «Secret Net Studio» (для защиты конфиденциальной информации) и «Secret Net Studio-C» (для защиты гостайны). Редакция «Secret Net Studio» содержит антивирусный модуль и модуль системы обнаружения и предотвращения вторжений. Обе редакции «Secret Net Studio 8.4» будут переданы на инспекционный контроль в системе сертификации ФСТЭК России.

Источник: https://www.itweek.ru/security/news-company/detail.php?ID=20499 (дата размещения материала 20.04.2018).

R2D2 поможет защититься от программ-вайперов

По данным сайта threatpost.ru, американские исследователи университета Пердью представили технологию, которая в будущем может стать надежной защитой от зловредов, уничтожающих пользовательские данные. Они назвали свою разработку R2D2 – Reactive Redundancy for Data Destruction («своевременная реакция на удаление данных»).

Метод заключается в создании точки восстановления системы при выявлении характерных для программ-вайперов операций. Как известно, при удалении файла ОС не стирает его физически, а помечает занимаемое им пространство как свободное. Чтобы не дать пользователю восстановить данные, вредоносное ПО заполняет их место на жестком диске случайной информацией. R2D2 способен отслеживать такую «мусорную» активность, игнорируя при этом обычные операции удаления. Таким же образом новая технология идентифицирует работу специальных программ безопасного уничтожения данных. Система распознает 13 наиболее популярных методов очистки, которые применяются в подобных утилитах. Если она замечает на устройстве похожие процессы, то создает резервные копии файлов.



Пока R2D2 существует в качестве прототипа, функционирующего на виртуальной машине в среде Windows 7. Применение эмулятора обусловлено принципом работы программы – она должна находиться вне ОС, чтобы иметь возможность отслеживать подозрительную активность. По мнению специалистов, нет никаких препятствий для развертывания системы на других версиях Windows, а также на Linux-платформах.

Прототип показал блестящие результаты – из 989 деструктивных действий были пропущены всего два, а на таком же количестве легальных операций с файлами произошло лишь пять ложных срабатываний.

Источник: https://www.threatpost.ru/r2d2-protects-from-wipers/25231/ (дата размещения материала 23.03.2018).

Браузер, скрывающий IP-адрес

Как информирует сайт edtechrussia.ru, практически все современные веб-сайты и интернет-форумы записывают реальный IP-адрес каждого посетителя. Это позволяет при необходимости легко заблокировать ему возможность входить на сайт. Но, кроме этого, по IP-адресу возможно разыскать реального человека, который с этого адреса выходит в Интернет. Поэтому при работе в сети Интернет желательно маскировать свой IP-адрес.

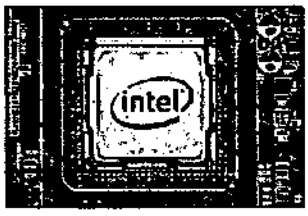
FreeHide IP – бесплатная утилита, предназначенная для скрытия реального IP-адреса компьютера при работе в сети Интернет. С помощью этой программы можно анонимно просматривать веб-сайты и отправлять конфиденциальную электронную почту. Помимо анонимности, скрытие реального IP-адреса защищает компьютер от хакерских атак и кражи личных данных. Так же FreeHide IP будет полезна, если нужно зайти на сайт, не доступный для страны или IP-адреса.

Программа FreeHide IP полностью совместима со всеми браузерами (Mozilla Firefox, Internet Explorer, Opera, Google Chrome и т.д.).

Источник: http://www.edtechrussia.ru/brauzer-skryivayuschij-ip/ (дата размещения материала 22.04.2018).

Компания «Intel» намерена использовать ресурсы графического процессора для обнаружения вредоносного ПО[9]

Согласно информации, опубликованной на сайте muyseguridad.net, «Intel» работает над улучшением своего имиджа в области безопасности. Для этого она использует Технологию обнаружения угроз (TDT), состоящую из двух функций: Advanced Memory Scanning (расширенное сканирование памяти) и Advanced Platform Telemetry (расширенная телеметрия платформы).



Какая-то часть вредоносного ПО не постоянно заражает компьютер или ОС, а делает это каждый раз при перезагрузке компьютера, что значительно усложняет процесс обнаружения и анализа. Для этого необходимо сканировать вредоносную деятельность в памяти, что, по данным исследователей, снижает производительность центрального процессора (CPU) на 20%. Вместо этого «Intel» предлагает использовать для сканирования памяти GPU (графический процессор), при этом нагрузка на CPU падает до 2%. В конце апреля Microsoft включит эту первую функцию расширенного сканирования памяти в свое решение «Windows Defender Advanced Threat Protection».

Вторая функция – это расширенная телеметрия платформы, которая в основном использует такие элементы, как счетчики производительности в про-

[9] Перевод с испанского выполнен ГНИИИ ПТЗИ ФСТЭК России.

цессоре для обнаружения необычной или аномальной деятельности, вместо использования элементов высокого уровня ОС.

Источник: https://www.muyseguridad.net/2018/04/17/intel-recursos-gpu-deteccion-malware/ (дата размещения материала 17.04.2018).

«Tenable» представила решение по управлению киберрисками

По данным сайта anti-malware.ru, компания «Tenable» представила «Tenable.io Lumin», новое приложение на основе платформы Tenable.io, благодаря которому руководители, отвечающие за информационную безопасность, смогут визуализировать, анализировать и измерять киберриски своих организаций. Наиболее сложным элементом этого процесса является определение приоритетов – какие уязвимости необходимо устранять в первую очередь. «Tenable.io Lumin» позволяет решить эту проблему, измеряя, анализируя и визуализируя данные об уязвимостях с оценкой критичности их угрозы для бизнеса, что должно способствовать увеличению эффективности информационной безопасности на предприятии. С помощью «Tenable.io Lumin» пользователи смогут опереться на опыт других крупных компаний отрасли, что позволит принять более эффективные решения.

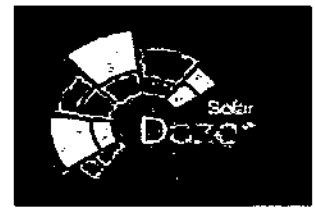
Ключевые возможности «Tenable.io Lumin»: аналитика уровня киберриска и сравнение с аналогичными компаниями; оценка и приоритизация уязвимостей на основе уровня киберриска; интеграция с внешними системами через API. Бета-тестирование «Tenable.io Lumin» пройдет в апреле 2018 года, в его процессе будут добавлены новые возможности продукта.

Источник: https://www.anti-malware.ru/news/2018-03-23-1447/25808 (дата размещения материала 23.03.2018).

«Solar Dozor» делает шаг в облака

Как сообщается на сайте solarsecurity.ru, компания «Solar Security» представила «Solar Dozor 6.6» – новую версию системы контроля коммуникаций сотрудников, выявления ранних признаков корпоративного мошенничества и проведения расследований.

Исследователи «Solar Security» встроили в новую версию «Solar Dozor» облачный краулер. Это специализированный инструмент, позволяющий специалисту по информационной безопасности сканировать облачные хранилища, которые используют сотрудники.



Кроме того, возможности «Solar Dozor» существенно расширены за счет функций собственной безопасности DLP-системы. Проблема контроля привилегированных пользователей стоит достаточно остро: по данным недавнего исследования Solar JSOC, примерно в трети случаев виновниками внутренних инцидентов являются штатные администраторы компаний. «Solar Dozor 6.6» предлагает бизнесу инструменты, позволяющие «контролировать контролеров».

Гибкая система управления правами доступа пользователей позволяет легко управлять учетными записями и ролями пользователей. Решение поддерживает гранулированное управление доступом, разграничивающее права на отдельные разделы интерфейса, объекты и функции системы.

Журнал действий пользователей «Solar Dozor 6.6» содержит максимально детализированные записи о том, кто, когда и что делал в системе. С его помощью можно контролировать действия как конкретных специалистов по информационной безопасности, так и всех пользователей DLP-системы. Если кто-либо попытается совершить недопустимые действия в системе, заинтересованным лицам немедленно будет отправлено уведомление об инциденте. Оперативное информирование и реакция на происшествие позволит владельцам бизнеса минимизировать ущерб от нелегитимных действий сотрудников.

Источник: https://www.solarsecurity.ru/events/news/1050/ (дата размещения материала 11.04.2018).

«Fortinet» представила решение для автоматизированного и реагирования на угрозы

На сайте safe.cnews.ru компания «Fortinet» объявила о выходе первого в своей области специально разработанного решения «NOC-SOC», которое устраняет разрывы между рабочими процессами, операциями анализа и автоматизированными функциями реагирования в рамках операционных процессов и процессов обеспечения безопасности. Компания объединила новые функции решений «FortiManager 6.0», «FortiAnalyzer 6.0» и «FortiSIEM 5.0» на базе адаптивной системы сетевой безопасности «Fortinet» в целях разработки уникального средства управления и анализа «NOC-SOC».

Подход к управлению, задействующий центры «NOC-SOC», повышает эффективность отслеживания операций безопасности, благодаря новому графическому представлению топологии адаптивной системы сетевой безопасности и расширениям, которые внедряются в частные и общедоступные облачные среды с помощью динамических объектов политики. Новая функция оценки систем безопасности сочетает аналитические компоненты решений FortiGate, FortiAnalyzer и FortiManager со службами сбора данных об угрозах FortiGuard в целях обеспечения таких характеристик корпоративной безопасности, которые поддаются количественному определению.

Благодаря новым функциям отслеживания мер реагирования на угрозы пользователи могут автоматизировать принятие мер реагирования для отдельных решений как на основе определенных триггеров (системные события, оповещения об угрозах, состояние пользователей и устройств), так и за счет непосредственной интеграции с функцией ServiceNow IT Service Managemen.

Источник: http://www.safe.cnews.ru/news/line/2018-04-24_fortinet_predstavila_reshenie_dlya_avtomatizatsii (дата размещения материала 24.04.2018).

«Mozilla» выпустила расширение для защиты пользователей Firefox от слежки со стороны Facebook

Как информирует сайт vc.ru, компания «Mozilla» выпустила для своего браузера Firefox расширение «Facebook Container», призванное защитить личные данные пользователя от слежки со стороны Facebook. Данное расширение изолирует идентификационные данные пользователя Facebook от остальных посещаемых сайтов. После его установки Firefox будет открывать сайт Facebook на специальной вкладке-контейнере, предварительно удалив cookie-файлы.

Если пользователь перейдет на страницу в Facebook по ссылке с другого сайта, она откроется на вкладке-контейнере, и соцсеть не получит cookie-файлы. Это затруднит для Facebook сбор данных пользователя для показа рекламы и других таргетированных сообщений. Если пользователь перейдет по внешней ссылке из Facebook, она откроется в обычной вкладке.

В «Mozilla» предупредили, что после установки расширения такая функция, как авторизация на сайтах с помощью Facebook, может не работать должным образом. Кроме того, могут возникнуть сложности с отображением встроенных на других сайтах комментариев и кнопки «нравится» из Facebook.

Источник: https://www.vc.ru/35373-mozilla-vypustila-rasshirenie-dlya-zashchity-polzovateley-firefox-ot-slezhki-so-storony-facebook (дата размещения материала 28.03.2018).

«Лаборатория Касперского» открыла исходный код сканера «KLara»

Согласно информации сайта anti-malware.ru, эксперты «Лаборатории Касперского» опубликовали на портале GitHub исходный код сканера «KLara». Это внутренний инструмент компании для более эффективного поиска образцов вредоносных программ. Теперь сканером могут воспользоваться все желающие. Основная задача «KLara» – обнаружение родственных образцов вредоносного кода. Это один из ключевых аспектов исследований киберугроз, который помогает экспертам отслеживать развитие вредоносов. Как правило, в таких случаях прибегают к YARA-правилам, которые сопоставляют различные образцы кода и ищут совпадения по уникальным характеристикам или шаблонам. Такой инструмент незаменим при исследовании сложных киберугроз, операций с применением «бесфайловых» троянцев или внешне легитимных инструментов, а также случаев, когда вредоносный код дорабатывается под конкретную жертву.

Самостоятельная разработка и тестирование YARA – крайне трудоемкий процесс. Чтобы решить эту проблему, исследователи создали «KLara». Это распределенная система, которая может производить быстрый поиск сразу по нескольким базам с применением нескольких правил. Такой подход позволяет

быстрее выявлять образцы вредоносного кода, а значит более эффективно защищать пользователей.

Источник: https://www.anti-malware.ru/news/2018-04-10-1447/25962 (дата размещения материала 10.04.2018).

«Symantec» впервые выпустила на рынок используемые в компании инструменты для обнаружения угроз

По данным сайта servernews.ru, компания «Symantec» впервые открыла клиентам доступ к инструментам для обнаружения угроз, которыми она пользовалась самостоятельно. Речь идет о технологии «Targeted Attack Analytics», способной обнаруживать более сложные кибератаки по сравнению с традиционными ИБ-решениями.

Система «Targeted Attack Analytics» интегрирована с «Symantec Advanced Threat Protection» (ATP) и доступна пользователям этого продукта без дополнительных платежей. ATP, который пока ориентирован на средние и крупные компании, может быть востребован и среди представителей малого бизнеса после появления в продукте «Targeted Attack Analytics».

Большинство традиционных решений для обеспечения ИБ, включая «Symantec Endpoint Protection», сканируют файлы, часть сетевого потока или другие отдельные элементы, тогда как «Targeted Attack Analytics» может вести мониторинг всего компьютерного оборудования в компании и сопоставлять данные с телеметрической картиной и с конечными точками, чтобы проверить активность атаки в сети.

Источник: https://www.servernews.ru/968488 (дата размещения материала 18.04.2018).

«Trend Micro» защитит корпоративные email-аккаунты с помощью искусственного интеллекта

По информации, размещенной на сайте anti-malware.ru, «Trend Micro» представила новую технологию, позволяющую продуктам компании выявлять попытки онлайн-мошенничества через электронную почту. Система анализа основана на использовании искусственного интеллекта. Компания интегрировала новое решение «Writing Style DNA» в несколько своих продуктов. Искусственный интеллект будет использоваться для создания неких шаблонов стиля написания пользователя на основе более 7000 характеристик. Текст каждого входящего письма будет сравниваться с подготовленной моделью. Если он не будет соответствовать определенному стилю написания, получателю будет отправлено соответствующее оповещение. Такая функция очень пригодится в случае, если корпоративный email-аккаунт был взломан и с него рассылаются вредоносные письма.

«Writing Style DNA» также позволит руководителям предоставлять обратную связь по подозрительным письмам, это улучшит работу системы,

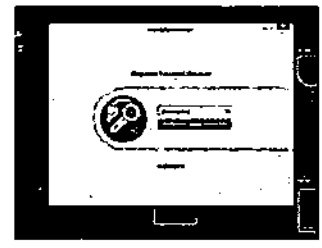
например, снизит процент ложных срабатываний, а также поможет лучше детектировать по-настоящему злонамеренные электронные письма. Новые возможности станут доступны пользователям в июне 2018 года в рамках продукта «Cloud App Security» для Microsoft Office, а также «ScanMail Suite» для Microsoft Exchange.

Источник: https://www.anti-malware.ru/news/2018-04-19-1447/26039 (дата размещения материала 19.04.2018).

«Лаборатория Касперского» представила новое поколение своего решения «Kaspersky Password Manager»

По информации ряда сайтов, «Лаборатория Касперского» представила новое поколение своего решения «Kaspersky Password Manager». Теперь продукт безопасно хранит в зашифрованном виде не только логины и пароли от всевозможных аккаунтов, но также платежные данные, сканы и фото важных документов. При этом вся информация автоматически вставляется в соответствующие регистрационные формы на проверенных сайтах и синхронизируется между всеми устройствами пользователя и веб-версией решения на портале My Kaspersky.

«Kaspersky Password Manager» автоматически проверяет надежность и устойчивость к взлому тех паролей, которые пользователь придумал сам, и создает сложные комбинации символов, для того чтобы злоумышленники не могли угадать пароль методом перебора.



В новой версии решения появилась возможность хранить и автоматически вводить на сайтах для оплаты адресные сведения и банковские данные пользователя. Для обеспечения дополнительной безопасности ценной информации и во избежание возможной кражи, продукт передает данные сайтам только после их проверки на благонадежность. Также решение может безопасно хранить изображения важных документов – например, сканов паспорта или страховки, которые многие люди оставляют в электронном виде.

Источники: https://www.itweek.ru/security/news-company/detail.php?ID=200254 (дата размещения материала 29.03.2018); https://www.cfo-russia.ru/novosti/index.php?article=36347.

МТС запускает сервис для хранения и обработки персональных данных в облаке

Как сообщает сайт akm.ru, ПАО «МТС» запускает облачный сервис, который поможет бизнесу обеспечить защиту персональных данных клиентов и сотрудников в соответствии с последними требованиями российского законодательства. В основе сервиса – выделенный защищенный сегмент облака #CloudMTC. Это отказоустойчивая инфраструктура на базе виртуальной платформы VMware. Сервис позволяет раз-

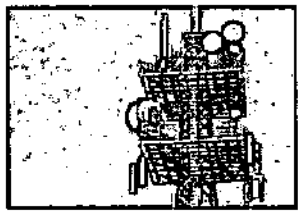
мещать в облаке информационные системы, которые участвуют в процессе сбора и обработки персональных данных – системы управления кадрами, корпоративным контентом, взаимодействием с клиентами. Решение актуально для компаний, которые в процессе работы взаимодействуют с персональными данными: банки, страховые компании, медицинские организации, логистические компании, ритейлеры с программами лояльности и др.

Защищенный сегмент облака #CloudMTC аттестован ФСТЭК России и полностью соответствует требованиям 152-ФЗ «О персональных данных» и подзаконных актов. Безопасность данных обеспечивают системы межсетевого экранирования, защита каналов связи, антивирусная защита и анализ уязвимостей. Сервис дает возможность обрабатывать персональные данные третьего уровня защищенности.

Источник: http://www.akm.ru/rus/news/2018/april/16/ns_6005939.htm (дата размещения материала 16.04.2018).

В России представлено решение для защиты сигнальных сетей

Согласно сообщению на ряде сайтов, компании «Positive Technologies» и «Sparkle» представили специализированное решение «Signaling Protection Suite», предназначенное для защиты сигнальных сетей 3G и 4G.



Несмотря на то, что технологии 4G более современны по сравнению с предыдущими поколениями, вопрос их безопасности все еще остается открытым. Инфраструктура сетей 4G остается уязвимой перед такими же атаками, как и более ранний протокол SS7. Злоумышленники могут красть персональные данные абонентов, отслеживать их местоположение, совершать различные мошеннические действия и провоцировать отказ в обслуживании.

«Signaling Protection Suite» является универсальным пакетом решений по защите сигнальных сетей мобильных операторов. Выявление и блокирование нелегитимного трафика позволит избежать утечки персональных данных, сбоев в работе и финансовых убытков.

Компании «Sparkle» и «Positive Technologies» будут совместно предоставлять клиентам широкий спектр услуг по обеспечению информационной безопасности, включая тестирование на уязвимости, оценку уровня соответствия передовым практикам, сигнальный межсетевой экран и мониторинг защищенности в режиме реального времени.

Источники: https://www.servernews.ru/967808 (дата размещения материала 30.03.2018); https://www.itweek.ru/security/news-company/detail.php?ID=200271; https://www.ptsecurity.com/ru-ru/about/news/291513/.

В России разработают единый стандарт биометрии

По информации сайта itsec.ru со ссылкой на газету «Известия», в рамках национальной технологической инициативы будет разработана единая биомет-

рическая платформа. Предполагается, что созданная нормативная и техническая база позволит сделать совместимыми российские системы идентификации людей по отпечаткам пальцев, сетчатке глаза, расположению сосудов на руках, голосу и т.д.

Разработчики поставили себе цель – за год создать национальную биометрическую платформу. Она будет мультимодальной – использующей различные способы идентификации (отпечатки пальцев, голос и др.).

Источник: http://www.itsec.ru/newstext.php?news_id=122815 (дата размещения материала 03.05.2018).

Новый стандарт позволит использовать биометрию для авторизации на сайтах

Как сообщает сайт securitylab.ru, в скором времени процесс авторизации на многих сайтах упростится и будет осуществляться с помощью аппаратных ключей в лэптопах, специальных приложений или даже датчиков отпечатков пальцев на смартфонах. Ряд организаций и компаний, в том числе «Microsoft» и «Google», выступили в поддержку нового стандарта, благодаря которому web-разработчики будут реализовывать на своих сайтах дополнительные механизмы авторизации, призванные надежно защитить учетные записи и данные пользователей.

Новый стандарт под названием WebAuthn позволит сайтам или web-сервисам использовать приложения, аппаратные токены или биометрические данные для авторизации пользователей вместо паролей или в качестве второго этапа двухфакторной аутентификации.

Источник: http://www.securitylab.ru/news/492552.php (дата размещения материала 10.04.2018).

«Cisco» анонсировала новые сервисы для защиты почты и конечных точек

По данным сайта anti-malware.ru, «Cisco» анонсировала новое решение «Cisco AMP» для защиты электронной почты и конечных точек. Новая технология обеспечит защиту от фишинга, программ-вымогателей, криптомайнинга и бестелесных вредоносных программ.

Технология использует сложную систему определения и защиты устройств от бестелесных вредоносных программ и программ-вымогателей. Главная причина популярности среди злоумышленников бестелесных вредоносных программ – их деятельность сложно обнаружить. Лежащий в основе «Cisco AMP» новый защитный механизм противостоит этим угрозам. Он обеспечивает защиту от уязвимостей необновленного ПО. Сервис работает беспрерывно, даже если пользователь «оффлайн». Он не требует настройки или регулировки от пользователя. Все новые сервисы «Cisco»

управляются из облачного пространства и не требуют установки на жесткий диск. Чтобы обезопасить свои домены от фишинга, «Cisco» обратилась к технологии DMARC. С его помощью «Cisco Domain Protection» отслеживает любую подозрительную активность своих доменов. Затем «Cisco Advanced Phishing Protection» определяет почтовый адрес, который использует злоумышленник, будь то попытки спуфинга или фишинга.

Источник: https://www.anti-malware.ru/news/2018-04-18-107504/26025 (дата размещения материала 18.04.2018).

«MaxPatrol SIEM» теперь выявляет продвинутые кибератаки на Microsoft Active Directory в автоматическом режиме

Как сообщает сайт ptsecurity.com, в систему управления событиями информационной безопасности «MaxPatrol SIEM» добавлены 26 новых правил обнаружения инцидентов, позволяющих выявлять кибератаки на Microsoft Active Directory. В конечном счете окно присутствия злоумышленника в инфраструктуре может быть сокращено до нескольких часов.

Создание специального пакета правил стало результатом работы экспертов компании «Positive Technologies». Они проанализировали полный цикл атак на Active Directory и выявили цепочку событий информационной безопасности и запросы в сетевом трафике, которые свидетельствуют о присутствии злоумышленников в инфраструктуре. Далее для автоматического анализа событий на наличие признаков таких атак и для уведомления ИБ-подразделения при помощи «MaxPatrol SIEM» был разработан пакет с алгоритмами обнаружения аномалий. Теперь стало возможным выявлять атаки на Active Directory на стадии разведки, продвижения внутри сети и удаленного исполнения команд.

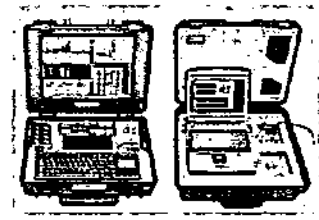
Источник: https://www.ptsecurity.com/ru-ru/about/news/292036/ (дата размещения материала 16.04.2018).

Новый мобильный терминал поможет бороться с вредоносами на USB

По данным сайта anti-malware.ru, компания «Orange Cyberdefense» запускает мобильный терминал для борьбы с вирусами на USB-накопителях. Работа с терминалом очень удобна и требует минимум времени. Достаточно лишь вставить в него USB-накопитель и терминал определит наличие или отсутствие вредоносных программ. В случае положительного ответа, устройство предложит удалить файлы или перенести их в карантин. Помимо этого, у пользователя будет возможность распечатать подробный отчет с информацией о зараженных файлах, сигнатурах распознанных угроз и названии поисковой системы антивируса, выявившей зараженный файл. Устройство также обладает встроенным механизмом обнаружения атак BadUSB, которые невозможно выявить с помощью традиционных антивирусных программ.

Источник: https://www.anti-malware.ru/news/2018-04-12-1447/25987 (дата размещения материала 12.04.2018).

ПАК выявления полуактивных электронных устройств перехвата акустической речевой информации



В статье, размещенной в журнале «INSIDE Защита информации», рассмотрены принципы построения и функционирования полуактивных электронных устройств перехвата акустической речевой информации типа эндовибраторов и аудиотранспондеров, а также методы их обнаружения.

Приведены основные характеристики полуактивных акустических радиозакладок типа SIM-ATP-16 и SIM-TP-40, а также отечественных программно-аппаратных комплексов Омега А10, Бастион-М, Ревиз-12000, Парнас-ЭХО 4, используемых для их выявления.

Источник: INSIDE Защита информации, 2018, № 2, с. 50-60.

Основные требования к защите информации в нормативной базе цифровой экономики

В статье, опубликованной в журнале «INSIDE Защита информации», рассматриваются основные положения нормативно-правовой базы цифровой экономики с точки зрения защиты информации и информационной безопасности. Обсуждается целесообразность корректировки понятия «защита информации» применительно к условиям цифровой экономики. Основные требования к защите информации анализируются на уровне Стратегии развития информационного общества и Программы «Цифровая экономика». Рассматриваются направления Программы «Нормативное регулирование» и «Информационная безопасность», а также требования информационной безопасности, связанные с обеспечением защищенности цифровых процессов согласно Основным направлениям реализации цифровой повестки Евразийского экономического союза.

Источник: INSIDE Защита информации, 2018, № 2, с. 45-49.

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

3.1. Документы Правительства Российской Федерации

Постановление Правительства Российской Федерации от 12.04.2018 № 445 «Об утверждении правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» (начало действия – с 1 июля 2018 г.)

Утверждены Правила хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи.

Операторы связи обязаны хранить собранные данные на территории Российской Федерации на принадлежащих им (либо другому оператору связи, если это согласовано с ФСБ России) серверах. Операторы обязаны защищать хранящуюся информацию и не допускать к ней несанкционированный доступ.

Телефонные разговоры и переписка должны будут храниться в течение 6 месяцев с момента окончания их приема, передачи, доставки или обработки. Переписку по электронной почте и мессенджерам операторы связи должны будут сохранять с 1 октября 2018 года. Емкость технических средств накопления, необходимых для сохранения информации, должна быть равной «объему сообщений электросвязи», отправленных и полученных пользователями за предыдущие 30 суток и увеличиваться на 15% каждые 5 лет.

По истечении 6 месяцев осуществляется автоматическое удаление записи разговоров и переписки в соответствии с предусмотренными программным обеспечением алгоритмами.

Источник: система Консультант-Плюс.

3.2. Документы ФСТЭК России

Информационное сообщение ФСТЭК России от 23 апреля 2018 г. № 240/11/1868 «О разработанных ФСТЭК России методических рекомендациях по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации»

Сообщается, что в целях оказания методической помощи организациям, осуществляющим образовательную деятельность, в подготовке рабочих дополнительных профессиональных программ в области информационной безопасности ФСТЭК России разработаны и утверждены 16 апреля 2018 г. Методиче-

ские рекомендации по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации.

Методические рекомендации по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденные ФСТЭК России 4 апреля 2015 г., считаются утратившими силу.

Обеспечение Методическими рекомендациями организаций, осуществляющих образовательную деятельность, производится на основании обращений в управления ФСТЭК России по федеральным округам.

Источник: www.fstec.ru (дата размещения материала 27.04.2018).

3.3. Патентные документы

Пат. 2 649 447 Российская Федерация, МПК G06F 21/00 (2013.01), G06Q 40/06 (2012.01), G06F 17/30 (2006.01). Способ выбора допустимых по стоимости вариантов построения системы защиты от компьютерных атак / Дроботун Е.Б.; патентообладатель: Дроботун Е.Б. – 2017117718, заявл. 22.05.2017, опубл. 03.04.2018.

Изобретение относится к области защиты информационно-вычислительных систем от компьютерных атак и может быть использовано для оценки стоимости жизненного цикла систем защиты от компьютерных атак и выбора допустимых по стоимости вариантов построения систем защиты от компьютерных атак. Техническим результатом является расширение функциональных возможностей системы защиты от компьютерных атак за счет выбора допустимых по стоимости вариантов построения систем защиты от компьютерных атак путем оценки жизненного цикла системы.

Пат. 2 651 196 Российская Федерация, G06F 21/56 (2013.01). Способ обнаружения аномальных событий по популярности свертки события / Монастырский А.В., Павлющик М.А., Романенко А.М., Головкин М.Ю.; патентообладатель: Акционерное общество «Лаборатория Касперского» – 2017117718, заявл. 22.05.2017, опубл. 03.04.2018.

Изобретение относится к способам обнаружения аномальных событий, возникающих в операционной системе, а именно к способам защиты компьютерных устройств от эксплуатации уязвимостей, содержащихся в программном обеспечении этих устройств. Технический результат заключается в обеспечении обнаружения аномальных событий, возникающих в ОС клиента в процессе исполнения ПО.

Пат. 2 649 789 Российская Федерация, H04L 12/801 (2013.01), H04L 29/06 (2006.01), H04L 9/32 (2006.01). Способ защиты вычислительных сетей / Мак-

симов Р.В., Орехов Д.Н., Проскуряков И.С., Соколовский С.П.; патентообладатель: Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное училище имени генерала армии С.М. Штеменко» Министерства обороны Российской Федерации – 2017125677, заявл. 17.07.2017, опубл. 04.04.2018.

Изобретение относится к области обнаружения атак с целью оперативного выявления и противодействия несанкционированным воздействиям в вычислительных сетях. Техническим результатом является повышение результативности защиты и введение в заблуждение нарушителя относительно структуры вычислительной сети за счет учета максимального количества принятых от отправителя и необработанных пакетов сообщений, которое может обработать вычислительная сеть без перегрузки, удержания в двухстороннем порядке соединения с отправителем пакетов сообщений при увеличении интенсивности несанкционированных информационных потоков и блокирования попыток отправителя разорвать соединение.

Пат. 2 649 793 Российская Федерация, G06F 21/31 (2013.01), G06F 15/18 (2006.01), G06F 21/00 (2013.01). Способ и система выявления удаленного подключения при работе на страницах веб-ресурса / Крылов П.В., Сачков И.К.; патентообладатель: ООО «Группа АйБи» – 2016131909, заявл. 03.08.2016, опубл. 04.04.2018.

Изобретение относится к области вычислительной техники. Технический результат заключается в расширении арсенала средств выявления удаленного подключения на основе данных о срабатывании и прерывании компьютерной мыши.

Пат. 2 649 794 Российская Федерация, G06F 21/53 (2013.01), G06F 21/56 (2013.01). Система и способ формирования журнала в виртуальной машине для проведения антивирусной проверки файла / Пинтийский В.В., Аникин Д.В., Кобычев Д.Ю., Головкин М.Ю., Бутузов В.В., Карасовский Д.В., Кирсанов Д.А.; патентообладатель: Акционерное общество «Лаборатория Касперского» – 2017115048, заявл. 28.04.2017, опубл. 04.04.2018.

Изобретение относится к решениям для выявления вредоносных файлов. Техническим результатом является повышение безопасности компьютерной системы, которое достигается путем принятия решения о признании вредоносным файла, открываемого в виртуальной машине.

4. Статистические данные по анализу защищенности информационных систем

«Лаборатория Касперского» представила отчет по уязвимостям в АСУ ТП за второе полугодие 2017 года

Как сообщает сайт securitylab.ru, «Лаборатория Касперского» опубликовала свой отчет по уязвимостям в АСУ ТП за второе полугодие 2017 года. В указанный период в различных компонентах АСУ ТП было обнаружено 322 уязвимости. Большая их часть выявлена в системах управления энергетикой (178). Далее следуют системы управления производственными процессами различных предприятий (164), водоснабжением (97) и транспортом (74).

По шкале оценки степени опасности уязвимостей CVSS 3.0 больше половины (194) уязвимостей получили 7 баллов, что соответствует высокой и критической степени. Все уязвимости с оценкой 10 баллов связаны с проблемами аутентификации, их можно эксплуатировать удаленно, и для эксплуатации особые навыки и техники не требуются.

Наиболее распространенными уязвимостями являются переполнение буфера (30) и неправильная аутентификация (23). 265 обнаруженных проблем с безопасностью могут эксплуатироваться удаленно без аутентификации даже малоопытным хакером. Более того, для 17 уязвимостей в Интернете доступны эксплоиты.

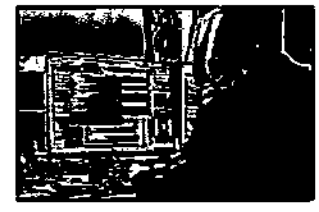
Наиболее уязвимыми оказались SCADA/HMI-компоненты – в них было обнаружено 88 проблем. Далее следуют сетевые устройства промышленного назначения (66), программируемые логические контроллеры (52) и инженерное ПО (52).

Источник: https://www.securitylab.ru/news/492303.php (дата размещения материала 26.03.2018).

ИТ-департаменты представляют собой наибольшую угрозу безопасности компаний

По информации сайта itsec.ru со ссылкой на исследования компании «Balabit», более трети ИТ-специалистов признают себя наиболее ценной мишенью злоумышленников, целью которых является взлом внутренней ИТ-инфраструктуры.

По данным исследования, 47% ИТ-специалистов признаются, что время и место авторизации – самая важная информация о пользователе для оперативного обнаружения вредоносных активностей. 41% опрошенных считают, что с точки зрения аналитики информационной безопасности важны данные по использованию корпоративных устройств в личных целях и 31% отметили, что поведенческие характеристики, такие как динамика нажатий на клавиши, также являются важным показателем для



идентификации действий злоумышленников. На вопрос о том, какую технологию безопасности они внедрили бы в следующем году (независимо от бюджета), почти 20% респондентов ответили, что планируют использовать инструменты аналитики для отслеживания поведения привилегированных пользователей.

В рамках опроса 42% ИТ-специалистов отметили системных администраторов как самое уязвимое звено в цепочке привилегированных пользователей в корпоративной сети, за ними следуют руководители высшего звена, это отметили 16% респондентов.

Исследование показало, что личные данные сотрудников компании тоже являются ценными активами для злоумышленников, поскольку их нетрудно продать – так ответили 56% опрошенных. 50% отметили, что не стоит пренебрегать защитой информации о клиентах, 46% сказали, что хакерам так же интересны финансовые показатели организаций.

Источник: http://www.itsec.ru/newstext.php?news_id=122460 (дата размещения материала 11.04.2018).

«Positive Technologies» проанализировала приложения банков

По данным сайта securitylab.ru, компания «Positive Technologies» проанализировала приложения банков. Больше половины систем дистанционного банковского обслуживания (ДБО) содержат критически опасные уязвимости. При этом доля систем ДБО, в которых обнаруживаются критически опасные уязвимости, снижается с каждым годом. Если в 2015 году уязвимости высокого уровня риска содержались в 90% проанализированных систем, а в 2016 году в 71%, то в 2017-м уже только в 56%. В среднем в 2017 году на каждую систему ДБО приходилось по 7 уязвимостей, что больше показателя 2016 года, когда на каждое финансовое приложение приходилось только 6 недостатков. Однако доли уязвимостей высокого и среднего уровня риска заметно снизились.

Наиболее распространенными уязвимостями онлайн-банков в 2017 году стали «Межсайтовое выполнение сценариев» (75% систем) и «Недостаточная защита от атак, направленных на перехват данных» (69%). Больше половины онлайн-банков (63%) содержали уязвимость высокого уровня риска «Недостаточная авторизация». Кроме того, уязвимости в 94% онлайн-банков могли быть использованы злоумышленниками для доступа к сведениям, составляющим банковскую тайну клиентов, и личной информации.

С мобильными банковскими приложениями ситуация похожа: снизились доли уязвимостей высокого (29% вместо 32% в 2016 году) и среднего уровня риска (56% вместо 60%). Соответственно, увеличилась доля уязвимостей низкого уровня риска. Тем не менее в половине систем (48%) была выявлена хотя бы одна критически опасная уязвимость. В 52% мобильных банков уязвимости позволяли расшифровать, перехватить, подобрать учетные данные для доступа в мобильное приложение или вовсе обойти процесс аутентификации.

Источник: https://www.securitylab.ru/news/492888.php (дата размещения материала 24.04.2018).

Компании не готовы к кибератакам «Пятого поколения»

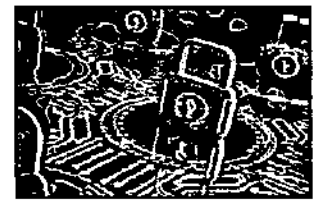
По информации ряда сайтов, количество облачных угроз, атак криптомайнеров, уязвимостей MacOS и IoT-устройств продолжает расти. И компании не чувствуют себя готовыми к новым вызовам. Сегодня наблюдается новое поколение кибератак – это многовекторные, крупномасштабные и стремительно распространяющиеся атаки «Пятого поколения» GenV. 77% ИБ-директоров выразили обеспокоенность тем, что организации не готовы к таким современным кибератакам и большинство инфраструктур безопасности компаний безнадежно устарели.

Чтобы получить больше информации о современном ландшафте киберугроз, исследователи «Check Point» опросили 443 специалиста по информационной безопасности о вызовах, с которыми они сталкиваются, отражая атаки «Пятого поколения». Результаты исследования показали, что защита большинства компаний отстает на 10 лет и как минимум на два поколения от современных кибератак Gen V. Это говорит о глобальной повсеместной уязвимости перед атаками «Пятого поколения». Риску подвержены все: медицинские учреждения, государственные сервисы, крупные корпорации. 97% компаний не обладают решениями, способными противостоять кибератакам Gen V.

Источники: http://www.iksmedia.ru/news/5492373-Kompanii-ne-gotovy-k-kiberatakam.html (дата размещения материала 16.04.2018); https://www.anti-malware.ru/news/2018-04-16-1447/26015.

Большинство руководителей объектов критической инфраструктуры не готовы к кибератакам

По данным сайта securitylab.ru, почти 60% руководителей объектов критической инфраструктуры заявили в ходе проведенного компанией «Ingedy» опроса об отсутствии рычагов управления, необходимых для защиты предприятий от киберугроз.



Несмотря на то, что организации вложили значительные средства в защиту ИТ-инфраструктуры, полностью устранить угрозы для среды операционных технологий не удалось. Как заявили 57 из 100 руководителей различных предприятий критической инфраструктуры, они не уверены, что их фирмы и другие связанные с инфраструктурой компании могут полностью контролировать безопасность операционных технологий.

Опрос также выявил отсутствие готовности противостоять кибератакам в ключевых секторах, включая энергетику, коммунальные услуги и производство. Например, 35% респондентов мало осведомлены о текущем состоянии кибербезопасности в своей среде, а 23% не осведомлены о ней вовсе.

Согласно мнению 63% опрошенных, угроза атак со стороны инсайдеров и неправильная конфигурация являются самыми большими рисками кибербезопасности, с которыми они в настоящее время сталкиваются. Вместе с тем 44% респондентов сообщили о планах увеличить расходы на кибербезопасность АСУ ТП в ближайшие год-два.

Источник: https://www.securitylab.ru/news/492484.php (дата размещения материала 05.04.2018).

Зафиксирована самая длительная DDoS-атака с 2015 года

Согласно информации, размещенной на сайте anti-malware.ru, исследователи «Лаборатории Касперского» проанализировали DDoS-атаки через ботнеты, организованные злоумышленниками в первом квартале 2018 года. Среди основных тенденций эксперты отмечают возвращение долгих многодневных кампаний, увеличившуюся популярность атак с усилением, а также рост активности старых и новых ботнетов. Первый квартал стал периодом длительных кампаний. Наиболее продолжительная из них не утихала в течение 297 часов (больше 12 дней), став самой долгой с конца 2015 года. Доля других относительно продолжительных атак (не менее 50 часов) выросла более чем в 6 раз – с 0,10% до 0,63%.

На киберарену вернулись атаки с усилением, в частности, через сервис Memcached. Они были беспрецедентными по своей мощности. В одном из случаев объем мусорного трафика превышал 1 Тб/с. Однако эксперты полагают, что их популярность продлится недолго.

В первом квартале 2018 года были зафиксированы атаки в 79 странах. Странами с наибольшим количеством атак стали Китай, США и Южная Корея. Россия в этом списке заняла десятое место (0,76% всех атак). Значительные изменения произошли в десятке стран с наибольшим количеством командных серверов. На смену Канаде, Турции, Литве и Дании пришли Италия, Гонконг, Германия и Великобритания. Резко выросло количество серверов для ботов Darkai (в США, Италии, Нидерландах и Франции) и AESDDoS (в Китае). Кроме того, возобновилась деятельность ботнетов Xor и Yoyo. Активность последнего увеличилась более чем в пять раз. Доля Linux-ботнетов снизилась по сравнению с концом прошлого года и составила 66% (против 71%).

Источник: https://www.anti-malware.ru/news/2018-04-26-1447/26116 (дата размещения материала 26.04.2018).

Хакеры могут проникнуть в корпоративную сеть 73% промышленных компаний

Как сообщается на ряде сайтов, подходы к обеспечению информационной безопасности промышленных объектов имеют свои особенности. Известные уязвимости в ИТ-системах часто не устраняются из-за нежелания вносить изменения и нарушать тем самым технологический процесс. Вместо этого основ-

ные усилия компании направляют на снижение вероятности их эксплуатации, например, путем отделения и изоляции внутренних технологических сетей от подключенных к Интернету корпоративных систем. Как показывает практика тестирования на проникновение, подобная изоляция не всегда реализуется эффективно, и у нарушителя остаются возможности для атаки.

Согласно собранной статистике, злоумышленники могут преодолеть периметр и попасть в корпоративную сеть 73% компаний промышленного сегмента. В 82% компаний возможно проникновение из корпоративной сети в технологическую, в которой функционируют компоненты АСУ ТП.

Одной из главных возможностей для получения взломщиком доступа к корпоративной сети оказались административные каналы управления. Часто администраторы промышленных систем создают для себя возможности удаленного подключения к ним – это позволяет им, например, не находиться все время на объекте, а работать из офиса. Наиболее распространенными уязвимостями корпоративных сетей стали словарные пароли и устаревшее ПО. Именно эти недостатки позволяют развить вектор атаки до получения максимальных привилегий в домене и контролировать всю корпоративную инфраструктуру.

Источники: https://www.ptsecurity.com/ru-ru/about/news/292232/ (дата размещения материала 26.04.2018); https://servernews.ru/969006.

Трояны-шифровальщики составили почти 40% атак в 2017 году

По данным сайта comss.info, телекоммуникационная компания «Verizon» выпустила отчет по киберугрозам ушедшего года. В исследовании приняли участие 67 организаций из 65 стран, которые предоставили информацию более чем о 53 тыс. инцидентов информационной безопасности. Почти три четверти случаев связаны с внешними угрозами, причем за половиной из них стоят организованные преступные группировки.

Инсайдеры оказались ответственны за 27% инцидентов. При этом 17% утечек произошли по небрежности – из-за вовремя не уничтоженных документов, важных писем, ушедших не тому получателю, или ошибок в конфигурации веб-серверов.

В 2017 году участились атаки на отделы кадров. Они располагают важной информацией о сотрудниках, необходимой для реализации мошеннических схем с налогами и финансами. При этом большинство фишинговых рассылок, которые традиционно используются для кражи подобных данных, не имеют успеха. Почти 80% пользователей в прошлом году ни разу не кликнули по вредоносным ссылкам.

Самой распространенной угрозой в прошедшем году стали шифровальщики – они составили 39% от всех атак с применением зловредного ПО. Авторы исследования связывают это со все большей доступностью вымогательского

софта – его несложно внедрить жертве, а вероятность попасться правоохранителям стремится к нулю.

Источник: http://www.comss.info/page.php?al=Trojany_shifrovalshhiki_sostavili_pochti_40_pr_atak_v_2017_godu (дата размещения материала 18.04.2018).

Мировой объем утечек данных в 2017 году вырос в 4,2 раза

Как информирует ряд сайтов, мировой объем утечек информации и скомпрометированных данных в 2017 году вырос в 4,2 раза по сравнению с 2016 годом. За год было зафиксировано 2,13 тыс. случаев утечки данных – на 37% больше показателя 2016 года.

В «InfoWatch» указывают, что 99% объема украденных данных приходится на 39 мега-утечек объемом от 10 млн. записей каждая. За год число таких утечек сократилось на 12%, тогда как объем скомпрометированных записей на одну мега-утечку увеличился почти в 5 раз (до 336 млн. записей). В 2017 году доля утечек персональных данных составила 64,8% от их общего объема, платежной информации – 21,1%, коммерческой тайны – 8%, гостайны – 6,1%.

В прошлом году в 70% случаев основным каналом утечки данных стал Интернет (браузеры, облачные сервисы), еще в 13,3% случаев утечки произошли через электронную почту.

Чаще всего утечки данных происходили в медицинских организациях (17,4%), компаниях сферы высоких технологий (16,7%) и госсекторе (16,5%). Наибольший объем скомпрометированных данных пришелся на компании сфер высоких технологий (32%), торговли (27%) и госорганы (23%). В высокотехнологичных компаниях и банках более половины утечек носили умышленный характер – 64,3% и 55,6% соответственно. Основными виновниками утечки данных в 50,3% случаев стали «внутренние нарушители», в 41,7% – внешние злоумышленники. Бывшие сотрудники организаций стали причиной 2,4% утечек.

Источники: http://www.interfax.ru/world/609698 (дата размещения материала 23.04.2018); https://www.itweek.ru/security/news-company/detail.php?ID=200508.

5. Сведения об инцидентах информационной безопасности

Хакеры атаковали объекты российской критической информационной инфраструктуры

Как сообщает сайт iksmedia.ru, массовая атака с использованием уязвимости в устройствах «Cisco», начавшаяся вечером 6 апреля 2018 года, была нацелена на значимые объекты КИИ Российской Федерации.

Сравнив атаки, совершаемые на объекты КИИ и прочие российские компании, аналитики центра мониторинга и реагирования на кибератаки «Solar JSOC» обнаружили, что интенсивность атаки возрастала в 20-30 раз, если была направлена на критическую информационную инфраструктуру. Пул адресов, с которых производились атаки на значимые объекты КИИ, также существенно шире, чем тот, с которого атаковали остальные компании.

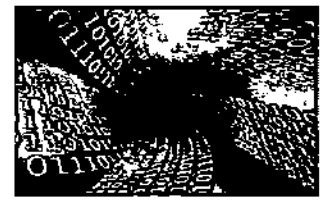
Для широковещательных атак, таких как WannaCry и Bad Rabbit, характерна массовость и ненаправленность действий злоумышленников. Они атакуют веерно, и во всех компаниях, оказавшихся уязвимыми, атака развивается по одному и тому же сценарию. В данном случае наблюдается существенное отличие: киберпреступники явно прикладывали больше усилий именно для поражения значимых объектов КИИ, и это дает основание говорить о нацеленности атак.

Источник: http://www.iksmedia.ru/news/5490253-Xakery-atakovali-obek-ty-rossijskoj.html (дата размещения материала 09.04.2018).

Крупнейшие утечки в первом квартале 2018 года

По данным сайта infowatch.ru, в январе-марте 2018 года аналитический центр компании «InfoWatch» зарегистрировал на 20% больше утечек конфиденциальной информации по сравнению с аналогичным периодом прошлого года.

В начале года индийские журналисты сообщили о компрометации персональных данных более миллиарда человек. Неизвестные злоумышленники взломали систему AADHAAR – крупнейшего национального идентификатора. Добычей хакеров в конце февраля стала информация 150 млн. человек, использующих приложение для похудения MyFitnessPal. Украдены адреса электронной почты, логины и зашифрованные пароли подписчиков.



Информационной «бомбой» стала компрометация данных 50 млн. пользователей Facebook. К расследованию инцидента уже приступила Федеральная торговая комиссия США. В результате крупнейшая социальная сеть уже потеряла десятки миллиардов долларов, от нее отвернулся ряд крупных рекламодателей.

Украинский исследователь безопасности обнаружил в сети две базы данных, содержащих информацию о более чем 18,5 млн. клиентов почтовой службы, то есть более 40% населения страны.

Утечка медицинских данных около 3 млн. граждан Норвегии произошла в результате хакерской атаки на информационную систему Юго-Восточной службы здравоохранения. Официальные лица не исключают, что данные украдены по заказу иностранного государства с целью нанести серьезный удар национальным интересам.

Источник: https://www.infowatch.ru/analytics/digest/20163 (дата размещения материала 02.04.2018).

В США несколько газотранспортных фирм стали жертвами кибератаки

Согласно информации сайта internetua.com со ссылкой на информационное агентство «Bloomberg», в США несколько фирм, занимающихся обслуживанием газопроводов, стали жертвами кибератаки. В частности, четыре компании заявили, что их электронные системы для обмена данными с клиентами EDI не работали в течение нескольких дней, три из них подтвердили связь неполадок с кибератаками.

Изначально кибератака была нацелена на подразделение «Latitude Technologies» компании «Energy Services Group», предоставляющей EDI и другие технологические услуги более чем 100 газотранспортным компаниям, хранилищам, коммунальным предприятиям, юридическим фирмам и маркетологам. EDI представляет собой платформу, используемую компаниями для обмена документами, такими как заказы на поставку и счета-фактуры. Система используется для шифрования, дешифрования, перевода и отслеживания ключевых сделок по купле и продаже электроэнергии.

Подробности кибератаки неизвестны, однако согласно данным компании «Latitude Technologies», информация о клиентах не была скомпрометирована, и другие системы не пострадали. В настоящее время восстановление служб EDI завершено.

Источник: http://www.internetua.com/v-ssha-neskolko-gazotransportnh-firm-stali-jertvami-kiberataki (дата размещения материала 04.04.2018).

Системы компании «Boeing» атаковал вирус WannaCry

По информации сайта securitylab.ru со ссылкой на ТАСС, информационные системы корпорации «Boeing» атаковали хакеры. Злоумышленники использовали знаменитый вирус WannaCry. Главный инженер компании М.Вандервел рассказал, что вирус, подобно метастазам, стремительно распространяется за пределы предприятия в Норт-Чарльстоне. Он не ис-

ключил, что WannaCry может добраться до ПО бортовых компьютеров собираемых самолетов.

Позднее руководство «Boeing» заявило, что первоначальные опасения были преувеличены. Центр операций обеспечения кибербезопасности выявил ограниченное по масштабу вторжение вредоносной программы, затронувшей незначительное количество систем. Были проведены восстановительные мероприятия, проблема не затронула производство и поставку товара заказчику.

Источник: https://www.securitylab.ru/news/492247.php (дата размещения материала 14.04.2018).

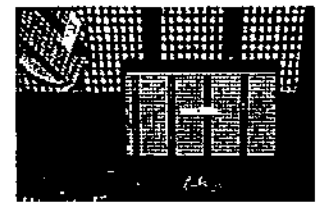
Хакеры украли данные пяти миллионов банковских карт

Как сообщает сайт gazeta.ru со ссылкой на издание «Associated Press», утечка данных из магазинов американских компаний «Saks Fifth Avenue», «Saks Off Fifth» и «Lord & Taylor» позволила хакерам получить данные около пяти миллионов банковских карт. Материнская компания «Hudson's Bay» признала, что хакерам удалось встроить вредоносное ПО через брешь в платежной системе. Незадолго до этого компания в области кибербезопасности «Gemini Advisory» заявила, что обнаружила в даркнете сообщения хакеров о похищенных пяти миллионов кредитных и дебетовых карт. Эксперты указывали, что хакеры собирали данные на протяжении года.

Источник: https://www.gazeta.ru/tech/news/2018/04/02/n_11362250.shtml (дата размещения материала 02.04.2018).

Австралия обвинила Россию в массированных кибератаках в августе 2017 года

По данным ряда сайтов, министр по вопросам кибербезопасности Австралии А.Тейлор возложил на Россию ответственность за попытки совершить массированные кибератаки на компании его страны в прошлом году. Он заявил, что на основании информации разведывательных агентств и после консультаций с союзниками правительство Австралии пришло к выводу о том, что ответственность за эти действия, предпринятые в 2017 году, лежит на лицах, пользовавшихся российской господдержкой. Объектами этих действий было значительное число австралийских организаций, однако нет свидетельств того, что им был нанесен ущерб.



В свою очередь министр обороны Австралии М.Пейн сообщила, что мишенями для российских кибератак «потенциально могли стать примерно 400 австралийских компаний».

Источники: http://www.tass.ru/mezhdunarodnaya-panorama/5132592 (дата размещения материала 17.04.2018); https://www.iz.ru/733069/2018-04-17/avstraliia-obvinila-rf-v-popytkakh-kiberatak-v-minuvshem-godu.

Хакеры проникли в сети двух немецких поставщиков электроэнергии

По информации ряда сайтов со ссылкой на газету «Süddeutsche Zeitung», два поставщика электроэнергии в Германии в прошлом году подверглись хакерским атакам. Хакеры проникли во внутренние сети компаний летом 2017 года. Немецким службам безопасности удалось быстро обнаружить атаку и отразить ее.

Как отмечает издание, нападение могла осуществить та же группа хакеров, которая ответственна за проникновение в компьютерные сети энергокомпаний на Украине в декабре 2016 года. За теми атаками, как утверждает газета, могла стоять спецслужба какой-то страны. Ответственных за случившееся установить не удалось.

Источники: https://www.kommersant.ru/doc/3619890 (дата размещения материала 04.05.2018); http://www.tass.ru/ekonomika/5175352.

Британское антидопинговое агентство подверглось хакерской атаке

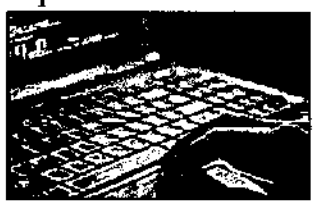
По данным, размещенным на ряде сайтов со ссылкой на издание «The Independent», британское антидопинговое агентство «UKAD», чья база содержит тысячи допинг-тестов спортсменов, подверглось хакерской атаке. В руки хакеров могли попасть медицинские данные футболистов английской премьер-лиги, известных атлетов-олимпийцев и велосипедистов.

После происшествия сотрудники «UKAD» были приглашены на экстренное совещание, но по его окончании пресс-служба агентства заявила, что кибератака не была удачной, данные не были утеряны или раскрыты, так как агентство имеет высокий уровень компьютерной безопасности. Однако «UKAD» продолжит расследовать этот вопрос для урегулирования ситуации.

Источники: https://www.championat.com/other/news-3386633-britanskoe-antidopingovoe-agentstvo-podverglos-hakerskoj-atake.html (дата размещения материала 26.03.2018); https://www.lenta.ru/news/2018/03/26/britain_hacked/.

У японских чиновников «утекли» пароли и адреса электронной почты

По данным сайта ria.ru, адреса электронной почты и пароли для доступа к закрытым сайтам чиновников ключевых министерств Японии оказались в Интернете.



Как сообщают японские СМИ, выставленными на продажу в Интернет оказались данные 2111 чиновников министерства экономики, торговли и промышленности, внешнеполитического ведомства, министерства общенациональных дел, министерства транспорта и других ключевых министерств. Утечка произошла с сайтов, не принадлежащих правитель-

ству, но на которых чиновники регистрировали свои адреса и пароли для получения доступа к информации юридического, статистического и другого характера для использования в служебных целях.

Несмотря на то, что правительство не считает утечку спланированной атакой, японские специалисты предупреждают о возможности использования данных для кибератак на конкретные адреса чиновников для отправки им вирусов и заражения их компьютеров.

Источник: https://www.ria.ru/world/20180404/1517883233.html (дата размещения материала 04.04.2018).

Хакеры атаковали государственные сайты Израиля

По информации сайта rosbalt.ru, ряд сайтов израильских государственных учреждений, в том числе интернет-страницы профсоюза учителей, израильской оперы и медицинского центра «Хиллель-Яффе», подверглись хакерской атаке.

На главной странице сайтов хакеры, назвавшиеся группой Th3Falcon, разместили фотографию столкновений палестинцев с израильской армией на границе с сектором Газа. По данным израильской телерадиокорпорации, аналогичной хакерской атаке также подверглись сайты местных властей.

Источник: http://www.rosbalt.ru/world/2018/04/04/1693804.html (дата размещения материала 04.04.2018).

Хакеры взломали индийскую энергокомпанию и потребовали выкуп

Согласно информации сайта internetua.com, хакеры получили доступ к компьютерным системам энергетической компании «UHBVN» в Индии и зашифровали биллинговые данные ее клиентов. Злоумышленники потребовали 10 млн. рупий в биткоинах за восстановление данных.

По словам представителей компании, в настоящее время данные восстанавливаются с помощью журналов и других источников. Зашифрованная информация содержала данные о задолженностях, а также текущем количестве потребленной электроэнергии.

Источник: http://www.internetua.com/haker-vzlomali-indiiskuua-energo-kompaniua-i-potrebovali-vkup-v-10-mln-rupii (дата размещения материала 30.03.2018).

Хакеры атаковали серверы агентства гражданской авиации Грузии

Как сообщает сайт newsgeorgia.ge, серверы агентства гражданской авиации минэкономики Грузии 2 мая подверглись кибератаке. Во время атаки были

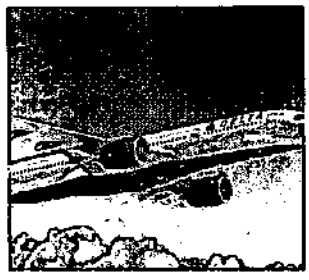
повреждены базы данных, программы и электронные адреса агентства. В настоящее время авиакомпании, авиационные предприятия, операторы и авиаспециалисты могут связаться с агентством только по нескольким адресам электронной почты.

Для устранения проблем, возникших в результате атаки, вместе с агентством участвуют все соответствующие ведомства. В МВД Грузии в связи с произошедшим начали следствие, детали которого пока не разглашаются.

Источник: https://www.newsgeorgia.ge/hakery-atakovali-servery-agentstva-grazhdanskoj-aviatsii-gruzii/ (дата размещения материала 04.05.2018).

«Delta Air Lines» сообщила о возможной утечке платежных данных ряда клиентов

По информации сайта internetua.com, платежные данные ряда клиентов авиакомпании «Delta Air Lines» могли оказаться в руках хакеров в результате кибератаки на электронные системы одного из партнеров перевозчика. Согласно заявлению авиакомпании, в сентябре-октябре 2017 года неизвестные злоумышленники получили доступ к серверам сторонней компании, предоставляющей авиаперевозчику, в частности, услуги online-чата для работы с клиентами. В результате инцидента хакеры могли получить доступ к «небольшой части» платежных данных клиентов компании. Паспортные данные и другая персональная информация не пострадали.



В настоящее время «Delta Air Lines» проводит расследование инцидента в сотрудничестве с федеральными и правоохранительными органами.

Источник: http://www.internetua.com/delta-air-lines-soobsxila-o-vozmojnoi-utecske-platejnh-dannh-ryada-klientov (дата размещения материала 05.04.2018).

Хакер взломал сайт одного из министерств Украины

Согласно информации портала securenews.ru, неизвестный хакер взломал официальный сайт министерства энергетики Украины, оставив чиновникам послание. В нем говорится, что вся информация на сайте, который он взломал, находится в зашифрованном виде. А также было указано, что искать способ восстановления информации не имеет никакого смысла, так как без специального сервиса не получится дешифровать закодированную информацию и файлы.

Чтобы вернуть доступ к сайту, чиновники должны заплатить за «услугу» дешифровки файлов, находящихся на портале, посредством перевода денежных средств в криптовалюте. В случае, если требования хакера не будут удовлетворены, то в течение суток все содержимое сайта будет удалено.