

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

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



## ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ СБОРНИК

ВЫПУСК 6 (26)



# ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

(по материалам из открытых источников)

ВОРОНЕЖ  
2015

к и в а - 49409



Федеральная служба по техническому и экспортному контролю

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

ГРНТИ 81.93.29  
УДК 002:004.056

Экз. № 23

## **ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ СБОРНИК**

### *ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ*

(по материалам из открытых источников)

ВЫПУСК 6 (26)

Воронеж  
2015



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

## **СОДЕРЖАНИЕ**

1. Сведения о развитии и реализации новых технологий в сфере ответственности ФСТЭК России .....	3
1.1. Противодействие техническим разведкам .....	3
1.2. Техническая защита информации .....	14
1.3. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры .....	40
2. Сведения о перспективах развития и достижениях в создании способов и средств защиты информации .....	43
3. Сведения о новых документах, регламентирующих вопросы в области защиты информации .....	59
3.1. Нормативные правовые акты федерального уровня.....	59
3.2. Документы ФСТЭК России .....	60
3.3. Патентные документы .....	61
4. Статистические данные по анализу защищенности информационных систем .....	63
5. Сведения об инцидентах информационной безопасности .....	70



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

## 1.1. Противодействие техническим разведкам

### *Пентагон усилит космический контроль России и Китая*

Ряд сайтов сообщает о создании в срочном порядке министерством обороны США Объединенного космического операционного центра. Источником этой информации стало выступление заместителя министра обороны США Роберта Уорка на ежегодном симпозиуме спецслужб GEOINT, спонсором которого является Фонд геопространственной разведки США.



По планам Пентагона космический центр должен быть развернут в структуре министерства в течение ближайших шести месяцев и его основной задачей станет контроль за работой всех военных и правительственных спутников.

Разведывательная деятельность нового центра Пентагона будет направлена на два государства – Россию и Китай. Отмечается, что центр также должен укрепить американское технологическое преимущество в космосе перед Россией и Китаем, обеспечить доминирование США в конфликтах, которые переходят теперь и в космическое пространство.

Объединенный космический операционный центр планируется разместить на военно-воздушной базе Ванденберг в штате Калифорния.

**Источники:** <http://www.aex.ru/news/2015/6/24/136710/> (дата размещения материала 24.06.2015); <http://topwar.ru/77663-pentagon-hochet-kontrolirovat-kitay-i-rf-iz-kosmosa.html>; [http://ria.ru/radio\\_brief/20150626/109017\\_9867.html](http://ria.ru/radio_brief/20150626/109017_9867.html); <http://www3.vz.ru/news/2015/6/24/752550.html>; <http://russianweek.ru/2015/06/26/kosmicheskij-centr-ssha-sozhdadut-dlya-kontrolya-iz-kosmosa-rossii-i-kitaya/>.

### *Определена орбита секретного космического аппарата Пентагона X-37B*

Согласно данным ряда сайтов, астрономы-любители обнаружили на орбите секретный американский космический аппарат X-37B, запущенный 20 мая этого года. Они засекли его на орбите высотой от 312 до 325 км с наклоном 38 градусов к экватору.

Проекция траектории аппарата на поверхность Земли повторяется каждые два дня, что является отличительной чертой полета X-37B. Это может свидетельствовать о том, что с его помощью ведется разведка.



**Источники:** [http://www.topnews.ru/news\\_id\\_78284.html](http://www.topnews.ru/news_id_78284.html) (дата размещения материала 29.05.2015); <http://altapress.ru/story/158570>; <http://news.rambler.ru/scitech/30355872>.



## *Разведывательный спутник Израиля «Ofeq-10»*

В журнале «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления» опубликована информация о запуске Израилем разведывательного спутника «Ofeq-10» («Горизонт»). Аппарат обеспечивает круглосуточное наблюдение за странами арабского мира и Ираном. Он может обнаруживать не только наземные цели, но и подводные лодки. В состав разведывательной аппаратуры входят усовершенствованная радиолокационная станция (РЛС) с синтезированием апертуры EL/M-2070 и многорежимная камера «Jupiter».



РЛС ELM-2070 позволяет получать видовую информацию в любое время суток и в любых погодных условиях с разрешением, сравнимым с разрешением аэрофотоснимков. Она работает в секторе 20-45 градусов и создает на местности полосу наблюдения шириной до 100 км. Камера «Jupiter» позволяет получать черно-белые и цветные изображения с разрешающей способностью 0,5 м и менее 2 м соответственно. При высоте полета около 600 км камера обеспечивает обзор полосы местности шириной 15 км.

РЛС ELM-2070 позволяет получать видовую информацию в любое время суток и в любых погодных условиях с разрешением, сравнимым с разрешением аэрофотоснимков. Она работает в секторе 20-45 градусов и создает на местности полосу наблюдения шириной до 100 км. Камера «Jupiter» позволяет получать черно-белые и цветные изображения с разрешающей способностью 0,5 м и менее 2 м соответственно. При высоте полета около 600 км камера обеспечивает обзор полосы местности шириной 15 км.

**Источник:** Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 5, с. 4-5.

## *Компания «Elecnor» продает свои спутники канадской компании<sup>1</sup>*

На сайте infoespacial.com сообщается, что испанская компания «Elecnor Deimos» заключила соглашение о продаже канадской компании «UrtheCast» двух спутников дистанционного зондирования Земли (ДЗЗ) – «Deimos-1» и «Deimos-2». Компании также договорились сотрудничать в рамках программы



«Constellation», цель которой заключается в построении группировки, полностью состоящей из спутников ДЗЗ, на которых будут установлены РЛС с синтезированием апертуры антенн.

Программа «Constellation» предполагает разработку спутников, которые будут размещены на орбите группами по два аппарата, один из которых будет вести оптическую съемку, а другой – радиолокационную. Данная система позволит снимать видео земной поверхности высокого разрешения.

**Источник:** <http://www.infoespacial.com/?noticia=elecnor-vende-sus-satelites-deimos-1-y-deimos-2-a-una-empresa-canadiense-por-742-millones> (дата размещения материала 24.06.2015).

---

<sup>1</sup> Перевод с испанского выполнен ГНИИИ ПТЗИ ФСТЭК России.



## *Азербайджан планирует использовать свой космический арсенал в интересах обороны<sup>2</sup>*

Согласно информации сайта [le-caucase.com](http://le-caucase.com), специалисты французской компании «Airbus Defence and Space» провели презентацию возможностей использования снимков, полученных с азербайджанского спутника «AzerSky», для получения разведданных, в военной картографии, контроля, мониторинга и других целей.

Спутник «AzerSky» запущен в июне 2014 г. в рамках стратегического сотрудничества Азербайджана и Франции в сфере космической промышленности. Аппарат способен ежедневно вести съемку участков поверхности Земли площадью 6 млн. квадратных километров. Разрешение полученных снимков составляет 1,5 метра.



**Источник:** <http://www.le-caucase.com/2015/05/28/lazerbaidjan-souhaite-utiliser-son-arsenal-spatial-pour-assurer-sa-defense/> (дата размещения материала 28.05.2015).

## *Радар системы противоракетной обороны будет размещен на Аляске*

На сайте [vpk.name](http://vpk.name) со ссылкой на пресс-службу министерства обороны США сообщается, что в планы военного ведомства входит размещение на Аляске нового радара селекции баллистических целей LRDR. После постановки на боевое дежурство в 2020 г. радар станет частью системы противоракетной обороны (ПРО). В настоящее время Агентство ПРО США занимается сбором предложений относительно того, какие технологии могут быть использованы в LRDR.



РЛС будет предназначена для обнаружения и селекции истинных баллистических целей и передачи информации на пункты ПРО. Радар должен функционировать в режиме широкого сектора обзора для обнаружения целей и узкого – для точного их распознавания и сопровождения. Одним из наиболее вероятных мест размещения радара называют авиабазу Клир.

**Источник:** [http://vpk.name/news/132484\\_pentagon\\_nameren\\_razmestit\\_na\\_alyaske\\_eshe\\_odin\\_radar\\_sistemyi\\_pro.html](http://vpk.name/news/132484_pentagon_nameren_razmestit_na_alyaske_eshe_odin_radar_sistemyi_pro.html) (дата размещения материала 25.05.2015).

## *Раскрыта новая шпионская роль «Pine Gap»<sup>3</sup>*

Согласно информации, размещенной на ряде сайтов, шпионская база «Pine Gap», расположенная в центральной части Австралии, стала выполнять новую роль по ведению электронной разведки. Теперь она обеспечивает сбор

<sup>2</sup> Перевод с французского выполнен ГНИИИ ПТЗИ ФСТЭК России.

<sup>3</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.



информации в рамках одной из задач разведывательного альянса «Пять глаз» по слежению за линиями связи и глобальным интернет-трафиком.

Сообщается об увеличении объема перехватываемых спутниковых линий



связи, а также об увеличении количества антенн, расположенных на разведывательных объектах «Пяти глаз». Кроме этого, появилась информация о размещении большого количества усовершенствованных квазипараболических многолучевых антенн Торус, каждая из которых может использовать до 35 лучей для перехвата со-

общений спутников связи.

«Pine Gap» является наземным пунктом управления для спутников радио- и радиотехнической разведок Национального управления космической разведки США, перехватывающих телеметрическую информацию об испытаниях баллистических ракет.

**Источники:** <http://www.smh.com.au/technology/technology-news/pine-gaps-new-spy-role-revealed-20150531-ghdefc.html> (дата размещения материала 31.05.2015); <http://www.wired.co.uk/news/archive/2015-05/28/torus-duncan-campbell-report>.

### *Грузия закупает РЛС GroundMaster GM 200*

Согласно информации, размещенной на сайте [forum.militaryparitet.com](http://forum.militaryparitet.com),



Грузия собирается приобрести несколько трехкоординатных мобильных РЛС обнаружения воздушных целей французской компании «Thales Raytheon Systems» Ground Master 200 (GM 200).

Это позволит восстановить военную систему контроля воздушного пространства, серьезно пострадавшую в ходе Пятидневной войны 2008 г. РЛС GM 200 является «средней» моделью в линейке «Ground Master» (наряду с РЛС GM 400 и GM 60). В настоящее время они состоят на вооружении ВВС Франции и Сингапура.

**Источник:** <http://forum.militaryparitet.com/viewtopic.php?id=2523&p=85> (дата размещения материала 17.06.2015).

### *На выставке в Париже впервые представлено семейство РЛС сверхвысокой частоты<sup>4</sup>*

Как сообщает сайт [janes.com](http://janes.com), израильская компания «Israel Aerospace Industries» (IAI) представила новое семейство цифровых РЛС раннего обнаружения диапазона сверхвысоких частот ULTRA, в которых внедрена технология активных антенных решеток с электронным сканированием. Станции предназначены для обнаружения целей с малой эффективной поверхностью рассеяния на очень больших расстояниях.



Israel Aerospace Industries

<sup>4</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.



РЛС построены по модульному принципу, каждый компонент имеет размеры 3х3 метра. Например, компонент под названием ULTRA-C1 предназначен для использования в качестве легкой разведывательной РЛС для мобильных платформ, обеспечивающей обзор в 360°. Представители IAI утверждают, что ULTRA-C1 позволяет обнаруживать истребитель на расстоянии до 500 км.

**Источник:** <http://www.janes.com/article/52396/paris-air-show-2015-elta-s-ultra-uhf-radar-family-makes-paris-debut> (дата размещения материала 17.06.2015).

### *Радар для обнаружения беспилотников*

Как сообщает сайт [popmech.ru](http://popmech.ru), японская компания «Alsok» разработала акустическую систему обнаружения мультикоптеров. Система построена на основе датчиков, способных распознать звук летящего квадрокоптера на расстоянии до 150 метров.

Как только звук от лопастей пропеллеров дрона попадает в зону действия датчиков, система сверяет его с базой данных, в которой собраны образцы звуков, издаваемых различными мультикоптерами. Система может точно определить модель беспилотника и направление его движения.

**Источник:** [http://www.popmech.ru/technologies/164736-sozdan-pervyy-radar-dlya-obnaruzheniya-bespilotnikov/?utm\\_source=popmech&utm\\_medium=rss&utm\\_campaign=public-all-articles](http://www.popmech.ru/technologies/164736-sozdan-pervyy-radar-dlya-obnaruzheniya-bespilotnikov/?utm_source=popmech&utm_medium=rss&utm_campaign=public-all-articles) (дата размещения материала 22.05.2015).



### *Япония намерена приобрести в США*

*самолеты дальнего радиолокационного обнаружения и управления  
Е-2D «Эдвансд Хоукэй»*

По информации, размещенной на ряде сайтов, государственный департамент США одобрил поставку Японии четырех самолетов дальнего радиолокационного обнаружения и управления (ДРЛОиУ) Е-2D «Эдвансд Хоукэй». Данный самолет представляет собой наиболее современную модификацию машины ДРЛОиУ на платформе Е-2. Машины этого типа используются в качестве летающих радаров корабельного базирования.

Модификация Е-2D отличается от предшественника радаром с активной фазированной антенной решеткой и более совершенным оборудованием передачи данных, позволяющим в сочетании с соответствующим оборудованием на борту самолетов создавать сетцентрические системы боевого управления.

**Источники:** <http://www.armstrade.org/includes/periodics/news/2015/0603/112029475/detail.shtml> (дата размещения материала 03.06.2015); <http://lenta.ru/news/2015/06/03/flyingradar>.





### *ВВС США получают беспилотный летательный аппарат «Reaper»*

Согласно сообщению сайта [absrf.ru](http://absrf.ru), компания «General Atomics – Aeronautical Systems Inc.» поставит ВВС США восемь дополнительных беспилотных летательных аппаратов (БПЛА) MQ-9 «Reaper» в модификации Block 5.



Модификация Block 5 – модернизированная версия БПЛА «Predator B» Block 1 – имеет увеличенную мощность двигателя и грузоподъемность, расширенные возможности связи и интеграции полезных нагрузок.

Поставки аппарата завершатся в 2017 г.

**Источник:** <http://absrf.ru/ru/uav/2015-06-01.htm> (дата размещения материала 01.06.2015).

### *Построен первый «Global Hawk» для стран НАТО*

На сайте [vpk.name](http://vpk.name) размещена информация о завершении производства первого БПЛА RQ-4B Block 40 «Global Hawk», построенного для европейской системы воздушной разведки НАТО AGS. Аппарат является модификацией «Global Hawk» Block 40 ВВС США с некоторыми изменениями. Значительными из них являются установка широкополосной линии передачи данных Link 16 от «Selex ES». Кроме того, в системе воздушной разведки будут применены два различных типа пункта управления. Программное обеспечение (ПО) управления БПЛА также будет отличаться.



Основной датчик БПЛА системы AGS такой же, как у американского «Global Hawk» Block 40 – мультиплатформенный радар MP-RTIP, получивший в ВВС США обозначение AN/ZPY-2. Этот радар X-диапазона обеспечивает шесть режимов работы: индикатор движущихся наземных целей, с синтезированной апертурой, воздушная маршрутизация, одновременная индикация движущихся целей, поисковый и с изображением высокой четкости земной поверхности.

**Источник:** [http://vpk.name/news/133408\\_postroen\\_pervyiy\\_global\\_hauk\\_dlya\\_stran\\_nato.html](http://vpk.name/news/133408_postroen_pervyiy_global_hauk_dlya_stran_nato.html) (дата размещения материала 08.06.2015).

### *Средневысотный беспилотник «Super Heron» большой продолжительности полета*

Согласно информации, опубликованной журналом «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления», израильская компания «Israel Aerospace Industries» намерена поставлять на экспорт средневысотный БПЛА большой продолжительности





полета «Super Heron», предназначенный для сбора информации, наблюдения и разведки, целеуказания и морского патрулирования. Аппарат оборудован комплектом бортового радиоэлектронного оборудования с тройным резервированием и винглетами. Благодаря наличию винглетов продолжительность его полета превышает 45 часов. Оптико-электронная станция наблюдения позволяет обнаруживать и идентифицировать корабли на дальности до 40 км.

В состав полезной нагрузки БПЛА входят две новые РЛС семейства ELM-2022, включая ELM-2022ES с активной антенной решеткой с электронным сканированием и РЛС ELM-2022ML с антенной решеткой с механическим сканированием.

**Источник:** Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 5, с. 5-6.

#### *Разработка самолета-разведчика U-2 в беспилотной версии*

В журнале «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления» опубликована информация о планах компании «Lockheed Martin» по разработке летательного аппарата U-2 в беспилотной версии для осуществления воздушной разведки. Предлагаемая новая модель будет аналогична по своим параметрам БПЛА RQ-4B «Global Hawk».



Сопоставление некоторых технических характеристик показывает, что U-2 может выполнять разведывательные задачи на большей высоте и нести больше полезной нагрузки. Кроме того, U-2 обладает большим защитным арсеналом по сравнению с «Global Hawk». Единственное преимущество БПЛА «Global Hawk» заключается в том, что продолжительность его нахождения в воздухе составляет более 24 часов, в то время как у U-2 этот показатель равен 12 часам.

**Источник:** Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 5, с. 10-11.

#### *Франция, Италия и Германия начинают совместный проект по разработке беспилотных летательных аппаратов*

По данным сайта svpressa.ru, страны Евросоюза планируют заменить американские разведывательные БПЛА аппаратами своей разработки. В проекте примут участие три крупных европейских оборонных подрядчика: «Airbus», «Finmeccanica» и «Dassault Aviation». Будет осуществляться сразу несколько программ по разработке БПЛА, одна из которых – создание средневысотных аппаратов MALE-класса. Другая



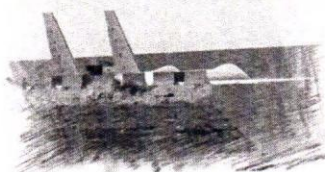


разработка будет направлена на создание разведывательно-ударного малогабаритного БПЛА «nEUROn».

**Источник:** [http://svpressa.ru/war21/article/122669/?rss=1&google\\_editors\\_picks=true](http://svpressa.ru/war21/article/122669/?rss=1&google_editors_picks=true) (дата размещения материала 28.05.2015).

### *Прототип китайского двухфюзеляжного высотного БПЛА<sup>5</sup>*

На сайте [janes.com](http://janes.com) приводятся снимки нового китайского двухфюзеляжного БПЛА, способного выполнять разведывательные задачи на большой высоте в околоземном пространстве. Прототип аппарата назван «Shen Diao» («Небесный орел»).



Ранее предполагалось, что на БПЛА между фюзеляжами будет установлена большая антенна метрового диапазона для выполнения задач по противодействию стелс-технологиям. Однако велика вероятность того, что внутри фюзеляжей могут устанавливаться радиолокационные антенные решетки и оптико-электронные системы.

**Источник:** <http://www.janes.com/article/51759/images-emerge-of-new-chinese-twin-fuselage-hale-uav-concept> (дата размещения материала 28.05.2015).

### *Беспилотник королевского военно-морского флота Австралии*

В соответствии с информацией сайта [absrf.ru](http://absrf.ru), в Австралии проведены испытания БПЛА CAMCORTER S-100 производства компании «Schiebel». В качестве



полезных грузов при выполнении испытательных полетов в прибрежных зонах и над открытым океаном использовались устройство радиоэлектронной разведки SAGE, радар PicoSAR компании «Selex ES» и прибор наблюдения MX-10 компании «L-3 Wescam».

БПЛА S-100 является единственным в своем классе аппаратом, позволяющим комбинировать различные полезные нагрузки, тем самым можно получать изображения с оптических и инфракрасных камер, обнаруживать и идентифицировать радиоэлектронные объекты и использовать радиолокатор с синтезированной апертурой в режиме реального времени.

**Источник:** <http://absrf.ru/ru/policy/2015-06-18.htm> (дата размещения материала 18.06.2015).

### *Авиационные программы Индии*

Журнал «Авиация и космонавтика» публикует информацию о программах Индии по созданию БПЛА различных классов. Компания «HAL» ведет разработку всепогодного беспилотника, оснащенного РЛС с синтезированной апертурой и продолжительностью полета около 50 часов, а также беспилотного

<sup>5</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.



варианта вертолета «Дхрув». Управление аэроисследований «ADE» разработало средневысотный БПЛА «Рустом-1» с продолжительностью нахождения в воздухе 12-15 часов и дальностью полета до 250 км.

Перспективы данного БПЛА не совсем ясны: возможно он будет принят на вооружение индийской армии, но также не исключается, что он послужит лишь в качестве промежуточного этапа на пути к созданию более совершенного аппарата.



**Источник:** Авиация и космонавтика, 2015, № 6, с. 42-46.

### *Новая мультидатчиковая система видовой разведки M-19 HD*

Как информирует журнал «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления», компания «Israel Aerospace Industries» успешно завершила серию летных испытаний мультидатчиковой системы видовой разведки M-19 HD на пилотируемых и беспилотных платформах. Конструктивно система представляет собой единый компактный блок, в котором может быть установлено одновременно до семи датчиков.



Система M-19 HD обеспечивает ведение непрерывного наблюдения и разведки в любое время суток и в любых погодных условиях. Благодаря высоким уровням чувствительности датчиков и стабилизации, а также уникальным возможностям обработки изображений обеспечивается возможность обнаружения и захвата целей на максимальных дальностях.

M-19 HD устанавливается на современных разведывательных БПЛА, таких как «Heron-1» и «Heron-TP», а также на аэростатах и пилотируемых самолетах, способных решать стратегические задачи.

**Источник:** Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 5, с. 3.

### *Беспилотные летательные аппараты НАТО будут барражировать над Литвой*

По данным ряда сайтов, беспилотники НАТО с 2017 г. начнут выполнять разведывательные полеты над Литвой в рамках проекта альянса «Системы наблюдения с воздуха». Литва с 2013 г. вовлечена в проект наряду с еще 14 странами.

Первый беспилотник данного проекта будет представлен в США уже в июне этого года. Аппараты такого типа могут находиться в воздухе почти сутки, подниматься на вы-





соту 20 км и наблюдать за местностью в любых погодных условиях. В состав полезной нагрузки будут входить радары, детекторы движущихся целей, инфракрасные камеры и другие средства разведки.

Подготовка к старту проекта «Системы наблюдения с воздуха» идет и в Европе: в Италии, на военной базе США в Сицилии, создается главный опорный пункт для выполнения таких операций. С этой базы беспилотники-разведчики будут вылетать для выполнения разведывательных задач. Полеты дронов также планируются над Эстонией.

**Источники:** [http://rus.tvnet.lv/novosti/za\\_rubjezhom/292775jespilotniki\\_nato\\_budut\\_barrazhirovat\\_nad\\_litvoy\\_dlja\\_pjerjedachi\\_razvjeddannih\\_v\\_sluchaje\\_voyni](http://rus.tvnet.lv/novosti/za_rubjezhom/292775jespilotniki_nato_budut_barrazhirovat_nad_litvoy_dlja_pjerjedachi_razvjeddannih_v_sluchaje_voyni) (дата размещения материала 25.05.2015); <http://vpk-news.ru/news/25348>; <http://zn.ua/WORLD/bespilotniki-nato-budut-vesti-razvedku-nad-litvoy-177261>; <http://www.kompravda.eu/online/news/2064951>.

### *США и Норвегия проведут авиаинспекцию над территорией России*

На сайте [vpk-news.ru](http://vpk-news.ru) со ссылкой на начальника российского национального Центра по уменьшению ядерной опасности С.Рыжкова сообщается, что



специалисты из США и Норвегии оценят обстановку в России с самолета наблюдения CN-235 в рамках Договора по открытому небу. Полет будет проходить по согласованному маршруту. На борту самолета российские специалисты смогут проконтролировать строгое соблюдение параметров полета и применение предусмотренной Договором аппаратуры наблюдения. Самолет наблюдения CN-235 относится к классу самолетов, не предназначенных для применения какого-либо оружия.

**Источник:** <http://vpk-news.ru/news/25338> (дата размещения материала 24.05.2015).

### *Новые боевые корабли приспособлены к ведению сетецентрической войны*

По данным сайта [army-news.ru](http://army-news.ru), на вооружение ВМС стран Европы и США принимаются корабли, имеющие морские боевые информационно-



управляющие системы, позволяющие осуществить системную увязку гидроакустических комплексов, радиолокационных комплексов, РЛС зенитных ракетных комплексов, навигационных систем, противолодочного и противокорабельного комплексов. Системная интеграция оборудования осуществляется в рамках концепции ведения современной сетцентрической войны. Аналогичной по архитектуре системой оснащены корабли ВМС Китая.

**Источник:** <http://army-news.ru/2015/05/vms-avstralii-na-puti-k-pervym-idzhisam> (дата размещения материала 22.05.2015).



### *Заход корабля НАТО в территориальные воды Эстонии*

Как сообщает сайт [regnum.ru](http://regnum.ru) со ссылкой на британское информагентство «ВВС», в территориальные воды Эстонии вошла одна из самых современных немецких подводных лодок U34. Главная задача визита – получение данных об обстановке в акватории северной части Балтийского моря. Также визит корабля ВМС Германии демонстрирует готовность НАТО защитить данный регион. Расширение своего военного присутствия в Прибалтике североатлантический альянс обосновывает «российской угрозой».



**Источник:** <http://www.regnum.ru/news/1929176.html> (дата размещения материала 31.05.2015).

### *Заход эсминца ВМС США «Росс» в Черное море*

По информации ряда сайтов со ссылкой на материалы агентства «Reuters», российский штурмовик Су-24 Черноморского флота вынудил эсминец «Росс» ВМС США отойти в нейтральные воды в восточной части Черного моря. Ранее сообщалось, что эсминец «Росс» зашел в Черное море для выполнения поставленных перед ним задач, в том числе разведывательных. Подойдя к границе российских территориальных вод, он начал курсировать вдоль самой кромки.



Эти действия были восприняты российской стороной как провокационные и агрессивные. Ракетный эсминец ВМС США «Росс» оснащен системой противоракетной обороны «Aegis».

**Источники:** <http://www.kommersant.ru/doc/2738683> (дата размещения материала 30.05.2015); <http://www.regnum.ru/news/polit/1929074.html>, <http://33live.ru/novosti/31-05-2015-vms-ssha-esminec-ross-ne-sbezhal-ot-su-24-a-professionalno-otoshel.html>.

### *Французский корабль электронной разведки вошел в акваторию Черного моря*

Как сообщает портал [lenta.ru](http://lenta.ru), разведывательный корабль французских ВМС «Дюпюи де Лом» вошел в акваторию Черного моря. Корабль предназначен для ведения радиотехнической разведки (обнаружения и анализа излучений радиоэлектронных средств). Он также несет специальную аппаратуру для разведки каналов спутниковой связи. По мнению специалистов, оборудование корабля реализует прослушивание сотовой связи и перехват интернет-трафика.



**Источник:** <http://lenta.ru/news/2015/06/03/france> (дата размещения материала 30.05.2015).



## *Система ES-3701 компании «Exelis» для подводных лодок ВМС Швеции*

По информации, размещенной в журнале «Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления», компания «Exelis» будет поставлять для шведских подводных лодок системы радиотехнической разведки ES-3701 последней версии, возможности которой обеспечат существенную поддержку в формировании ситуационной осведомленности, выдаче целеуказания и решении задач наблюдения.



Система ES-3701 использует круговую интерферометрическую антенную решетку, которая обеспечивает всенаправленное пеленгование по азимуту и широкий обзор по углу места с вероятностью перехвата почти 100%. В стандартной поставке ES-3701 имеет частотный диапазон от 2 до 18 ГГц, который может быть расширен на полосы 0,5-2 и 18-40 ГГц.

Система функционирует при потоке сигналов до 1 млн. импульсов/с, способна отслеживать до 500 сигналов одновременно, имеет настраиваемые режекторные фильтры для перехвата непрерывных излучений диапазона 2-18 ГГц в каналах всенаправленного приема и пеленгования.

**Источник:** Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления, 2015, № 5, с. 20-21.

### *1.2. Техническая защита информации*

*FIRST представила третью версию базы  
данных уязвимостей CVSS <sup>6</sup>*

Как информирует портал Форума по реагированию на инциденты безопасности first.org, вышла третья версия базы данных уязвимостей CVSS. Обновленная версия CVSSv3 содержит раздел аналитической информации, сообщающей специалистам о возможных ущербах и методах парирования уязвимостей. По заявлениям специалистов, усовершенствованная база данных в состоянии прогнозировать возможные будущие уязвимости.

**Источник:** <http://www.first.org/newsroom/releases/20150610> (дата размещения материала 10.06.2015).



*Уязвимости нулевого дня в операционных  
системах iOS и OS X*

На сайте [samsung-fun.ru](http://samsung-fun.ru) размещена информация об обнаружении критических уязвимостей в операционных системах iOS и OS X компании «Apple».

---

<sup>6</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.



Эксплуатация брешей, выявленных в механизмах взаимодействия приложений, позволяет похитить конфиденциальные данные жертвы, хранящиеся в сторонних программах, в том числе в Evernote, Facebook и многих других. Разработчики компании «Apple» не устранили обнаруженные уязвимости в течение шести месяцев после их обнаружения.



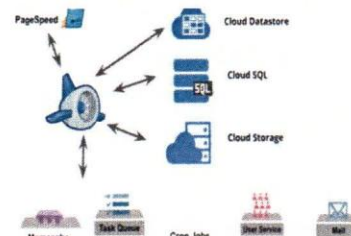
**Источник:** <http://samsung-fun.ru/news/205525> (дата размещения материала 17.06.2015).

### *Уязвимости облачного хостинга Google App Engine*

Как информирует сайт [hacker.ru](http://hacker.ru), эксперты польской компании «Security Explorations» обнаружили семь уязвимостей в Java-платформе, которая лежит в основе облачного хостинга Google App Engine (GAE).

Используя эти баги, злоумышленник, владея одной из виртуальных машин на хостинге GAE, может выйти далеко за пределы своих полномочий.

Три из семи багов допускают полный выход из песочницы GAE Java, которая используется для изоляции виртуальных машин в целях безопасности. Злоумышленник может извлечь информацию о Java Runtime Environment, внутренних сервисах и протоколах «Google», что позволяет ему осуществить атаку с учетом этих данных, нацеливаясь уже на саму платформу GAE.



**Источник:** <https://hacker.ru/2015/05/28/google-app-engine> (дата размещения материала 28.05.2015).

### *Уязвимости в Oracle PeopleSoft могут привести к краже персональной информации*

На ряде сайтов размещена информация об уязвимостях платформы Oracle PeopleSoft, эксплуатация которых позволит злоумышленникам легко получить пароли администратора. Учетные данные клиентов PeopleSoft могут быть извлечены из токенов, содержащихся на сайтах для восстановления паролей, и подобраны при помощи графического процессора.



Уязвимость связана со слабыми стандартами генерации ключей. В отдельных случаях злоумышленнику даже не потребуется наличие учетной записи, чтобы извлечь ключ, поскольку некоторые публичные web-страницы генерируют ключи автоматически. Единственным выходом из ситуации будет установка сильного пароля для узла или замена аутентификации с помощью пароля на авторизацию сертификатами.

Платформу Oracle PeopleSoft использует более 7 тыс. предприятий, часть из которых входит в список самых крупных компаний США.



**Источник:** <http://www.securitylab.ru/news/473081.php> (дата размещения материала 28.05.2015); <http://www.anti-malware.ru/news/2015-06-03/16241>.

### *Уязвимость во встроенном почтовом клиенте операционной системы iOS 8.3*

На сайте securitylab.ru со ссылкой на заявление главы компании «Ernst and Young» Жана Соучека (<https://github.com/jansoucek/iOS-Mail.app-inject-kit>) сообщается об обнаружении уязвимости во встроенном почтовом клиенте опе-



рационной системы iOS 8.3. Эксплуатация уязвимости позволяет реалистично отображать всплывающие уведомления от операционной системы. Она позволяет удаленно загружать на целевое устройство HTML-контент, заменяя им содержимое исходного сообщения электронной почты. В этом случае нельзя использовать JavaScript, однако даже

без него сохраняется возможность создания программы, к примеру, перехватывающей пароли.

По словам специалистов, уязвимость затрагивает миллионы активных пользователей компьютеров «Apple».

**Источник:** <http://www.securitylab.ru/news/473300.php> (дата размещения материала 10.06.2015).

### *Критическая уязвимость в коде эмуляции Ethernet-адаптера AMD PCnet в составе QEMU*

По информации сайта anti-malware.ru со ссылкой на портал googleprojectzero.blogspot.co.uk, в коде эмуляции Ethernet-адаптера AMD PCnet,



поставляемого в составе QEMU, выявлена критическая уязвимость. Эта работа проведена участниками группы «Zero», созданной компанией «Google» для предотвращения атак, совершаемых с использованием ранее неизвестных уязвимостей. Выявленная уязвимость позволяет выйти за пределы гостевого окружения, выполняемого с

использованием компонентов эмуляции аппаратных устройств. В случае успешной эксплуатации уязвимости злоумышленник может выполнить свой код с правами процесса qemu на стороне хост-системы.

Кроме QEMU, уязвимость проявляется в Xen, KVM (qemu-kvm) и других системах виртуализации, использующих компоненты QEMU. Для устранения проблемы в QEMU подготовлено обновление ПО.

**Источник:** <http://www.anti-malware.ru/news/2015-06-11/16287> (дата размещения материала 11.06.2015).

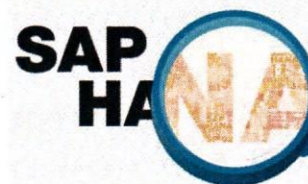
### *В SAP HANA обнаружена серьезная проблема безопасности*

Как сообщает ряд сайтов, специалисты компании «Digital Security» обнаружили серьезную проблему безопасности в SAP HANA. Злоумышленники по-



тениально могут получить доступ к паролям пользователей системы и ключам шифрования, а после этого – ко всем данным предприятия, которые обрабатывает данное решение.

SAP HANA является платформой для управления базами данных и предназначена для обработки больших объемов информации в режиме реального времени. Число активных пользователей платформы из сферы производства, финансов, информационных технологий и розничных продаж превышает 800 тыс. человек. Компания «SAP» уведомлена о наличии уязвимости в системе защиты. Однако до сих пор проблема не устранена.



**Источники:** <http://www.pcweek.ru/security/news-company/detail.php?ID=175453> (дата размещения материала 22.06.2015); <https://threatpost.ru/2015/06/19/static-encryption-key-found-in-sap-hana-database>.

### *Скомпрометированные SSH ключи могли использовать для получения доступа к репозиториям GitHub*

На сайте securitylab.ru исследователи безопасности из «CloudFlare» сообщили, что официальные репозитории британского правительства, а также разработчиков «Spotify» и «Python» были доступны сторонним пользователям из-за скомпрометированных SSH ключей. Последние были взломаны через уязвимость в Debian OpenSSL. Уязвимость затрагивает функционал генерации случайных чисел. Любые сгенерированные таким образом ключи рассматриваются как скомпрометированные. Эксплуатация бреши позволяет существенно упростить взлом методом перебора.



Последствия эксплуатации бреши могут быть очень серьезными, поскольку ключи SSH используют почти две трети всех пользователей GitHub. При этом администраторы важных хранилищ сменяют ключи довольно редко.

**Источник:** <http://www.securitylab.ru/news/473194.php> (дата размещения материала 03.06.2015).

### *Кража криптографических ключей персональных компьютеров по электромагнитному каналу утечки информации<sup>7</sup>*

Согласно данным сайта securityaffairs.co, исследователями из университета Тель-Авива была продемонстрирована возможность перехвата информации, содержащей криптоключи, за счет побочных электромагнитных излучений (ПЭМИ).

В своем исследовании они опирались на результаты более ранней работы компании «Genkin», в рамках которой 409-битные RSA ключи удалось вскрыть при помощи зву-



<sup>7</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.



ковых волн, излучаемых компьютером в процессе расшифровки ключей. Сейчас же специалисты с помощью самого дешевого набора устройств перехватывали ПЭМИ компьютеров на базе GnuPG, что позволило раскрыть криптографические ключи в течение нескольких секунд. Во время эксперимента специалисты использовали приставку Funcube Dongle Pro+, подключенную к миниатюрному Android-компьютеру Rikomagic MK802 IV (перехват происходил на частотах 1,6 МГц и 1,75 МГц).

**Источник:** <http://securityaffairs.co/wordpress/37950/hacking/stealing-crypto-keys-radio-emissions.html> (дата размещения материала 20.06.2015).

### *Уязвимость в Apache Cordova*

На сайте securitylab.ru размещена информация о найденной специалистами «Trend Micro» (trendmicro.com) уязвимости во фреймворке Apache Cordova. Apache Cordova используется в Android-программах и представляет собой



группу методов API, позволяющих разрабатывать кросс-платформенные приложения с помощью стандартных web-технологий.

Приложение запускается на мобильном устройстве и может получать доступ к оригинальным функциям устройства, таким как GPS или камера. Эксплуатация уязвимости позволяет злоумышленнику модифицировать поведение приложения. По данным разработчика Apache Cordova уже выпущена исправленная версия программы.

**Источник:** <http://www.securitylab.ru/news/473122.php> (дата размещения материала 01.06.2015).

### *Уязвимость файловой системы Ubuntu*

Сайт anti-malware.ru со ссылкой на официальный портал разработчиков операционной системы Ubuntu (Ubuntu.com) сообщает об обнаружении уязвимости файловой системы OverlayFS операционной системы Ubuntu. Данную



уязвимость можно использовать для получения root-доступа на системах, в которых разрешено монтирование разделов OverlayFS непривилегированным пользователем. Достаточные для эксплуатации уязвимости настройки по умолчанию обнаружены во всех поддерживаемых ветках Ubuntu (12.04, 14.04, 14.10 и 15.04). Опасность проблемы

продемонстрирована готовым эксплойтом, позволяющим запустить shell с правами root.

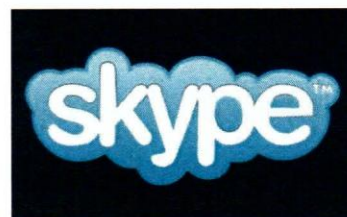
Разработчики Ubuntu уже оперативно выпустили обновление ядра Linux с исправленным модулем OverlayFS.

**Источник:** <http://www.anti-malware.ru/news/2015-06-16/16310> (дата размещения материала 16.06.2015).



### *Ошибка в Skype позволяет дистанционно вызывать сбой в приложении на компьютере собеседника*

По данным сайта securitylab.ru со ссылкой на российских блогеров, пользователи Skype обнаружили неприятную ошибку при обработке строки «http://:», позволяющую дистанционно вызвать сбой в приложении на компьютере собеседника. Если указать эту строку в сообщении, Skype получателя завершает свою работу аварийно каждый раз, когда пользователь пытается авторизоваться. Это же наблюдается и в поле «Настройка». Ошибка влияет на работу Skype для некоторых версий Windows, Android и IOS.



Устранить неполадки можно, если пользователь, получивший вредоносную строку, удалит сообщение или будет использовать более старые версии Skype (уязвимость распространяется только на версию 7.4.0.102). Разработчики Skype уже начали работу над ее устранением.

**Источник:** <http://www.securitylab.ru/news/473174.php> (дата размещения материала 03.06.2015).

### *Уязвимость в компьютерах производства компании «Apple»*

На сайте informing.ru со ссылкой на блог специалиста по информационной безопасности Педро Вилака сообщается, что в компьютерах корпорации «Apple», выпущенных до середины 2014 г., обнаружена критическая уязвимость. Она дает хакерам возможность сменить прошивку устройства, параллельно инкапсулируя в загрузочную область вредоносную программу. Такую программу сложно найти и удалить, так как стандартные антивирусные сканеры ее не выявляют.



Проблема обнаруженной уязвимости в том, что после выхода устройства из ждущего режима защита от перепрошивки UEFI в разных моделях компьютеров «Apple» пропадает. Злоумышленники могут без особых усилий внедрить в прошивку вредоносную программу. Причем, чтобы избавиться от защиты, злоумышленнику достаточно перевести компьютер в ждущий режим и сразу же вывести его из него.

**Источник:** <http://informing.ru/2015/06/02/v-kompyuterah-apple-obnaruzhena-dyra-blagodarya-kotoroy-mozhno-ustanavlivat-vechnye-troyany.html> (дата размещения материала 26.05.2015).

### *Обнаружены 60 уязвимостей в 22 моделях маршрутизаторов от разных производителей*

По информации ряда сайтов со ссылкой на информационный портал компании разработчика сканеров уязвимостей «Nmap Security» (seclists.org), обнаружено около 60 уязвимостей в 22 моделях маршрутизаторов от разных производителей. Большинство из уязвимых устройств были получены пользователя-



ми от их интернет-провайдеров. Брешы позволяют злоумышленникам обойти аутентификацию, считывать и записывать информацию на USB-устройства, подключенные к уязвимому маршрутизатору, перегружать, а также выполнять вредоносный код через web-интерфейс управления.



К уязвимым моделям относятся: Observa Telecom AW4062, RTA01N, Home Station BHS-RTA и VH4032N; Comtrend WAP-5813n, CT-5365, AR-5387un и 536+; Sagem LiveBox Pro 2 SP и Fast 1201; Huawei HG553 и HG556a; Amper Xavi 7968, 7968+ и ASL-26555; D-Link DSL-2750B и DIR-600; Belkin F5D7632-4; Linksys WRT54GL; Astoria ARV7510; Netgear CG3100D и Zyxel P 660HW-B1A.

**Источники:** <http://www.securitylab.ru/news/473169.php> (дата размещения материала 03.06.2015); <http://deleysk.ru/muzhskaya-stranitsa/obnaruzheny-desyatki-uyazvimostey-v-22-modelyah-routerov-ot-raznyh-proizvoditeley>.

### *Обнаружены критические уязвимости в устройствах D-Link*

Как сообщает сайт securitylab.ru, исследователи из компании «Search-Lab» (search-lab.hu) обнаружили множественные уязвимости в нескольких продуктах «D-Link». Некоторые брешы позволяют злоумышленнику обойти аутентификацию или загрузить произвольные файлы на целевое устройство.

Уязвимости выявлены в сетевых устройствах хранения данных D-Link, включая D-Link DNS-320, 320L, 326, 327L, 320B, 345, 325 и 322L. Эксперты сообщили, что не каждая модель подвержена всем уязвимостям. Самой распространенной отмечается брешь, которая позволяет обойти аутентификацию.

Также обнаружен бэкдор в D-Link DNS-320L, 327L, 320B, 345, 325, 322L и DNR-326, с помощью которого злоумышленник может получить полный доступ к устройству. «D-Link» уже выпустила обновления прошивки для устранения некоторых из данных проблем.

**Источник:** <http://www.securitylab.ru/news/473148.php> (дата размещения материала 02.06.2015).

### *Предлагаемые мобильными операторами 3G- и 4G-модемы уязвимы для хакерских атак*

В соответствии с информацией, размещенной на сайте threatpost.ru ссылкой на новостной портал csoonline.com, почти все 3G- и 4G-модемы, предлагаемые мобильными операторами клиентам, уязвимы для хакерских атак.



Уязвимости позволяют хакерам красть или изменять текстовые сообщения пользователей, получать список контактов, данные соединения Wi-Fi и DNS-конфигурацию. Кроме того, злоумышленники могут заставлять операционные системы выполнять их команды. В ряде случаев устройства могут быть превращены во вредоносные платформы, которые зара-



жают другие компьютеры.

**Источник:** <https://threatpost.ru/2015/06/02/operatory-razdayut-polzovatelyam-opasnye-3g-i-4g-modemy> (дата размещения материала 02.06.2015).

### *Уязвимость в Bluetooth*

Как сообщает ряд сайтов со ссылкой на информационный ресурс contextis.com, обнаружена уязвимость в реализации технологии Bluetooth, которая дает злоумышленнику возможность отследить местонахождение устройства на расстоянии до 100 метров. Злоумышленник может использовать данные о местонахождении конкретного устройства для социальной инженерии либо физически осуществляемого преступления.



Эксперты компании «Context» разработали приложение, названное Ramble, которое сканирует, обнаруживает и регистрирует уязвимые устройства. Оно позволяет собрать данные о 150 устройствах за 30 минут. В список уязвимых продуктов попали фитнес-трекеры от FitBit и Jawbone, а также iPhone.

**Источники:** <http://www.klerk.ru/soft/news/420220/> (дата размещения материала 25.05.2015); <http://www.securitylab.ru/news/473036.php>.

### *Уязвимости технологических медицинских информационных систем*

На сайте securitylab.ru размещен аналитический обзор специалистов компании «TrapX Security» о наличии уязвимостей в медицинских информационных системах. По данным отчета, локальные сети медицинских учреждений США могут эксплуатироваться киберпреступниками с целью получения контроля над медицинскими устройствами, которые используют устаревшее ПО.



Дело в том, что большинство больниц используют для безопасности своих сетей межсетевые экраны. Однако обновления ПО для медицинских устройств зачастую не устанавливаются. Из-за того, что оборудование работает постоянно, сотрудники IT-отделов больниц не имеют возможности проверить актуальность версии используемого ПО, которое обеспечивает работу устройств.

**Источник:** <http://www.securitylab.ru/news/473270.php> (дата размещения материала 09.06.2015).

### *Корпорация «Microsoft» выпустила 8 плановых обновлений для своих продуктов*

Согласно информации сайта securitylab.ru со ссылкой на официальный портал «Microsoft» (microsoft.com), корпорацией выпущено 8 плановых обновлений для своих продуктов. Обновления ПО исправляют уязвимости в Internet Explorer, Windows, Office, Windows Media Player, Ac-





tive Directory и Exchange Server. Системным администраторам рекомендуется установить обновления для Office 2007, Office 2010 и Office 2013. Серьезные уязвимости в этих продуктах могут позволить злоумышленникам получить контроль над компьютером, заставив жертву открыть вредоносный файл.

**Источник:** <http://www.securitylab.ru/news/473284.php> (дата размещения материала 10.06.2015).

### *«Apple» заблокировала старые версии Adobe Flash Player*



По данным сайта [freesoft.ru](http://freesoft.ru) со ссылкой на официальный сайт компании «Apple» ([apple.com](http://apple.com)), компания обновила свой «черный список» ПО, включив в него устаревшие версии плагина от «Adobe». «Adobe» выпустила обновленную версию Flash Player для Windows и Mac OS X, которая исправила 18 уязвимостей нарушения целостности памяти, брешь переполнения динамически распределяемой области памяти, ошибку переполнения целочисленного типа памяти и уязвимость использования освобожденной памяти.

Каждая из брешей позволяла злоумышленнику получить удаленный доступ к компьютеру жертвы. Пользователям Mac OS X было настоятельно рекомендовано обновить Flash Player до версии 17.0.0.188.

**Источник:** <http://freesoft.ru/?news=2765> (дата размещения материала 29.05.2015).

### *Устранена опасная уязвимость системы управления контентом Drupal*



Как сообщает сайт [stfw.ru](http://stfw.ru) со ссылкой на заявление разработчиков популярной системы управления контентом Drupal ([drupal.org](http://drupal.org)), в новой версии системы устранен ряд уязвимостей. Одна из них получила критический рейтинг опасности. Уязвимость позволяла атакующему удаленно захватить контроль над чужой учетной записью с административными правами доступа. Три другие уязвимости в Drupal имели меньший рейтинг опасности из-за того, что применить их в ходе нападения на порядок сложнее. Тем не менее, потенциальный вред от эксплуатации этих брешей довольно высок. К примеру, ошибка в модуле Field UI позволяет злоумышленникам при соблюдении ряда условий использовать параметр «destinations» для перенаправления пользователя на произвольный web-сайт.

**Источник:** <http://stfw.ru/page.php?id=50230> (дата размещения материала 22.06.2015).

### *Исправлены уязвимости в программном обеспечении сетевых накопителей компании «Synology»*

По информации сайта [securitylab.ru](http://securitylab.ru) со ссылкой на официальный портал компании «Synology» ([synology.com](http://synology.com)), исправлены две уязвимости в ПО сетевых



накопителей. XSS-уязвимость в DiskStation Manager может позволить злоумышленнику выполнить произвольный код JavaScript-сценария в браузере жертвы и получить доступ к сеансовому идентификатору.

Уязвимость в online-фотоальбоме Synology Photo Station, используемом пользователями для обмена фото- и видеоматериалами, позволяет выполнить произвольные системные команды с привилегиями web-сервера. Обе уязвимости исправлены в соответствующем обновлении ПО.

**Источник:** <http://www.securitylab.ru/news/473051.php> (дата размещения материала 26.05.2015).

### *Исправлены уязвимости в платформе электронной почты Sendio ESP*

Как сообщает сайт threatpost.ru, исправлена уязвимость в платформе электронной почты Sendio ESP компании «Sendio» (sendio.com). Уязвимость содержала две проблемы, приводящие к раскрытию информации. Первая уязвимость приводит к раскрытию куки сессии через URL в веб-интерфейсе Sendio.

Второй баг вызван некорректной обработкой пользовательских сессий все тем же веб-интерфейсом. Обе уязвимости присутствовали в некоторых версиях этого ПО. Они могли послужить причиной утечки конфиденциальной информации, такой как идентификаторы сессии и/или сообщения электронной почты.

**Источник:** <https://threatpost.ru/2015/05/25/sendio-email-platform-patches-remote-security-bypass-vulnerability> (дата размещения материала 25.05.2015).

### *«Blue Coat» устранила четыре бреши в платформе SSL Visibility Appliance*

Согласно данным, приведенным на сайте securitylab.ru, компания «Blue Coat» (bluecoat.com) выпустила исправленное обновление для своей платформы Blue Coat SSL Visibility Appliance, устраняющее четыре бреши, которые затрагивают административную консоль WebUI.

Платформа разработана в качестве решения для управления зашифрованным трафиком, позволяющего проводить оценку угроз и предотвращать потерю данных. Компонент WebUI позволяет клиентам конфигурировать продукт и управлять им. Первая из уязвимостей (CVE-2015-2852) – это CSRF (межсайтовая подделка запроса), которая может быть проэксплуатирована удаленным пользователем с целью получения доступа к административной платформе и осуществления различных действий с правами администратора.

Кроме того, компонент WebUI уязвим к кликджекинг-атакам (из-за некорректной проверки правильности запроса (CVE-2015-2854)), а также к похи-





щению файлов cookie (CVE-2015-2855) и к фиксации сессии (CVE-2015-2853). Компания уже выпустила обновление SSL Visibility 3.8.4, исправляющее уязвимости.

**Источник:** <http://www.securitylab.ru/news/473168.php> (дата размещения материала 03.06.2015).

### *Новое вымогательское программное обеспечение Troldash*

На сайте freesoft.ru со ссылкой на заявление специалистов компании



«Check Point» (checkpoint.com) размещена информация о появлении в Интернете нового вымогательского ПО Troldash. Вредоносное ПО распространяется при помощи спама. Сразу после того, как вредоносный файл попадает в систему, запускается процесс шифрования, а затем жертва

видит сообщение с инструкциями по проведению оплаты.

**Источник:** <http://freesoft.ru/?news=2797> (дата размещения материала 04.06.2015).

### *Набор эксплоитов Angler использован для распространения вымогательского программного обеспечения CryptoWall*

Как сообщает сайт securitylab.ru со ссылкой на аналитический отчет

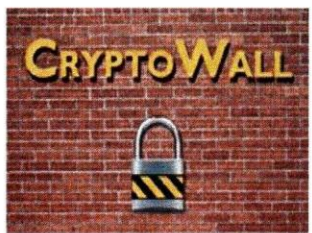


«SANS Internet Storm Center» (sans.org), обнаружено два случая распространения вымогателя CryptoWall 3.0 с помощью набора эксплоитов Angler. В обоих случаях для оплаты дешифровки предоставлялся один и тот же адрес Bitcoin-кошелька. Ранее CryptoWall 3.0 загружался набором эксплоитов Magnitude. Для реализации в Angler эксплуатируется уязвимость Adobe Flash Player.

**Источник:** <http://www.securitylab.ru/news/473108.php> (дата размещения материала 29.05.2015).

### *SVG-файлы используют для распространения вымогательского программного обеспечения*

Согласно размещенной на сайте internetua.com со ссылкой на заявление специалистов по информационной безопасности компании «AppRiver»



(appriver.com) информации, зафиксирована кампания, в ходе которой злоумышленники пытались распространять вымогательское ПО при помощи файлов SVG. Преступники рассылали электронные письма, к которым было прикреплено фальшивое резюме. Приложение к письму представляло собой ZIP-архив, содержащий файл с расширением SVG. Он включал небольшой код JavaScript, который перенаправлял жертв на страницу, распространявшую вымогательское ПО.

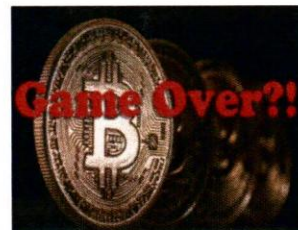


Для реализации своих целей хакерами применялся один из популярных представителей семейства вымогателей CryptoWall. Программа инфицировала компьютер жертвы и зашифровала важные файлы, требуя выкуп за их дешифрование.

**Источник:** <http://internetua.com/zlounishlenniki-ispolzovat-SVG-faili-dlya-rasprostraneniya-vimogatelyskogo-po> (дата размещения материала 25.05.2015).

*Для распространения вымогательского программного обеспечения TeslaCrypt использован набор эксплойтов Angler*

Сайт securitylab.ru со ссылкой на отчет специалистов компании «Dell SecureWorks» ([secureworks.com](http://secureworks.com)) сообщает, что специалисты компании «Dell SecureWorks» зарегистрировали мошенническую кампанию распространения вымогательского ПО TeslaCrypt. В ходе кампании преступники используют набор эксплойтов Angler и сеть Tor. Троян TeslaCrypt зашифровал файлы на инфицированной машине и требовал оплаты за их дешифрование. TeslaCrypt использует усовершенствованный алгоритм, предназначенный для зашифрования популярных файловых форматов Open Office и Microsoft Office, а также файлы, связанные с видеоиграми и приложениями для творчества.



Данная кампания является особо опасной из-за того, что Angler использует особые методы инфицирования, которые обычно не применяются в предназначенных для атак автоматизированных инструментах. Кроме этого, использование злоумышленниками сети Tor усложняет обнаружение источника атак.

**Источник:** <http://www.securitylab.ru/news/473074.php> (дата размещения материала 27.05.2015).

*Файлы PowerPoint используются в фишинговых атаках*

В соответствии с информацией, размещенной на сайте internetua.com со ссылкой на аналитический отчет специалистов по информационной безопасности компании «Fidelis Cybersecurity» ([fidelissecurity.com](http://fidelissecurity.com)), при помощи файлов PowerPoint с внедренным вредоносным кодом злоумышленники обходят антивирусную защиту. Для успешной атаки достаточно, чтобы пользователь целевой системы открыл документ в формате слайд-шоу.



Обнаруженная угроза основана на эксплуатации известной уязвимости, которая позволяет удаленное выполнение кода и затрагивает операционные системы Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows Server 2012, а также Windows RT 8.1.

**Источник:** <http://internetua.com/faili-PowerPoint-nacsali-ispolzovatsya-v-fishingovih-atakah> (дата размещения материала 15.06.2015).



*Панель Ask классифицирована как нежелательное программное обеспечение*

По данным сайта [threatpost.ru](http://threatpost.ru) со ссылкой на заявление специалистов компании «Microsoft» ([microsoft.com](http://microsoft.com)), панель инструментов Ask причислена к разряду нежелательного ПО. Панель Ask изменяет настройки браузеров, добавляя себя на панель инструментов браузера и заменяя настроенный по умолчанию поисковик на Ask.com. Средства защиты информации Windows Defender для Windows 8.1 и Microsoft Security Essentials для Windows 7 и Windows Vista будут детектировать и удалять данную панель. Решение компании «Microsoft» было с одобрением встречено профессионалами из сфер информационной безопасности и конфиденциальности и не только потому, что панель Ask считается уязвимым ПО, но также по причине того, что она вызывает снижение производительности браузеров.

**Источник:** <https://threatpost.ru/2015/06/16/microsoft-classifies-ask-toolbar-as-unwanted-software> (дата размещения материала 16.06.2015).

*Новая вредоносная программа для операционной системы Mac OS X*

Согласно информации, размещенной на сайте [pcweek.ru](http://pcweek.ru) со ссылкой на аналитический отчет специалистов компании «Доктор Веб» ([drweb.ru](http://drweb.ru)), обнаружена программа установщик рекламных и нежелательных приложений – троянец семейства Trojan.Crossrider.



Троянец создан с использованием ресурсов партнерской программы для монетизации приложений [macdownloadpro.com](http://macdownloadpro.com). Сайты многочисленных «партнеров» этой системы, как правило, содержат различную рекламу, автоматически открывают дополнительные вкладки, а сам установщик посетителям предлагается скачать под видом какого-либо «полезного» приложения или даже музыкального MP3-файла. В некоторых случаях загрузка установщика осуществляется с использованием автоматического перенаправления пользователя на соответствующую веб-страницу.

Сигнатуры вредоносных программ уже внесены в базы антивирусов.

**Источник:** <http://www.pcweek.ru/security/news-company/detail.php?ID=175448> (дата размещения материала 22.06.2015).

*Компания «Доктор Веб» обнаружила вредоносную программу, предназначенную для рассылки спама по электронной почте*



Как информирует сайт [drweb.ru](http://drweb.ru), новый троянец-спамер, исследованный недавно аналитиками компании «Доктор Веб», имеет несколько любопытных конструктивных особенностей. В частности, установка в систему программного кода вируса начинается с остановки ядра операционной системы. Основным предназначением



вредоносного ПО является рассылка почтового спама совместно с удаленным спам-сервером.

**Источник:** <http://news.drweb.ru/show/?i=9474&lng=ru&c=14> (дата размещения материала 03.06.2015).

### *Обнаружена новая кампания распространения банковских троянов Zeus*

Сайт threatpost.ru со ссылкой на отчет специалистов компании «PricewaterhouseCoopers» ([www.pwc.com](http://www.pwc.com)) сообщает, что найден модернизированный вариант банковского трояна Zeus. Особенностью обнаруженного вредоносного ПО является его повышенная скрытность от средств защиты информации и использование эксплойта Neutrino для заражения целевой ЭВМ. Как обнаружили эксперты, домен, из которого осуществляются вредоносные загрузки, принадлежит китайской компании.



В Интернете опубликованы простейшие сигнатуры нового Zeus и его управляющего центра для систем обнаружения вторжений Snort и Suricata.

**Источник:** [https://threatpost.ru/2015/06/08/novaja\\_zeus-kampanija\\_s\\_uchastiem\\_neutrino](https://threatpost.ru/2015/06/08/novaja_zeus-kampanija_s_uchastiem_neutrino) (дата размещения материала 06.06.2015).

### *Обнаружена обновленная версия банковского троянца Tinba*

На сайте threatpost.ru со ссылкой на заявление специалистов «IBM Trusteer» ([securityintelligence.com](http://securityintelligence.com)) размещена информация об обнаружении новой вредоносной кампании, нацеленной на распространение банковского троянца Tinba на территории Западной Европы.



Новый троянец имеет дополнительные свойства, повышающие его эффективность, а также жизнестойкость ботнетов, построенных на его основе. Зловред запрашивает у пользователя персональные и регистрационные данные в зависимости от банка-мишени, а также может сообщить о временной блокировке аккаунта и попросить срочно инициировать транзакцию под предлогом мнимой ошибки в денежном переводе. Анализ нового варианта Tinba выявил ряд технологий, защищающих его от обнаружения и захвата.

**Источник:** [https://threatpost.ru/2015/06/09/evropejtsev\\_atakuet\\_obnovlennyj\\_tinba](https://threatpost.ru/2015/06/09/evropejtsev_atakuet_obnovlennyj_tinba) (дата размещения материала 09.06.2015).

### *Новый банковский троянец для кражи денег с банковских счетов пользователей мобильных Android-устройств*

По данным сайта [news.drweb.ru](http://news.drweb.ru), специалисты компании «Доктор Веб» обнаружили нового троянца, предназначенного для кражи денег с банковских счетов пользователей мобильных Android-устройств.





приложения.

**Источник:** <http://news.drweb.ru/show/?i=9489&lng=ru&c=14> (дата размещения материала 10.06.2015).

### *Новый вирус заражает роутеры и медицинское оборудование*

Согласно сообщению, приведенному на сайте [ict-online.ru](http://ict-online.ru) со ссылкой на отчет компании «ESET» ([esetnod32.ru](http://esetnod32.ru)), обнаружен новый интернет-вирус, активно заражающий роутеры, точки доступа к Wi-Fi в общественных местах и некоторое медицинское оборудование. Вредоносное ПО под названием *elan* взламывает устройства посредством простого перебора ряда слабых паролей, которые чаще всего устанавливают производители или пользователи.



Уязвимыми уже признаны роутеры компаний «Actiontec», «Hik Vision», «Netgear», «Synology», «TP-Link», «ZyXEL» и «Zhone». После заражения вирус незаметно запускается на роутере и начинает перехватывать пароли от Instagram, Twitter, Facebook и YouTube. По мнению экспертов, заражению могло быть подвергнуто более 1 млн. устройств.

**Источник:** <http://ict-online.ru/news/n118670> (дата размещения материала 03.06.2015).

### *Обнаружен вирус, скрывающийся в изображениях*

На сайте [internetua.com](http://internetua.com) со ссылкой на сообщение специалистов компании «Dell SecureWorks» ([secureworks.com](http://secureworks.com)) размещена информация об активном распространении в Интернете малоизвестного семейства вредоносных программ, представляющих собой новую тенденцию развития вирусов. Обнаруженный вирус использует технологии цифровой стеганографии для сокрытия вредоносного кода от антивирусных инструментов.



В настоящий момент вирус распространяется через web-сайты с пиратским ПО, где злоумышленники публикуют инфицированный генератор лицензионных ключей. После запуска в целевой ЭВМ этот инструмент дополнительно загружает основной компонент – PNG-изображение, размещенное на веб-сайте и скрывающее вредоносный код.



**Источник:** <http://internetua.com/obnarujen-virus--skrivauasxiisya-v-razme-sxennih-na-legitimnih-web-saitah-izobrajeniyah> (дата размещения материала 17.06.2015).

### *Androi-троянец маскируется под входящее сообщение*

Как сообщает сайт [news.drweb.ru](http://news.drweb.ru), специалисты компании «Доктор Веб» обнаружили очередного «мобильного» троянца, который демонстрирует различные рекламные уведомления, ведущие к загрузке нежелательного и вредоносного ПО. Данная программа интересна тем, что отображаемые ею сообщения имитируют поступление СМС и email-корреспонденции, в результате чего потенциальные жертвы с большей вероятностью обратят на них внимание и принесут прибыль мошенникам, установив то или иное опасное приложение.

Вредоносная программа распространяется на посвященных мобильным приложениям сайтах и, по заявлению ее создателей, представляет собой своего рода телефонного помощника, демонстрирующего во время звонка на экране страну, регион собеседника, а также название предоставляющего ему услуги связи оператора.

**Источник:** <http://news.drweb.ru/show/?i=9499&lng=ru&c=14> (дата размещения материала 19.06.2015).

### *Международная операция по борьбе с банковским трояном Shylock*

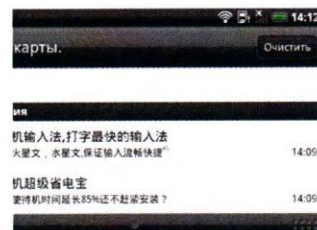
По информации сайта [itsec.ru](http://itsec.ru), Европол ([europol.europa.eu](http://europol.europa.eu)) завершил международную кампанию по борьбе с банковским вирусом Shylock. Shylock оснащен функционалом, позволяющим противостоять удалению, а также восстанавливать себя после перезагрузки системы.

Дополнительной преградой для борьбы с вредоносом является то, что все случаи инфицирования произошли с помощью предварительно скомпрометированных злоумышленниками легитимных web-сайтов. Содействие в расследовании оказали компании «Лаборатория Касперского» и «Microsoft». На сегодняшний день совместные усилия этих организаций позволили практически полностью демонтировать созданный Shylock ботнет.

**Источник:** [http://www.itsec.ru/newstext.php?news\\_id=105272](http://www.itsec.ru/newstext.php?news_id=105272) (дата размещения материала 19.06.2015).

### *Большинство популярных антивирусных продуктов могут быть уязвимы к несанкционированному доступу*

Сайт [astera.ru](http://astera.ru) со ссылкой на сообщение специалистов центра «Digital Security» ([dsec.ru](http://dsec.ru)) разместил информацию о результатах анализа ряда антиви-





русских продуктов. Установлено, что большинство популярных антивирусов могут быть успешно атакованы при помощи известных способов, доступных на публичных ресурсах. В ходе проведения исследований антивирусные программы были подвергнуты атакам при помощи универсальных способов, каждый из которых не был нацелен на конкретное решение и не использовал архитектурные слабости того или иного ПО.



В частности, были задействованы ProxyInject, Duplicate Handle, Reparse-Point, PageFile attack, RegSafe, RegRestore, Shim engine. Эти способы атак доступны на открытых ресурсах Интернета уже несколько лет.

**Источник:** <http://www.astera.ru/news/?id=111401> (дата размещения материала 28.05.2015).

### *Злоумышленники вернулись к тактике ложных антивирусов 10-летней давности*

На сайте securitylab.ru со ссылкой на блог исследователя уязвимостей ПО (blog.0x3a.com) сообщается о новой вредоносной кампании njRat, в ходе ко-



торой злоумышленники применяли довольно старые техники. Отличительной ее чертой является использование скомпрометированных web-сайтов в качестве прокси для C&C-сервера и тактика FakeAV. Использование фальшивого антивируса для заражения компьютеров было популярно десять лет назад и, похоже, применяется до сих пор. Заразить компьютер можно через Интернет, SMS-сообщения, спам, личные сообщения в мессенджерах и т.д. При запуске фальшивого антивируса появляется окно, в котором сообщается, что на компьютере вирусы не обнаружены.

Поддельное антивирусное ПО добавляет себя в процесс начальной загрузки компьютера, в результате чего оно запускается при каждом его включении. IP-адрес C&C-сервера свидетельствует о том, что управление операцией осуществляется из Саудовской Аравии.

**Источник:** <http://www.securitylab.ru/news/473157.php> (дата размещения материала 02.06.2015).

### *Мошенники получают доступ к личным данным через сервис «Microsoft»*

Согласно информации экспертов «Лаборатории Касперского» (kaspersky.ru), размещенной на сайте anti-malware.ru, обнаружена нетипичная уловка злоумышленников, направленная на получение доступа к личным данным пользователя. Мошенники используют в качестве посредника официальный сервис live.com компании «Microsoft», тем самым усыпляя бдительность потенциальной жертвы и подталкивая ее к добровольному разрешению доступа к конфиденциальной информации.





Мошенническая схема представляет собой классический фишинг. При этом пользователь не направляется на поддельную страницу, а переходит на страницу аутентификации легитимного сайта «Microsoft» live.com. После авторизации сервис «Microsoft» отображает запрос на разрешение некоему приложению доступа к личным данным. Если жертва дает свое согласие, авторы приложения получают личные сведения пользователя, которые можно позже использовать в мошеннических целях.

**Источник:** <http://www.anti-malware.ru/news/2015-05-21/16172> (дата размещения материала 21.05.2015).

### *Сайты двух крупных банков США используют слабое шифрование*

Как сообщает сайт securitylab.ru со ссылкой на мнение эксперта, занимающегося кибербезопасностью государственной службы США, Эрика Милла (konklone.com), используемый множеством сайтов протокол SHA-1 обеспечивает слабое шифрование.

Пользователи обозревателя Chrome могли заметить, что при входе на сайты крупных банков США – HSBC и Chase, поле адресной строки не обозначается зеленым фоном, поскольку шифрование не является надежным. Из-за слабого шифрования два разных документа могут иметь один и тот же хэш. Таким образом, цифровая подпись может повторно использоваться злоумышленниками.

«Google» заявила, что с 2017 г. все сайты с протоколом шифрования SHA-1 будут блокироваться в ее продуктах. Аналогичное решение приняли «Microsoft» и «Mozilla».

**Источник:** <http://www.securitylab.ru/news/473170.php> (дата размещения материала 03.06.2015).

### *Файлообменники Megaupload отправляют посетителей на ресурсы с вредоносным программным обеспечением*

Как сообщает сайт newsme.com.ua со ссылкой на издание «The Torrent Freak», несколько арестованных доменных имен Megaupload, в том числе Megaupload.com и Megavideo.com, начали перенаправлять пользователей на ресурсы с мошеннической рекламой и вредоносным ПО.

Вместо отображения уведомления о том, что доменные имена были арестованы в рамках уголовного расследования, они перенаправляют посетителей на рекламную ленту Zero-Click, ссылки на которую в большинстве случаев ведут на вредоносное ПО или рекламные объявления.

**Источник:** <http://newsme.com.ua/tech/technologies/2985252> (дата размещения материала 31.05.2015).





### *Игры в Android отслеживают местоположение устройства*

Согласно информации, размещенной на сайте [samsung-fun.ru](http://samsung-fun.ru) со ссылкой на заявление команды исследователей Датского технического университета (dtu.dk) под руководством Петра Сапезински, некоторые распространяемые через Google Play приложения могут отслеживать местонахождение устройства за счет использования данных о Wi-Fi-соединении. Это происходит даже в том случае, если пользователь не давал приложению разрешения на доступ к информации о подключаемых Wi-Fi-сетях. Слежение за пользователем смартфонов с Android осуществляется при помощи таких геолокационных сервисов, как Skyhook и Google Maps.

**Источник:** <http://samsung-fun.ru/news/202437> (дата размещения материала 26.05.2015).

### *Слежение за смартфонами Android с использованием акселерометра*



В соответствии с информацией, размещенной на сайте [threatpost.ru](http://threatpost.ru) со ссылкой на заявление китайских исследователей из Нанкинского университета ([arxiv.org](http://arxiv.org)), местонахождение владельцев устройств под управлением операционной системы Android легко определить на основе данных акселерометра и датчиков ориентации в смартфоне. В отличие от GPS-данных, данные акселерометра легко получить при помощи потенциально вредоносных приложений, так как доступ к сведениям, собираемым акселерометрами, не требует специальных разрешений.

**Источник:** <https://threatpost.ru/2015/05/27/za-polzovatelyami-smartfonov-android-mozh-no-tajno-sledit> (дата размещения материала 27.05.2015).

### *Камера GoPro Hero 4 может использоваться злоумышленниками для слежки за владельцем*



По сообщению сайта [stfw.ru](http://stfw.ru) со ссылкой на отчет специалистов в области информационной безопасности компании «Pen Test Partners» ([pentestpartners.com](http://pentestpartners.com)), злоумышленники могут получить доступ к выключенной видеокамере GoPro Hero 4, а также реализовать наблюдение или подслушивание разговора пользователя. Кроме того, можно удаленно просмотреть и удалить сохраненные на камере ролики. Несанкционированный доступ возможен в том случае, если пароль на устройстве жертвы недостаточно надежный, и его можно подобрать при помощи специального ПО.

Уязвимость обусловлена тем, что Wi-Fi-подключение в Hero 4 может оставаться активным даже после выключения самой камеры. В видеокамере используется стандартный для устройств такого класса протокол шифрования WPA2-PSK.



**Источник:** <http://stfw.ru/page.php?id=49629> (дата размещения материала 01.06.2015).

*Компания «Microsoft» открывает исходные коды  
программного обеспечения*

Как сообщает сайт [pcweek.ru](http://pcweek.ru), компания «Microsoft» ([microsoft.com](http://microsoft.com)) открыла Центр прозрачности в Брюсселе. Теперь представители правительственных органов смогут знакомиться с исходным кодом ПО «Microsoft» – как операционных систем Windows, так и других продуктов. Предоставление такой «прозрачности» должно убедить сомневающихся в отсутствии недекларированных функций в программных продуктах корпорации.



Создание центров прозрачности ведется в рамках программы сотрудничества «Microsoft» с правительственными структурами в области безопасности с целью повышения доверия к продуктам компании.

**Источник:** <http://www.pcweek.ru/security/article/detail.php?ID=175033> (дата размещения материала 04.06.2015).

*Новая волна спама, направленная на пользователей  
мессенджера WhatsApp*

На сайте [pcweek.ru](http://pcweek.ru) со ссылкой на специалистов компании «ESET» ([esetnod32.ru](http://esetnod32.ru)) размещена информация о резком росте спама, захлестнувшем пользователей популярного мессенджера WhatsApp. В последнее время пользователи WhatsApp активно пересылают друг другу сообщение о том, что сервис скоро станет платным.



Чтобы использовать его на прежних условиях, необходимо подтвердить свой статус активного пользователя, переслав предупреждение десяти контактам из своей адресной книги. Специалисты компании «ESET» рекомендуют игнорировать спам и не тратить время на его переадресацию.

**Источник:** <http://www.pcweek.ru/security/newscompany/detail.php?ID=174634> (дата размещения материала 20.05.2015).

*Тестирование средств засекречивания речи*

В журнале «Вопросы кибербезопасности» опубликована статья, в которой рассматриваются вопросы защиты речевой информации в каналах связи телефонной сети общего пользования. Авторами предложена методика тестирования аппаратно-программных средств засекречивания речи, а также приведены данные тестирования телефонных шифраторов и программ засекречивания речевых сигналов.



**Источник:** Вопросы кибербезопасности, 2015, № 2, с. 21-30.



## *Слабое звено в информационной безопасности*

Сайт pcweek.ru со ссылкой на информационный бюллетень компании «Microsoft» (microsoft.com) приводит результаты анализа проблем обеспечения политики безопасности информации различными категориями пользователей информационных систем. По результатам опытной эксплуатации информационных систем утверждается, что самым слабым звеном информационной безопасности является пользователь.



При этом руководители выделяются в отдельную группу доменных пользователей с совершенно избыточными правами. Также особую группу риска составляют сотрудники отделов IT- и информационной безопасности. Даются рекомендации для построения политики информационной безопасности, связанные с рассматриваемой проблемой.

**Источник:** <http://www.pcweek.ru/security/article/detail.php?ID=175413> (дата размещения материала 22.06.2015).

## *Издана книга о возможностях технических разведок в телекоммуникационной сфере*

На сайте forum.militaryparitet.com сообщается, что в научно-техническом издании «Защита и безопасность ведомственных интегрированных телекоммуникационных систем» рассмотрены новые аспекты информационной безопасности с учетом ранее неизвестных факторов. В книге подробно описаны основы технической защиты объектов ведомственных интегрированных инфокоммуникационных систем, показаны возможности технических разведок при использовании различных каналов утечки информации. Особое внимание уделено вопросам синтеза защищенных инфокоммуникационных систем и описанию методов оценки эффективности их защиты.



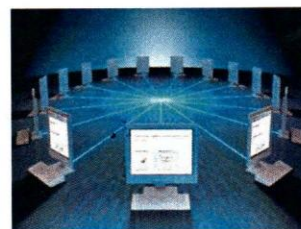
**Источник:** <http://forum.militaryparitet.com/viewtopic.php?id=2523&p=74> (дата размещения материала 15.06.2015).

## *Возможный подход к оценке ущерба от реализации угроз безопасности информации, обрабатываемой в государственных информационных системах*

В статье, опубликованной в журнале «Вопросы кибербезопасности», рассмотрены аспекты оценки риска в государственных информационных системах (ГИС). Основное внимание уделено задачам определения вариантов оценки ущерба. Рассмотрены вопросы классификации защищенности ГИС от угроз безопасности информации. Предложена классификация видов ущерба. Детально рассмотрены особенности финансового, морального, социального и экологического ущерба для ГИС.



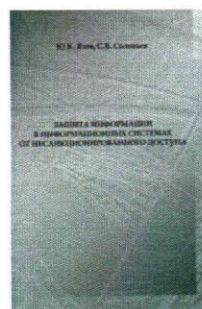
Разработан комплекс методических правил оценки различного вида ущерба в ГИС. Показана возможность использования предложенного подхода для определения уровня значимости защищаемой информации и обоснования класса защищенности ГИС. Рассмотрены вопросы последующего обоснования требований по защите информации в ГИС.



**Источник:** Вопросы кибербезопасности, 2015, № 2, с. 20-25.

### *Защита информации в информационных системах от несанкционированного доступа*

Издательство «Новый взгляд» выпустило пособие ведущих специалистов ГНИИИ ПТЗИ ФСТЭК России «Защита информации в информационных системах от несанкционированного доступа». В пособии рассматриваются организационные и технические аспекты технической защиты информации в информационных системах, дается характеристика угроз безопасности информации в таких системах и методического обеспечения их анализа, раскрывается порядок организации защиты информации и ее нормативное обеспечение.



Рассматриваются пути построения систем защиты информации от несанкционированного доступа и способы применения в них современных мер и средств технической защиты. Раскрываются особенности защиты информации в ГИС и информационных системах персональных данных.

**Источник:** Новый взгляд, Воронеж, 440 с.

### *Госдума обеспокоена защитой россиян от сбора данных через интернет-счетчики*

Сайт itsec.ru со ссылкой на заявление члена комитета Госдумы по безопасности и противодействию коррупции Ильи Костунова (duma.gov.ru) разместил информацию о доступности для сторонних компаний – «Google», «Яндекс» и др. персональных данных россиян, материалов их обращений в государственные органы и прочей важной информации. Утечка данных может происходить, если на сайтах установлены счетчики посещаемости пользователей от сторонних производителей.



Государственная Дума Российской Федерации инициировала проверку степени защищенности персональных данных российских граждан от несанкционированного доступа и запрета использования интернет-счетчиков производства европейских и американских компаний на государственных ресурсах.

**Источник:** [http://www.itsec.ru/newstext.php?news\\_id=105063](http://www.itsec.ru/newstext.php?news_id=105063) (дата размещения материала 28.05.2015).



### *Проверка уровня защиты российских банков от несанкционированного доступа*

По данным сайта stfw.ru, ссылающегося на публикацию в газете «Известия» (izvestia.ru), Центральный банк России планирует ввести дополнительные выездные проверки, предназначенные для выяснения, как банки реализуют защиту от нарушений, связанных с переводом денежных средств с помощью банкоматов и терминалов, Интернета, мобильного банкинга и банковских офисов.



Руководство Центробанка намерено осуществить контроль соблюдения банками правил обеспечения безопасности информации. Проверяющие будут оценивать наличие в банках обновлений систем информационной безопасности и устраивать тестирование системы дистанционного обслуживания банков.

**Источник:** <http://stfw.ru/page.php?id=50091> (дата размещения материала 17.06.2015).

### *Национальная ассоциация институтов закупок начала проект по реализации защиты персональных данных*

На сайте pcweek.ru ассоциация участников торгово-закупочной деятельности и развития конкуренции «Национальная ассоциация институтов закупок» сообщила об официальном запуске проекта «Защита персональных данных гражданина и человека» (personaguard.ru). Проект посвящен выявлению возможных нарушений и предоставлению помощи гражданам в защите их прав, в том числе при участии в закупках. В рамках проекта разработан специализированный портал, содержащий пополняемую базу возможных правонарушений, шаблоны обращений в уполномоченные государственные органы за защитой нарушенных прав, интерактивные формы таких обращений.



Также планируется разработать специальное ПО для использования в популярных браузерах Firefox, Google Chrome, Opera и мобильных приложениях на базе iOS и Android для автоматической проверки интернет-ресурсов на наличие жалоб пользователей, связанных с нарушением правового режима обработки персональных данных.

**Источник:** <http://www.pcweek.ru/security/news.company/detail.php?ID=174868> (дата размещения материала 29.05.2015).

### *ВМС США отказываются от использования серверов компании «IBM»*

Согласно информации, размещенной на сайте vpk.name со ссылкой на заявление Департамента внутренней безопасности США (dhs.gov), ВМС США намерены отказаться от использования серверов компании «IBM», при помощи которых осуществляется управление системами вооружения. Это связано с тем, что к технологиям «IBM» теперь имеет доступ китайская «Lenovo».



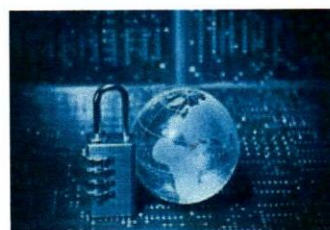
В 2014 г. «Lenovo» купила у «IBM» подразделение, отвечающее за выпуск серверов начального уровня на архитектуре x86. Департамент внутренней безопасности США увидел в этом угрозу национальной безопасности страны и наложил ограничения на государственные закупки серверов Lenovo/IBM BladeCenter. На серверах BladeCenter работает корабельная боевая информационно-управляющая система «Иджис».



**Источник:** [http://vpk.name/news/132485\\_vms\\_ssha\\_otkazhutsya\\_ot\\_ispolzovaniya\\_serverov\\_ibm.html](http://vpk.name/news/132485_vms_ssha_otkazhutsya_ot_ispolzovaniya_serverov_ibm.html) (дата размещения материала 23.05.2015).

### *Федеральные ведомства США переходят на HTTPS*

Как сообщает сайт threatpost.ru со ссылкой на Тони Скотта, федерального ИТ-директора правительства США, федеральным правительством принято решение последовать примеру крупнейших веб-служб и перевести все общедоступные сайты и службы правительства США на HTTPS-only. Переход планируется осуществить к концу 2016 г. В дополнение к переходу на HTTPS-only федеральные ведомства должны задействовать поддержку стандарта HSTS, принуждающего браузеры к использованию HTTPS для соединения с веб-сайтом. Это позволит защититься от downgrade-атак, пытающихся понизить уровень соединения до HTTP с открытым текстом. Эти изменения в веб-соединениях должны повысить доверие пользователей к федеральным ведомствам США.



**Источник:** <https://threatpost.ru/2015/06/10/federal-agencies-to-move-to-https-only-connections> (дата размещения материала 10.06.2015).

### *В США продляется действие «Патриотического акта»*

По данным ряда сайтов, ссылающихся на официальное заявление сената США (senate.gov), сенат США продляет действие «Патриотического акта» еще на год. Положения документа, за продление которых проголосовал сенат, включают возможность прослушивания переговоров лиц, создающих угрозу для национальной безопасности; изъятие собственности и документов при проведении антитеррористических операций, а также установление наблюдения за иностранными гражданами, не входящими в известные террористические организации, однако подозреваемыми в террористической деятельности. Прослушивание телефонных переговоров и изъятие документации разрешается лишь с санкции суда.



**Источники:** <http://www.ntv.ru/novosti/1417736/?fb#ixzz3bmsM4NM0> (дата размещения материала 01.06.2015); <http://ria.ru/world/20150601/1067495000.html#ixzz3bmsq9E2n>.



*Британское правительство хочет принять закон, разрешающий  
властям взламывать компьютеры граждан*

По информации сайта securitylab.ru со ссылкой на заявление бывшего сотрудника спецслужб США Э.Сноудена на телеконференции, организованной международной правозащитной организацией «Amnesty International», британское правительство пытается тайно принять так называемый «Закон о полномочиях следствия», который позволит властям «взломать компьютер любого гражданина». Закон разработан с целью предоставления больших полномочий разведслужбам для слежки за online-коммуникациями подозреваемых путем массового сбора персональных данных британцев.



Документ содержит ряд пунктов, изначально включенных в закон «О личных данных», прозванный «Шпионским уставом».

**Источник:** <http://www.securitylab.ru/news/473190.php> (дата размещения материала 03.06.2015).

*ООН: шифрование и анонимность являются необходимыми  
условиями соблюдения прав человека*

По информации сайта opennet.ru, комитет по правам человека при ООН в своем отчете (un.org/ru) сделал вывод, что возможности шифрования и сохранения анонимности в цифровых коммуникациях требуют защиты. Шифрование и анонимность отнесены к понятиям, которые обеспечивают конфиденциальность и безопасность, необходимые для осуществления права на свободу мнений и их свободного выражения в цифровую эпоху. Обеспечение данных прав имеет большое значение для осуществления других прав, таких как имущественные права, неприкосновенность частной жизни, свобода мирных собраний и ассоциации, право на жизнь и физическую неприкосновенность.



Также указано, что заслуживает порицания использование мер по ослаблению безопасности, таких как внедрение бэкдоров и оставления лазеек в связанных с шифрованием стандартах. Государствам рекомендовано избегать идентификации выходящих в сеть пользователей и регистрации используемых SIM-карт.

**Источник:** <http://www.opennet.ru/opennews/art.shtml?num=42330> (дата размещения материала 29.05.2015).

*Пятилетний план по обеспечению информационной  
безопасности Китая*

На сайте itexpert.org.ua со ссылкой на заявление правительства Китая агентству «Reuters» сообщается о подготовке пятилетнего плана защиты важнейших информационных ресурсов от угроз информационной безопасности. Основной его целью является повышение надежности программных решений,



используемых различными китайскими государственными ведомствами и финансовыми учреждениями. В соответствии с разрабатываемым правительством планом в скором времени ожидается переход государственных организаций на ПО отечественного производства.



**Источник:** <http://itexpert.org.ua/rubrikator/item/41997-kitaj-gotovit-pyatilet-nij-plan-po-obespecheniyu-natsionalnoj-informatsionnoj-bezopasnosti> (дата размещения материала 28.05.2015).

### *Хакеры из Китая финансируются правительством*

Как сообщает сайт [securitylab.ru](http://securitylab.ru) со ссылкой на заявление директора по профессиональным услугам компании «Masergy Communications» Дэвида Венебла, действия киберпреступников из Китая, наряду со сбором разведывательной информации, направлены на хищение объектов интеллектуальной собственности. В сводках об инцидентах в области безопасности часто фигурируют названия таких хакерских групп, как «Deep Panda», «Putter Panda/PLA Unit 61398», «Hidden Lynx», «APT1/Comment Crew» и «Axiom», тесно связанных с правительством Китая.



В своих действиях хакеры в основном используют фишинг с целью установки на компьютерах жертв вредоносного ПО. После этого киберпреступники берут под свой контроль серверы атакуемых компаний и похищают конфиденциальные данные.

**Источник:** <http://www.securitylab.ru/news/473070.php> (дата размещения материала 27.05.2015).

### *Северная Корея располагает армией из шести тысяч хакеров*

По данным сайта [securitylab.ru](http://securitylab.ru), ссылающегося на эксклюзивное интервью для компании «BBC» исполнительного директора диссидентской организации «Солидарность интеллектуалов Северной Кореи», КНДР имеет в составе разведывательного управления генерального штаба Корейской народной армии специальное подразделение «Бюро 121», численностью около 6 тыс. специалистов. Основной задачей этого подразделения является проведение военно-кибернетических операций.



По мнению специалистов, «Бюро 121» осуществляет кибератаки с территории Китая. Целями многих операций были объекты инфраструктуры Южной Кореи, например, электростанции и банки. Северная Корея создает вредоносное ПО на базе Stuxnet – червя, который использовался при кибератаках на системы обеспечения ядерных объектов Ирана.

**Источник:** <http://www.securitylab.ru/news/473110.php> (дата размещения материала 29.05.2015).



### 1.3. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

#### *Новый промышленный шлюз безопасности компаний «ИнфоТеКС» и «Symanitron»*

Сайт infotecs.ru информирует, что компаниями «ИнфоТеКС» и «Symanitron» представлен российский промышленный шлюз безопасности Symanitron ViPNet 100. Назначением изделия является обеспечение безопасного удаленного управления промышленными объектами, такими как трансформаторные и насосные станции, шкафы управления дорожным движением и городским освещением, а также производственными площадками металлургических и машиностроительных предприятий.

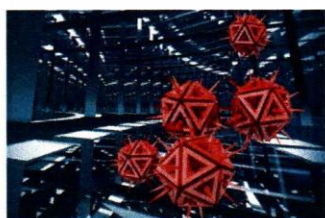


Шлюз безопасности обеспечивает целостность и конфиденциальность каналов управления и мониторинга средств автоматизированных систем управления (АСУ) технологическими процессами (ТП).

**Источник:** <http://www.infotecs.ru/press/news/15/14495> (дата размещения материала 22.06.2015).

#### *Защита автоматизированных систем управления технологическими процессами от киберугроз<sup>8</sup>*

По сообщению сайта itbrief.co.nz, компания «Check Point Software Technologies» расширила линейку продуктов в области защиты промышленных систем управления (ICS) и представила новый аппаратный шлюз безопасности 1200R. Check Point 1200R представляет собой специально разработанный шлюз безопасности повышенной прочности, рассчитанный на автономное использование в тяжелых условиях эксплуатации и на удаленных площадках, таких как производственные цеха, электрические подстанции и объекты электроэнергетики. Он поддерживает системы ICS/SCADA и обеспечивает высокий уровень защиты для самых ценных активов государства.



Компания также анонсировала ряд улучшений для гранулярного контроля сетей АСУ ТП и средств обнаружения и предотвращения угроз для АСУ ТП.

**Источник:** <http://itbrief.co.nz/story/check-point-protecting-ics-cyber-threats/> (дата размещения материала 02.06.2015).

#### *Национальный институт стандартов и технологий США выпустил рекомендации по безопасности автоматизированных систем управления*

По данным сайта threatpost.ru, Национальный институт стандартов и технологий (NIST) США выпустил вторую редакцию рекомендаций по безопасно-

<sup>8</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.



сти АСУ. Они содержат указания о том, как адаптировать традиционные средства управления безопасностью так, чтобы приспособить их к уникальным требованиям по производительности, надежности и функциональной безопасности АСУ. Обновлено главы, касающиеся угроз и уязвимостей, управления рисками, рекомендуемых практик, архитектур безопасности и инструментов. Из-за уникальных требований защита АСУ часто требует адаптации и расширений стандартов безопасности NIST и руководств, обычно используемых при защите традиционных ИТ-систем.



**Источник:** <https://threatpost.ru/2015/06/08/nist-vypustila-obnovlenie-rekomendatsij-po-bezopasnosti-asu> (дата размещения материала 08.06.2015).

### *Отчет компании «Digital Security» о состоянии информационной безопасности SCADA-систем*

На сайте anti-malware.ru размещен отчет компании «Digital Security» о состоянии информационной безопасности 20 мобильных приложений, разработанных для удаленного управления различными SCADA-системами. В отчете отмечено, что нет ни одного приложения, которое было бы разработано с соблюдением требований безопасности. Также компания исследовала протокол взаимодействия с сервером и пыталась вмешаться в диалог между мобильным приложением и сервером.



При этом обнаруживались такие ошибки проектирования, как передача пароля от сервера в открытом виде и SQL-инъекции на стороне сервера.

**Источник:** <http://www.anti-malware.ru/news/2015-06-11/16290> (дата размещения материала 11.06.2015).

### *Отчет об уязвимости беспроводных коммуникаций в самолетах*

Как сообщает ряд источников, в современной пассажирской авиации хакеры могут «взломать самолет», перехватив управление через Интернет или по Wi-Fi. Уже зафиксирован случай проникновения хакера в бортовую компьютерную сеть самолета и получения доступа к алгоритмам управления двигателями. Проблема заключается в использовании в системах управления самолетов таких же протоколов беспроводной передачи данных, какими пользуются для беспроводного доступа в Интернет.

По результатам расследования ФБР конкретных инцидентов проникновения хакеров в бортовую компьютерную сеть Boeing 737-800 определен список самолетов, имеющих уязвимости бортовой информационной сети. В список включены такие самолеты, как: Boeing 737-800, Boeing 737-900, Boeing 757-200, Airbus A350, Airbus A380. Кроме того, в отчете приведена информация об исполь-





зовании в самолетах Boeing 787 «Dreamliner» и Airbus A350 технологий, потенциально имеющих возможность перехвата управления с земли.

**Источники:** <https://xakep.ru/2015/04/26/airplane-hack> (дата размещения материала 26.05.2015); Комсомольская правда 4-11 июня 2015 г. с: 8.

### *Уязвимость в программном обеспечении ветрогенератора*

На сайте [threatpost.ru](http://threatpost.ru) со ссылкой на оповещение ICS-CERT ([ics-cert.us-cert.gov](http://ics-cert.us-cert.gov)) размещена информация об обнаружении уязвимости в ПО ветрогенератора компании «XZERES». Эта уязвимость может позволить злоумышленнику отключать подачу энергии ко всем системам, подключенным к целевой системе. Уязвимость содержится в ПО, работающем на ветрогенераторе модели 442SR. Пока эксплойт для этой уязвимости не обнаружен, но по мнению специалистов создать его несложно. Компания уже разработала исправление для данной уязвимости.



**Источник:** <https://threatpost.ru/2015/06/09/researcher-finds-csrf-bug-in-wind-turbine-software> (дата размещения материала 09.06.2015).

### *На BlackHat Mobile Security Summit эксперты «Digital Security» расскажут о безопасности приложений, превращающих смартфон в пульт управления заводом*

Сайт [dsec.ru](http://dsec.ru) сообщает, что эксперты «Digital Security», приглашенные в качестве докладчиков на это престижное мероприятие в сфере мобильной безопасности, продемонстрируют, как можно наблюдать за работой АСУ ТП и управлять ею со смартфона на Android или iOS.

Эксперты составили выборку мобильных приложений для SCADA, PLC, HMI и проанализировали их. В ходе доклада они продемонстрируют обнаруженные уязвимости, методы атак и другие возможные риски. Будет показано два сценария: атаки на инфраструктуру АСУ ТП со скомпрометированного смартфона и на мобильные устройства из скомпрометированной среды АСУ ТП (атака «снизу вверх»). Также будет представлена подробная статистика найденных недостатков и механизмов безопасности.



Саммит пройдет в рамках London Technology Week (<https://www.blackhat.com/ldn-15/summit.html#scada-and-mobile-security-assessment-of-the-applications-that-turns-your-smartphone-into-a-factory-control-room>) и призван поднять самые острые вопросы отрасли мобильной безопасности и предоставить информацию о самых продвинутых технологиях защиты.

**Источник:** [https://www.dsec.ru/news/events/blackhat\\_london\\_2015/?sphrase\\_id=4246](https://www.dsec.ru/news/events/blackhat_london_2015/?sphrase_id=4246) (дата размещения материала 16.06.2015).



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

### *Новые отечественные образцы доверенного телекоммуникационного оборудования*

По данным сайта mashportal.ru, «Объединенная приборостроительная корпорация» представила первые образцы доверенного телекоммуникационного оборудования – современные IP-АТС «Александрит» и маршрутизаторы операторского класса. Техника полностью разработана российскими специалистами, базируется на отечественных схемотехнических решениях и ПО, которые полностью исключают возможность негласного съема данных. В частности, IP-АТС «Александрит» соответствует требованиям, предъявляемым к средствам вычислительной техники 4 класса, и 3 уровню контроля недеklarированных возможностей, что подтверждено сертификатом Минобороны России.



**Источник:** [http://www.mashportal.ru/company\\_news-39057.aspx](http://www.mashportal.ru/company_news-39057.aspx) (дата размещения материала 27.05.2015).

### *Новая версия программного комплекса «АК-ВС» прошла сертификацию ФСТЭК России*

Как сообщает сайт НПО «Эшелон» pro-echelon.ru, программный комплекс «Анализатор исходных текстов программ «АК-ВС 2» получил сертификат ФСТЭК России, который свидетельствует о том, что комплекс соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» по 4 уровню контроля.



Программный комплекс «АК-ВС 2» предназначен для проведения сертификационных испытаний на отсутствие недеklarированных возможностей и проведения аудита безопасности кода. С помощью «АК-ВС 2» можно осуществлять статический, динамический и сигнатурный анализ исходных текстов на языках C/C++/Java/C# вплоть до 1 уровня контроля.

**Источник:** <http://www.npo-echelon.ru/news/10882> (дата размещения материала 21.05.2015).

### *Компания «ИВК» объявляет о выпуске новой линейки продуктов*

На сайте re-port.ru компания «ИВК» объявила о выпуске новой линейки продуктов «ИВК Юпитер Кripto», объединяющих функции межсетевых экранов с расширенной функциональностью и криптозащиту данных, передаваемых по сетям передачи данных между территориально-удаленными объектами.



Все входящие в линейку продукты разработаны и серийно производятся в России. Новая разработка ИВК имеет сертификаты ФСБ России и ФСТЭК России. Модели «Юпитер Кripto» обеспечивают криптографическую защиту потоков со скоростью передачи данных от 90 до 300 Мбит/сек. При этом все модели рассчитаны на длительную работу без специального обслуживания. В программно-аппаратном комплексе «ИВК Юпитер Кripto» используется ПО отечественной разработки.



**Источник:** [http://report.ru/pressreleases/ivk\\_vypustila\\_semeistvo\\_mezhsetevy\\_h\\_ykranov\\_i\\_ustroystv\\_kripto\\_zashity\\_na\\_traktah\\_svjazi](http://report.ru/pressreleases/ivk_vypustila_semeistvo_mezhsetevy_h_ykranov_i_ustroystv_kripto_zashity_na_traktah_svjazi) (дата размещения материала 02.06.2015).

### *Новая серия межсетевых экранов компании «Dell»*

Как сообщает сайт stfw.ru со ссылкой на информационный портал компании «Dell» (Dell.com), указанная компания выпустила новую серию межсетевых экранов SonicWALL TZ Series. Они отличаются улучшенной производительностью для поддержки более высоких скоростей Интернета, способностью анализировать зашифрованный трафик SSL и наличием интегрированного контроллера беспроводной сети.

Устройства обеспечивают сетевой интерфейс 1GbE в настольном варианте, эффективную защиту от вредоносного ПО, защиту от вторжений, фильтрацию контента и URL, контроль на уровне приложений, а также защищенный мобильный доступ к корпоративной сети с ноутбуков, смартфонов и планшетов. Механизм глубокого анализа пакетов позволяет устройствам SonicWALL TZ Series сканировать каждый байт каждого пакета для всех портов и протоколов практически с нулевой задержкой.



**Источник:** <http://stfw.ru/page.php?al=novaya-seriya-mezhsetevyx-ekranov-sonicwall-tz-series-ot-dell-predostavlyaet-zashhitu-korporativnogo-klassa-dostupnuyu-dlya-malogo-i-srednego-biznesa> (дата размещения материала 08.06.2015).

### *Унифицированные межсетевые экраны «АльтЭль»*

Сайт cnews.ru, ссылаясь на заявление руководства компании «АльтЭль» (AltEll.ru), разместил информацию о разработке компанией нового средства защиты от киберугроз. В состав продукта Altell Neo входят межсетевой экран, система обнаружения и предотвращения вторжений, криптографический шлюз, веб-фильтр, а также антивирус и антиспам. Перечисленный набор средств защиты информации, объединенных в одном устройстве, позволяет обеспечить надежную защиту периметра локальной сети организации, предоставляет защищенный доступ в Интернет, организует демилитаризованные зоны, создает защищенные ка-





налы связи по сетям общего пользования.

Решение ориентировано на требования Федерального закона «О защите персональных данных». UTM-устройство Altell Neo имеет сертификаты ФСТЭК России на межсетевой экран по 2 классу защиты и на отсутствие недеklarированных возможностей по 2 уровню контроля.

**Источник:** <http://b2bsecurity.cnews.ru/reviews/index.shtml?2015/05/25/595896> (дата размещения материала 25.05.2015).

### *Система защиты информации Secret Net для операционной системы Linux*

Как сообщает ряд сайтов, компания «Код Безопасности» ([securitycode.ru](http://securitycode.ru)) подготовила технический релиз средства защиты информации (СЗИ) от несанкционированного доступа для компьютеров под управлением операционной системы Linux Secret Net LSP 1.3. Главной его особенностью стала возможность использования средств централизованного управления. В СЗИ Secret Net LSP 1.3 реализована поддержка доменной аутентификации пользователей. Настройки режима удаленного управления доступны как в графической панели безопасности Secret Net LSP, так и через новую консольную утилиту.



Кроме того, обеспечена сквозная аутентификация с использованием электронного идентификатора на сервере Citrix с установленным СЗИ Secret Net. Новая версия Secret Net LSP передана на инспекционный контроль в ФСТЭК России для подтверждения соответствия ранее выданному сертификату № 2790.

**Источники:** <http://www.securitycode.ru/company/news/dostupen-tekhnic-heskiy-reliz-secret-net-lsp-1-3-dlya-oc-linux-s-podderzhkoy-sredstv-tsentralizovannogo-upravleniya> (дата размещения материала 15.06.2015); <http://www.securitycode.ru/company/news/vyshel-tekhnicheskiy-reliz-obnovlennoy-versii-secret-net-7-c-vozmozhnostyu-podderzhki-avtonomnogo-upravleniya-k-serveru>.

### *ФСТЭК России сертифицировала последнюю версию DLP-системы «Zecurion»*

На сайте [zecurion.ru](http://zecurion.ru) размещена информация о получении компанией «Zecurion» сертификата ФСТЭК России на DLP-систему. Комплексная система защиты от утечек корпоративной информации состоит из решений Zgate, Zlock, Zserver и Zdiscovery. Все четыре продукта могут использоваться самостоятельно в зависимости от выполняемых компанией задач, а вместе они составляют комплексную систему, обеспечивающую максимально эффективную защиту от утечек информации.



Сертификация проведена на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по



уровню контроля отсутствия недеklarированных возможностей» по 4 уровню контроля.

**Источник:** <http://www.zecurion.ru/press/5650> (дата размещения материала 24.05.2015).

### *Программный комплекс С-Терра Виртуальный Шлюз 4.1*

В журнале «Информационная безопасность/Information Security» опубликована информация о программном комплексе С-Терра Виртуальный Шлюз 4.1, предназначенном для построения VPN, защиты периметра облачной информационной системы, защиты взаимодействия между виртуальными машинами. Особенностью программного комплекса является возможность его работы в виртуальной машине, созданной в одном из наиболее популярных гипервизоров (VMware, Hyper-V, Xen, KVM).

По результатам тестирования на совместимость с XenServer 6.2 С-Терра Виртуальный Шлюз получил статус Citrix Ready. Комплекс имеет высокую пропускную способность, обладает оперативной адаптацией к меняющимся задачам и требованиям сетевых приложений и инфраструктуры. Продукт имеет сертификаты ФСБ России.

**Источник:** Информационная безопасность/Information Security, 2015, № 2, с. 47.

### *Протестирован новый коммутатор с защитой от DDoS-атак*

По сообщению сайта [pr.adcontext.net](http://pr.adcontext.net), специалисты компании «Саотрон» ([saotron.ru](http://saotron.ru)) протестировали инновационный и функциональный коммутатор – Symbol RFS4000, который работает под управлением мощной и надежной операционной системы WiNG OS. Особенно отмечается способность устройства обеспечивать достойный уровень защиты от DDoS-атак в зависимости от требований пользователя. Интегрированный коммутатор подходит для построения как проводной, так и беспроводной сети.



**Источник:** <http://pr.adcontext.net/15/06/19/205992> (дата размещения материала 19.06.2015).

### *Новая версия системы защиты СУБД «Гарда БД» от «МФИ Софт»*

Как информирует сайт [anti-malware.ru](http://anti-malware.ru), корпорация «МФИ Софт» – российский разработчик систем информационной безопасности ([mfisoft.ru](http://mfisoft.ru)) – выпустила новую версию интеллектуальной системы защиты баз данных «Гарда БД».



Новое решение позволяет находить в сети неконтролируемые базы данных, о существовании которых службе безопасности может быть неизвестно, классифицировать их и ставить на автоматический контроль по выбранным политикам безопасности.



**Гарда БД**  
Защита баз данных

В системе реализованы технологии выявления аномальной активности пользователей, формально не превышающих своих прав доступа. Для защиты баз данных от действий администраторов система также контролирует действия пользователей непосредственно на сервере базы данных. Кроме того, технологии анализа легитимности обращений к системе управления базами данных позволят своевременно выявить попытки внедрения SQL-кода.

**Источник:** <http://www.anti-malware.ru/news/2015-06-05/16262> (дата размещения материала 06.05.2015).

### *Начата поставка в Россию криптомаршрутизаторов «Dionis-DPS»*

На сайте [safe.cnews.ru](http://safe.cnews.ru) со ссылкой на заявление руководства компании «Фактор-ТС» ([factor-ts.ru](http://factor-ts.ru)) сообщается о начале поставки в Россию продуктовой линейки криптомаршрутизаторов «Dionis-DPS», которые представляют собой современные российские маршрутизаторы, сертифицированные ФСБ России и ФСТЭК России и предназначенные для использования в сетях различных ведомств для защиты персональных данных и конфиденциальной информации.

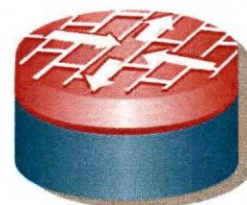


Использование российских сертифицированных маршрутизаторов «Dionis-DPS» является альтернативой применения зарубежных аналогов.

**Источник:** <http://safe.cnews.ru/news/line/index.shtml?2015/05/29/596062> (дата размещения материала 29.05.2015).

### *Новые технологии обеспечения безопасности информации компании «Cisco»*

На сайте [cisco.com](http://cisco.com) размещена информация о новых решениях компании «Cisco», обеспечивающих информационную безопасность и значительно улучшающих возможности мониторинга и контроля безопасности информации на всем протяжении расширенной сети – от центров обработки данных, облачных инфраструктур и удаленных офисов до конечных устройств.



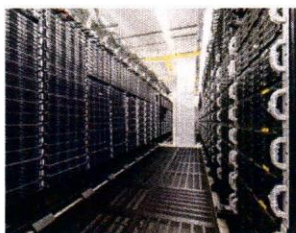
Интеграция технологий повсеместной безопасности позволит заказчикам и поставщикам услуг использовать преимущества угроз-ориентированной защиты, поскольку именно такой тип защиты наиболее актуален для противодействия современному динамическому ландшафту угроз.

**Источник:** <http://www.cisco.com/web/RU/news/releases/txt/2015/06/16b.html> (дата размещения материала 16.06.2015).



### *Новое решение для обеспечения информационной безопасности центров обработки данных компании «Intel Security»*

По данным сайта [astera.ru](http://astera.ru), компания «Intel Security» ([intelsecurity.com](http://intelsecurity.com)) выпустила интегрированное решение, использующее преимущества технологии



программно-определяемых центров обработки данных и платформы виртуализации VMware NSX. Решение позволяет обеспечить автоматическое распространение и развертывание системы защиты от вторжений McAfee Network Security Platform для обеспечения безопасности внутреннего трафика.

Решение включает в себя McAfee NSP IPS, McAfee Network Security Manager, Intel Security Controller и платформу виртуализации VMware NSX. Благодаря этому трафик между виртуальными машинами защищен в соответствии с определенными политиками и требованиями безопасности. При этом обеспечивается поддержка микросегментации, политик безопасности, документооборота и групп пользователей в сложных средах облачных вычислений.

**Источник:** <http://www.astera.ru/news/?id=111602> (дата размещения материала 15.06.2015).

### *«Eset» представила решение для комплексной защиты пяти устройств*

На сайте [anti-malware.ru](http://anti-malware.ru) со ссылкой на информационный портал компании «Eset» ([esetnod32.ru](http://esetnod32.ru)) размещена информация о новом решении для комплексной защиты компьютеров, ноутбуков, планшетов или смартфонов на базе операционных систем Windows, Linux, Mac OS X и Android Eset NOD32 Smart Security Family. Систему отличает простота установки, высокая скорость работы, а также оптимально сбалансированный для различных пользователей функционал.



функционал.

Функция «Антивор» помогает в поисках ноутбука, планшета или смартфона в случае его кражи или потери. Модуль «Антифишинг» защищает от мошеннических ссылок, которые ведут на фальшивые версии популярных сайтов. Модуль «Антиспам» помогает сэкономить время пользователя, осуществляя фильтрацию нежелательной почты по заданным настройкам.

Комплекс интеллектуальных функций обеспечивает проактивную защиту от вредоносного ПО, включая банковские трояны, шпионские программы и шифраторы.

**Источник:** <http://www.anti-malware.ru/news/2015-06-03/16237> (дата размещения материала 03.06.2015).



*Компания «ECI» представила новое решение для построения защищенных облачных сервисов<sup>9</sup>*

По данным информационного портала компании «ECI» (ecitele.com), специалисты компании представили новое решение для построения защищенных облачных сервисов Elasti CLOUD. Новое решение разработано в рамках общей стратегии адаптивного развития сетевых технологий компании и позволяет заказчику развернуть адаптивную облачную информационную технологию. Решение Elasti CLOUD включает три программных продукта: Cloud Connect, SAN Connect, Data Center Interconnect Backbone.



**Источник:** [http://www2.ecitele.com/SocialNewsRoom/News/Pages/ECI\\_to\\_Debut\\_its\\_ELASTIC\\_Network\\_Strategy.aspx](http://www2.ecitele.com/SocialNewsRoom/News/Pages/ECI_to_Debut_its_ELASTIC_Network_Strategy.aspx) (дата размещения материала 03.06.2015).

*Единая платформа для безопасного доступа и хранения информации*

На сайте pcweek.ru размещена информация о появлении в России единой платформы для безопасного доступа и хранения информации Vaultize индийской компании «Vaultize Technologies» (vaultize.com). ПО позволяет контролировать и централизованно управлять данными вне зависимости от месторасположения пользователя, а также обеспечивает комплексную защиту корпоративной информации от утечек как со стационарных, так и с мобильных устройств.



Все данные передаются по защищенному SSL-протоколу и предварительно шифруются по алгоритму AES-256 для создания дополнительного уровня защиты. Уникальность платформы Vaultize заключается в ее модульности и практически неограниченных возможностях масштабирования.

**Источник:** <http://www.pcweek.ru/security/news-company/detail.php?ID=174957> (дата размещения материала 02.06.2015).

*Браузер «Яндекс» с защитой от слежения*

Как сообщает сайт comss.info со ссылкой на информацию компании «Яндекс» (yandex.ru), в результате совместной разработки компаний «Яндекс» и «Adguard» создана экспериментальная сборка Яндекс Браузера со встроенным дополнением, позволяющим скрыть информацию от большинства отслеживающих скриптов. Дополнение Яндекс Браузера блокирует все скрипты, отслеживающие действия пользователя и социальные виджеты, а также маскирует user agent, очищает cookies, удаляет referrer из запроса, отправ-



<sup>9</sup> Перевод с английского выполнен ГНИИИ ПТЗИ ФСТЭК России.

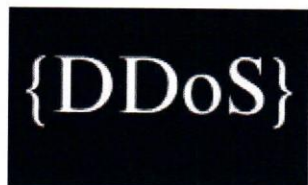


ляет метку do-not-track на каждый посещаемый сайт. Это значительно затруднит выявление действий пользователя в сети.

**Источник:** [http://www.comss.info/page.php?al=yandex\\_browser\\_adds\\_advanced\\_privacy\\_features](http://www.comss.info/page.php?al=yandex_browser_adds_advanced_privacy_features) (дата размещения материала 30.05.2015).

*«Лаборатория Касперского» начинает предоставлять  
свой сервис защиты от DDoS-атак*

Согласно информации сайта [kaspersky.ru](http://kaspersky.ru), «Лаборатория Касперского» начинает предоставлять сервис защиты от DDoS-атак через партнерские дата-центры. Компания уже продолжительное время успешно борется с такими атаками с помощью Kaspersky DDoS Prevention – сервиса, способного оградить клиентов от мощнейших DDoS-атак благодаря распределенной сети высокотехнологичных центров очистки. Сервис Kaspersky DDoS Prevention осуществляет защиту за счет переключения на время атаки клиентского трафика на центры очистки данных.



Центры расположены как в России, так и в других странах и подключены к Сети по высокоскоростным каналам связи. При выявлении факта DDoS-атаки вредоносный трафик отфильтровывается, и до клиента доходят только запросы легитимных пользователей, что спасает инфраструктуру и сервисы от перегрузки.

**Источник:** <http://www.kaspersky.ru/about/news/business/2015/kaspersky-ddos-prevention> (дата размещения материала 25.05.2015).

*Новый сервис по предотвращению  
киберпреступлений*

По данным сайта [solarsecurity.ru](http://solarsecurity.ru), компании «Solar Security» и «Group-IB» запустили новый сервис – «JSOC. Противодействие киберпреступности», гарантирующий клиентам высокий уровень защиты от угроз информационной безопасности.



Особенностью нового сервиса является возможность оперировать потоком данных о реальных инцидентах информационной безопасности, зарегистрированных платформами Bot-Trek CI и TDS в российских компаниях конкретной отрасли. Это делается для своевременного обновления корреляционных правил центра мониторинга и раннего детектирования схожих инцидентов у подключенных к JSOC клиентов.

Сервис включает в себя оперативную проверку всей инфраструктуры клиента, обработку аналитиками JSOC скомпрометированных данных и проверку подозрительных с точки зрения Bot-Trek TDS средств вычислительной техники.

**Источник:** <http://solarsecurity.ru/events/news/529/> (дата размещения материала 28.05.2015).



### *Драйвер ядра компании «Abatis» защитит от сетевых атак*

По данным сайта хакер.ru, фирменный драйвер ядра компании «Abatis» (abatis-hdf.com) размером менее 100 Кб защищает диск от записи, не требует сигнатур или белых списков, не использует эвристик или песочницы, снижает расходы электричества на 7%, работает на 40% быстрее, чем антивирус с сигнатурами, совместим с Windows NT4, работает на любых версиях Linux. В ближайшее время ожидается появление версии и для Android. По отзывам специалистов ПО в состоянии защитить корпоративные сети от уязвимостей нулевого дня.



**Источник:** <https://haker.ru/2015/06/05/abatis> (дата размещения материала 05.06.2015).

### *Корпорация «Microsoft» ограничивает использование программного обеспечения поиска защиты*

Согласно сообщению сайта securitylab.ru со ссылкой на информационный портал компании «Microsoft» (microsoft.com), средства по обеспечению безопасности центра корпорации по защите от вредоносных программ начнут отслеживать все ПО, содержащие код поиска защиты, и классифицировать ПО как вредоносное, независимо от того, включена или скрыта функция поискового цензурирования. Производители ПО используют поиск защиты для того, чтобы предотвратить деинсталляцию программ или изменение настроек по умолчанию поисковой системы. Также поиск защиты используется для того, чтобы пользователь не мог отключить или включить определенные расширения браузера.



Компания начала блокировать программы, которые мешают или ограничивают пользователя в изменении настроек и функций браузера, еще в 2014 г.

**Источник:** <http://www.securitylab.ru/news/473077.php> (дата размещения материала 28.05.2015).

### *Система управления событиями безопасности компании «Positive Technologies»*

На ряде сайтов со ссылкой на объявление компании «Positive Technologies» (ptsecurity.ru), сообщается о выпуске собственной системы управления событиями безопасности MaxPatrol. Система позволяет выявлять уязвимости в корпоративной информационной системе и обнаруживать попытки применения того или иного средства организации атак.

При построении MaxPatrol использована технология нереляционных баз данных, таких как Elasticsearch или MongoDB. Это позволяет оперативно обрабатывать большие объемы информации о событиях безопасности и выявлять в них признаки известных типов





нападений. Кроме этого, система снабжена модулем подготовки отчетов, который можно использовать для проведения расследования инцидентов и выявления проблемных вопросов.

**Источники:** <http://www.anti-malware.ru/news/2015-05-24/16175> (дата размещения материала 24.05.2015); <http://ptsecurity.ru/about/news/41049>.

### *Программы с аппаратной защитой компании «1С-Рарус»*

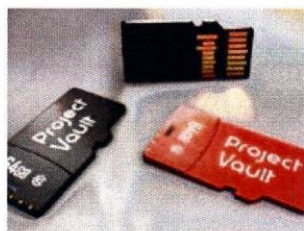
Как сообщается на ряде сайтов, компания «1С-Рарус» (rarus.ru) модернизировала отраслевое решение 1С-Рарус: Учет ценных бумаг. Программа выпущена с аппаратной защитой. Главный элемент данного вида защиты – аппаратный ключ, выполненный по технологии USB. Внешняя сторона каждого ключа содержит информацию о названии программного продукта, для которого он предназначен, уникальный номер (s/n) ключа защиты и его штрих-код.

Программа 1С-Рарус: Учет ценных бумаг является дополнением к программе 1С:Бухгалтерия 8 ПРОФ редакции 3.0 на платформе 1С:Предприятие 8.3.

**Источник:** <http://12news.ru/newsfeed/ext4all6388.html> (дата размещения материала 23.05.2015); <http://www.pcweek.ru/security/news-company>.

### *Google Project Vault защитит личную информацию пользователей*

Как сообщает сайт internetua.com, компания «Google» (google.com) обратила внимание на проблему защиты паролей пользователей и для ее решения запустила проект Vault, разработав специальное устройство в виде microSD-карты. Его можно подключить как к компьютеру, так и к мобильному устройству.



Устройство работает на собственной операционной системе, которая отделена от принимающего устройства 4 Гб дискового пространства для хранения самых важных данных пользователя. Система работает на Real-Time Operating System с набором криптографических решений для обеспечения безопасности данных, а также обмена сообщениями между пользователями, которые также установили Vault в свои девайсы. «Google» намерена сделать Vault максимально понятным, чтобы принимающее устройство могло взаимодействовать с Vault без дополнительных действий со стороны пользователя.

**Источник:** <http://internetua.com/Google-Project-Vault-zasxтит-licsnuua-informaciua-polzovatelei> (дата размещения материала 01.06.2015).

### *Новая технология оперативного обнаружения утечек данных Matchlight*

По данным сайта tcinet.ru со ссылкой на заявление специалистов компании «Terbium Labs» (terbiumlabs.com), ими создана эффективная технология



обнаружения данных, похищаемых киберпреступниками у крупных компаний. Принцип действия технологии Matchlight заключается в постоянном слежении за хакерскими ресурсами и сравнении размещенной на них информации с преобразованными специальными алгоритмами конфиденциальными данными корпораций.



В ходе предстартового тестирования Matchlight обнаружила, что на хакерских ресурсах ежедневно выставляется на продажу до 30 тыс. номеров новых банковских карт и порядка 6 тыс. адресов электронной почты и паролей к ним.

**Источник:** <http://www.tcinet.ru/press-centre/technology-news/2327> (дата размещения материала 04.06.2015).

### *Google Project Abacus избавит от необходимости использовать пароли*

Сайт internetua.com сообщает об одном из самых масштабных проектов компании «Google» (google.com). Project Abacus стал результатом взаимодействия 33 университетов из 28 штатов США по созданию мультимодальной системы защиты персональных данных.

Проект объединяет известные методы защиты (пароли, аутентификацию по отпечаткам пальцев, голосу, рисунку сетчатки глаза) и добавляет еще одну надстройку: уровень доверия к пользователю на основании его поведения при работе с электронным устройством.



Решение способно с высокой точностью определить разницу между пользователями и заблокировать устройство, если посчитает, что девайсом внезапно завладел посторонний человек.

**Источник:** <http://internetua.com/Google-Project-Abacus-izbavit-nas-ot-neobhodimosti-ispolzovat-paroli> (дата размещения материала 01.06.2015).

### *Поддержка сканера отпечатков пальцев реализуется на уровне операционной системы*

По данным сайта gizmonews.ru, новую версию операционной системы Android 6.0 компания «Google» (google.com) планирует оснастить встроенной поддержкой сканера отпечатков пальцев. Наличие биометрической аутентификации в смартфоне решает сразу несколько проблем информационной безопасности. Сканер отпечатков пальцев позволит отказаться от морально устаревшего способа авторизации через ввод пароля.

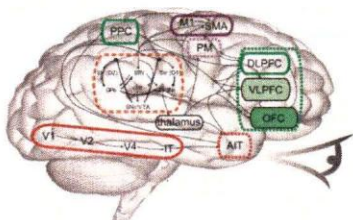


**Источник:** <http://www.gizmonews.ru/2015/05/23/android-6-0-podderzhku-skanera-otpechatkov-palcev-realizuyut-na-urovne-os/> (дата размещения материала 23.05.2015).



## *Идентификация личности по реакции мозга на слова*

На сайте хакер.ru размещена информация об исследованиях, проводимых Блэром Армстронгом из Баскского центра изучения мозга, познания и языка в Испании, по разработке нового метода биометрической идентификации пользователей. Суть метода заключается в приеме и распознавании мозговых волн, излучаемых индивидуально каждым человеком в ответ на различные слова.



Экспериментальная точность распознавания составила 94%. Волны принимались электродами с участка мозга, который отвечает за чтение и распознавание слов. В перспективе идентификация личности по уникальному отпечатку его семантической памяти может стать более надежной, чем идентификация по сетчатке глаза или отпечаткам пальцев.

**Источник:** <https://xaker.ru/2015/06/02/brain-fingerprint> (дата размещения материала 02.06.2015).

## *Выпущена версия Android в защищенном исполнении*

По данным сайта ko.com.ua, американская компания «USMobile» (usmobile.com) выпустила Android-приложение Scrambl3, реализующее безопасный обмен сообщениями и голосовую связь по публичным сетям. Новая программа создает смартфонный эквивалент VPN, обеспечивающий невидимость сообщений в Интернете. От других мобильных решений для защиты коммуникаций Scrambl3 отличается дополнительным слоем шифрования с использованием технологии АНБ США Fishbowl.



**Источник:** [http://ko.com.ua/razrabotka\\_anb\\_zashhitit\\_privatnye\\_kommunikacii\\_ot\\_nadzo\\_ra\\_110705](http://ko.com.ua/razrabotka_anb_zashhitit_privatnye_kommunikacii_ot_nadzo_ra_110705) (дата размещения материала 02.06.2015).

## *Новая версия антивируса компании «ESET»*



На информационном портале компании «ESET» esetnod32.ru представлено специальное решение для комплексной безопасности – ESET NOD32 Smart Security Family. Новый продукт предназначен для защиты персональных компьютеров, ноутбуков, планшетов или смартфонов на базе операционных систем Windows, Linux, Mac OS X и Android. В ПО имеются функции «Родительский контроль», «Антивор», «Антифишинг» и «Антиспам».

**Источник:** <http://www.esetnod32.ru/company/press/center/semeynye-tsenosti-pod-zashchitoy-eset-nod32> (дата размещения материала 03.06.2015).



### *Новый почтовый антивирус компании «ESET»*

В соответствии с информацией, размещенной на сайте [pcweek.ru](http://pcweek.ru), со ссылкой на портал компании «ESET» ([esetnod32.ru](http://esetnod32.ru)), запущено бета-тестирование нового поколения корпоративного решения для защиты почтовых серверов ESET Mail Security для Microsoft Exchange Server. Антивирус обеспечивает новый, принципиально более высокий уровень информационной безопасности. Продукт ESET Mail Security оптимизирован для достижения высоких результатов с точки зрения эффективности и быстродействия. Обновленное решение включает дополнительные уровни защиты, в числе которых модули «Расширенное сканирование памяти», «Защита от эксплойтов» и «Антифишинг».



**Источник:** <http://www.pcweek.ru/security/news-company/detail.php?ID=175210> (дата размещения материала 11.06.2015).

### *Тестирование новой версии антивируса компании «ESET»*

Информационный портал компании «ESET» [esetnod32.ru](http://esetnod32.ru) сообщает о начале бета-тестирования новых версий продуктов ESET NOD32 Smart Security и ESET NOD32 Антивирус. В комплексный продукт ESET NOD32 Smart Security внедрен модуль «Защита онлайн-платежей и банковских операций». Решение также поддерживает функцию «Анализ репутации» на базе облачной технологии ESET LiveGrid, которая оценивает файлы, программы и сайты и позволяет мгновенно блокировать угрозы. В модуле «Защита от ботнетов» появилась поддержка сетевых сигнатур, более точно определяющая вредоносный и исходящий трафик с зараженных компьютеров, входящих в состав ботнета.



Новое поколение антивирусных продуктов ESET NOD32 поддерживает операционную систему Microsoft Windows 10.

**Источник:** <http://www.esetnod32.ru/company/press/center/eset-nod32-obespechivaet-zashchitu-polzovatelyam-internet-banka> (дата размещения материала 05.06.2015).

### *Защита личных счетов абонентов от вирусных атак компании «МТС»*

Как информирует официальный сайт компании «МТС» [company.mts.ru](http://company.mts.ru), в компании начата реализация нового сервиса для абонентов, обеспечивающего защиту как личных данных в телефоне, так и денежных средств от вирусных атак. Новая услуга «Экстренная блокировка платежей с лицевого счета» позволит владельцам смартфонов с операционной системой Android временно заблокировать финансовые сервисы, с помощью которых вирусы могут вывести денежные средства с лицевых сче-





тов. При этом абоненты гарантированно остаются на связи, так как блокируются все платежи, кроме тех, что направлены на оплату услуг связи.

**Источник:** [http://www.company.mts.ru/comp/press-centre/press\\_release/2015-06-04-4621989](http://www.company.mts.ru/comp/press-centre/press_release/2015-06-04-4621989) (дата размещения материала 04.06.2015).

### *Ноутбук в защищенном исполнении корпорации «Panasonic»*

На сайте vesti.ru со ссылкой на сайт корпорации «Panasonic» (panasonic.com) размещена информация о поступлении в продажу ноутбуков корпорации в защищенном исполнении. В ноутбуке используется аппаратно-программный модуль доверенной загрузки российской компании «Kraftway», который контролирует процессы включения/выключения и режимы пониженного энергопотребления для обеспечения приоритетного запуска встроенных средств защиты информации. Применение отечественного ПО для защиты информации от несанкционированного доступа позволяет позиционировать устройство для российского госсектора.



**Источник:** <http://hitech.vesti.ru/news/view/id/7048> (дата размещения материала 27.05.2015).

### *Новое средство выявления целенаправленных атак компании «InfoWatch»*

Согласно данным сайта infowatch.ru, разработана новая версия решения по обнаружению целенаправленных атак – InfoWatch Targeted Attack Detector 3.0. Решение разработано специально для обнаружения сложных целенаправленных атак, использующих уникальные вредоносные программы, уязвимости нулевого дня и социальную инженерию. Принцип работы продукта основан на том, что любое вредоносное ПО создает нетипичные изменения в системе (аномалии).



InfoWatch Targeted Attack Detector на регулярной основе проводит сканирование ИТ-системы организации и собирает информацию о состоянии критических объектов. Полученные данные отправляются в облако, сравниваются с результатами прошлых сканирований, после чего осуществляется интеллектуальный анализ произошедших изменений.

В новой версии продукта пользователям доступна централизованная установка, обновление и удаление агентов на рабочих станциях.

**Источник:** <http://www.infowatch.ru/presscenter/news/14753> (дата размещения материала 18.06.2015).

### *Компания «Facebook» внедряет технологии защиты информации OpenPGP*

По сообщению сайта threatpost.ru со ссылкой на заявление руководства компании «Facebook», сервис «Facebook» осуществляет внедрение поддержки



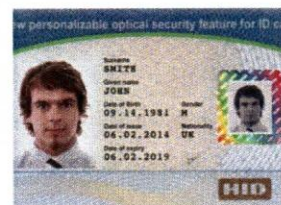
шифрования OpenPGP, которое позволит пользователям, требующим конфиденциальности, размещать открытые ключи в своем профиле. В результате будет обеспечен более высокий уровень защиты сообщений, посылаемых через сервис на личную электронную почту пользователей. При реализации данной технологии предполагается использовать стандарт GNU Privacy Guard и поддерживать шифрование при помощи алгоритмов RSA или ElGamal.



**Источник:** <https://threatpost.ru/2015/06/03/facebook-bolsters-message-security-adds-openpgp> (дата размещения материала 03.06.2015).

### *Техническое решение предотвращения подделки идентификационных карт*

Как сообщает сайт sec4all.net, компания «HID Global» (hidglobal.com) разработала новую технологию для предотвращения подделки идентификационных данных. С помощью технологии визуальной безопасности vanGO на карты горячим тиснением наносится специальный квадратный металлический патч, на который записывается изображение лица владельца карты. Этот образ создает уникальную связь между картой и ее держателем, и такую карту практически невозможно подделать.



Добавление персонифицированного, не поддающегося подделыванию изображения владельца карты гарантирует, что территория будет защищена от проникновения нарушителей, не имеющих права доступа.

**Источник:** <http://sec4all.net/modules/news/article.php?storyid=4510> (дата размещения материала 09.06.2015).

### *Компанией «Trend Micro» выпущен тренажер для специалистов по информационной безопасности*

По данным сайта 12news.ru, компания «Trend Micro» (trendmicro.com) выпустила тренажер для обучения специалистов по информационной безопасности. Он позволяет проверить их готовность принимать верные решения в сложных ситуациях, связанных с информационной безопасностью компании и ее продуктов в условиях, максимально приближенных к реальным. Тренажер реализован в виде браузерного приложения.



**Источник:** <http://12news.ru/newsfeed/ext4all6405.html> (дата размещения материала 08.06.2015).

### *Разработан банкомат с функцией распознавания лиц*

Согласно информации, размещенной на сайте rusevik.ru со ссылкой на китайское новостное агентство «Синьхуа», в Китае разработан банкомат, использующий технологии распознавания лиц. Биометрический банкомат явля-





ется совместной разработкой университета Цинхуа и технологической компании «Tzekwan» в городе Ханчжоу. Машина не выдаст наличные пользователю, если его лицо не пройдет проверку на соответствие идентификационному номеру владельца банковской карты.

**Источник:** <http://rusevik.ru/news/306602> (дата размещения материала 01.06.2015).

### *Мультипликативный метод оценки качества систем защиты информации*

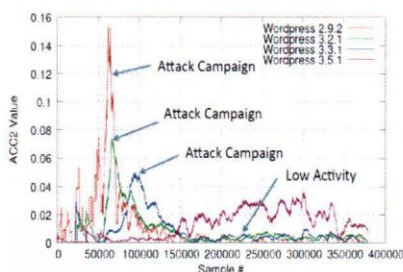
В журнале «Стратегическая стабильность» опубликована статья, рассматривающая различные методы оценки качества систем защиты информации. На основе анализа допущений и ограничений различных методов оценки предложен модифицированный мультипликативный метод оценки качества систем защиты информации. В качестве иллюстрации возможностей предложенного метода в статье приведен расчет показателей качества нескольких широко применяемых на практике систем защиты.



**Источник:** Стратегическая стабильность, 2015, № 2, с. 55.

### *Методика автоматического детектирования уязвимых сайтов в Интернете*

Как сообщает сайт хакер.ru, специалистами университета Карнеги-Меллона ([www.cmu.edu](http://www.cmu.edu)) разработана методика автоматического де-



тектирования уязвимых сайтов в Интернете, которая позволяет определить с высокой степенью вероятности, с каких сайтов начнется распространение вредоносных программ в будущем.

В методике использованы техники дата-майнинга и машинного обучения. Во время испытаний методику проверили на выборке из 444519 сайтов, содержащих 4916203 страницы. Выяснилось, что найденные подозрительные сайты действительно часто подвергались взлому в течение года.

**Источник:** <https://xakep.ru/2015/05/28/www-scan> (дата размещения материала 28.05.2015).



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



#### 3.1. Нормативные правовые акты федерального уровня

*Указ Президента Российской Федерации от 30.05.2015 № 220  
«О временном порядке ввоза в Российскую Федерацию и вывоза  
из Российской Федерации продукции военного назначения в интересах  
расположенных на территории Республики Крым и г. Севастополя  
организаций – разработчиков и производителей такой продукции»  
(начало действия документа – с момента подписания)*

Утвержден временный порядок ввоза в Российскую Федерацию и вывоза из Российской Федерации продукции военного назначения в интересах расположенных на территории Республики Крым и г. Севастополя организаций – разработчиков и производителей такой продукции по обязательствам, возникшим до 21 марта 2014 г.

Государственным посредником при осуществлении внешнеторговой деятельности определено открытое акционерное общество «Рособоронэкспорт».

**Источник:** система Консультант Плюс.

*Указ Президента Российской Федерации от 10.05.2015 № 239  
«О внесении изменений в перечень федеральных округов, утвержденный  
Указом Президента Российской Федерации от 13 мая 2000 г. № 489»  
(начало действия документа – с момента подписания)*

Внесены изменения в перечень федеральных округов, утвержденный Указом Президента Российской Федерации от 13 мая 2000 г. № 849 «О полномочном представителе Президента Российской Федерации в федеральном округе».

Изменения коснулись Приволжского, Сибирского и Дальневосточного федеральных округов.

Изменено название Ханты-Мансийского автономного округа на «Ханты-Мансийский автономный округ – Югра».

**Источник:** система Консультант Плюс.

*Постановление Правительства Российской Федерации от 28.04.2015 № 417  
«О внесении изменений в Положение о проведении международных выставок  
образцов продукции военного назначения на территории Российской  
Федерации и об участии российских организаций в таких  
выставках на территориях иностранных государств»*

Утверждены изменения в Положение о проведении международных выставок образцов продукции военного назначения на территории Российской Федерации и об участии российских организаций в таких выставках на территориях иностранных государств, утвержденное постановлением Правительства Российской Федерации от 2 июня 2007 г. № 339. Изменения касаются порядка утверждения Федеральной службой по военно-техническому сотрудничеству и



порядка согласования Министерством обороны Российской Федерации и при необходимости иными федеральными органами исполнительной власти объемов информации об экспортной комплектации и тактико-технических характеристиках продукции или об основных параметрах научно-исследовательских и опытно-конструкторских работ по ее созданию (модернизации).

Определены сроки представления перечня образцов продукции военного назначения на согласование в Минобороны России, ФСТЭК России, МИД, Минпромторг России, ФСБ России и СВР России.

**Источник:** система Консультант Плюс.

*Постановление Правительства Российской Федерации от 28.04.2015 № 415  
«О правилах формирования и ведения единого реестра проверок»*

Утверждены Правила формирования и ведения единого реестра проверок при осуществлении государственного контроля (надзора) и муниципального контроля в Российской Федерации.

Установлено, что положения Правил в части присвоения учетного номера проверкам и включения в единый реестр проверок информации о проверках применяются в отношении проверок, проводимых при осуществлении федерального государственного контроля (надзора) органами исполнительной власти субъектов Российской Федерации, и проверок, проводимых при осуществлении регионального государственного контроля (надзора), вступают в силу с 1 июля 2016 г.

**Источник:** система Консультант Плюс.



### 3.2. Документы ФСТЭК России

*Приказ ФСТЭК России от 10.04.2015 № 33*

*«Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности»*

Утверждены Правила выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы в установленной ФСТЭК России сфере деятельности.

Правила определяют порядок выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий и включают детализированные критерии и процедуры аккредитации, предусмотренные Правилами аккредитации. Приводится порядок проведения экспертами по аккредитации оценки соответствия заявителя критериям аккредитации, а также порядок



принятия решения по результатам оценки соответствия заявителя критериям аккредитации.

**Источник:** система Консультант Плюс.

### 3.3. Патентные документы



*Пат. 2551802 Российская Федерация, МПК G06F21/00 (2013.01), H04K3/00 (2006.01), H04L9/00 (2006.01). Устройство защиты оптической сети от несанкционированного зондирования методами оптической рефлектометрии. / Гришачев В.В.; патентообладатель Гришачев В.В. – 2012154691/08, заявл. 18.12.2012, опубл. 27.05.2015.*

Устройство предназначено для предотвращения несанкционированного зондирования защищаемых сегментов оптических кабельных систем и сетей различного назначения. Технический результат изобретения заключается в повышении эффективности защиты информации методами зашумления оптического канала.

*Пат. 2551820 Российская Федерация, МПК G06F21/56 (2013.01). Способ и устройство для проверки файловой системы на наличие вирусов. / Ниемеля Я., Хармонен Т., Зирвальд Й., Стохлберг М.; патентообладатель Ф-Секьюэ Корпорейшен. – 2012102818/08, заявл. 07.07.2010, опубл. 27.05.2015.*

Изобретение относится к средствам для выполнения антивирусного сканирования файловой системы. Технический результат заключается в увеличении скорости сканирования файла.

*Пат. 2552135 Российская Федерация, МПК G06F21/72 (2013.01). Устройство защиты от атак для сетевых систем. / Пузанов Н.А., Шубин Д.Л.; патентообладатель Общество с ограниченной ответственностью «СмартТелеМакс». – 2013141238/08, заявл. 09.09.2013, опубл. 10.06.2015.*

Изобретение относится к области обеспечения информационной безопасности. Техническим результатом является повышение эффективности защиты от атак для сетевых систем.

*Пат. 2552166 Российская Федерация, МПК H04L29/06 (2006.01). Способ и устройство для аутентификации вызов-ответ. / Шрикс Л., Мансхолт М., Стайнбринк М.; патентообладатель ЗМ ИННОВЕЙТИВ ПРОПЕРТИЗ КОМПАНИ. – 2013106951/08, заявл. 28.07.2011, опубл. 10.06.2015.*

Изобретение относится к способам выполнения аутентификации. Технический результат заключается в повышении безопасности передачи данных.

*Пат. 2552189 Российская Федерация, МПК G06K9/62 (2006.01). Способ биометрической аутентификации пользователя. / Никитин В.В., Басов О.О., Офицеров А.И., Стародубцев П.Ю.; патентообладатель Государственное казенное образовательное учреждение высшего профессионального образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России). – 2014129267/08, заявл. 15.07.2014, опубл. 10.06.2015.*



Изобретение относится к области биометрической аутентификации пользователя. Техническим результатом является уменьшение вероятности ошибки первого рода аутентификации пользователя, когда допущенный в систему пользователь, параметры образца почерка которого имеются в базе данных системы контроля допуска, отвергается системой допуска.

*Пат. 2552903 Российская Федерация, МПК F41H3/00 (2006.01). Способ инфракрасной маскировки и устройство для инфракрасной маскировки (варианты). / Староверов Н.Е.; патентообладатель Староверов Н.Е. – 2013143090/12, заявл. 23.09.2013, опубл. 10.06.2015.*

Изобретение относится к маскировке военных объектов, в частности военной техники. Техническим результатом изобретения является невозможность инфракрасного обнаружения военного объекта, даже высокоскоростного.

*Пат. 2552978 Российская Федерация, МПК F41H3/00 (2006.01). Устройство адаптивной маскировки объектов. / Афанасьева Е.М., Ельцов О.Н., Петещенков Э.В.; патентообладатель Российская Федерация, от имени которой выступает Министерство обороны Российской Федерации, Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж) Министерства обороны Российской Федерации. – 2014116935/12, заявл. 25.04.2014, опубл. 10.06.2015.*

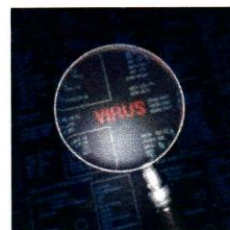
Изобретение предназначено для маскировки стационарных или движущихся объектов с помощью адаптивных маскировочных устройств, работающих в оптическом диапазоне длин волн. Техническими результатами заявленного изобретения являются устранение демаскирования объекта в инфракрасном диапазоне длин волн за счет снижения радиационного контраста объекта более чем в три раза и расширение диапазона условий применения устройства для маскировки в видимом диапазоне длин волн за счет использования люминесцентных красок, обладающих повышенными яркостями свечения, и, следовательно, повышение эффективности маскировки.



#### 4. Статистические данные по анализу защищенности информационных систем

*В мире остаются SCADA-системы,  
зараженные Stuxnet*

Как сообщает сайт securitylab.ru со ссылкой на главного исполнительного директора компании «Kleissner & Associates», специалисты компании определили, что 153 компьютера в мире остаются зараженными вирусом Stuxnet. В том числе и ЭВМ, работающие в составе SCADA-систем. Целью Stuxnet при этом является выведение из строя машинного оборудования SCADA-систем.



В половине всех случаев инфицирования вредоносное ПО распространялось с территории Ирана, где оно было выявлено впервые. При этом 23% зараженных устройств находятся в Индии, 8% приходится на Индонезию и 7% на Саудовскую Аравию.

**Источник:** <http://www.securitylab.ru/news/473303.php> (дата размещения материала 11.06.2015).

*Отчет компании «Лаборатория Касперского» о целенаправленной  
реализации угрозы безопасности информации Grabit*

На сайте kaspersky.ru размещен отчет компании «Лаборатория Касперского» о кибершпионской кампании Grabit, в рамках которой были украдены тысячи учетных записей сотрудников небольших организаций, расположенных в основном в Таиланде, Индии и США. Заражение осуществлялось с помощью рассылки почтовых сообщений с вложенным файлом, выглядящим как документ Microsoft Office Word.



В качестве иллюстрации масштаба Grabit служит собранная «Лабораторией Касперского» статистика. На одном управляющем сервере злоумышленников было обнаружено 2997 паролей, 1053 электронных письма, 3023 имени пользователей от 4928 различных серверов (внутренних и внешних), включая учетные записи Outlook, Facebook, Skype, Google Mail, Pinterest, Yahoo, LinkedIn и Twitter, а также ряд банковских счетов.

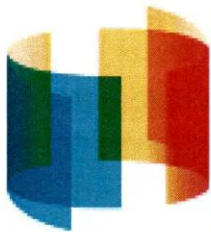
**Источник:** <http://www.kaspersky.ru/about/news/virus/2015/who-grabit-accounts-facebook-gmail-outlook-kaspersky-lab-research> (дата размещения материала 28.05.2015).

*Аналитический отчет по уязвимостям  
компании «Информзащита»*

По данным ряда сайтов, ссылающихся на старшего аудитора отдела безопасности банковских систем компании «Информзащита» Евгения Сачкова, компания «Информзащита» опубликовала отчет об уязвимостях, выявленных при проведении ASV-сканирований в ходе аудита информационной безопасно-



сти в компаниях разных отраслей. Были собраны и проанализированы данные по уязвимостям за 2014 г. и I квартал 2015 г.



Наиболее часто встречающиеся уязвимости обнаружены в устаревших версиях ПО Apache, Microsoft IIS и Open SSL, а в протоколах IPSec, SSL и Microsoft RDP выявлено использование слабого шифрования. В среднем в месяц выявляется около 100 новых уязвимостей, часть из которых может иметь средний и высокий уровни критичности. Значительная часть уязвимостей может быть очень быстро устранена, поэтому в вопросах управления уязвимостями главную роль играет знание об их существовании.

**Источники:** <http://www.infosec.ru/news/8689> (дата размещения материала 08.06.2015); <http://www.pcweek.ru/security/news-company/detail.php?ID=175126>.

#### *Отчет компании «Sonatype» об использовании уязвимых компонентов программного обеспечения*

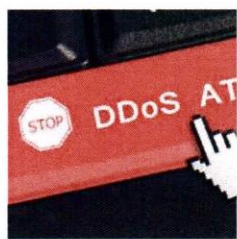
На сайте securitylab.ru со ссылкой на данные центрального репозитория компании «Sonatype» (sonatype.org) размещен отчет о бесконтрольном использовании компаниями компонентов с открытым исходным кодом. Отмечено, что в 2014 г. крупные финансовые компании и производители ПО загрузили более 240 тысяч компонентов с одного из крупнейших публичных хранилищ с элементами Java с открытым исходным кодом. Более 15 тысяч из них (7,5%) содержали опасные уязвимости. При этом 29 крупнейших финансовых и технологических компаний в среднем используют 27 различных версий каждого компонента.



Это означает, что большинство предприятий в разработках своих приложений обращаются к потенциально уязвимым версиям. С их помощью разработано более 1,5 тысяч приложений, каждое из которых содержало в среднем 24 опасных или критических уязвимости.

**Источник:** <http://www.securitylab.ru/news/473356.php> (дата размещения материала 17.06.2015).

#### *DDoS-атаки в России случаются все чаще*



По информации ряда сайтов, ссылающихся на данные, полученные «Лабораторией Касперского» в ходе анализа внутренней статистической информации за первые три месяца 2015 г., количество DDoS-атак с использованием ботнетов в России в I квартале этого года увеличилось и составило почти 1400. При этом выросло и число жертв, пострадавших от действий атакующих. В итоге Россия заняла четвертую позицию в рейтинге стран, чьи веб-ресурсы наиболее часто оказывались под прицелом организаторов DDoS-атак.

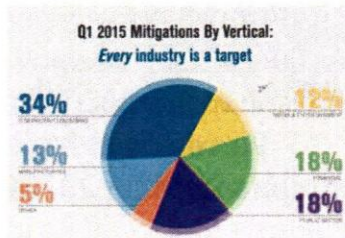


Всего же в I квартале 2015 г. киберпреступники совершили более 23 тыс. DDoS-атак с применением ботсетей на ресурсы, расположенные в 76 странах. При этом мишенями, помимо России, чаще всего были серверы на территориях Китая, США и Канады. В первой десятке жертв также оказались ресурсы из разных стран Европы и Азиатско-Тихоокеанского региона. В общей сложности ботнеты атаковали более 12 тыс. жертв по всему миру. Самая продолжительная зафиксированная DDoS-атака длилась 140 часов, а наибольшая продолжительность атак, которые пришлось вынести одному ресурсу, составила 21 день.

**Источники:** <http://www.pcweek.ru/security/news-company/detail.php?ID=1749440> (дата размещения материала 30.05.2015); <https://threatpost.ru/2015/05/30/issledovanie-ddos-atak-na-rossiyu-stalo-bolshe/>.

#### *Отчет компании «Verisign» об уровне распространения DDoS-атак*

На сайте [comss.info](http://comss.info) со ссылкой на материалы специалистов компании «Verisign» ([ddos-protection-services-review.toptenreviews.com](http://ddos-protection-services-review.toptenreviews.com)) сообщается о количестве DDoS-атак в Интернете в I квартале 2015 г., рост которых в сравнении с предыдущим периодом составил 7%. Частота подобных нападений увеличилась на компьютерные сети как государственного, так и финансового секторов. Так, в IV квартале прошлого года доля DDoS-атак от их общего количества составляла 15% против 18% за текущий период. Вместе с тем, треть всех нападений по-прежнему приходится на IT и SaaS сервисы.



Среди ключевых факторов, спровоцировавших текущее увеличение количества инцидентов, исследователи перечисляют повышение доступности различных инструментов для DDoS-атак, процветание подпольного бизнеса по сдаче ботнетов в аренду, а также ряд громких политических событий мирового значения.

**Источник:** [http://www.comss.info/page.php?al=V\\_pervom\\_kvartale\\_2015\\_goda\\_DDoS\\_atak\\_bylo\\_bolshe](http://www.comss.info/page.php?al=V_pervom_kvartale_2015_goda_DDoS_atak_bylo_bolshe) (дата размещения материала 05.06.2015).

#### *Отчет компании «NopSec» о состоянии информационной безопасности в банковской сфере*

Как сообщает сайт [threatpost.ru](http://threatpost.ru), ссылающийся на электронное издание [zdnet.com](http://zdnet.com), компания «NopSec» провела исследование 65 тыс. уязвимостей, зарегистрированных в банковской сфере на протяжении 20 последних лет. Результаты показали, что компании тратят на ликвидацию уязвимостей примерно по 176 дней. При этом почти у трети организаций, связанных с финансами, на это уходит до года. У 30% крупных компаний вообще нет никакого плана по реагированию на киберинциденты. Из тех компаний, у которых все-таки существует такого рода план, свыше половины (57%) никогда не обновляли и не пересматривали





его. Большое количество компаний в состоянии выявить утечку только через несколько недель после того, как важные данные могут попасть в руки злоумышленников.

**Источник:** <https://threatpost.ru/2015/06/03/banki-zakryvayut-odnu-uyazv-most-po-polgota> (дата размещения материала 03.06.2015).

*Отчет компании «IBM X-Force» о защищенности персональных данных*

По данным сайта securitylab.ru со ссылкой на сайт компании «IBM» (ibm.com), в 2014 г. в Сеть утекло более 1 млрд. записей персональных данных.



Об этом сообщается в отчете компании «IBM X-Force». При этом характер утечек включал похищение персональных данных не только с целью получения финансовой выгоды, но и для осуществления террористических угроз и дискредитации организаций. Самыми атакуемыми компаниями оказались компьютерные сервисы (28,7%), компании ритейл-индустрии (13%), правительственные организации (10,7%), организации, связанные со сферой образования (8%), финучреждения (7,3%), учреждения здравоохранения (6,9%), медиа и туристические компании (5,7%).

**Источник:** <http://www.securitylab.ru/news/473228.php> (дата размещения материала 08.06.2015).

*Отчет компании «WhiteHat» о состоянии информационной безопасности сайтов*

Согласно информации, размещенной на сайте threatpost.ru со ссылкой на



портал scmagazine.com, 86% сайтов содержат как минимум одну серьезную уязвимость в приложениях и эти бреши длительное время остаются открытыми. Статистика компании «WhiteHat» основана на результатах мониторинга более чем 30 тыс. сайтов. В отчете отмечено, что в 70% случаев риски для сайта высоки из-за слабой их защиты на транспортном уровне, в 56% случаев ресурсу грозит утечка информации.

За год были исправлены 61% обнаруженных уязвимостей, причем на их устранение у владельцев сайтов в среднем уходило 193 дня (с момента получения первой нотификации).

**Источник:** [https://threatpost.ru/2015/05/26/whitehat\\_86\\_protsentov\\_sajtov\\_ot\\_kryty\\_dlja\\_vzloma](https://threatpost.ru/2015/05/26/whitehat_86_protsentov_sajtov_ot_kryty_dlja_vzloma) (дата размещения материала 26.05.2015).

*Отчет компании «Лаборатория Касперского» об анализе спам-сообщений*

На сайте [russpamcismagazine.com](http://russpamcismagazine.com) со ссылкой на данные компании «Лаборатория Касперского» (kaspersky.ru) размещена информация о результатах проведенного компанией исследования спам-сообщений. Доля спама в мировом почтовом трафике за I квартал 2015 г. составила 59%, что на 6% меньше, чем в



предыдущем квартале. Спам становится более опасным, поскольку злоумышленники все чаще начинают рассылать по электронной почте вредоносное ПО. Больше всего спама отправляется из США (14,5%), России (7,27%) и Украины (5,56%). Вредоносные вложения в спам-сообщениях в основном маскируют под различные финансовые документы. Если пользователь открывает прикрепленные файлы с таким вложением, на его компьютер автоматически начнут устанавливаться вирусы.



**Источник:** <http://payspacemagazine.com/spam-stanovitsya-opasnym-kaspersky.html> (дата размещения материала 29.05.2015).

*Отчет компании «McAfee» об анализе распространения в Интернете вирусов-вымогателей*

Сайт d-russia.ru разместил отчет компании «McAfee» (reuters.com), содержащий анализ распространения вирусов вымогателей в течение первых трех месяцев 2015 г. Отмечен рост их количества более чем в два раза по сравнению с аналогичным периодом 2014 г. Эксперты компании обнаружили 700 тыс. образцов вымогателей на компьютерах, телефонах и в сетях своих клиентов. Число вредоносных программ, использующих уязвимости в Adobe Flash, в I квартале 2015 г. выросло на 317%. Было обнаружено 200 тыс. образцов подобного вредоносного ПО среди клиентской базы «McAfee».



**Источник:** <http://d-russia.ru/chislo-virusov-vymogatelej-bolee-chem-udvoilos-v-i-kvartale-mcafee.html> (дата размещения материала 09.06.2015).

*Отчет компании «ESET» о возможности получения доступа к корпоративной информации через социальные сети*

Ряд сайтов приводит информацию об отчете специалистов компании «ESET» (esetnod32.ru), который содержит результаты анализа возможностей несанкционированного доступа к корпоративной информации через социальные сети. Отмечено, что сети компаний могут быть взломаны через аккаунты сотрудников, использующих социальные медиа на работе. В 12% организаций уже сталкивались с подобными инцидентами.



Киберпреступники используют социальные сети для распространения вредоносного ПО в обход корпоративных межсетевых экранов и перенаправляют пользователей на фишинговые сайты с целью кражи конфиденциальной информации.

**Источники:** <http://www.esetnod32.ru/company/press/center/eset-36-kompaniy-mogut-byt-vzlomany-cherez-sotsseti> (дата размещения материала 09.06.2015); <http://www.computerworld.kz/news/8808>.



## *Отчет об уровне информационной безопасности Android устройств компании «Google»*

В журнале «Chip» опубликован отчет об уровне информационной безопасности мобильных телефонов и планшетных компьютеров с операционной системой Android за 2014 г. Общий уровень зараженности устройств с операционной системой Android составляет 1%. Для устройств, устанавливающих приложения только из Play Store, уровень зараженности составляет порядка 0,15 %. Такой низкий уровень вирусной активности компании «Google» удалось достигнуть путем устранения ряда критических уязвимостей операционной системы Android.



**Источник:** Chip, 2015 г. № 6, с. 12.

## *Защита от отслеживания Firefox сокращает время загрузки страниц*

По данным сайта [opennet.ru](http://opennet.ru) со ссылкой на специалиста компании «Mozilla» Монику Чу ([monica-at-mozilla.blogspot.ru](mailto:monica-at-mozilla.blogspot.ru)), эффективность добавленных в браузер Firefox средств защиты от попыток отслеживания перемещения пользователя между сайтами увеличивает эффективность работы пользователя. При этом снижается время загрузки страниц в среднем на 44%, размер загружаемых данных уменьшается на 39%, а число устанавливаемых Cookie сокращается на 67,5%. Почти все заблокированные Cookie связаны с работой 11 типовых блоков отслеживания, встречающихся на половине из протестированных сайтов.



mozilla  
**Firefox**

Реализованная в Firefox система использует метод блокирования внешних JavaScript-скриптов, изображений и iframe-страниц с сайтов, занесенных в черный список [disconnect.me](http://disconnect.me). В настоящее время в список блокировки входит около 1500 доменов, с которых загружается код, обеспечивающий отслеживание перемещения пользователей между сайтами.

**Источник:** <http://www.opennet.ru/opennews/art.shtml?num=42291> (дата размещения материала 24.05.2015).

## *Правоохранители просматривают конфиденциальные данные британцев «каждые две минуты»*

На сайте [securitylab.ru](http://securitylab.ru) размещена информация об отчете группы «Big Brother Watch», стоящей на защите гражданских прав и личной информации.



Согласно официальной правительственной статистике, разрешение на перехват телефонных разговоров и электронной почты выдается в 96% случаев. Отказ следует лишь в одном из 25 случаев.

В течение последних трех лет сотрудники британской полиции на территории всей страны получали доступ к конфиденциальной информации местных жителей не менее 733237 раз.



Таким образом, в период с января 2012 г. по декабрь 2014 г. полиция направляла соответствующие запросы в среднем каждые две минуты.

**Источник:** <http://www.securitylab.ru/news/473166.php> (дата размещения материала 03.06.2015).

*Данные сотрудников топовых компаний  
Европы доступны онлайн*

По сообщению сайта [threatpost.ru](http://threatpost.ru) со ссылкой на данные исследователей из компании «Recorded Future», адреса корпоративной электронной почты и пароли работников половины крупнейших европейских компаний можно получить в Интернете. Речь идет о 49% компаний из числа топ-500, то есть о 224 предприятиях. Туда входят самые большие банки Европы, нефтяные и газовые компании, лидеры телеком-рынка. Данные их сотрудников были обнаружены на многочисленных сайтах и форумах, которыми пользуются киберпреступники. Хакеры добывали эти данные не из компьютерных систем компаний, а взламывая сторонние сайты. Сотрудники сами регистрировались на каком-либо интернет-сервисе и оставляли адреса корпоративной электронной почты.



В 2014 г. количество записей, утечка которых была допущена, увеличилось на 25% по сравнению с предыдущим годом. В общей сложности скомпрометированных записей оказался 1 млрд. Еще в 2014 г. таких записей было 800 млн., а в 2012 – около 300 млн.

**Источник:** <https://threatpost.ru/2015/06/02/dannye-sotrudnikov-topovyh-kompanij-evropy-dostupny-onlajn/> (дата размещения материала 02.06.2015).



## 5. Сведения об инцидентах информационной безопасности

### *Разведки США и Германии следят за полумиллионом объектов в Европе*

Согласно данным сайта [pronedra.ru](http://pronedra.ru) со ссылкой на журнал «Spiegel», разведывательные службы США и Германии осуществляют тесное сотрудничество в ходе своей профессиональной деятельности. На компьютерах Федеральной разведывательной службы Германии хранятся данные о более чем 459 тыс. объектах слежки. Информация содержит номера телефонов, IP-адреса, данные электронной почты и аккаунты в социальных сетях. Спецслужбы обеих стран постоянно обмениваются информацией между собой. Объектами слежки, как правило, являются высокопоставленные чиновники, компании, а также научно-исследовательские учреждения.

**Источник:** <http://pronedra.ru/globalpolitics/2015/05/22/frg-ssha-slezhkavev-gore> (дата размещения материала 24.05.2015).

### *Канадские спецслужбы шпионили за пользователями через UC Browser*

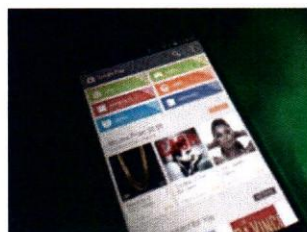
По информации, размещенной на сайте [gizmonews.ru](http://gizmonews.ru) со ссылкой на опубликованные материалы расследования американского популярного ресурса «The Intercept» вместе с телевизионным каналом «СВС», канадские спецслужбы организовали слежку за некоторыми категориями граждан, используя для этой цели смартфоны. ПО для ведения слежки встраивалось в популярный UC Browser, являющийся приложением под операционную систему Android. С его помощью осуществлялась слежка за представителями Китая, Индии, США и других стран.

**Источники:** [http://news.rambler.ru/internet/30571570/?track=topic\\_newslist](http://news.rambler.ru/internet/30571570/?track=topic_newslist) (дата размещения материала 23.06.2015); <http://www.vedomosti.ru/politics/news/2015/06/23/597566-anb-pitalos-vzlomat-antivirusi-laboratorii-kasperskogo>, <http://tass.ru/mezhdunarodnaya-panorama/2063331>.

### *Крупная атака на государственную службу США*

По данным ряда сайтов, ссылающихся на информацию издания «Wall Street Journal», на компьютерную сеть Службы управления персоналом США совершена атака. Данная служба хранит информацию о бывших и нынешних государственных служащих.

Скомпрометированы персональные данные примерно 4 млн. человек. Со стороны властей этим людям предложена помощь по отслеживанию платежей с банковской карты и противодействию использованию личных данных третьими лицами. Как заявляет ряд специалистов, источником атаки является Китай.





**Источник:** <https://xakep.ru/2015/06/05/opm-hack> (дата размещения материала 05.06.2015); <http://safe.cnews.ru/news/top/index.shtml?2015/06/05/596296>.

### *Хакерские атаки на налоговое ведомство США*

На сайте [ria.ru](http://ria.ru) со ссылкой на материалы американского информгентства «AP» ([ap.org](http://ap.org)) размещена информация о взломе сайта Службы внутренних доходов США. Для доступа к сайтам злоумышленники блокировали так называемую «страницу безопасности», которая запрашивает сведения о налогоплательщике, включая его номер социального страхования, дату рождения, налоговый статус и почтовый адрес. В целом с подозрительных электронных адресов было сделано порядка 200 тыс. запросов. Более 100 тыс. таких попыток оказались успешными.



**Источник:** <http://ria.ru/world/20150527/1066654718.html#ixzz3bKzjRul1> (дата размещения материала 27.05.2015).

### *Компьютеры NASA оказались инфицированы CryptoLocker*

В соответствии с информацией, размещенной на сайте [tavasardze.lv](http://tavasardze.lv) со ссылкой на электронный журнал [motherboard.vice.com](http://motherboard.vice.com), два компьютера Национального управления по воздухоплаванию и исследованию космоса (NASA) США были поражены вымогательским ПО CryptoLocker. Это привело к потере доступа к данным. Однако специалистам исследовательского ведомства удалось восстановить часть из них благодаря резервному копированию.



**Источник:** <http://ru.tavasardze.lv/dva-kompyutera-nasa-okazalis-ificirovany-cryptolocker> (дата размещения материала 08.06.2015).

### *Сирийская электронная армия взломала сайт сухопутных войск США*

Как сообщает сайт [interfax.ru](http://interfax.ru) со ссылкой на заявление пресс-секретаря армии США бригадного генерала Малкольма Фроста, сайт сухопутных войск США [Army.mil](http://Army.mil) был взломан специалистами Сирийской электронной армии и временно прекратил работу. Хакеры разместили на сайте ряд сообщений, которые подвергают критике вербовку и подготовку американскими военными бойцов из числа сирийской оппозиции для борьбы против правительственных войск.



Сайт [Army.mil](http://Army.mil) является сайтом общего пользования и не содержит значимой информации военного характера или персональных данных американских военнослужащих.



**Источник:** <http://www.interfax.ru/world/446482> (дата размещения материала 05.06.2015).

*Взлом федерации компаний, предоставляющих услуги  
медицинского страхования в США*

По информации, размещенной на сайте [threatpost.ru](http://threatpost.ru) со ссылкой на заявление гендиректора компании «CareFirst» Чета Баррелла и других представителей компании, хакеры смогли получить доступ к одной из баз данных «CareFirst BlueCross BlueShield» (BCBS) – федерации компаний, предоставляющих услуги медицинского страхования в США. Клиентами BCBS является почти треть населения страны.



Во взломанной базе данных содержались имена, даты рождения, адреса электронной почты и идентификационные номера абонентов. Компания в настоящее время проводит оповещение клиентов о взломе и возможных последствиях. Также предусмотрены мероприятия по кредитному мониторингу пострадавших.

**Источник:** <https://threatpost.ru/2015/05/29/1-1-million-affected-by-carefirst-bluecross-blueshield-breach> (дата размещения материала 29.05.2015).

*Опубликованы документы, полученные в результате взлома  
корпоративной сети компании «Sony Pictures»*

Как сообщает сайт [securitylab.ru](http://securitylab.ru) со ссылкой на ресурс WikiLeaks, в Интернете опубликованы 276394 документа, похищенные в результате взлома корпоративной сети компании «Sony Pictures». Документы вызвали общественный интерес, так как компания «Sony» тесно связана с Белым домом США и с американским военно-промышленным комплексом, а также из-за влияния компании на принятие законов, касающихся Интернета. По данным ряда специалистов, атака проведена по указанию руководства Северной Кореи.



**Источник:** <http://www.securitylab.ru/news/473387.php> (дата размещения материала 18.06.2015).

*Источник кибератаки на внутреннюю сеть Бундестага  
до сих пор остается тайной*

Согласно информации сайта [securitylab.ru](http://securitylab.ru) со ссылкой на материалы расследования Федеральной прокуратуры Германии, в парламенте Германии подтвердили факт утечки данных после проведенной атаки на компьютерную сеть Бундестага. О пострадавших в результате взлома службах и характере похищенной информации пока не сообщается. Специалисты не смогли определить ни источник атаки, ни точную дату ее начала. Вредоносное ПО, инфицировавшее всю сеть Бундестага, включая ком-





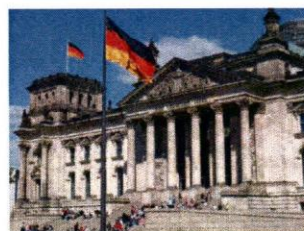
пьютеры членов парламента, могло находиться на них в течение месяцев, а то и лет. Сама по себе атака довольно сложна и, скорее всего, ее авторы далеко не дилетанты.

Депутаты не исключают вероятности того, что за кибернападением могут стоять правительства Китая, Северной Кореи, Великобритании или США, владеющие значительными хакерскими возможностями.

**Источник:** <http://www.securitylab.ru/news/473152.php> (дата размещения материала 02.06.2015).

### *Парламент Германии обсуждает полную замену аппаратного и программного обеспечения внутренней сети*

Как информирует со ссылкой на издание «Spiegel» сайт securitylab.ru, необходимость замены аппаратного и программного обеспечения внутренней сети немецкого парламента может возникнуть из-за недавней атаки неизвестных хакеров, спонсируемых, по мнению «Spiegel», российским Правительством. Спустя четыре недели после инцидента, власти так и не смогли удалить с зараженных систем шпионские программы. Внедренный в сеть Бундестага троян по-прежнему функционирует и продолжает отправлять данные на сторонние серверы. При этом получатель этой конфиденциальной информации остается неизвестным.



Ранее сообщалось о причастности к инциденту российских спецслужб. IT-специалисты из технического департамента при немецком парламенте получили часть исходного кода трояна и по итогам анализа обнаружили доказательства того, что его создателями являются спецслужбы России. В настоящий момент сами парламентарии начали обсуждение возможности полностью заменить все компоненты внутренней сети. С учетом этих масштабов это может вылиться в месяцы технических работ.

**Источник:** <http://www.securitylab.ru/news/473307.php> (дата размещения материала 11.06.2015).

### *Хакеры атаковали сайты правительства Канады*

По информации сайта regnum.ru со ссылкой на видеообращение группы хакеров «Anonymous», участники группы атаковали несколько сайтов правительства Канады. Помимо сайта правительства, атаке подверглись также веб-ресурсы Службы безопасности и разведки и Центра безопасности коммуникаций. Также взлом затронул работу электронной почты. Атака стала ответом на недавнее принятие канадским парламентом нового антитеррористического закона, расширяющего полномочия спецслужб, который, по их мнению, нарушает права человека.



**Источник:** <http://www.regnum.ru/news/polit/1934550.html> (дата размещения материала 18.06.2015).



### *Взломан сайт Объединенного штаба вооруженных сил Литвы*



Как сообщает сайт [lenta.ru](http://lenta.ru) со ссылкой на заявление пресс-секретаря министерства обороны страны Виктории Цемините, взломана компьютерная сеть Объединенного штаба вооруженных сил Литвы. В результате хакеры получили несанкционированный доступ к данным о начавшихся 1 июня в странах Балтии и Польше учениях НАТО «Удар меча». В результате атаки на сайте Объединенного штаба размещена компрометирующая литовские власти информация.

**Источник:** <http://lenta.ru/news/2015/06/11/kaliningrad> (дата размещения материала 11.06.2015).

### *Хакерская атака на Варшавский аэропорт*



По данным ряда сайтов, ссылающихся на заявление представителя авиакомпании «LOT» Адриана Кубицкого, аэропорт Варшавы «Окенче» атаковали хакеры, после чего случилась авария IT-системы, отвечающей за регистрацию пассажиров. В результате атаки ряд рейсов был задержан или отменен. Проблемы с атакой хакеров в аэропорту коснулись более 1,4 тысяч пассажиров. По данным персонала аэропорта система управления воздушным движением затронута не была.

**Источники:** <http://mir24.tv/news/incident/12808482> (дата размещения материала 22.06.2015); <http://world.fedpress.ru/news/europe/1434950294-khakery-atakovali-aeroport-varshavy>; <https://hi-tech.mail.ru/news/hackers-attack-warsaw-airport.html>, <https://job.1tv.ru/news/techno/286270>.

### *Киберпреступная группировка три года атаковала страны Юго-Восточной Азии*



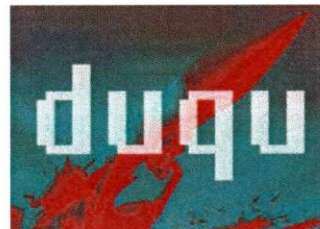
Согласно сообщению сайта [securitylab.ru](http://securitylab.ru) со ссылкой на заявление специалистов компании «Palo Alto Networks», обнаружена целенаправленная атака группы хакеров под названием «Lotus Blossom» на правительственные и военные организации в Юго-Восточной Азии. В ходе трехлетней кампании злоумышленники осуществили более 50 кибератак. Злоумышленники применяли фишинг, используя вредоносные документы и файл-приманку, содержащий контент, связанный с родом занятий жертвы. Вложение электронных писем обычно содержало код эксплойта для известной уязвимости в Microsoft Office. В ходе атаки использовался троян Elise.

**Источник:** <http://www.securitylab.ru/news/473358.php> (дата размещения материала 17.06.2015).



*Атака на корпоративную сеть компании  
«Лаборатория Касперского»*

На ряде сайтов размещена информация со ссылкой на заявление Евгения Касперского, генерального директора «Лаборатории Касперского», об атаке на корпоративную сеть компании «Лаборатория Касперского» под названием Duqu 2.0. Хакеры использовали уникальные и ранее не встречавшиеся инструменты и практически не оставляли следов в системе. Атака осуществлялась при помощи эксплойтов, использовавших уязвимости нулевого дня в ОС Windows, а дополнительное вредоносное ПО доставлялось в атакованные системы под видом Microsoft Software Installers – установочных файлов, используемых системными администраторами для инсталляции ПО на компьютеры в удаленном режиме. Вредоносное ПО не создавало и не модифицировало какие-либо дисковые файлы или системные настройки, что делало детектирование атаки затруднительным.



Эксперты компании обнаружили и другие жертвы атаки в ряде западных, ближневосточных и азиатских стран.

**Источники:** <http://www.kaspersky.ru/about/news/virus/2015/duqu-is-back> (дата размещения материала 10.06.2015); <http://aksakal.tv/news/internet/10017-korporativnuyu-set-rossiyskoy-laboratorii-kasperskogo-atakovali-neizvestnye.html>, <http://www.securitylab.ru/news/473301.php>.

*АНБ США и британский Центр правительственной связи пытались  
взломать ПО компании «Лаборатория Касперского»*

В соответствии с информацией ряда сайтов, ссылающихся на документы бывшего сотрудника американских спецслужб Эдварда Сноудена, опубликованные американским новостным порталом «The Intercept», АНБ США и британский Центр правительственной связи изучали слабые места и пытались, по сути, взломать ПО компании «Лаборатория Касперского». Британская спецслужба преследовала цель препятствовать работе ПО с помощью технологии так называемой обратной разработки ПО. АНБ также изучало ПО «Лаборатории Касперского» на предмет его уязвимости, чтобы получить конфиденциальную информацию клиентов.



**Источники:** [http://news.rambler.ru/internet/30571570/?track=topic\\_newslist](http://news.rambler.ru/internet/30571570/?track=topic_newslist) (дата размещения материала 23.06.2015); <http://www.vedomosti.ru/politics/news/2015/06/23/597566-anb-pitalos-vzlomat-antivirusi-laboratorii-kasperskogo>, <http://tass.ru/mezhdunarodnaya-panorama/2063331>.

*Хакеры взломали сайт Всероссийского центра изучения  
общественного мнения России*

По сообщению сайта [news.softodrom.ru](http://news.softodrom.ru) со ссылкой на данные компании «Доктор Веб» ([news.drweb.ru](http://news.drweb.ru)), хакеры взломали сайт Всероссийского центра



изучения общественного мнения (ВЦИОМ). Взлому подверглась как русскоязычная, так и англоязычная версии сайта ВЦИОМ. Киберпреступники создали на скомпрометированном сервере специальный раздел, в котором размещались веб-страницы с заголовками, пользующимися высокой популярностью согласно статистике поисковых систем.



При попытке открыть такую ссылку в окне браузера пользователю демонстрировалась поддельная веб-страница популярной службы хранения файлов «Яндекс.Диск» или же веб-страница с заголовком WCIOM.RU, на которой потенциальной жертве предлагалось скачать архив с неким «полезным» содержанием. Все размещенные злоумышленниками на сайте ВЦИОМ архивы содержали вредоносную программу, относящуюся к семейству Trojan.Down Loader.

**Источник:** <http://news.softodrom.ru/ap/b22268.shtml> (дата размещения материала 17.06.2015).

#### *Хакеры атаковали сайт видеонаблюдения за единым государственным экзаменом*

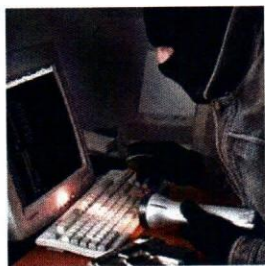
Согласно данным сайта fedpress.ru со ссылкой на заявление главы Рособнадзора Сергея Кравцова, специалистами Рособнадзора Российской Федерации зафиксирована хакерская атака на сайт видеонаблюдения за единым государственным экзаменом. Заблокированы четыре IP-адреса, с которых велись атаки. Экспертами атака определена как слабая, к отказам работы сайта видеонаблюдения она не привела.



**Источник:** [http://fedpress.ru/news/society/news\\_society/1433754192-khake-ry-atakuyut-sait-videonablyudeniya-za-ege](http://fedpress.ru/news/society/news_society/1433754192-khake-ry-atakuyut-sait-videonablyudeniya-za-ege) (дата размещения материала 08.06.2015).

#### *Хакеры похитили из пенсионного фонда Японии персональные данные 1,25 млн. граждан*

По информации сайта securitylab.ru со ссылкой на заявление главы пенсионного фонда Японии Тоитиро Мидзусима, в результате масштабного взлома компьютерной системы Государственного пенсионного фонда Японии неизвестные злоумышленники похитили персональные данные 1,25 млн. граждан. Похищенная информация включала имена, идентификационные номера, даты рождения и адреса пенсионеров. Инфицировавший систему вирус содержался в электронном письме, которое было открыто на одном из компьютеров фонда.



Проводится расследование инцидента и принимаются все необходимые меры для предотвращения подобной ситуации в будущем. Пенсионный фонд



намерен присвоить новые идентификационные номера всем лицам, чьи данные были похищены в результате взлома.

**Источник:** <http://www.securitylab.ru/news/473158.php> (дата размещения материала 02.06.2015).

*В результате утечки данных сеть супермаркетов «подарила» клиентам скидочные купоны стоимостью в \$1 млн.*

По данным сайта [internetua.com](http://internetua.com), ссылающегося на данные австралийских СМИ, произошла масштабная утечка данных клиентов сети крупных супермаркетов «Woolworths». Более тысячи человек по ошибке получили по электронной почте список, содержащий имена и адреса покупателей, а также ссылку на загрузку 7941 ваучера на сумму в \$1 308 505. У получивших ссылку пользователей появился доступ к кодам подарочных карт, а значит и возможность использовать их для осуществления покупок.



По словам представителя «Woolworths», произошла утечка только электронных адресов клиентов, другая персональная информация скомпрометирована не была. Пользователи, ставшие жертвами утечки, были предупреждены об инциденте сразу же после его обнаружения, а подарочные карты отменены.

**Источник:** <http://internetua.com/v-rezultate-utecski-set-supermarketov-podara-rila--klientam-skidocsnie-kuponi-stoimostua-v--1-mln> (дата размещения материала 01.06.2015).

*Один из web-сайтов компании «Microsoft» взломан неизвестными хакерами*

Сайт [itsec.ru](http://itsec.ru) со ссылкой на электронный журнал, издаваемый компанией «CBS Interactive» ZDNet, сообщил, что один из принадлежащих компании «Microsoft» web-сайтов ([digitalconstitution.com](http://digitalconstitution.com)) был взломан неизвестными хакерами. В настоящий момент корпорация использует ресурс для распространения информации о своем отношении к программам наблюдения АНБ, а также для публичного обсуждения инициативы по введению международных ордеров на обыск. Предполагается, что атака стала возможной благодаря тому, что администрация [digitalconstitution.com](http://digitalconstitution.com) вовремя не обновила CMS. Несмотря на то, что актуальной сборкой WordPress является 4.2.2, ресурс все еще использует версию 4.0.5.



**Источник:** [http://www.itsec.ru/newstext.php?news\\_id=105273](http://www.itsec.ru/newstext.php?news_id=105273) (дата размещения материала 19.06.2015).

*Взломан сайт фотохостинга «Photobucket»*

На сайте [хакер.ru](http://хакер.ru) со ссылкой на заявление министерства юстиции США размещена информация о взломе сайта фотохостинга Photobucket. Несанкцио-



нированный доступ реализовался с применением программного приложения под названием Photofuck. Его пользователи могли получить доступ к чужим приватным фотографиям и видео.



Photobucket представляет собой сервис для хранения мультимедийных файлов с возможностью конвертации в любой формат.

**Источник:** <https://xaker.ru/2015/05/25/photobucket> (дата размещения материала 25.05.2015).

*Киберпреступник из Пакистана взломал сайт  
музыкального сервиса Gaana*

Как информирует ряд сайтов, ссылающихся на официальную страницу компании «Gaana» в Twitter, сайт музыкального сервиса Индии Gaana был взломан хакером с помощью SQL-инъекции. Хакер из Пакистана похитил личную информацию 10 млн. пользователей, которая включает логины, даты рождения, адреса электронной почты и зашифрованные при помощи алгоритма MD5 пароли, которые поместил в Интернете в виде базы данных с возможностью поиска.



Работа сервиса приостановлена, а все пользователи будут вынуждены сменить пароль после восстановления сайта Gaana.

**Источники:** <http://zhacker.net/it-news/2848-haker-iz-pakistana-vzlomal-muzykalnyy-servis.html> (дата размещения материала 30.05.2015); <http://internetua.com/kiberprestupnik-iz-pakistana-polucsil-dostup-k-10-mln-ucsetnih-zapisei-servisa-Gaana>.