Консорциум дизайн-центров российской электронной и микроэлектронной промышленности

Ежемесячный мониторинг. Выпуск № 1 (ноябрь, 2018)

Тренды События Мнения

Тема выпуска «Обеспечение безопасности критической информационной инфраструктуры»

Оглавление

Данный мониторинг сформирован на основе информации из открытых источников. Мониторинг предназначен для повышения информированности участников и партнёров Консорциума о событиях и трендах, относящихся к новым рынкам. Консорциум не несёт ответственность за достоверность и качество приведённой в мониторинге информации

Сайт Консорциума http://microelectronica.pro/konsortsium/

Тренды

Количество подключённых к ГосСОПКЕ субъектов критической информационной инфраструктуры будет расти

Подключением небольших компаний к государственной системе защиты от компьютерных атак (ГосСОПКА) займется «дочка» Сбербанка «Безопасная информационная зона» («Бизон»)

https://www.vedomosti.ru/technology/news/2018/10/17/783864-malii-biznes-kiberatak

Компании Solar Security и Positive Technologies совместно займутся созданием «под ключ» корпоративных и ведомственных центров ГосСОПКА. Закон «О безопасности критической информационной инфраструктуры» требует от госорганов и госкорпораций вводить их уже с начала 2018 года. Сейчас объем этого рынка не превышает 200 млн руб., но уже к 2020 году должен увеличиться до нескольких миллиардов.

https://www.kommersant.ru/doc/3472959

Недавно вышли «Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». Попробуем разобраться, чего же ждет регулятор от компаний, строящих у себя центры ГосСОПКА, и исследовать этот вопрос.

https://habr.com/company/solarsecurity/blog/422819/

Безопасность КИИ находится в центре внимания международных и национальных органов власти

Практически все ведущие страны мира закрепляют в законодательстве обеспечение безопасности КИИ. В частности, создаются региональные сегменты и системы предупреждения и борьбы с кибератаками на объекты КИИ, сюда же относится и шпионаж.

ЕС

Критическая инфраструктура. Защита и устойчивость Европы (Critical Infrastructure. Protection and Resilience Europe)

Директива Европарламента и Совета ЕС «Об общих мерах высокого уровня безопасности сетевых и информационных систем в рамках Союза» от 6 июля 2016. «Директива NIS».

США

Безопасность и устойчивость критической инфраструктуры (США) (Critical Infrastructure Security and Resilience) Директива Президента США 12.02.2013)

КНР

Закон КНР «Закон о кибербезоасности» (Cyber Security Law) 1 июня 2017 г.

Индия

«Закон об информационных технологиях» Индии (Information Technology Act 2008)

Российская Федерация

Отношения в области участия государства в оперативном управлении сетями связи общего пользования в целях минимизации последствий атак на КИИ в основном урегулированы законодательством в области связи. Предусмотрено, что такое управление со стороны федерального органа исполнительной власти в области связи может осуществляться в чрезвычайных ситуациях во взаимодействии с центрами управления сетями связи специального назначения и имеющими присоединение к сетям связи общего пользования и технологическим сетям связи. Других случаев участия государства в оперативном управлении сетями связи общего пользования не предусмотрено.

http://internetinside.ru/problemy-pravovogo-obespecheniya-bezo/

Нормативно-правовая база Российской Федерации по безопасности критической информационной инфраструктуры

Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»

Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

Указ Президента РФ №569 от 25.11.2017 «О внесении изменений в Положение о ФСТЭК»

Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

Постановление Правительства РФ №808 от 11.07.2018 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК»

Приказ ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»

Приказ ФСТЭК России №229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»

Приказ ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»

Приказ ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»

Приказ ФСТЭК России №72 от 26.04.2018 «О внесении изменений в Регламент ФСТЭК»

Приказ ФСТЭК России №138 от 09.08.2018 «О внесении изменений в Требования к обеспечению ЗИ в АСУ П и ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК №31, и в Требования по обеспечению безопасности ЗО КИИ РФ, утвержденные приказом ФСТЭК №239»

Приказ ФСБ России №366 от 24.07.2018 «О НКЦКИ»

Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»

Приказ ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения

субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ»

Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Инфраструктура – приоритетный объект угроз

Примененный против Ирана вирус Stuxnet был создан для проникновения в АСУ атомной промышленности. Первоначально никто не брал на себя ответственность за создание и использование этого вируса, однако, не так давно американские официальные лица подтвердили, что он был создан в системе АНБ с участием израильских компаний для противодействия иранской атомной программе. Еще более сложная, многокомпонентная боевая программа была применена американцами и израильтянами против нефтяных терминалов и нефтеперерабатывающих заводов Ирана. Кроме того, были зафиксированы случаи использования компьютерных вирусов для вывода из строя систем SCADA крупнейшей саудовской нефтяной и катарской газовых компаний.

https://lenta.ru/news/2010/12/15/stuxnet/

Крупнейшая нефтедобывающая компания в мире, саудовская Saudi Aramco, восстановила работу своих основных компьютерных сетей после того, как вирус заразил около 30 000 компьютеров компании.

https://www.vedomosti.ru/business/articles/2012/08/27/saudi_aramco_postradala_ot_kompyuternoj_ataki

«Массовая атака на устройства Cisco, начавшаяся вечером 6 апреля 2018 года, была нацелена на значимые объекты критической информационной инфраструктуры (КИИ) РФ». Ранее Cisco зафиксировала атаки на свои свитчи, в которых хакеры использовали уязвимость в программе Cisco Smart Install Client. Это сетевое оборудование Cisco практически повсеместно используются в центрах обработки данных.

https://news2.ru/story/543425/

События

IV Ялтинская конференция «Транспортная безопасность в Российской Федерации»

http://tb-inform.ru/iv-yaltinskaya-konferentsiya-transportnaya-bezopasnost-v-rossijskoj-federatsii/

Ассоциация банков России запустила пилотный проект платформы обмена данными о киберугрозах на базе продуктов компании Bi.zone — технического провайдера сервиса

https://www.vestifinance.ru/articles/102798

Ростех и ФСБ подписали соглашение в сфере информационной безопасности

https://rostec.ru/news/rostekh-i-fsb-podpisali-soglashenie-v-sfere-informatsionnoy-bezopasnosti/

В Евросоюзе будут созданы силы быстрого реагирования сообщества на киберугрозы

https://tass.ru/mezhdunarodnaya-panorama/5320432

Опубликованы проекты приказов ФСБ о средствах обнаружения, предупреждения и ликвидации кибератак на критическую инфраструктуру

http://d-russia.ru/opublikovany-zakonoproekty-o-sredstvah-obnaruzheniya-preduprezhdeniya-i-likvidatsii-kiberatak-na-kriticheskuyu-infrastrukturu.html

Мнения

Актуальные киберугрозы. I квартал 2018 г.
https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q1/

Безопасность КИИ: что нас ждет в 2018 году. Краткий обзор о внедрении ФЗ по КИИ

https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/Webinar_284799.pdf

Избранные комментарии начальника управления ФСТЭК о том, как субъект КИИ сам определяет свои объекты и проводит границы

https://lukatsky.blogspot.com/2018/02/blog-post_9.html

Анализ рынка систем автоматизации в нефтегазовом комплексе: достигнутые результаты и перспективы роста

https://techart.ru/files/publications/neftegazovaya-vertikal-02-2018.pdf

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)
Подробнее: tadviser

Обзор мер по защите критической информационной инфраструктуры России
Подробнее: tadviser

Информационная безопасность в энергетике: мнения экспертов
https://securenews.ru/energy_facilities/

Информационная безопасность в электроэнергетике. Отраслевые нюансы
https://elvis.ru/upload/iblock/0f2/ib_energy.PDF