ЭКОНОМИКА Data Economy Russia 2024

МОНИТОРИНГ СМИ

13 ОКТЯБРЯ 2021

ДАЙДЖЕСТ

ПОВЕСТКА Д. Н. ЧЕРНЫШЕНКО

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

ЦИФРОВЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КАДРЫ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ

ЦИФРОВОЕ ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ

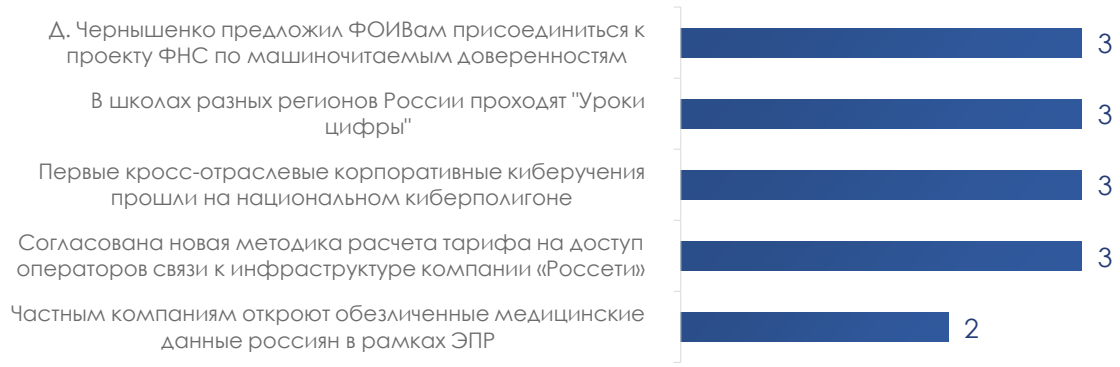
РЕГИОНАЛЬНАЯ ПОЛИТИКА

ПОЛНЫЕ ТЕКСТЫ СООБЩЕНИЙ

Цифровая экономика (АНО)

Подготовлено Пост Медиа
vaa@post-media.org
+7 905 5521660

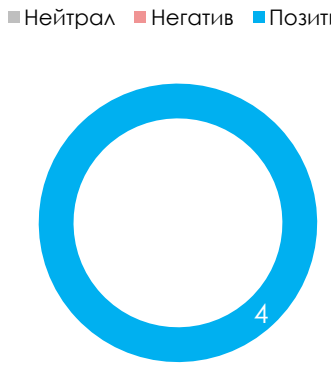
РЕЙТИНГ КЛЮЧЕВЫХ ИНФОПОВОДОВ



КОЛИЧЕСТВО ПУБЛИКАЦИЙ ПО РУБРИКАМ

ТОНАЛЬНОСТЬ ЗА СУТКИ

АНО «Цифровая экономика»



НП «Цифровая экономика»

ДАЙДЖЕСТЫ ПУБЛИКАЦИЙ

ПОВЕСТКА Д. Н. ЧЕРНЫШЕНКО

ТАСС, Москва, 12.10.2021

ЧЕРНЫШЕНКО ПРЕДЛОЖИЛ ФОИВАМ ПРИСОЕДИНИТЬСЯ К ПРОЕКТУ ФНС ПО МАШИНОЧИТАЕМЫМ ДОВЕРЕННОСТЯМ

Вице-премьер РФ **Дмитрий Чернышенко** рекомендовал ФОИВ присоединиться к проекту ФНС по машиночитаемым доверенностям на основе цифровой платформы распределенного реестра.

«*Бизнес в целях адаптации своих информационных систем ожидает от госсектора регулирования и создания инфраструктуры машиночитаемых доверенностей. Отмечу инициативу и опережающую работу в этом направлении Федеральной налоговой службы. Ими в короткие сроки был подготовлен и запущен пилотный проект по машиночитаемым доверенностям на основе цифровой платформы распределенного реестра. К пилоту присоединились операторы ЭДО, крупные банки и Федеральное казначейство. Считаю целесообразным ФОИВам изучить пилотный проект ФНС и присоединяться к его проведению для получения единой распределенной системы управления доверенностями и полномочиями*», - приводятся в сообщении слова **Чернышенко**.

Вице-премьер также назвал электронный документооборот инструментом снижения рисков и затрат бизнеса.

«*Электронный документооборот - инструмент снижения рисков и затрат бизнеса. В рамках рабочей группы при участии предпринимателей уже сейчас найдены решения по унификации подходов при разработке форматов электронных документов, определены правила общения в цифре между хозяйствующими субъектами. По последним исследованиям, крупные компании видят потребность в переводе на ЭДО, считая это крайне эффективным механизмом развития бизнеса и повышение производительности в целом*», - отметил **Чернышенко**.

https://tass.ru/ekonomika/12642987

НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

Tadviser.ru, Москва, 12.10.2021

БЕСПИЛОТНЫЙ ЛЕТАТЕЛЬНЫЙ АППАРАТ (ДРОН, БПЛА)

Правительство РФ утвердило концепцию интеграции беспилотников в единое воздушное пространство России. Председатель правительства Михаил Мишустин подписал соответствующее распоряжение. Концепция предусматривает поэтапную интеграцию беспилотников к 2030 г. Заместитель генерального директора, директор по направлению «Нормативное регулирование» **АНО «Цифровая экономика»** **Дмитрий Тер-Степанов** отмечает, что регулирование авиации - это очень чувствительная сфера, правовые барьеры в ней связаны с безопасностью полетов и защитой жизни и здоровья граждан.

ИКС (iksmedia.ru), Москва, 12.10.2021

МЕДИЦИНСКУЮ ИНФОРМАЦИЮ ГРАЖДАН СОБЕРУТ ДЛЯ АНАЛИЗА

Правительство РФ готовит регулирование, которое обеспечит возможность передачи обезличенных медицинских данных россиян компаниям, которые разрабатывают решения в области искусственного интеллекта. Для реализации проекта на три года будет установлен экспериментальный правовой режим, а оператором данных станет «Дата Матрикс». Закон об ЭПР позволяет тестировать инновации на определенной территории, обходя требования закона: тайну связи, врачебную тайну и др. «Наша задача сделать так, чтобы три года эксперимента были эффективными и безопасными для граждан, а также проверить заложенную в его основе правовую гипотезу», - пояснил директор направления «Нормативное регулирование» **АНО «Цифровая экономика» Дмитрий Тер-Степанов**.

Forbes.ru, Москва, 12.10.2021

ПРАВИТЕЛЬСТВО ДАСТ БИЗНЕСУ ДОСТУП К МЕДИЦИНСКИМ ДАННЫМ РОССИЯН ДЛЯ IT-РЕШЕНИЙ

Правительство готовит механизм, который обеспечит передачу обезличенных медицинских данных россиян частным компаниям, разрабатывающим решения в области искусственного интеллекта.

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

Экспертный центр электронного государства (d-russia.ru), Москва, 12.10.2021

ФАС СОГЛАСОВАЛА НОВУЮ МЕТОДИКУ РАСЧЕТА ТАРИФА НА ДОСТУП ОПЕРАТОРОВ СВЯЗИ К ИНФРАСТРУКТУРЕ КОМПАНИИ «РОССЕТИ»

Во всех дочерних обществах группы «Россети» с конца 2021 года будет применяться согласованная ФАС методика расчета стоимости услуг на размещение волоконно-оптических линий связи на объектах сетевого комплекса. Методика соответствует требованиям антимонопольного законодательства, учитывает дополнительные затраты на обслуживание и ремонт ЛЭП, на которых размещены ВОЛС, расходы на обеспечение целостности линий связи при переустройстве сетевой инфраструктуры

ТАСС, Москва, 12.10.2021

ЭКСПЕРТ: ДОСТУП ОПЕРАТОРОВ СВЯЗИ К ЛЭП ПОЗВОЛИТ УСКОРИТЬ РАЗВИТИЕ РЫНКА СВЯЗИ

Доступ телекоммуникационных компаний к линиям электропередачи для размещения на них волоконно-оптических кабелей, а также формирование группой «Россети» единой методики определения стоимости доступа позволят ускорить развитие рынка связи.

Аналогичные публикации
cnews.ru, 12.10.2021

Национальные проекты России (национальныепроекты.рф), Москва, 12.10.2021

РОССИЯНЕ ВЫБЕРУТ, КУДА ПРОВЕСТИ МОБИЛЬНУЮ СВЯЗЬ 4G

Россияне проголосуют на портале госуслуг за населенные пункты, которые подключат к высокоскоростному интернету в 2022 году. Специальный раздел с формой для голосования открылся на портале госуслуг.

Ura.ru (ura.news), Екатеринбург, 12.10.2021

ЖИТЕЛИ АЛТАЯ ИСПУГАЛИСЬ СМЕРТИ ПТИЦ ИЗ-ЗА ВЫШЕК 5G

Жители Республики Алтай в соцсетях испугались смерти около десятка птиц, которая попала на видео. Многие россияне связали гибель животных с вышками сотовой связи пятого поколения. Ранее министр цифрового развития, связи и массовых коммуникаций РФ **Максут Шадаев** заявил, что связь 5G не несет никакого вреда здоровью человека.

ЦИФРОВЫЕ ТЕХНОЛОГИИ

Российская газета, Москва, 13.10.2021

КОД БЕЗ СЕКРЕТА

Что такое «Университет открытого кода»? Как студенты вовлекаются в науку? Почему бизнес приходит в научные лаборатории? Об этом в интервью рассказывает первый проректор, руководитель программы развития Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО) Дарья Козлова.

РИА Новости, Москва, 12.10.2021

В СКОЛТЕХЕ СОЗДАДУТ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

На базе Сколтеха начнет работать исследовательский центр искусственного интеллекта. Основным направлением исследований станет создание технологий ИИ для оптимизации управленческих решений в целях снижения углеродного следа.

Парламентская газета (pnp.ru), Москва, 13.10.2021

СОЗДАТЕЛЯМ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПОМОГУТ ГРАНТАМИ

Проекты малых предприятий по разработке, применению и коммерциализации цифровых решений могут претендовать на получение грантов. Постановление Правительства, уточняющее условия и порядок их предоставления, вступает в силу 13 октября.

3DNews.ru, Москва, 12.10.2021

ПРИНЦИПЫ OPEN SOURCE - КЛЮЧ К СОЗДАНИЮ ВЫСОКОНКУРЕНТНОГО IT-РЫНКА

В Москве 1 октября прошел саммит Russia Open Source Summit, посвященный вопросам развития и внедрения Open Source технологий в России, а также теме снижения зависимости отечественного IT-рынка от зарубежных вендеров.

Национальные проекты России (национальныепроекты.рф), Москва, 12.10.2021

ГЛАВНЫЕ ЛАЙФХАКИ ОТ ПОБЕДИТЕЛЕЙ МЕЖДУНАРОДНОЙ ОЛИМПИАДЫ ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Технологии не стоят на месте и, к сожалению, вместе с ними развиваются и методы мошенничества. Сегодня преступники виртуозно пользуются знаниями по психологии и обманывают доверчивых граждан по телефону или электронной почте. О том, как не попасть на удочку мошенников, рассказали победители I Международной олимпиады по финансовой безопасности. Организаторы приурочили ее проведение к Году науки и технологий, а кроме того, мероприятие помогает достичь целей нацпроектов « Образование « и «**Цифровая экономика**».

Экспертный центр электронного государства (d-russia.ru), Москва, 12.10.2021

ПЕРВЫЕ КРОСС-ОТРАСЛЕВЫЕ КОРПОРАТИВНЫЕ КИБЕРУЧЕНИЯ ПРОШЛИ НА НАЦИОНАЛЬНОМ КИБЕРПОЛИГОНЕ

«Ростелеком-Солар» совместно с Корпоративным университетом TMK2U организовали для сотрудников Трубной металлургической компании и Группы «Синара» масштабные кросс-отраслевые корпоративные учения на Национальном киберполигоне, сообщает «Ростелеком» во вторник. Это первые в России киберучения, охватывающие отработку всех ключевых процессов служб информационной безопасности - от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак, говорится в сообщении.

Rspectr.com, Москва, 12.10.2021

ПОДВЕДЕНЫ ИТОГИ КОРПОРАТИВНЫХ КИБЕРУЧЕНИЙ В ПРОМЫШЛЕННОСТИ

Среди сотрудников Трубной Металлургической Компании и Группы Синара прошли кросс-отраслевые корпоративные учения на Национальном киберполигоне. Мероприятие охватило отработку всех ключевых процессов служб информбезопасности - от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак. Учения организовали «Ростелеком-Солар» совместно с Корпоративным университетом TMK2U, сообщила пресс-служба «Ростелеком».

Tadviser.ru, Москва, 12.10.2021

КИБЕРПОЛИГОН РОССИИ ДЛЯ ОБУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания «Ростелеком-Солар» совместно с Корпоративным университетом TMK2U организовали для сотрудников Трубной Металлургической Компании и Группы Синара масштабные кросс-отраслевые корпоративные учения на Национальном киберполигоне. Это киберучения, охватывающие отработку всех ключевых процессов служб информационной безопасности - от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак.

КАДРЫ ДЛЯ ЦИФРОВОЙ ЭКОНОМИКИ

Российская газета, Москва, 13.10.2021

КАК ТРАТИТЬ И КОПИТЬ

Школьники из Ингушетии научились копить родительские деньги на карманные расходы с помощью уроков финансовой и цифровой грамотности. На будущем уроке цифры ингушский учитель расскажет ребятам о применении искусственного интеллекта в сфере медицины. Уроки цифры по искусственному интеллекту и машинному обучению проходят по всей стране в рамках образовательного проекта **АНО «Цифровая экономика»**, Минцифры и Минпросвещения России. Стратегический партнер и разработчик - благотворительный фонд Сбербанка «Вклад в будущее».

ТАСС, Москва, 12.10.2021

ДЛЯ ПРИМОРСКИХ ШКОЛЬНИКОВ С НАЧАЛА ГОДА ПРОВЕЛИ ПОЧТИ 180 «УРОКОВ ЦИФРЫ»

Почти 180 «уроков цифры» провели для более чем 30 тыс. приморских школьников с начала года в рамках нацпроекта «**Цифровая экономика**».

Российское образование (edu.ru), Москва, 12.10.2021

СТУДЕНТЫ АЛТАЙСКОГО ПЕДУНИВЕРСИТЕТА ПРОВЕЛИ «УРОК ЦИФРЫ» В СЕМИ ШКОЛАХ РЕГИОНА

Студенты Алтайского государственного педагогического университета провели «Урок цифры» в семи школах региона.

ЦИФРОВОЕ ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ

ТАСС, Москва, 12.10.2021

МИНИСТРЫ ЮСТИЦИИ РФ И САУДОВСКОЙ АРАВИИ ПОДПИСАЛИ В МОСКВЕ МЕМОРАНДУМ О СОТРУДНИЧЕСТВЕ

Главы министерств юстиции России и Саудовской Аравии подписали в Москве меморандум о взаимопонимании и сотрудничестве между Министерством юстиции Российской Федерации и Министерством юстиции Королевства Саудовская Аравия. Глава российского Минюста Константин Чуйченко подчеркнул особую важность сотрудничества в сфере цифровизации государственных услуг органов юстиции.

ТАСС, Москва, 12.10.2021

ЧЕРНЫШЕНКО ПРЕДЛОЖИЛ ФОИВАМ ПРИСОЕДИНИТЬСЯ К ПРОЕКТУ ФНС ПО МАШИНОЧИТАЕМЫМ ДОВЕРЕННОСТЯМ

Вице-премьер РФ **Дмитрий Чернышенко** рекомендовал федеральным органам исполнительной власти присоединиться к проекту Федеральной налоговой службы по машиночитаемым доверенностям на основе цифровой платформы распределенного реестра.

Российская газета (rg.ru), Москва, 12.10.2021

ЧЕРНЫШЕНКО РАССКАЗАЛ О ПРЕИМУЩЕСТВАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ДЛЯ БИЗНЕСА

Развитие электронного документооборота, которое является одной из 42 стратегических инициатив правительства, позволит снизить риски и затраты бизнеса. Об этом заявил вице-премьер **Дмитрий Чернышенко** во время заседания межведомственной рабочей группы.

Парламентская газета (pnp.ru), Москва, 12.10.2021

ГРАЖДАНЕ ПОЛУЧАТ ВОЗМОЖНОСТЬ ДЕЛАТЬ КОМПЛЕКСНЫЙ ЗАПРОС В ПФР

Пенсионный Фонд России разработал проект постановления, устанавливающий форму и порядок комплексного запроса гражданина, а также перечень госуслуг, предоставляемых на его основании.

Российская газета (rg.ru), Москва, 12.10.2021

РОСТРУД ПЛАНИРУЕТ РАЗВИВАТЬ ДИСТАНЦИОННЫЙ НАДЗОР

Трудовые инспекторы будут проверять работодателей в том числе - дистанционно. Об этом рассказал руководитель Роструда Михаил Иванков. Роль дистанционного надзора возрастает в условиях цифровизации, подчеркнул замминистра цифрового развития **Максим Паршин**. По его словам, рынок трудовых отношений изменился. Так, стало возможным дистанционное заключение трудового договора, когда работодатель и работник не встречаются, но при этом между ними возникают трудовые отношения.

Вести.ru, Москва, 12.10.2021

НАЦПРОЕКТ «ЦИФРОВАЯ ЭКОНОМИКА». «ГОСУСЛУГИ. АВТО». НОВОЕ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ. УТРО РОССИИ

Пользователи платформы «Госуслуги Авто» получили доступ к новым сервисам - «делегирование» и «история автомобиля». Само приложение было запущено в пилотном режиме в сентябре в рамках нацпроекта «**Цифровая экономика**». И за первые несколько дней стало лидером по количеству скачиваний.

РЕГИОНАЛЬНАЯ ПОЛИТИКА

ТАСС, Москва, 12.10.2021

«РОСТЕЛЕКОМ» ЗАВЕРШИЛ ПОДКЛЮЧЕНИЕ СВЕРДЛОВСКИХ СОЦИАЛЬНЫХ ОБЪЕКТОВ ПО НАЦПРОЕКТУ

«Ростелеком» завершил подключение образовательных, медицинских и других социальных учреждений в Свердловской области по нацпроекту «**Цифровая экономика**». Всего с 2019 года подключен 1 641 объект.

Ura.ru (ura.news), Екатеринбург, 12.10.2021

В СВЕРДЛОВСКОЙ ОБЛАСТИ ЗАВЕРШИЛИ ГЛОБАЛЬНЫЙ ПРОЕКТ ДЛЯ ШКОЛ

В Свердловской области завершили проект по подключению к интернету социально-значимых учреждений в отдаленных районах региона.

Ura.ru (ura.news), Екатеринбург, 12.10.2021

В СВЕРДЛОВСКОЙ ОБЛАСТИ МЕНЯЮТ КОЛИЧЕСТВО СЕЛ, КУДА ПРОВЕДУТ СВЯЗЬ

В Свердловской области увеличат число населенных пунктов, которым будут проведены сотовая связь и интернет. Об этом объявил новый министр цифрового развития Свердловской области Михаил Пономарьков на пресс-конференции посвященной проекту устранения цифрового неравенства в регионе.

Комсомольская правда (tula.kp.ru), Тула, 12.10.2021

«ПМП «ПРОТОН» - ОСВАИВАЯ НОВЫЕ ГОРИЗОНТЫ

Интервью с Александром Болдиным, генеральным директором ООО «ПМП «ПРОТОН» о производстве и поставке медицинского оборудования для диагностики. По результатам рейтинга цифровой трансформации регионов, который ежемесячно проводит Минцифры РФ в рамках нацпроекта «**Цифровая экономика**», Тульская область заняла второе место.

Ura.ru (ura.news), Екатеринбург, 12.10.2021

ПРОЕКТ О ПРОБЛЕМЕ ХМАО ПОБЕДИЛ НА КРУПНОМ КОНКУРСЕ УРФО

Порядка 23 тысяч жителей ХМАО не имеют возможности круглогодично добраться до крупных городов региона. Команда, выступившая на Уральском хакатоне с данной проблемой, стала победителем конкурса. Об этом рассказал один из участников победившей команды Евгений Шилинг.

Комсомольская правда (krsk.kp.ru), Красноярск, 12.10.2021

КРАСНОЯРЦЫ ОТПРАВЛЯЮТСЯ НА МАРС: БУМАЖНЫХ КВИТАНЦИЙ БОЛЬШЕ НЕ БУДЕТ!

Бумажные квитанции совсем скоро станут историей и уйдут из жизни людей. Переход на электронный документооборот - дело ближайшего будущего, на которое работает Национальная **программа «Цифровая экономика Российской Федерации»**. Электронная квитанция - это такой же законный документ, как и бумажная, только удобнее и надежнее. В этом уже убедились более 100 000 абонентов Красноярскэнергосбыта.

ПОЛНОТЕКСТЫ ПУБЛИКАЦИЙ

Tadviser.ru, Москва, 12.10.2021

БЕСПИЛОТНЫЙ ЛЕТАТЕЛЬНЫЙ АППАРАТ (ДРОН, БПЛА)

Беспилотники интегрируют в воздушное пространство России

Правительство РФ утвердило концепцию интеграции беспилотников в единое воздушное пространство России. Председатель правительства Михаил Мишустин подписал соответствующее распоряжение. Концепция предусматривает поэтапную интеграцию беспилотников к 2030 г. Об этом стало известно 11 октября 2021 года.

До 2023 г. продлится организационный период, во время которого будут разработаны меры по упрощению процедур и снятию ограничений для полетов беспилотных воздушных судов (БВС). Также на этом этапе будут внедрены специальные сервисы для электронной регистрации и учета БВС, установлены правила подготовки и выполнения таких полетов.

На втором этапе - до 2027 г. - предусматривается разработка и внедрение технологий для обеспечения безопасности полетов БВС, создание необходимой инфраструктуры связи, систем навигации и наблюдения. Параллельно будет идти законодательная работа. Например, будут утверждены технические требования к системам и оборудованию, которые будут обеспечивать безопасность полетов, принят порядок использования воздушного пространства при совместных полетах беспилотных и пилотных судов. На этом же этапе начнутся их пробные полеты в едином воздушном пространстве.

На третьем этапе - до 2030 г. - планируется завершить создание технической инфраструктуры для обеспечения безопасности полетов БВС, внедрить цифровые технологии в части управления полетами беспилотных и пилотируемых воздушных судов в едином пространстве, принять нормативно-правовые акты, которые будут регулировать эту сферу.

Заместитель руководителя законодательной рабочей группы Национальной технологической инициативы (НТИ) «Аэронет» Андрей Шнырев считает, что концепция чрезвычайно важна.

Он полагает, что в ходе реализации концепции можно увидеть, какие изменения стоит в документ внести.

Эксперт считает: есть вероятность, что заложенная концепция будет исполнена раньше времени.

Вице-президент, исполнительный директор кластера передовых производственных технологий фонда «Сколково» Алексей Беляков также считает, что концепция абсолютно необходима поскольку для открытия рынка услуг с использованием беспилотных летательных аппаратов (БПЛА) нужна координация разного рода участников - прежде всего заказчиков этих услуг, эксплуатантов, производителей дронов и регуляторов.

По мнению Алексея Белякова, в концепции учтены все особенности развития отрасли.

Заместитель генерального директора, директор по направлению «Нормативное регулирование» **АНО «Цифровая экономика»** **Дмитрий Тер-Степанов** отмечает, что регулирование авиации - это очень чувствительная сфера, правовые барьеры в ней связаны с безопасностью полетов и защитой жизни и здоровья граждан.

https://www.tadviser.ru/a/341580

К аннотации

ИКС (iksmedia.ru), Москва, 12.10.2021

МЕДИЦИНСКУЮ ИНФОРМАЦИЮ ГРАЖДАН СОБЕРУТ ДЛЯ АНАЛИЗА

Правительство РФ готовит регулирование, которое обеспечит возможность передачи обезличенных медицинских данных россиян компаниям, которые разрабатывают решения в области искусственного интеллекта (ИИ).

Как пишет «КоммерсантЪ» со ссылкой на собственные источники, для реализации проекта на три года будет установлен экспериментальный правовой режим (ЭПР), а оператором данных станет «Дата Матрикс». Из проекта постановления об ЭПР (есть у «Ъ») следует, что компания подготовит аналитические отчеты, которые могут быть использованы в «хозяйственных или научно-исследовательских целях», в частности «для анализа фармакоэкономики».

В «Дата Матрикс» подтвердили, что проект «на финальной стадии рассмотрения в Минэкономики». В министерстве сообщили, что ЭПР предполагает обработку «больших» медицинских данных в обезличенном виде с соблюдением мер «по исключению рисков их утечки». Поставлять данные будут национальные медицинские исследовательские центры, онкологические больницы и прочие учреждения медицинского профиля. В Минцифры уточнили, что «вопрос определения операторов данных, их прав и обязанностей прорабатывается». В Минздраве «Ъ» также говорят, что «определение операторов находится в стадии проработки».

Закон об ЭПР, или так называемых регуляторных песочницах, Владимир Путин подписал в июле 2020 года. Он позволяет тестировать инновации на определенной территории, обходя требования закона: тайну связи, врачебную тайну и др. «Наша задача сделать так, чтобы три года эксперимента были эффективными и безопасными для граждан, а также проверить заложенную в его основе правовую гипотезу», - пояснил директор направления «Нормативное регулирование» **АНО «Цифровая экономика» Дмитрий Тер-Степанов** (организация занималась нормативно-правовой стороной проекта).

ЭПР в части сбора обезличенных медицинских данных установят по всей России, они будут использоваться для исследований, отмечает юрист практики здравоохранения и технологий BGP Litigation Иван Зарайский.

Результаты, по его мнению, интересны фармацевтическим и страховым компаниям, госорганам. «Это позволит повысить эффективность назначений препаратов, а госорганы смогут совершенствовать клинические рекомендации, которые применяются при обучении врачей», - добавили в «Дата Матрикс».

О планах властей передавать обезличенные медданные россиян IT-компаниям стало известно весной (см. «Ъ» от 16 марта). Государственные медучреждения будут передавать информацию из медкарт пациентов в отдельный репозиторий, доступ к ним получат компании, разрабатывающие решения в области медтеха.

Существует два метода обезличивания данных: когда персональная информация полностью удаляется и когда она скрывается под нечитаемыми символами, поясняет руководитель отдела аналитики «СерчИнформ» Алексей Парфентьев. По его мнению, первый метод позволяет исследователям получить информацию, но при этом нет возможности связать конкретную строку с человеком. Второй метод менее надежный, поскольку оператор может заменять символы частично.

Даже при удалении ФИО и прочих личных данных сохраняется достаточно уникального для больного контекста (анамнез, анализы и т. п.), чтобы при желании восстановить личность, поэтому обезличивание почти всегда обратимо, считает президент ГК InfoWatch Наталья Касперская.

Нельзя допустить, чтобы медучреждения приводили данные к определенному формату вручную, подчеркивает исполнительный директор Artezio Павел Адылин, это может грозить утечкой информации о пациентах и ее искажением.

https://www.iksmedia.ru/news/5856168-Medicinskuyu-informaciyu-grazhdan.html

К аннотации

Forbes.ru, Москва, 12.10.2021

ПРАВИТЕЛЬСТВО ДАСТ БИЗНЕСУ ДОСТУП К МЕДИЦИНСКИМ ДАННЫМ РОССИЯН ДЛЯ IT-РЕШЕНИЙ

Автор: Злобин Андрей

Правительство подготовит механизм, который позволит бизнесу, разрабатывающему решения в области искусственного интеллекта, получать обезличенные медицинские данные россиян. Эксперты отмечают, что методы обезличивания пока недостаточно совершенны

Правительство готовит механизм, который обеспечит передачу обезличенных медицинских данных россиян частным компаниям, разрабатывающим решения в области искусственного интеллекта, рассказали источники «Коммерсанта».

Для реализации проекта будет установлен экспериментальный правовой режим (ЭПР) сроком на три года. Оператором данных станет компания «Дата Матрикс». Проект постановления об ЭПР, с которым ознакомилось издание, позволяет ей создать национальный банк биомедицинских данных и готовить на их основе отчеты для использования, в том числе «для анализа фармакоэкономики».

По данным СПАРК, ООО «Дата Матрикс» учреждено в 2011 году в Петербурге, занимается разработкой IT-решений в области медицины. Выручка по итогам 2020 года составила 36,5 млн рублей, убыток - 21 млн рублей.

Компания подтвердила изданию, что проект находится «на финальной стадии рассмотрения в Минэкономики». Представитель министерства заверил, что ЭПР предполагает обработку «больших» медицинских данных в обезличенном виде с соблюдением мер «по исключению рисков их утечки». Данные будут поставляться в национальные медицинские исследовательские центры, онкологические больницы и прочие учреждения медицинского профиля. В Минцифры и Минздраве изданию сообщили, что вопрос определения операторов и их обязанностей прорабатывается.

Президент Владимир Путин подписал закон об ЭПР в июле 2020 года. Он позволяет тестировать инновации на определенных территориях, обходя в том числе требования о врачебной тайне. По словам юриста практики здравоохранения и технологий BGP Litigation Ивана Зарайского, полученные данные интересны фармацевтическим и страховым компаниям, а также госорганам. «Это позволит повысить эффективность назначений препаратов, а госорганы смогут совершенствовать клинические рекомендации, которые применяются при обучении врачей», - сообщила «Дата Матрикс».

Глава отдела аналитики «СерчИнформ» Алексей Парфентьев рассказал изданию, что один из методов обезличивания данных - полное удаление персональных данных - позволяет исследователям получить информацию, не давая им возможности связать конкретную строку с человеком. Президент ГК InfoWatch Наталья Касперская отметила, что даже при удалении ФИО и других личных данных сохраняется достаточное количество уникального для пациента контекста, который при желании позволяет восстановить его личность. Обезличивание почти всегда обратимо, предупредила она

https://www.forbes.ru/tekhnologii/442643-pravitel-stvo-dast-biznesu-dostup-k-medicinskim-dannym-rossian-dla-it-resenij

К аннотации

Российская газета, Москва, 13.10.2021

КАК ТРАТИТЬ И КОПИТЬ

Автор: Ларина Алена

Школьники из Ингушетии научились копить родительские деньги на карманные расходы с помощью уроков финансовой и цифровой грамотности.

В школе № 1 самого молодого города страны Сунжи их проводит учитель Зухра Хасиева. Она сама активно пользуется современными цифровыми технологиями. Один из уроков Зухры Хасиевой был о пользовании банковскими онлайн-услугами для учащихся десятых и одиннадцатых классов. Ранее учитель показала ребятам, как составить план личных расходов на неделю. Например, чтобы накопить на роликовые коньки или самокат.

«Родители дают мне по тысяче рублей в неделю, раньше я тратила все за три-четыре дня, - рассказала восьмиклассница Залина Евлоева. - На занятиях научилась планировать недельный бюджет. К следующему понедельнику у меня начал появляться остаток 300 - 400 рублей. За несколько месяцев накопила около пяти тысяч». Девочка начала хранить накопленные деньги на банковской карте. И здесь как нельзя кстати пригодился урок на тему цифровизации в банковской сфере.

Чтобы подготовиться к такому уроку, Зухра проконсультировалась в крупном банке и подготовила слайды. Кроме того, на занятие пригласили сотрудника финансового учреждения, который также выступил перед детьми.

А вот на будущем уроке цифры ингушский учитель расскажет ребятам о применении искусственного интеллекта в сфере медицины. «В нашей школе около 40 процентов детей хотят стать врачами, - объяснила свой выбор Зухра Хасиева. Надеюсь, такое занятие поможет им в выборе профессии». И поможет в жизни.

Справка «РГ»

Уроки цифры по искусственному интеллекту и машинному обучению проходят по всей стране в рамках образовательного проекта **АНО «Цифровая экономика»**, Минцифры и Минпросвещения России. Стратегический партнер и разработчик - благотворительный фонд Сбербанка «Вклад в будущее».

Знания, полученные на уроках финансовой грамотности, ученица школы № 1 города Сунжи применила на практике. И за месяц скопила пять тысяч. Фото ЕЛЕНА ОНЕГИНА

https://rg.ru/2021/10/12/kak-lgotnye-kredity-novye-znaniia-i-peremeny-v-cehah-meniaiut-zhizn.html

К аннотации

Парламентская газета (pnp.ru), Москва, 13.10.2021

СОЗДАТЕЛЯМ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПОМОГУТ ГРАНТАМИ

Автор: Литвинов Дмитрий

Проекты малых предприятий по разработке, применению и коммерциализации цифровых решений могут претендовать на получение грантов. Постановление Правительства, уточняющее условия и порядок их предоставления, вступает в силу 13 октября.

Правила предоставления средств из федерального бюджета на поддержку внедрения цифровых технологий кабмин утвердил в 2019 году. Грантами можно покрыть часть расходов на разработку и внедрение цифровых платформ и технологий для них, развитие информационной инфраструктуры, а также расходы на разработку, применение и коммерциализацию «сквозных» цифровых технологий. К последним относятся компоненты робототехники и сенсорика, нейротехнологии и искусственный интеллект, системы распределенного реестра, квантовые технологии и другие.

Гранты предоставляются на основании конкурса, который проводит Фонд содействия развитию малых форм предприятий в научно-технической сфере. Согласно новому постановлению кабмина, не менее чем за месяц до истечения срока подачи заявок на гранты Фонд должен разместить на своем официальном сайте объявление о проведении конкурсного отбора и положение о конкурсе. Установлено, что форма договора о предоставлении гранта разрабатывается на основе типовой формы, утвержденной Минфином. Договор подписывается усиленной квалифицированной электронной подписью в автоматизированной системе в электронной форме.

Согласно нацпроекту «**Цифровая экономика**», к 2022 году поддержку должны получить не менее 60 проектов по преобразованию приоритетных отраслей экономики и соцсферы и увеличению экспорта высокотехнологичной продукции, созданной с использованием «сквозных» цифровых технологий.

https://www.pnp.ru/economics/sozdatelyam-cifrovykh-tekhnologiy-pomogut-grantami.html

К аннотации

Ura.ru (ura.news), Екатеринбург, 12.10.2021

ПРОЕКТ О ПРОБЛЕМЕ ХМАО ПОБЕДИЛ НА КРУПНОМ КОНКУРСЕ УРФО

Автор: Мелещенков Илья

Порядка 23 тысяч жителей ХМАО не имеют возможности круглогодично добраться до крупных городов региона. Команда, выступившая на Уральском хакатоне с данной проблемой, стала победителем конкурса. Об этом URA.RU рассказал один из участников победившей команды Евгений Шилинг.

«Мы собрали данные и выяснили, что существует такая проблема. В некоторых районах, например, Ханты-Мансийском районе, порядка 40% населения отрезано от крупных городов. Они не могут добраться туда круглогодично. Мы считали тот или иной населенный пункт изолированным, если в нем отсутствовало круглогодичное дорожное сообщение», - сказал Шилинг.

Согласно данным, которые собрала команда, больше 40% населения Ханты-Мансийского района не имеют возможности круглогодично выехать из населенного пункта. На втором месте находится Березовский район - 34%. Такая же проблема существует в Октябрьском, Кондинском, Белоярском и Нижневартовском районах. Всего в ХМАО порядка 23 тысяч жителей труднодоступных поселений отрезаны от крупных городов региона. Конкурс Хакатон реализован в рамках национальной **программы «Цифровая экономика»**.

https://ura.news/news/1052510518

К аннотации

ТАСС, Москва, 12.10.2021

МИНИСТРЫ ЮСТИЦИИ РФ И САУДОВСКОЙ АРАВИИ ПОДПИСАЛИ В МОСКВЕ МЕМОРАНДУМ О СОТРУДНИЧЕСТВЕ

На встрече особо подчеркивалась необходимость выработки новых правовых механизмов защиты прав граждан и безопасности государства

МОСКВА, 12 октября. /ТАСС/. Главы министерств юстиции России и Саудовской Аравии подписали в Москве меморандум о взаимопонимании и сотрудничестве между Министерством юстиции Российской Федерации и Министерством юстиции Королевства Саудовская Аравия. Как сообщили журналистам в российском Минюсте, в ходе встречи с министром юстиции, председателем Высшего судебного совета Королевства Саудовская Аравия Валидом бен Мухаммедом ас-Самаани, прошедшей в Доме приемов МИД России, глава российского Минюста Константин Чуйченко подчеркнул особую важность сотрудничества в сфере цифровизации государственных услуг органов юстиции.

«Как и программа «Сауди вижн - 2030» в Королевстве Саудовская Аравия, так и национальная **программа «Цифровая экономика»** в Российской Федерации предусматривают цифровизацию государственных услуг для того, чтобы сделать их более доступными для граждан», - отметил он.

На встрече особо подчеркивалась необходимость выработки новых правовых механизмов защиты прав граждан и безопасности государства, в связи с чем сотрудничество в сфере правового регулирования информационной безопасности будет представлять интерес для обеих сторон.

Глава Минюста России также предложил приступить к подготовке программы сотрудничества органов юстиции Королевства Саудовская Аравия и Российской Федерации на 2022-2023 годы, которая станет первым шагом в реализации положений меморандума.

https://tass.ru/ekonomika/12643919

К аннотации

ТАСС, Москва, 12.10.2021

«РОСТЕЛЕКОМ» ЗАВЕРШИЛ ПОДКЛЮЧЕНИЕ СВЕРДЛОВСКИХ СОЦИАЛЬНЫХ ОБЪЕКТОВ ПО НАЦПРОЕКТУ

Всего за три года в регионе был подключен 1 641 объект, среди них школы, фельдшерские пункты, пожарные части и участковые пункты полиции

ЕКАТЕРИНБУРГ, 12 октября. /ТАСС/. «Ростелеком» завершил подключение образовательных, медицинских и других социальных учреждений в Свердловской области по нацпроекту «**Цифровая экономика**». Всего с 2019 года подключен 1 641 объект, сообщил министр цифрового развития и связи региона Михаил Пономарьков в Уральском региональном информационном центре ТАСС во вторник.

«Это важный проект, который в условиях распространения коронавирусной инфекции стал еще более актуальным. Всего за время действия проекта подключен 1 641 объект», - сказал министр.

По словам директора екатеринбургского филиала ПАО «Ростелеком» Ивана Пичугина, подключено 696 образовательных учреждений, 466 фельдшерских пунктов, 209 пожарных частей и постов, 25 объектов - участковые пункты полиции и объекты вневедомственной охраны, 170 территориальных администраций, 75 библиотек. «Это глобальный проект. Мы его завершили, и я

хочу сказать, что в рамках цифровой жизни региона - это самый масштабный проект, который когда-либо осуществлялся», - отметил он.

Директор филиала также добавил, что в этом году завершается проект по устранению цифрового неравенства (УЦН). «Нашей компанией были установлены точки доступа в 214 населенных пунктах, 64 городских округах, благодаря чему доступ в интернет получили около 135 тыс. человек. Кроме того, мы также получили дополнительное задание - восемь точек доступа на четвертый квартал [2021 года], и в целом проект УЦН до конца года завершаем», - сказал Пичугин.

В августе началась реализация проект УЦН 2.0, нововведениями которого стало то, что теперь устанавливаются не точки доступа, а базовые станции. При этом вышки будут появляться в селах и деревнях, в которых живет от 100 человек, тогда как в первый проект попадали населенные пункты от 250 до 500 человек.

Национальный проект «Цифровая экономика РФ» рассчитан до 2024 года. Его основные цели - сделать интернет доступным для всех, обеспечить связью 5G крупнейшие города, повысить эффективность основных отраслей экономики за счет внедрения новых технологий. Общий объем финансирования нацпроекта - свыше 1,5 трлн рублей.

https://tass.ru/nacionalnye-proekty/12642629

К аннотации

Ura.ru (ura.news), Екатеринбург, 12.10.2021

В СВЕРДЛОВСКОЙ ОБЛАСТИ МЕНЯЮТ КОЛИЧЕСТВО СЕЛ, КУДА ПРОВЕДУТ СВЯЗЬ

Автор: Шабалина Анна

В Свердловской области увеличат число населенных пунктов, которым будут проведены сотовая связь и интернет. Об этом объявил новый министр цифрового развития Свердловской области Михаил Пономарьков на пресс-конференции посвященной проекту устранения цифрового неравенства в регионе.

«В прошлом году был дан старт продолжению проекта устранения цифрового неравенства, но требования изменились. На сегодняшний день для участия в этом проекте доступны населенные пункты с численностью жителей от 100 до 500 человек» - рассказал Пономарьков.

Данный проект действует на территории региона с 2014 года. Ранее в программе могли принять участие только села с численностью жителей от 250 человек. Но в 2020 году требования изменились, в результате чего порог был понижен. До 2030 года планируется подключить к связи и сети интернет 561 населенный пункт по всей области.

Ранее сообщалось, каким образом можно будет выбрать населенный пункт, кому в следующем году проведут высокоскоростной интернет. Программа устранения цифрового неравенства реализуется Минцифры России и компанией ПАО «Ростелеком» в рамках национальной **программы «Цифровая экономика»**.

https://ura.news/news/1052510506

К аннотации

Tadviser.ru, Москва, 12.10.2021

КИБЕРПОЛИГОН РОССИИ ДЛЯ ОБУЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТМК и Группа «Синара» провели первые кросс-отраслевые корпоративные киберучения в промышленности на Национальном киберполигоне

«Ростелеком-Солар» 12 октября 2021 года сообщила о том, что совместно с Корпоративным университетом TMK2U организовали для сотрудников Трубной Металлургической Компании (ТМК) и Группы Синара масштабные кросс-отраслевые корпоративные учения на Национальном киберполигоне. Это киберучения, охватывающие отработку всех ключевых процессов служб информационной безопасности - от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак.

Безопасность промышленных предприятий - тема, значимость которой остается недооцененной. Ее сложность связана с необходимостью очень специфических компетенций от защитников, будь то внутренний ИБ-департамент или сервис-провайдер, особенностями функционирования технологических сегментов и одновременно - максимально недопустимыми рисками от успешной хакерской атаки. Поэтому мы очень рады тому, что ТМК и Группа Синара так тщательно прорабатывают вопросы киберустойчивости предприятия, используя максимум инструментов для ее проверки и повышения, - отметил вице-президент «Ростелекома» по информационной безопасности Игорь Ляпунов.

Киберучения - это отличная возможность объективно оценить уровень своих компетенций и отработать практические навыки реагирования на инциденты информационной безопасности, а формат соревнования привнес в них элемент азарта. Важно, что в ходе мероприятия отрабатывались сценарии, близкие к жизни, релевантные именно для промышленных предприятий. Подобный формат используется впервые в металлургической отрасли. Результаты учений подтвердили высокий профессионализм нашей команды кибербезопасности, - подчеркнул директор по информационным технологиям ТМК Дмитрий Якоб.

В первый день киберучений команды должны были провести максимально полную инвентаризацию инфраструктуры, специально созданной на базе промышленного сегмента киберполигона. Затем им необходимо было выполнить поиск уязвимостей в ней и настроить источники событий в SIEM-системе. На данном этапе оценивались полнота и точность данных от каждой команды.

Во второй день команды противостояли целенаправленным атакам, и на этом этапе ключевым показателем стала скорость обнаружения инцидента и реагирования на него. По итогам каждой атаки команды предоставляли отчеты с описанием как цепочки шагов злоумышленника, так и мер, необходимых для того, чтобы избежать повторения инцидента.

В заключительный день киберучений были подведены общие итоги, а также проведен подробный разбор сценариев учебных кибератак и действий команд.

Киберучения электроэнергетической отрасли

Под эгидой Минэнерго России на Национальном киберполигоне «Ростелекома» прошли киберучения, в которых приняли участие ключевые игроки электроэнергетической отрасли, представители силовых ведомств, регуляторов и госорганов. Об этом 25 июня 2021 года сообщила компания «Ростелеком-Солар».

Цель киберучений - повысить практическую готовность организаций сферы ТЭК к отражению комплексных распределенных компьютерных атак на целую отрасль, включая уровень взаимодействия и скорость реагирования.

Важно понимать, что не со всеми вызовами, с которыми мы сталкиваемся, нужно бороться. Некоторые из них, наоборот, подталкивают нас к развитию. Бурное развитие цифровых технологий, в том числе в энергетике, создает стимулы и возможности для развития энергетического сектора, при этом одновременно является вызовом энергетической безопасности России. И нам необходимо создать такие условия, чтобы при цифровой трансформации отраслей ТЭК этот вызов не перерос в угрозу, способную нанести серьезный ущерб экономике страны, - пояснил директор Департамента экономической безопасности в ТЭК Антон Семейкин.

Киберучения включали практическую и штабную часть. Практическая часть проводилась на Национальном киберполигоне, созданном компанией «Ростелеком» на базе ресурсов дочерней структуры «Ростелеком-Солар». В учениях на киберполигоне приняли участие ключевые компании электроэнергетики России, включая АО «ЕвроСибЭнерго», ПАО «Интер РАО», ПАО «Россети», ПАО «РусГидро», АО «Сетевая компания», АО «СО ЕЭС», ПАО «Фортум», а также представители иных субъектов критической информационной инфраструктуры энергетической отрасли.

Системные тренировки по отражению кибератак на субъекты КИИ позволят существенно повысить киберустойчивость страны в целом, и мы стремимся этому способствовать. С начала 2021 года мы провели уже 25 киберучений, в которых приняли участие более 300 специалистов по информационной безопасности. Это также наглядное подтверждение потребности рынка в таких мероприятиях и необходимости создания сегментов киберполигона для других отраслей, - подчеркнул заместитель генерального директора компании «Ростелеком-Солар» Александр Чечин.

Согласно сценарию учений, с целью дестабилизации социально-экономической обстановки хакерская группировка производила серию скоординированных компьютерных атак на инфраструктуру энергоснабжения вымышленного региона. Электросети региона были разделены на семь районов, за защиту каждого из которых отвечала отдельная команда. Все сценарии атак были разработаны экспертами «Ростелеком-Солар» специально для данных учений и основывались на реальных кейсах атак на компании электроэнергетической отрасли. Задачей команд было выявить атаки на ИТ-инфраструктуру региона и сохранить наблюдаемость и управляемость районов электросетей в зоне ответственности.

Параллельно командам работал отраслевой координационный центр, в который вошли представители НКЦКИ и Минэнерго России, а также специалисты «Ростелекома», обладающие навыками реагирования на компьютерные атаки с учетом отраслевой специфики. Координационный центр проводил анализ информации об инцидентах, поступавшей от команд, и информировал участников об угрозах, а также рекомендуемых мерах по противодействию и ликвидации инцидентов.

В ходе штабной части учений участники рассмотрели последствия реализации атак, с которыми сталкивались команды, оценили достаточность типовых планов по ликвидации чрезвычайной ситуации в условиях веерного отключения подстанций региона, а также выработали первоочередные меры по локализации последствий кибератак и недопущению их в будущем.

Открытие программы по поиску уязвимостей в программном и аппаратном обеспечении (bug bounty)

3 июня 2021 года «Ростелеком» объявил об открытии на базе Национального киберполигона масштабной программы по поиску уязвимостей в программном и аппаратном обеспечении (bug bounty). Ее целью является проверка и повышение уровня защищенности решений, используемых в организациях государственного сектора, крупнейших коммерческих компаниях и на объектах критической информационной инфраструктуры России. Программа запущена в рамках

реализации Федерального проекта «Информационная безопасность» Национальной программы «Цифровая экономика Российской Федерации».

Первым участником программы стал один из ключевых российских производителей средств криптографической защиты информации - компания «Код Безопасности». Исследования уязвимостей программных и аппаратных решений на Национальном киберполигоне будут проводиться на регулярной основе в сотрудничестве с российскими и зарубежными разработчиками. До конца 2021 года «Ростелеком» планирует заключить не менее 6 партнерств в этой сфере.

В рамках bug bounty исследователи будут тестировать предложенные решения на предмет устойчивости к различным типам кибератак. Вся информация, собранная по итогам программ, будет передаваться вендорам для устранения ошибок. Таким образом крупнейшие российские разработчики смогут проверить безопасность своих продуктов в условиях, максимально приближенных к ситуации реальных кибератак, а эксперты в сфере кибербезопасности - получить вознаграждение за нахождение ошибок и уязвимостей. Эта программа поможет на практике верифицировать безопасность решений, которые широко применяются в ключевых отраслях экономики и тем самым повысить киберустойчивость страны в цифровом пространстве.

«В рамках данной инициативы мы выступаем как партнер государства в сфере кибербезопасности, помогая на практике проверить уровень защищенности тех решений, которые используются в наиболее значимых для страны организациях. Данная программа является логичным продолжением курса на импортозамещение: отечественные решения завоевывают все большую долю присутствия в государственном секторе, промышленности, на объектах КИИ, и мы должны быть уверены в их безопасности. При этом мы рады приветствовать среди участников программы и зарубежных вендоров, со стороны которых уже поступают запросы на участие», - заявил вице-президент «Ростелекома» по информационной безопасности Игорь Ляпунов.

Первое исследование стартует в июне 2021 года. Его объектом станет решение «Континент АП» компании «Код Безопасности» - средство криптографической защиты информации, которое обеспечивает защищенный доступ в корпоративную сеть с удаленных персональных компьютеров и смартфонов сотрудников. «Континент АП» применяется для защиты государственных информационных систем и объектов критической информационной структуры России.

«Системы, обеспечивающие защиту критической информационной инфраструктуры страны, должны в полной мере охватывать все возможные риски уязвимостей, и лучший способ обеспечить такую полную защиту - постоянное тестирование систем информационной безопасности. Мы приветствуем проект Ростелекома, направленный на выявление возможных рисков, и рады предоставить для соответствующего тестирования наши решения. Защита информационной безопасности страны - это большая ответственность, и мы это очень хорошо понимаем», - отметил генеральный директор компании «Код Безопасности» Андрей Голов.

В ходе первой программы bug bounty на Национальном киберполигоне исследователям необходимо будет получить удаленный доступ к аппаратно-программному комплексу шифрования «Континент» и в течение трех недель искать уязвимости в реализации функциональности продукта. Верифицировать их будет экспертная группа «Ростелеком-Солар», дочерней структуры «Ростелекома». Вся информация будет передана вендору для повышения защищенности решения.

«Ростелеком» открыл опорный центр Национального киберполигона на базе СибГУТИ

«Ростелеком» открыл в Новосибирске опорный центр Национального киберполигона на базе СибГУТИ. Об этом 17 мая 2021 года сообщил «Ростелеком-Солар». Подробнее здесь.

«Банк России» проведет учения на «Национальном киберполигоне»

Банк России проведет учения на Национальном киберполигоне. Об этом «Ростелеком-Солар» сообщил 26 марта 2021 года. Подробнее здесь.

2020

Архитектура киберполигона

Национальный киберполигон в РФ строят на базе ПО «Лаборатории Касперского»

22 декабря 2020 года «Ростелеком» сообщил о заключении с «Лабораторией Касперского» соглашения, по условиям которого программное обеспечение российского производителя антивирусных решений будет использоваться в создании инфраструктуры национального киберполигона.

Речь идет о платформе, имитирующей бизнес-процессы предприятий из ключевых отраслей экономики, с целью практического обучения специалистов по кибербезопасности. Киберполигон получит несколько взаимосвязанных сегментов, представляющих ИТ- и индустриальную инфраструктуры. Для создания сегментов первой категории будут применяться такие B2B-решения «Лаборатории Касперского», как Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Security и Kaspersky Security для интернет-шлюзов.

Национальный киберполигон в России строят на базе продуктов «Лаборатории Касперского»

В индустриальную инфраструктуру киберполигона внедрят корпоративные решения Kaspersky Industrial CyberSecurity for Networks, анализатор трафика промышленной сети, и Kaspersky Industrial CyberSecurity for Nodes, комплексное решение для защиты рабочих мест и инженерных станций в автоматизированных системах управления технологическими процессами (АСУ ТП).

Ожидается, что инфраструктура для финансовых организаций будет включать системы банковского обслуживания и процессинга, индустриальная инфраструктура - системы релейной защиты и автоматики, мониторинга переходных процессов, диспетчерского управления и т.д. Участники киберучений столкнутся с различными типами атак, действиями внутренних и внешних нарушителей.

В «Лаборатории Касперского» отметили, что создание киберполигона, на котором будут отрабатываться различные типы атак, станет существенным вкладом в развитие индустрии кибербезопасности. В рамках проекта также можно будет опробовать надежные защитные решения, подчеркнули в компании.

Минцифры продлевает создание киберполигона в России до 2024 года

В начале декабря 2020 года стало известно о решении Минцифры продлить до 2024 года сроки реализации проекта по созданию киберполигона в России. Изначально его планировалось выполнить к 2021 году, однако, как сообщило ведомство в проекте с изменениями в постановлении правительства, нужно больше времени, поскольку потребуется создать сегменты инфраструктуры для проведения киберучений не только для банковской и энергетической отраслей, но и телекоммуникационной, транспортной, нефтяной и др.

Как рассказали «Коммерсанту» в пресс-службе Минцифры, в декабре 2020 года киберполигон будет запущен в опытную эксплуатацию, а на 2021-2024 гг. намечены отраслевое и функциональное развитие его инфраструктуры.

Минцифры продлевает создание киберполигона в РФ до 2024 года

По словам директора по развитию направления «Национальный киберполигон» компании «Ростелеком-Солар» Михаила Климова, до конца 2020 года в опытную эксплуатацию будут введены два сегмента, создаваемые для кредитно-финансового сектора и энергетической отрасли.

Киберполигон будет состоять из четырех опорных центров в регионах, которые подключатся к инфраструктуре оператора. Государственная субсидия на проект на 2019-2020 годы составила 364,55 млн рублей, на 2021-2024 годы запланировано выделение 600 млн рублей.

Практическая подготовка специалистов в области информационной безопасности на территории СНГ отстает от зарубежной, и в сфере наблюдается кадровый голод, приводит издание мнение руководителя группы по оказанию услуг в области кибербезопасности KPMG в России и СНГ Ильи Шаленкова.

Партнер и руководитель практики управления киберрисками Deloitte Денис Липов считает, что киберполигон полезен для изучения информационной безопасности и моделирования киберугроз, которые вызывают отказ производственного оборудования и ИТ-систем. [1]

«Ростелеком» провел тестовые учения на киберполигоне во Владивостоке

Специалисты компании «Ростелеком-Солар», компании группы ПАО «Ростелеком», провели для студентов Дальневосточного федерального университета тестовые киберучения на платформе Национального киберполигона. В мероприятии приняли участие около 30 учащихся 2-6 курсов направлений «Информационная безопасность» и «Компьютерная безопасность», сообщили 20 ноября 2020 года в «Ростелекоме». Подробнее здесь.

Открытие опорного пункта киберполигона на базе университета «Сириус»

Фонд «Талант и успех» и «Ростелеком» подписали соглашение о сотрудничестве. Партнеры договорились о строительстве опорного центра национального киберполигона для практической подготовки специалистов в области информационной безопасности. Об этом 5 ноября 2020 года сообщила компания «Ростелеком-Солар».

Киберполигон - это один из проектов по информационной безопасности, реализуемых в рамках Национальной программы **«Цифровая экономика»** в 2020 году. Он выполняется силами «Ростелекома» с привлечением экспертизы сотрудников его дочерней компании «Ростелеком-Солар», национального провайдера технологий и сервисов кибербезопасности. Опорные центры киберполигона создаются также в Москве и Владивостоке.

Киберполигон представляет собой виртуальную копию инфраструктуры компаний различных отраслей. Он позволяет отрабатывать практические навыки по быстрому выявлению и предотвращению кибератак. Киберполгон идеально подходит для проведения киберучений и стресс-тестов информационных систем, программного обеспечения. Особенно это актуально для отраслей промышленности, имеющих стратегическое значение, таких как электроэнергетика, транспорт, связь, оборонно-промышленный комплекс.

Обеспечение безопасности в киберпространстве важно для каждого отдельного человека и национальных интересов страны в целом. Необходима системная и комплексная подготовка кадров, конкурентных в этой области. В «Сириусе» мы формируем среду, где объединяем талантливых школьников и студентов с отраслевыми компаниями в работе на передовом оборудовании, чтобы совместными усилиями обеспечить поиск ответов на Большие вызовы научно-технологического развития России, - подчеркнула руководитель Фонда «Талант и успех» Елена Шмелева.

Опорный пункт киберполигона в Научно-технологическом университете «Сириус» будет включать специализированную инфраструктуру и образовательные программы. Это позволит развивать таланты и усиливать практическую подготовку студентов профильных кафедр российских вузов. Пользоваться киберполигоном смогут и школьники профильных программ Образовательного центра «Сириус». Планируется, что специалисты «Ростелекома» также будут участвовать в образовательном процессе и выступят для ребят наставниками.

Киберполигон - один из ключевых инструментов стратегической задачи по повышению уровня компетенций специалистов по информационной безопасности в России. Мы очень рады видеть, что к его созданию подключаются крупные организации страны в различных сферах деятельности. Сотрудничество с Фондом «Талант и успех» и Образовательным центром «Сириус» позволит создать и распространить обучающую программу для тех, кто только приходит в профессию. Благодаря программе киберучений молодые специалисты по информационной безопасности получат то, чего обычно больше всего недостает на старте, - практический опыт выявления и отражения кибератак, - отметил Игорь Ляпунов, вице-президент «Ростелекома» по информационной безопасности, генеральный директор компании «Ростелеком-Солар».

Процессинг от RBK.money станет основной платежной средой киберполигона «Ростелеком-Солар»

Опенсорс-решение, разработанное международной финтех-компанией RBK.money, будет использоваться в виртуальной модели города на киберполигоне «Ростелекома» как основная платежная система. Об этом 10 сентября 2020 года сообщил «Ростелеком-Солар». Процессинг позволит моделировать финансовую деятельность «города» с полноценными интеграциями между банками, платежными системами и мерчантами.

Киберполигон - это один из проектов по информационной безопасности, реализуемых в рамках Национальной программы «Цифровая экономика России» в 2020 году. Он выполняется силами «Ростелекома» с привлечением экспертизы сотрудников его дочерней компании «Ростелеком-Солар», национального провайдера технологий и сервисов кибербезопасности.

Киберполигон предназначен для обучения и тренировок специалистов по информационной безопасности, и представляет собой достоверную модель города с полноценной инфраструктурой: банками, магазинами и имитацией различных сетей, включая ИТ-инфраструктуру транспортных сетей и энергетического сектора.

Использование процессинга RBK.money позволит полноценно эмулировать e-commerce сферу со стороны платежной индустрии - обеспечить прием и проведение платежей в виртуальной валюте как со стороны конечного пользователя-плательщика, покупающего товары или услуги в интернет-магазине, так и со стороны оператора платежной системы, позволяющей предоставить облачный сервис для подключения интернет-магазинов и любых других поставщиков услуг.

В дополнение к платежной системе мы специально разработали искусственные уязвимости и сценарии хакерских атак, которые специалисты по информационной безопасности должны будут обнаружить и преодолеть в ходе тренировок на киберполигоне, - рассказывает генеральный директор RBK.money Денис Бурлаков. - Типовые сценарии атак на банковскую сферу, такие как кража денег со счетов юрлиц, внедрение зловредных программ-шифровальщиков, взлом системы управления балансами юридических лиц с последующим выводом «нарисованных» денег на карты злоумышленников и прочие существующие в реальности векторы атак позволят специалистам по кибербезопасности в режиме реального времени провести эти атаки и выработать навыки и средства защиты от них. Наш процессинг представляет собой многофункциональную распределенную платежную систему для управления транзакциями онлайн, и особенное внимание мы уделяем вопросам безопасности финансовых операций,

постоянно привлекаем представителей ИТ-сообщества к совместной работе для развития безопасных платежей в России.

Платформа построена на основе опенсорс-технологий и соответствует стандарту безопасности данных PCI DSS и СТО БР. Архитектура разработана на основе микросервисного подхода и возможностей линейного масштабирования производительности. Процессинг содержит интерфейсы платежных протоколов для host-to-host интеграций с банками, платежными системами и мерчантами, а также пользовательские интерфейсы для плательщиков и мерчантов. Система может работать как основной процессинг, а также как предпроцессинг или как маршрутизатор платежей между разными процессингами одновременно.

Разработчики сервиса использовали модель распространения, при которой все исходные коды и бинарные экземпляры микросервисов процессинга полностью открыты в опенсорс, и доступны любому участнику рынка бесплатно. В такой модели даже небольшой финтех-стартап может развернуть платежную платформу и предоставлять услуги клиентам, не затрачивая значительные финансовые и технические ресурсы на покупку проприетарного решения или разработку собственного.

Для национального киберполигона мы выбрали компанию с серьезным опытом в сфере платежных операций - RBK.money работает на финансовом рынке свыше 17 лет, обслуживая организации в 60 странах мира. Процессинг станет одним из важных элементов виртуальной банковской инфраструктуры, на которой участники киберучений смогут отработать навыки отражения специализированных, актуальных для финансовых организаций компьютерных атак, - сообщил директор по развитию направления «Национальный Киберполигон» компании «Ростелеком-Солар» Михаил Климов.

Партнерство «Ростелекома» и «Диасофт» с целью создания банковского сегмента киберполигона

Компания «Диасофт», российский разработчик ИТ-решений для финансового сектора, заключила соглашение с «Ростелекомом» в лице дочерней компании «Ростелеком-Солар», национального провайдера кибербезопасности. Целью сотрудничества является построение банковского сегмента киберполигона, который предоставит банкам возможность отрабатывать практические навыки отражения кибератак. Об этом «Диасофт» сообщил 3 сентября 2020 года.

Киберполигон - это один из проектов по информационной безопасности, реализуемых в рамках Национальной программы «Цифровая экономика России» в 2020 году. Задача по его созданию возложена на «Ростелеком», проект реализуется с привлечением экспертизы его дочерней компании «Ростелеком-Солар». Киберполигон включает ряд сегментов, повторяющих типовую инфраструктуру организаций различных отраслей, в том числе кредитно-финансового сектора.

Чтобы киберучения служб безопасности были максимально приближены к реальным условиям, виртуальная инфраструктура киберполигона должна включать всю совокупность информационных систем банков - АБС и смежных с ней компонентов. В качестве автоматизированной банковской системы было выбрано соответствующее решение компании «Диасофт», которое используется кредитно-финансовыми организациями России.

По данным центра мониторинга и реагирования на киберугрозы Solar JSOC, в 2019 году примерно каждая пятая атака была направлена на банки. Методики и инструментарий злоумышленников постоянно совершенствуются, и проникновение хакеров в инфраструктуры любой финансово-кредитной организации - вопрос времени. Поэтому на первый план выходит обнаружение атаки на ранних этапах, а также быстрое и эффективное противодействие ей. Учитывая, что даже банки, использующие внешние сервисы мониторинга и реагирования на кибератаки, предпочитают осуществлять техническое реагирование самостоятельно, практическая отработка действий

внутренней службы информационной безопасности становится необходимым элементом защиты, - рассказал директор по развитию направления «Национальный Киберполигон» компании «Ростелеком-Солар» Михаил Климов.

Как отмечают эксперты «Диасофт», в процессе автоматизации банковской деятельности существует множество точек взаимодействия между различными системами, что неминуемо ведет к появлению уязвимых мест. Поэтому компания с энтузиазмом встретила инициативу «Ростелеком», направленную на повышение безопасности финансовой сферы в стране.

Помимо проведения киберучений, виртуальная инфраструктура киберполигона будет использоваться для проведения стресс-тестов российских решений, используемых в комплексных проектах по обеспечению информационной безопасности банков.

В будущем к цифровой платформе «Ростелекома» будут подключены еще три опорных центра киберполигона в регионах - на Дальнем Востоке, в Приволжском и Южном федеральном округе, что позволит повысить уровень защищенности всех ключевых отраслей экономики страны.

2019

«Ростелеком» выбран исполнителем проекта по созданию киберполигона

В декабре 2019 года «Ростелеком» выиграла конкурс на создание киберполигона для обучения и тренировки специалистов по информационной безопасности. На реализацию этого проекта госоператор получит из бюджета РФ около 364,55 млн рублей, сообщает ТАСС со ссылкой на протокол конкурсной комиссии. Документ размещен на сайте Минкомсвязи.

Как следует из обнародованный документации, максимальный объем предоставляемой субсидии на каждый год реализации мероприятия составляет: 314,55 млн рублей на 2019 год и 50 млн рублей на 2020 год. Источник финансирования - субсидия из федерального бюджета, собственные и/или привлеченные средства победителя конкурсного отбора.

«Ростелеком» выиграла конкурс на создание киберполигона для обучения и тренировки специалистов по информационной безопасности

Минкомсвязи предоставит «Ростелекому» субсидию на реализацию следующих мероприятий:

создание киберполигона, реализованного в том числе с использованием облачных технологий, для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности;

создание независимых центров по техническому тестированию программного и аппаратного обеспечения, в том числе средств обеспечения безопасности информации, позволяющих компаниям получить доступ к аналитической информации и результатам независимого тестирования предлагаемых на рынке решений.

Как пояснил президент «Ростелекома» Михаил Осеевский в кулуарах Национального промышленного форума в Москве, речь идет о создании не физического объекта, а о разработке программы, которая имитирует основные потенциальные угрозы.

Сегодня вопросы информационной безопасности перетекают из области финансовых услуг и медиа, они начинают все больше погружаться в тему обеспечения информационной безопасности промышленности и основных технологических процессов. Это гораздо более сложные решения, и риски, которые там существуют, совершенно другие. Поэтому правительство

справедливо приняло решение создать такой макет, который бы имитировал собой некоторые типы предприятий, - сообщил он. [2]

Создание двух киберполигонов для обучения информационной безопасности

В октябре 2019 года премьер-министр России Дмитрий Медведев подписал указ о правиле предоставления из федерального бюджета субсидий на создание киберполигонов.

Как сообщается в документе, опубликованном на портале правовой информации, киберполигон представляет собой инфраструктуру для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информбезопасности и информтехнологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них.

Премьер-министр России Дмитрий Медведев подписал указ о правиле предоставления из федерального бюджета субсидий на создание киберполигонов

Минкомсвязи выберет получателя субсидий на конкурсе. Победитель должен будет создать два киберполигона, в том числе с использованием облачных технологий:

один - минимум для двух информационных технологических инфраструктур, эмулирующих корпоративные сети организаций банковской системы в России;

второй - для индустриальной инфраструктуры энергетического сектора.

Также исполнителю проекта нужно будет создать более четырех учебно-практических центров по техническому тестированию программного и аппаратного обеспечения в партнерстве с ВУЗами.

Чтобы принять участие в конкурсе, компании должны быть зарегистрированы в России, с долей иностранного владения менее 50%. В число других требований также вошли:

наличие собственной вычислительной инфраструктурой для создания и функционирования киберполигона;

опыт оказания услуг по мониторингу информационной безопасности;

опыт взаимодействия с организациями высшего профессионального образования в сфере подготовки кадров по ИБ-направления. [3]

В начале сентября 2019 года «Ростелеком», Минкомсвязи, Минвостокразвития и Дальневосточный федеральный университет (ДВФУ) в рамках ВЭФ-2019 подписали соглашение, направленное на создание Дальневосточного центра киберполигона. Он будет нацелен на развитие талантов и практическую подготовку кадров в области информационной безопасности на Дальнем Востоке.

Смотрите также

Контроль и блокировки сайтов

Цензура в интернете. Мировой опыт

Цензура (контроль) в интернете. Опыт Китая, Компьютерная группа реагирования на чрезвычайные ситуации Китая (CERT)

Цензура (контроль) в интернете. Опыт России, Политика Роскомнадзора по контролю интернета, ГРЧЦ

Запросы силовиков на телефонные и банковские данные в России

Закон о регулировании Рунета

Национальная система фильтрации интернет-трафика (НаСФИТ)

Как обойти интернет-цензуру дома и в офисе: 5 простых способов

Блокировка сайтов в России

Ревизор - система контроля блокировки сайтов в России

Анонимность

Даркнет (теневой интернет, DarkNet)

VPN и приватность (анонимность, анонимайзеры)

VPN - Виртуальные частные сети

СОРМ (Система оперативно-розыскных мероприятий)

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

Ястреб-М Статистика телефонных разговоров

Критическая инфраструктура

Цифровая экономика России

Электронное правительство России

Информационная безопасность цифровой экономики России

Защита критической информационной инфраструктуры России

Закон О безопасности критической информационной инфраструктуры Российской Федерации

Основы государственной политики РФ в области международной информационной безопасности

Доктрина информационной безопасности России

Стратегия национальной безопасности России

Соглашение стран СНГ в борьбе с преступлениями в сфере информационных технологий

Автономный интернет в России

Киберполигон России для обучения информационной безопасности

Национальная биометрическая платформа (НБП)

Единая биометрическая система (ЕБС) данных клиентов банков

Биометрическая идентификация (рынок России)

Каталог решений и проектов биометрии

Единая сеть передачи данных (ЕСПД) для госорганов (Russian State Network, RSNet)

Статья:Единая система программной документации (ЕСПД).

Сеть передачи данных органов государственной власти (СПДОВ)

Единая сеть электросвязи РФ

Единый портал государственных услуг (ФГИС ЕПГУ)

Гособлако - Государственная единая облачная платформа (ГЕОП)

Госвеб Единая платформа интернет-порталов органов государственной власти

Импортозамещение

Импортозамещение в сфере информационной безопасности

Обзор: Импортозамещение информационных технологий в России

Главные проблемы и препятствия импортозамещения ИТ в России

Преимущества замещения иностранных ИТ-решений отечественными

Основные риски импортозамещения ИТ

Импортозамещение информационных технологий: 5 «За» и 5 «Против»

Как импортозамещение ИТ сказалось на бизнесе иностранных вендоров? Взгляд из России

Как запуск реестра отечественного ПО повлиял на бизнес российских вендоров

Какие изменения происходят на российском ИТ-рынке под влиянием импортозамещения

Оценки перспектив импортозамещения в госсекторе участниками рынка

Информационная безопасность и киберпреступность

Обзор громких киберинцидентов 2020 года

Киберпреступность в мире

CERT NZ

Национальный центр по защите данных системы здравоохранения Норвегии (HelseCERT)

Требования NIST

Глобальный индекс кибербезопасности

Кибервойны, Кибервойна России и США, Кибервойна России и Великобритании

Киберпреступность и киберконфликты : Россия, ФСБ, Национальный координационный центр по компьютерным инцидентам (НКЦКИ), Центр информационной безопасности (ЦИБ) ФСБ, Следственный комитет при прокуратуре РФ, Управление К БСТМ МВД России, МВД РФ, Министерство обороны РФ, Росгвардия, ФинЦЕРТ

Число киберпреступлений в России

Киберпреступность и киберконфликты : Украина, Киберцентр UA30, Национальные кибервойска Украины

CERT-UZ Отдел технической безопасности в структуре государственного унитарного Центра UZINFOCOM

* Регулирование интернета в Казахстане, KZ-CERT

Киберпреступность и киберконфликты : США, Пентагон, ЦРУ, АНБ, NSA Cybersecurity Directorate, ФБР, Киберкомандование США (US Cybercom), Министерства обороны США, NATO, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)

Как США шпионили за производством микросхем в СССР

Киберпреступность и киберконфликты : Европа, ENISA, ANSSI, Joint Cyber Unit, National Cyber Force

Стратегия кибербезопасности ЕС

Регулирование интернета в странах Евросоюза

Информационная безопасность в Германии

Информационная безопасность во Франции

Информационная безопасность в Австралии

Tactical Edge Networking (военный интернет)

Киберпреступность и киберконфликты : Израиль

Киберпреступность и киберконфликты : Иран

Киберпреступность и киберконфликты : Китай

Импортозамещение информационных технологий в Китае

Киберпреступность и киберконфликты : КНДР

Безопасность в интернете

Безопасность интернет-сайтов

Безопасность программного обеспечения (ПО)

Безопасность веб-приложений

Угрозы безопасности общения в мобильной сети

Безопасность в социальных сетях

Киберзапугивание (кибербуллинг, кибersталкинг)

Информационная безопасность в банках

CERT-GIB Computer Emergency Response Team - Group-IB

Мошенничество с банковскими картами

Взлом банкоматов

Обзор: ИТ в банках 2016

Политика ЦБ в сфере защиты информации (кибербезопасности)

Потери организаций от киберпреступности

Потери банков от киберпреступности

Тренды развития ИТ в страховании (киберстрахование)

Кибератаки

Обзор: Безопасность информационных систем

Информационная безопасность

Информационная безопасность в компании

Информационная безопасность в медицине

Информационная безопасность в электронной коммерции

Информационная безопасность в ритейле

Информационная безопасность (мировой рынок)

Информационная безопасность (рынок России)

Информационная безопасность на Украине

Информационная безопасность в Белоруссии

Главные тенденции в защите информации

ПО для защиты информации (мировой рынок)

ПО для защиты информации (рынок России)

Pentesting (пентестинг)

ИБ - Средства шифрования

Криптография

Управление инцидентами безопасности: проблемы и их решения

Системы аутентификации

Директор по информационной безопасности (Chief information security officer, CISO)

Коррупция (мошенничество, взятки): Россия и мир

Отмывание денег (Money Muling)

Закон о персональных данных №152-ФЗ

Защита персональных данных в Евросоюзе и США

Расценки пользовательских данных на рынке киберпреступников

Джекпоттинг_(Jackpotting)

Вирус-вымогатель (шифровальщик), Ramsomware, WannaCry, Petya/ExPetr/GoldenEye, CovidLock, Ragnar Locker, Ryuk, EvilQuest Вредонос-вымогатель для MacOS, Ransomware of Things (RoT), RegretLocker, Pay2Key, DoppelPaymer, Conti, DemonWare (вирус-вымогатель)

Защита от программ-вымогателей: существует ли она?

MrbMiner (вирус-майнер)

Защита от вирусов-вымогателей (шифровальщиков)

Вредоносная программа (зловред)

APT - Таргетированные или целевые атаки

Исследование TAdviser и Microsoft: 39% российских СМБ-компаний столкнулись с целенаправленными кибератаками

DDoS и DeOS

Атаки на DNS-сервера

DoS-атаки на сети доставки контента, CDN Content Delivery Network

Как защититься от DDoS-атаки. TADетали

Визуальная защита информации - Визуальное хакерство - Подглядывание

Ханипоты (ловушки для хакеров)

Руткит (Rootkit)

Fraud Detection System (fraud, фрод, система обнаружения мошенничества)

Каталог Антифрод-решений и проектов

Как выбрать антифрод-систему для банка? TADетали

Security Information and Event Management (SIEM)

Каталог SIEM-решений и проектов

Чем полезна SIEM-система и как ее внедрить?

Для чего нужна система SIEM и как ее внедрить TADетали

Системы обнаружения и предотвращения вторжений

Отражения локальных угроз (HIPS)

Защита конфиденциальной информации от внутренних угроз (IPC)

Спуфинг (spoofing) - кибератака

Фишинг, Фишинг в России, DMARC, SMTP

Сталкерское ПО (программы-шпионы)

Троян

Ботнет Боты, TeamTNT (ботнет), Meris (ботнет)

Backdoor

Черви Stuxnet Regin Conficker EternalBlue

Рынок безопасности АСУ ТП

Флуд (Flood)

Предотвращения утечек информации (DLP)

Скимминг (шимминг)

Спам, Мошенничество с электронной почтой

Социальная инженерия

Телефонное мошенничество

Звуковые атаки

Warshipping (кибератака Военный корабль)

Антиспам программные решения

Классические файловые вирусы

Антивирусы

ИБ : средства защиты

Система резервного копирования

Система резервного копирования (технологии)

Система резервного копирования (безопасность)

Межсетевые экраны

Системы видеонаблюдения

Видеоаналитика

https://www.tadviser.ru/a/480551

К аннотации

Комсомольская правда (tula.kp.ru), Тула, 12.10.2021

«ПМП «ПРОТОН» - ОСВАИВАЯ НОВЫЕ ГОРИЗОНТЫ

Автор: Копаница Михаил

Сегодня мы продолжаем разговор с Александром Болдиным, генеральным директором ООО «ПМП «ПРОТОН» - тульской компании, специализирующейся на производстве и поставке медицинского оборудования для диагностики

Продукция предприятия хорошо известна не только в масштабе всей России, но и за рубежом.

- По результатам рейтинга цифровой трансформации регионов, который ежемесячно проводит Минцифры РФ в рамках нацпроекта «**Цифровая экономика**», Тульская область на втором месте. «Стратегия цифровой трансформации» касается и социальной сферы...

- Конечно, в сфере здравоохранения речь идет прежде всего о развитии цифровой медицины. Это одно из важнейших направлений нашей деятельности. Девиз «ПМП «ПРОТОН» - работать для будущего медицины. Все, что мы делаем в этом направлении, напрямую связано с последующей верной постановкой диагноза. Именно диагностика - быстрая и точная - залог высокого качества медицинских услуг.

В плане цифровизации на первый план выходит наша работа по модернизации оборудования лечебно-профилактических учреждений. Здесь мы выстроили деятельность по двум направлениям. Первое подразумевает полное обновление комплектующих действующего оборудования при сохранении конструктива. Наши сотрудники выезжают в медучреждение, оценивают состояние прибора, укомплектовывают его цифровыми панелями, делаем его современным, обучаем персонал, обустраиваем новое рабочее место врача - этот путь высоко оценен нашими клиентами. Второе направление - полное обновление медицинского оборудования: вместо морально устаревших приборов в медицину приходят новые со всех точек зрения комплексы для точной диагностики.

- Линейка производимого предприятием оборудования серьезная: цифровые комплексы для диагностики заболеваний, передвижные комплексы различной специализации на базе автомобилей с использованием рентгеновского оборудования и малогабаритных теплоэнергоустановок и мн. др. Кто ваши основные заказчики?

- Наши основные заказчики - медучреждения различных уровней (федеральные, региональные), Министерство обороны РФ, частные клиники. География поставок продукции в России - от Калининграда до Владивостока. Основной покупательский спрос - в Тульской, Калужской и Московской областях, много заказов поступают из Твери, Самары, Нижнего Новгорода, Липецка, Казани, Санкт-Петербурга, Башкирии и Хабаровского края.

- «ПРОТОН» - постоянный участник профильных российских и международных выставок, научно-практических конференций...

- Обязательно, так как это напрямую способствует продвижению нашей продукции. Многие клиенты находят нас сами по рекомендациям: причина простая - большая часть оборудования, которое мы производим, пока не имеет сертифицированных аналогов в нашей стране.

Нас выбирают и потому, что мы ведем клиента и после приобретения у нас оборудования. Сервисное обслуживание - важная составляющая обеспечения качественной работы. Для оперативного решения этого вопроса у нас есть собственная сервисно-монтажная служба. Она осуществляет монтаж, гарантийный и постгарантийный ремонты, плановое сервисное обслуживание. Высококвалифицированные специалисты предприятия прошли обучение в ряде ведущих зарубежных компаний.

Пристальное внимание мы уделяем и обучению персонала медицинских учреждений для работы на произведенном нашей компанией оборудовании.

- Пандемия коронавируса сказалась на работе компании?

- «ПМП «ПРОТОН» с апреля 2020 года входит в список системообразующих предприятий Тульской области, поэтому мы еженедельно отчитываемся по ситуации с ковидом. Более 70% сотрудников нашей компании прошли вакцинацию, поэтому работа продолжает вестись системно и без сбоев.

Про экспорт

- Александр Викторович, в прошлый раз вы рассказали о начале работы с иностранными партнерами, в частности с Египтом. Как тут идут дела?

- Дела по выходу на внешний рынок идут в рамках намеченных графиков. В настоящее время в финальной стадии находится договорной процесс с египетскими партнерами. На прошлой неделе наша делегация побывала в Египте и обсудила окончательные условия сотрудничества. Подготовительная работа проходит долго, например, много времени занимает технический перевод документов.

В конце октября мы представим заказчику обновленный вариант презентации нашей продукции, и выступим перед комиссией, которая принимает решение - это то, что касается сотрудничества с министерством обороны Египта. Теперь по гражданской продукции: до конца ноября мы поставим одной из местных компаний наши диагностические изделия, которые пройдут апробацию у египетских партнеров. Надеюсь, эта работа будет закончена уже в текущем году, и мы подпишем контракт на поставку. Также подготовлен меморандум о начале общей работы, направленной на выпуск и продвижение совместного продукта для оснащения стерилизационных помещений в медучреждениях. До конца года мы должны его доработать совместно с египетскими партнерами. Таковы ключевые задачи «ПМП «ПРОТОН» на ближайшую перспективу.

ООО «ПМП «ПРОТОН»:

Тула, ул. Болдина, 98-а.

Тел.: (4872) 25-05-87, 25-05-86.

protontula.ru

ООО

Передвижные комплексы на базе автомобилей, производимые ООО

В линейке производимого предприятием оборудования - передвижные комплексы различной специализации на базе автомобилей с использованием рентгеновского оборудования и малогабаритных теплоэнергоустановок.

Внутреннее оснащение передвижного комплекса на базе автомобилей с использованием рентгеновского оборудования.

https://www.tula.kp.ru/daily/28342/4488368/

К аннотации

Экспертный центр электронного государства (d-russia.ru), Москва, 12.10.2021

ПЕРВЫЕ КРОСС-ОТРАСЛЕВЫЕ КОРПОРАТИВНЫЕ КИБЕРУЧЕНИЯ ПРОШЛИ НА НАЦИОНАЛЬНОМ КИБЕРПОЛИГОНЕ

«Ростелеком-Солар» совместно с Корпоративным университетом TMK2U организовали для сотрудников Трубной металлургической компании (ТМК) и Группы «Синара» масштабные кросс-отраслевые корпоративные учения на Национальном киберполигоне, сообщает «Ростелеком» во вторник.

Это первые в России киберучения, охватывающие отработку всех ключевых процессов служб информационной безопасности - от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак, говорится в сообщении.

Киберучения прошли в рамках международного корпоративного форума ТМК и Группы «Синара» «Горизонты» и длились три дня, в течение которых семь команд, состоящих из IT- и ИБ-специалистов компаний, боролись за первенство в выявлении, отражении и расследовании кибератак.

В первый день киберучений команды должны были провести максимально полную инвентаризацию инфраструктуры, специально созданной на базе промышленного сегмента киберполигона. Затем им необходимо было выполнить поиск уязвимостей в ней и настроить источники событий в SIEM-системе. На данном этапе оценивались полнота и точность данных от каждой команды.

Во второй день команды противостояли целенаправленным атакам, и на этом этапе ключевым показателем стала скорость обнаружения инцидента и реагирования на него. По итогам каждой атаки команды предоставляли отчеты с описанием как цепочки шагов злоумышленника, так и мер, необходимых для того, чтобы избежать повторения инцидента.

В заключительный день киберучений были подведены общие итоги, а также проведен подробный разбор сценариев учебных кибератак и действий команд.

Наилучший результат по отражению кибератак продемонстрировала команда управляющей компании ТМК, второе место заняла сборная Первоуральского новотрубного и Челябинского трубопрокатного заводов (ПНТЗ и ЧТПЗ), третье место - у команды Северского трубного завода (СТЗ).

Напомним, национальный киберполигон создан по поручению Минцифры России в рамках **программы «Цифровая экономика»**. Целью его создания является отработка процессов выявления и реагирования на компьютерные атаки на уровне отраслей и ключевых организаций России.

К настоящему моменту «Ростелеком» на базе ресурсов дочерней компании «Ростелеком-Солар» создал три первых сегмента киберполигона, которые представляют собой цифровые копии типовых IT-инфраструктур, существующих в организациях ключевых отраслей экономики.

В мае вице-премьер Дмитрий Чернышенко сообщал, что тренировки по кибербезопасности для разных отраслей экономики в 2021 году пройдут на пяти киберполигонах.

https://d-russia.ru/pervye-kross-otraslevye-korporativnye-kiberuchenija-proshli-na-nacionalnom-kiberpoligone.html

К аннотации

Ura.ru (ura.news), Екатеринбург, 12.10.2021

В СВЕРДЛОВСКОЙ ОБЛАСТИ ЗАВЕРШИЛИ ГЛОБАЛЬНЫЙ ПРОЕКТ ДЛЯ ШКОЛ

Автор: Шабалина Анна

В Свердловской области завершили проект по подключению к интернету социально-значимых учреждений в отдаленных районах региона. Об этом объявил директор екатеринбургского филиала ПАО «Ростелеком» Иван Пичугин на пресс-конференции с новым министром цифрового развития Свердловской области Михаилом Пономарьковым.

«Это глобальный проект, который компания «Ростелеком» совместно с правительством СО реализует третий год. Мы его завершили. Хочу сказать, что, наверное, в рамках цифровой жизни региона это самый масштабный проект, который когда-либо осуществлялся» - рассказал Пичугин.

Проект был рассчитан на три года, и за это время было подключено 1641 учреждение - это школы, библиотеки, пожарные части, администрации и фельдшерские пункты. Ранее сообщалось, что власти предложили россиянам выбрать населенные пункты с численностью жителей от 100 до 500 человек, в которые в следующем году проведут высокоскоростной интернет в рамках национальной **программы «Цифровая экономика»**. До 2030 года мобильная связь по ней станет доступна более чем в 24 тысячах населенных пунктов страны.

https://ura.news/news/1052510451

К аннотации

Rspectr.com, Москва, 12.10.2021

ПОДВЕДЕНЫ ИТОГИ КОРПОРАТИВНЫХ КИБЕРУЧЕНИЙ В ПРОМЫШЛЕННОСТИ

Среди сотрудников Трубной Металлургической Компании (ТМК) и Группы Синара прошли кросс-отраслевые корпоративные учения на Национальном киберполигоне. Мероприятие охватило отработку всех ключевых процессов служб информбезопасности - от анализа защищенности и выстраивания системы комплексной безопасности инфраструктуры до выявления и отражения хакерских атак.

Учения организовали «Ростелеком-Солар» совместно с Корпоративным университетом ТМК2U, сообщила пресс-служба «Ростелеком».

Киберучения длились три дня. В течение этого времени семь команд, состоящих из ИТ- и ИБ-специалистов компаний, выявляли, отражали и расследовали кибератаки. В последний день мероприятия был проведен разбор сценариев кибернападений и тактик реагирования команд защитников.

«Важно, что в ходе мероприятия отрабатывались сценарии, близкие к жизни, релевантные именно для промышленных предприятий. Подобный формат используется впервые в металлургической отрасли. Результаты учений подтвердили высокий профессионализм нашей команды кибербезопасности», - подчеркнул директор по информационным технологиям ТМК Дмитрий Якоб.

В результате мероприятий лучший результат по отражению кибератак продемонстрировала команда управляющей компании ТМК, второе место заняла сборная Первоуральского новотрубного и Челябинского трубопрокатного заводов (ПНТЗ и ЧТПЗ), третье место - у команды Северского трубного завода (СТЗ).

Национальный киберполигон создан по поручению Минцифры в рамках **программы «Цифровая экономика»**.

Изображение: пресс-служба «Ростелеком»

https://rspectr.com/novosti/63200/podvedeny-itogi-korporativnyh-kiberuchenij-v-promyshlennosti

К аннотации

Национальные проекты России (национальныепроекты.рф), Москва, 12.10.2021

ГЛАВНЫЕ ЛАЙФХАКИ ОТ ПОБЕДИТЕЛЕЙ МЕЖДУНАРОДНОЙ ОЛИМПИАДЫ ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Технологии не стоят на месте и, к сожалению, вместе с ними развиваются и методы мошенничества. Сегодня преступники виртуозно пользуются знаниями по психологии и обманывают доверчивых граждан по телефону или электронной почте. О том, как не попасть на удочку мошенников, портал национальныепроекты.рф расспросил победителей I Международной олимпиады по финансовой безопасности (о ее итогах мы писали здесь). Организаторы приурочили ее проведение к Году науки и технологий, а кроме того, мероприятие помогает достичь целей нацпроектов « Образование « и « **Цифровая экономика** «.

Собеседники портала рассказали, что сегодня без должного уровня финансовой грамотности никуда, а разбираться в подобных вопросах - насущная необходимость. Так, Константин Исаченко отметил, что эти знания полезны при общении с банками и, конечно, когда с человеком связываются мошенники.

«У нас в России очень распространен вишинг - телефонное мошенничество. Мои родители в этом плане очень внимательные и осторожные люди, именно они во многом научили меня финансовой грамотности. Они очень верно себя ведут - как только понимают, что им звонят мошенники, сразу кладут трубку. И это самое правильное, что можно сделать. К счастью, мои ближайшие родственники и друзья обладают достаточной финансовой грамотностью, чтобы не попадаться на такие уловки», - продолжила тему Ульяна Костылева.

Ярослав Геращенко, в свою очередь, рассказал, что также применяет знания о финансах в инвестировании: при оценке стоимости акций, перспектив вложений в фонды и так далее. Он подчеркивает, что здесь необходим системный подход: нельзя единожды выучив что-то, пользоваться этим знанием еще много лет.

«Сегодня по возможности я стараюсь пропагандировать финансовую грамотность среди своих родственников, консультировать их в элементарных вещах ведения бизнеса, уплаты налогов, сохранения капитала на годы вперед. Каким же было мое удивление, когда руководитель Росфинмониторинга Юрий Анатольевич Чиханчин говорил на олимпиаде очень похожие слова о том, что каждый из нас должен начать со своей семьи, потом друзей, коллег. Он абсолютно прав:

сегодня у старшего поколения мало свободного времени, тем более для прочтения статей в интернете незнакомой тематики. Личная индивидуальная беседа является эффективным инструментом воздействия и обучения, особенно в непринужденной обстановке, за чашкой чая», - поделился Геращенко в беседе с порталом национальныепроекты.рф.

Победители I Международной олимпиады по финансовой безопасности отмечают, что очень важно общаться с родственниками и друзьями, делиться с ними опытом, обсуждать спорные ситуации.

«В основной зоне риска находятся дети и пожилые люди, поскольку они меньше знают об опасностях в этой сфере. Для предотвращения махинаций и снижения рисков их следует больше информировать о существующих угрозах. А представителей старшего поколения нужно убедить в том, что перед совершением каких-либо финансовых операций лучше посоветоваться с ближайшими родственниками», - отмечает Исаченко.

Ярослав Геращенко также рекомендует внимательнее относиться к своим родителям, дедушкам и бабушкам. По его мнению, необходимо массовое просвещение в области финансовой грамотности. При этом должны быть не только классические обучающие курсы, но и, например, программы по федеральным каналам, социальная реклама. Собеседник портала предупреждает, что от действий мошенников никто не застрахован.

«Недавно, до моего отъезда в «Сириус» с одним знакомым случилась неприятная ситуация. Ему также позвонили из банка, все прошло в стандартной схеме: мошенники пугают мошенниками. Оказывается, потерпевший сначала не верил мошенникам, принимал все со смехом, но к середине разговора он начал внимать им, все предоставляемые доказательства казались логичны, и он начал обсуждать перевод денег! Мошенник даже помог выбрать подходящий банкомат неподалеку, сервис на уровне. Лишь стараниями друга удалось остановить это происшествие. Парню 22 года, он учится на программе, связанной с IT и финансами, но попал в капкан», - рассказал Геращенко.

Ульяна Костылева соглашается, что в основную группу риска входят люди пожилого возраста, а также малолетние дети. Это происходит потому, что они в силу возраста, особенностей психики и доверчивости не могут осознавать опасность того или иного звонка, ссылки или сайта. Она объяснила, что пенсионеры часто очень сострадательны, и когда им звонят и говорят, что с кем-то из их близких случилась беда (сын попал в аварию, внучку сбил автомобиль и прочее), они тут же бросаются переводить деньги, чтобы спасти семью. В таких случаях победительница олимпиады советует обязательно позвонить «пострадавшим» лично и узнать, требуется ли им помощь.

«Чтобы предотвратить подобные случаи, важно, в первую очередь, разговаривать - и детям, и пожилым людям нужно объяснять, что не стоит сразу переводить деньги, нужно проявлять осторожность и осмотрительность и объяснять это все на конкретных примерах. Мошенники всегда работают по определенному сценарию - важно все обдумать и составить план действий. Нельзя торопиться и поддаваться на провокации», - подчеркнула она.

Кроме того, Костылева напомнила, что сегодня могут помочь нововведения от некоторых банков. Так, ряд кредитных организаций не дает пенсионерам проводить некоторые операции через мобильное приложение, им нужно лично прийти в банк. Безусловно, это не помогает полностью, но снижает риск того, что преступление будет доведено до конца.

Собеседники портала особо подчеркнули, что главное правило для сохранения финансов - это минимум общения с подозрительными лицами. Константин Исаченко советует обращать внимание на номер входящего вызова, так как банки имеют общеизвестные официальные номера, а если звонок поступает с мессенджеров, не стоит отвечать вовсе. Если сомнения все же

остались, он советует самостоятельно перезвонить в свой банк по номеру справочной службы. Ярослав Геращенко советует также установить себе определитель номера: приложение позволит сразу выявить мошенников.

Узнать подробнее о том, как нацпроект «**Цифровая экономика**» защищает персональные данные россиян, вы можете из этого материала.

Ульяна Костылева отмечает, что ни при каких обстоятельствах нельзя делиться своими данными с теми, кому вы не доверяете. Современные мошенники владеют навыками социальной инженерии, и могут вытягивать нужные им сведения самыми разными способами. «}},{«tpl»:»images

«Если вам звонит человек, который представляется сотрудником банка, сотрудником правоохранительных органов или иным уполномоченным лицом, а затем спрашивает данные вашей карты для «благих целей», ни в коем случае не сообщайте их. Это мошенники! Обычно сценарий с настоящим банковским сотрудником выглядит так:

- Здравствуйте, минуту назад с Вашего счета была произведена сомнительная операция. Скажите, это Вы ее совершали?

- Да, это был я.

- Хорошо, спасибо, всего доброго», - объяснила она.

Кроме того, наша героиня советует обращать внимание на поведение звонящего. Если он вас торопит, старается вывести на эмоции и запугивает, это точно мошенник. По ее словам, преступники давят на два основных рычага: желание легкой наживы и чувство страха. Ульяна отметила, что необходимо сохранять критическое мышление, холодный рассудок и анализировать ситуацию, не принимая поспешных решений. Если мошенник настойчив и убедителен, а вы хотите проверить, действительно ли он сотрудник банка, можно начать задавать ему вопросы, ответы на которые могут знать только в банке: сколько денег у вас на счетах, есть ли кредит, и когда дата платежа по нему.

«Во всем остальном советую проявлять крайнюю осмотрительность. Чаще меняйте пароли в социальных сетях и личных кабинетах, не оставляйте в свободном доступе свои паспортные данные, не регистрируйтесь и не совершайте покупки на незнакомых и подозрительных сайтах с огромным количеством рекламы. Используйте только проверенные информационные источники», - посоветовала Костылева.

https://национальныепроекты.рф/news/glavnye-layfkhaki-ot-pobediteley-mezhdunarodnoy-olimpiady-po-finansovoy-bezopasnosti

К аннотации

Ura.ru (ura.news), Екатеринбург, 12.10.2021

ЖИТЕЛИ АЛТАЯ ИСПУГАЛИСЬ СМЕРТИ ПТИЦ ИЗ-ЗА ВЫШЕК 5G

Автор: Королев Ульяна

Жители Республики Алтай в соцсетях испугались смерти около десятка птиц, которая попала на видео. Многие россияне связали гибель животных с вышками сотовой связи пятого поколения (5G).

В минувшие выходные в региональных соцсетях активно рассылалось видео, на котором зафиксирована гибель около десятка птиц. Также видеоролик размещен в нескольких группах в соцсетях с комментариями «экспертов» о пагубном влиянии вышек связи 5G. ЦУР зафиксировал и

направил информацию в Комитет охраны животного мира Республики Алтай. Установлено, что воробьи попали под крупногабаритное транспортное средство», - передает алтайский Центр управления регионом (ЦУР).

По информации Управления Роскомнадзора по Алтайскому краю и Республике Алтай, в регионе нет действующих вышек мобильной связи 5G. «Установка вышек сотовой связи не представляет опасности для человека», - подытожило ведомство.

Ранее министр цифрового развития, связи и массовых коммуникаций РФ **Максут Шадаев** заявил, что связь 5G не несет никакого вреда здоровью человека. **Шадаев** подчеркнул, что в России есть собственное производство оборудования для сетей 5G. По нацпроекту «**Цифровая экономика**», 10 крупных российских городов должны быть покрыты 5G к 2022 году, а к 2024 году вышки должны быть во всех городах-миллионниках, RT.

https://ura.news/news/1052510418

К аннотации

ТАСС, Москва, 12.10.2021

ДЛЯ ПРИМОРСКИХ ШКОЛЬНИКОВ С НАЧАЛА ГОДА ПРОВЕЛИ ПОЧТИ 180 «УРОКОВ ЦИФРЫ»

Детям рассказали о приватности в цифровом мире, беспилотном транспорте, цифровом производстве и искусственном интеллекте в образовании

ВЛАДИВОСТОК, 12 октября. /ТАСС/. Почти 180 «уроков цифры» провели для более чем 30 тыс. приморских школьников с начала года в рамках нацпроекта «**Цифровая экономика**», сообщает во вторник пресс-служба краевого правительства.

«С начала года уже проведено 178 «цифровых уроков» с охватом аудитории более 30 тыс. школьников. Детям рассказали о приватности в цифровом мире, беспилотном транспорте, цифровом производстве, искусственном интеллекте в образовании», - пояснили в пресс-службе.

Проект «Урок цифры» реализуется в поддержку федерального проекта «Кадры для цифровой экономики». Его задачами являются развитие у школьников цифровых компетенций и ранняя профориентация: уроки помогают детям определиться в мире профессий, связанных с компьютерными технологиями и программированием. В Приморском крае проект также реализуется в рамках программы «Информационное общество».

«Эти уроки о том, как искусственный интеллект помогает человеку в повседневной жизни, повышает продуктивность. Ученики смогут попробовать себя в роли настоящего исследователя данных и создать умного помощника для учителя», - добавили в пресс-службе.

https://tass.ru/obschestvo/12636201

К аннотации

Национальные проекты России (национальныепроекты.рф), Москва, 12.10.2021

РОССИЯНЕ ВЫБЕРУТ, КУДА ПРОВЕСТИ МОБИЛЬНУЮ СВЯЗЬ 4G

Россияне проголосуют на портале госуслуг за населенные пункты, которые подключат к высокоскоростному интернету в 2022 году. Специальный раздел с формой для голосования открылся на портале госуслуг, сообщает пресс-служба Минцифры России.

«Чтобы деревня, поселок, аул и другие населенные пункты подключились к мобильной связи 4G (LTE), необходимо проголосовать за них на портале госуслуг до 15 ноября 2021 года. В голосовании

принимают участие все населенные пункты с численностью населения от 100 до 500 человек. Проголосовать могут жители всех регионов, кроме Москвы и Санкт-Петербурга, которые не входят в программу устранения цифрового неравенства», - говорится в сообщении.

Для участия в голосовании гражданину нужна подтвержденная учетная запись на портале госуслуг и постоянная регистрация в регионе, за который голосует пользователь. Предусмотрена также возможность направить бумажное письмо в адрес Минцифры России. В письме нужно указать ФИО, адрес регистрации и название населенного пункта, в который требуется провести связь.

Через два месяца на «Госуслугах» будет опубликован список из 2000 населенных пунктов, которые будут подключены к интернету в следующем году. Таким образом, за 2022 год доступ к 4G получат не менее 10% всех населенных пунктов с численностью от 100 до 500 человек, а в 2024 году их количество увеличится до 30%. Всего до 2030 года мобильная связь в рамках программы станет доступной более чем в 24 тыс. населенных пунктах страны.

Обеспечение быстрого и качественного доступа в интернет входит в задачи нацпроекта «**Цифровая экономика**». Развитие инфраструктуры связи и расширение доступа к сети Интернет в малонаселенных, отдаленных и труднодоступных пунктах поможет преодолеть цифровое неравенство и обеспечить гражданам доступ к современным цифровым услугам, дистанционному образованию и телемедицине. Нацпроекты, инициированные президентом РФ Владимиром Путиным, стартовали в 2019 году.

Россияне проголосуют на портале госуслуг за населенные пункты, которые подключат к высокоскоростному интернету в 2022 году. Специальный раздел с формой для голосования открылся на портале госуслуг, сообщает пресс-служба Минцифры России.

«Чтобы деревня, поселок, аул и другие населенные пункты подключились к мобильной связи 4G (LTE), необходимо проголосовать за них на портале госуслуг до 15 ноября 2021 года. В голосовании принимают участие все населенные пункты с численностью населения от 100 до 500 человек. Проголосовать могут жители всех регионов, кроме Москвы и Санкт-Петербурга, которые не входят в программу устранения цифрового неравенства», - говорится в сообщении.

Для участия в голосовании гражданину нужна подтвержденная учетная запись на портале госуслуг и постоянная регистрация в регионе, за который голосует пользователь. Предусмотрена также возможность направить бумажное письмо в адрес Минцифры России. В письме нужно указать ФИО, адрес регистрации и название населенного пункта, в который требуется провести связь.

Через два месяца на «Госуслугах» будет опубликован список из 2000 населенных пунктов, которые будут подключены к интернету в следующем году. Таким образом, за 2022 год доступ к 4G получат не менее 10% всех населенных пунктов с численностью от 100 до 500 человек, а в 2024 году их количество увеличится до 30%. Всего до 2030 года мобильная связь в рамках программы станет доступной более чем в 24 тыс. населенных пунктах страны.

Обеспечение быстрого и качественного доступа в интернет входит в задачи нацпроекта «**Цифровая экономика**». Развитие инфраструктуры связи и расширение доступа к сети Интернет в малонаселенных, отдаленных и труднодоступных пунктах поможет преодолеть цифровое неравенство и обеспечить гражданам доступ к современным цифровым услугам, дистанционному образованию и телемедицине. Нацпроекты, инициированные президентом РФ Владимиром Путиным, стартовали в 2019 году. «}}],»tags»:[«интернет

https://национальныепроекты.рф/news/rossiyane-vyberut-kuda-provesti-mobilnuyu-svyaz-4g

К аннотации

Комсомольская правда (krsk.kp.ru), Красноярск, 12.10.2021

КРАСНОЯРЦЫ ОТПРАВЛЯЮТСЯ НА МАРС: БУМАЖНЫХ КВИТАНЦИЙ БОЛЬШЕ НЕ БУДЕТ!

Автор: Рябинина Татьяна

Разбираемся, как будет работать самая современная система расчетов за электроэнергию и в чем ее преимущества

Бумажные квитанции совсем скоро станут историей и уйдут из жизни людей так же, как ушли керосиновые лампы или примусы. Переход на электронный документооборот - дело ближайшего будущего, на которое работает Национальная **программа «Цифровая экономика Российской Федерации»**.

Электронная квитанция - это такой же законный документ как и бумажная, только удобнее и надежнее. В этом уже убедились более 100 000 абонентов Красноярскэнергосбыта и совсем скоро их станет еще больше!

Кто перейдет на электронную квитанцию в первую очередь, как можно сделать это самостоятельно прямо сегодня и в чем преимущество интернет-технологий перед бумагой?

Ответы на эти и другие вопросы вы найдете на сайте Красноярскэнергосбыта

https://www.krsk.kp.ru/daily/28342/4488070/

К аннотации

Вести.ru, Москва, 12.10.2021

НАЦПРОЕКТ «ЦИФРОВАЯ ЭКОНОМИКА». «ГОСУСЛУГИ. АВТО». НОВОЕ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ. УТРО РОССИИ

Пользователи платформы «Госуслуги Авто» получили доступ к новым сервисам - «делегирование» и «история автомобиля». Само приложение было запущено в пилотном режиме в сентябре в рамках нацпроекта «**Цифровая экономика**». И за первые несколько дней стало лидером по количеству скачиваний. Так какие возможности появились у автомобилистов? - давайте узнаем.

https://www.vesti.ru/video/2346938

К аннотации

Российская газета, Москва, 13.10.2021

КОД БЕЗ СЕКРЕТА

Автор: Медведев Юрий

Как университет из Санкт-Петербурга выиграл более 2 миллиардов рублей

Что такое «Университет открытого кода»? Как студенты вовлекаются в науку? Почему бизнес приходит в научные лаборатории? Об этом корреспондент «РГ» беседует с первым проректором, руководителем программы развития Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО) Дарьей Козловой.

Дарья Константиновна, еще пару лет назад научные проекты в 100 миллионов рублей воспринимались почти как сенсация. А теперь речь идет о сумме более двух миллиардов. Как вам удалось их получить?

ДАРЬЯ КОЗЛОВА: Мы их не получили, а выиграли в конкурентной борьбе в разных конкурсах. По программе «Приоритет-2030» мы оказались среди победителей, которым выделены самые крупные специальные гранты «Исследовательское лидерство» на научно-технологическое развитие. До конца будущего года сумма должна составить 994 миллиона рублей. А в рамках федерального проекта «Искусственный интеллект» нам на четыре года выделено 1,2 миллиарда рублей на открытие исследовательского центра «Сильный искусственный интеллект в промышленности». Ученые центра будут разрабатывать цифровые решения для разработки нефтегазовых месторождений, а также проектирования и эксплуатации сооружений в суровых условиях Арктики.

Понятно, что за миллиард развернулась серьезная борьба между лучшими вузами страны. Какие козыри вы выложили на стол требовательного совета, который возглавлял вице-премьер **Дмитрий Чернышенко**?

ДАРЬЯ КОЗЛОВА: Мы представляли программу развития на ближайшие 10 лет. А по сути, нашего гиперпрыжка от нынешнего университета, который завершил программу повышения международной конкурентоспособности «5-100», к «Университету открытого кода».

Что такое «открытый код»? Расшифруйте, пожалуйста.

ДАРЬЯ КОЗЛОВА: Перед вузом поставлена принципиально новая задача, которой раньше он практически не занимался. Речь о создании продукта, технологии, полного инновационного цикла научной разработки. Иными словами, она не должна оставаться в лаборатории, на стадии фундаментального исследования, ложиться на полку в виде отчета или статьи в журнале, а превращаться в конкретный продукт и доходить до потребителя.

Говоря попросту, идею надо доводить «от колбы до прилавка». О том, что у нас внедрение разработок идет очень трудно, что нет эффективной инновационной системы, говорят много лет и ученые, и политики. Вы взялись за сложнейшую задачу. И как будете ее решать?

ДАРЬЯ КОЗЛОВА: Разработан подробный план создания такой инновационной системы. Здесь важно подчеркнуть один принципиальный для вуза момент. Мы намерены выйти за его границу. Что имеется в виду? Понятно, что создать инновационные продукты своими силами мы не сможем. У нас нет и таких возможностей, и таких специалистов. Необходимы коллаборации с партнерами, прежде всего из бизнеса, привлечение к проектам новых людей. Для этого мы определили пять научно-технологических платформ по разным направлениям деятельности, через которые вовлекаем в наши проекты бизнес-партнеров.

В планах университета, например, создание квантовой сети для защищенной связи и поддержания работоспособности ключевых сфер экономики, повышение качества жизни с помощью новых технологий мониторинга и диагностики здоровья, развитие экосистемы цифровых личностей, так называемых аватаров, разработка автономной системы мониторинга железнодорожных магистралей «Шелковый путь» на основе дронов, смарт-сенсоров и т.д. И в каждый проект мы привлекаем бизнес-партнеров.

Говоря образно, вы намерены создать вокруг вуза бизнесожерелье. А у вас уже есть такой опыт? Ведь пока бизнес не удается вовлечь в нашу науку, его доля в финансировании исследований не более 30 процентов, в то время как в ведущих странах 70 - 80 процентов. А какова у вас доля внебюджетных средств?

ДАРЬЯ КОЗЛОВА: Годовой бюджет ИТМО в 2020 году составил около 9 млрд, из них 3,5 млрд получаем по госзаданиям на науку и образование, а все остальные зарабатываем, в том числе работая с бизнесом и выигрывая гранты. Что касается конкретных проектов, которые уже сейчас

реализует ИТМО, прежде всего, конечно, надо назвать создание первой магистральной квантовой сети, связывающей всю территорию РФ. Это новый уровень безопасной и быстрой передачи данных, основанный на стыке технологий фотоники и квантовой физики. Проект реализуется в коллаборации с РЖД.

Несколько крупных проектов связаны с так называемым сильным искусственным интеллектом. Как я говорила, наш совместный проект с «Газпромнефтью» победил в федеральном конкурсе. Важно отметить, что этот партнер вносит в проект около 300 миллионов рублей.

Вообще работы в области ИИ - наша сильная сторона. Уже есть готовые решения, которые потребители могут брать и внедрять у себя. Скажем, аватары или «цифровые инквизиторы» для борьбы с фейками и ложной информацией в соцсетях, системы мониторинга технологического состояния разных систем и т.д.

Но внедрение разработок, вклад в экономику - это лишь один из треков нашей программы. Назову еще несколько. Второй - научно-технологический прорыв. Понимаем, что, внедряя разработки, надо всегда иметь задел на будущее, вести поиск на самом крае фундаментальной науки. Генерировать новые знания, подтвержденные публикациями в высокорейтинговых изданиях. Поэтому будут созданы несколько топовых лабораторий, оснащенных современным оборудованием, привлекаться авторитетные ученые из России и других стран.

Привлекать лучших ученых - это здорово. А как увлечь наукой студента? У нас даже после аспирантуры защищаются около 12 процентов человек. Ссылаются на низкие стипендии, поэтому приходится подрабатывать, времени на науку не хватает.

ДАРЬЯ КОЗЛОВА: Думаю, мало кто знает, что в ИТМО самый большой в стране набор бюджетных магистрантов. Больше, чем, например, в МГУ и «Вышке». Их у нас больше, чем бакалавров. Это сложно, ведь мы своими бакалаврами не можем обеспечить магистратуру. Но мы осознанно пошли на эту модель. Почему? Потому что магистранты и аспиранты позволяют нам поддерживать высокий уровень науки. Готовить кадры, которые пойдут в наши научные лаборатории.

Приоткройте эту кухню подготовки.

ДАРЬЯ КОЗЛОВА: Здесь разные варианты. Скажем, для группы магистрантов мы разыгрываем по конкурсу грант на какую-то тему. Победители трудоустраиваются на инженерные и научные позиции, значит, им не надо подрабатывать вне вуза. Другой вариант, когда сами студенты предлагают инициативные проекты, чаще всего на стыке ИТ и ИИ. Мы эти проекты рассматриваем, победителей финансируем и тоже трудоустраиваем.

Третий вариант, когда магистрант присоединяется к одной из действующих лабораторий. Сегодня около 15 процентов наших студентов трудоустроены во время учебы. Хотим, чтобы к 2030 году их было 30 процентов. Это те, кто трудоустроен в самом вузе, а если посчитать наших партнеров, то эту цифру можно умножить на два. Пройдя такую систему подготовки, наши выпускники выйдут «в люди» с портфелем реализованных проектов. Им не надо готовиться к научной и инновационной деятельности. Они уже многое испытали через магистратуру, аспирантуру, предпринимательские инициативы.

Что такое сильный интеллект?

О проекте уникального Центра развития сильного искусственного интеллекта рассказывает директор национального центра когнитивных разработок ИТМО Александр Бухановский. ИТМО получит 1,2 млрд рублей на открытие исследовательского центра «Сильный искусственный интеллект в промышленности» в рамках федерального проекта «Искусственный интеллект». Что значит сильный? Может, у него высокий IQ?

Александр Бухановский | Это очень условное понятие, так как до сих пор нет четких общепризнанных определений, что же такое сильный ИИ. Но про IQ вы абсолютно правы. Можно сказать, что слабый ИИ имитирует простые когнитивные функции человека, например, обладает машинным зрением, может распознавать речь, совершать простейшие действия автопилота и т.д. Напротив, сильный ИИ способен выполнять высшие когнитивные функции - он имитирует творческую деятельность человека. Само собой, предварительно его надо основательно обучить, приобщить к той сфере, где ему предстоит работать. В нашем случае это разработка месторождений нефти и газа, в том числе и в суровых условиях Арктики. Важно уточнить, что из выделенных на проект 1,2 миллиарда рублей около 900 миллионов составляет федеральный грант, а около 300 миллионов вносит наш партнер «Газпромнефть».

Чтобы так расщедриться, то должен вам доверять. Быть уверен, что все получится.

Александр Бухановский | Верно. И у нас уже был положительный опыт работы с ними. Мы разрабатывали алгоритмы ИИ, которые решали для них различные задачи. Например, требовалось найти оптимальные режимы бурения или помочь в поиске новых месторождений по существующим аналогам. Это дало существенный экономический эффект. Но сейчас перед нами поставлена намного более сложная задача - перейти от фрагментарных решений к полному циклу. ИИ должен спланировать весь цикл освоения нового месторождения. От его поиска до ввода в эксплуатацию. Фактически создается «цифровой двойник» месторождения, который будет жить параллельно с объектом.

Но как создавать такого двойника, что называется, в чистом поле, когда о месторождении почти ничего не известно? Сплошные неопределенности. По сути, еще не начали копать, а ИИ уже должен представить планы развития. Причем в пространстве и во времени.

Александр Бухановский | Это и есть задача для сильного ИИ. Его привлекают, когда слишком много неопределенностей. Когда все ясно, ему делать нечего. Это не его уровень.

Честно говоря, трудно представить, что нефтяник может вот так довериться «двойнику», пусть и сильному, и по его плану осваивать месторождение. Риск огромен...

Александр Бухановский | Вы правы. Самый квалифицированный эксперт не может определить, правильно сильный ИИ решил задачу или нет. Но никто и собирается принимать его решения на веру. Чтобы заслужить доверие человека, ИИ обязан на пальцах объяснить, как он это сделал. Показать алгоритм, весь путь, как он пришел к ответу.

Значит, нейронные сети способны не только обучаться, решать сложнейшие задачи, но и объяснять, как они это сделали?

Александр Бухановский | К сожалению, как раз объясняют они плохо. Но с этим справляются другие механизмы, например, так называемые символьные модели на данных. Они плохо прогнозируют, но хорошо объясняют. Поэтому задача должна решаться одновременно двумя инструментами. Один будет прогнозировать, другой объяснять. Помимо создания системы принятия решений для планирования разработки нефтегазовых месторождений мы также работаем над ИИ, который будет проектировать морские объекты и сооружения на шельфе Арктики с учетом сложных климатических, географических условий.

Вашими работами заинтересовались знаменитые фирмы, в том числе и в сфере ИИ, в частности Siemens и Huawei. Готовы подключиться к проекту?

Александр Бухановский | Пока только скажу, что интерес есть. Детали раскрыть не могу.

АКЦЕНТ

Научная разработка не должна заканчиваться отчетом или статьей, а превращаться в инновацию, в конкретный продукт

Около 15 процентов студентов ИТМО сейчас занимаются в вузе наукой. Фото МАРГАРИТА ЕРУКОВА / ITMO.NEWS

Пройдя систему подготовки в магистратуре и аспирантуре, выпускники выйдут «в люди» с портфелем реализованных научных и инновационных проектов. Фото МАРГАРИТА ЕРУКОВА / ITMO.NEWS

К аннотации

РИА Новости, Москва, 12.10.2021

В СКОЛТЕХЕ СОЗДАДУТ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

МОСКВА, 12 окт - РИА Новости. На базе Сколтеха начнет работать исследовательский центр искусственного интеллекта. Основным направлением исследований станет создание технологий ИИ для оптимизации управленческих решений в целях снижения углеродного следа, сообщили в пресс-службе Сколтеха.

Отмечается, что внедрение разрабатываемых технологий позволит не только снизить выбросы парниковых газов, но и увеличить выручку компаний - оптимизировать затраты на применение ИИ и повысить привлекательность компаний в глазах акционеров. Предполагается, что трансфер разработанных технологий в индустрию, продвижение и развитие продуктов будет осуществляться компаниями при экспертной поддержке центра.

«В 2021 году Нобелевская премия по физике присуждена за исследования в области одной из наиболее горячих проблем современности, а именно «за физическое моделирование климата Земли, количественную оценку изменчивости и надежное прогнозирование глобального потепления». Это еще один аргумент в пользу того, что выбранное направление прикладных исследований центра крайне важно», - отметил руководитель исследовательского центра искусственного интеллекта Евгений Бурнаев.

В конкурсе на создание исследовательского центра искусственного интеллекта участвовали 36 организаций. Итоги отбора были оглашены на заседании рабочей группы, состоящей из 16 экспертов во главе с заместителем председателя правительства России **Дмитрием Чернышенко**.

Сколтех вошел в число шести российских университетов и научных центров, которые станут опорными точками развития технологии искусственного интеллекта и получат гранты до 1 миллиарда рублей. Общая сумма средств с учетом внебюджетного финансирования составит 7 миллиардов рублей.

«Цифровизация - необходимая вещь в современном мире. Через связанные с нею процессы мы делаем первый шаг к новому технологическому укладу. Сегодняшний успех Сколтеха неслучаен: 40% всех российских публикаций на мировых конференциях высшей категории А по искусственному интеллекту сделаны сотрудниками Сколтеха. С созданием нового центра по ИИ мы будем рады внести свой вклад в общее дело в интересах российского общества», - заявил ректор Сколтеха Александр Кулешов.

https://ria.ru/20211012/skoltekh-1754273970.html

К аннотации

ТАСС, Москва, 12.10.2021

ЧЕРНЫШЕНКО ПРЕДЛОЖИЛ ФОИВАМ ПРИСОЕДИНИТЬСЯ К ПРОЕКТУ ФНС ПО МАШИНОЧИТАЕМЫМ ДОВЕРЕННОСТЯМ

Вице-премьер также назвал электронный документооборот инструментом снижения рисков и затрат бизнеса

МОСКВА, 12 октября. /ТАСС/. Вице-премьер РФ **Дмитрий Чернышенко** рекомендовал федеральным органам исполнительной власти (ФОИВ) присоединиться к проекту Федеральной налоговой службы (ФНС) по машиночитаемым доверенностям на основе цифровой платформы распределенного реестра. Об этом ТАСС сообщили в аппарате вице-премьера по итогам заседания межведомственной рабочей группы по развитию электронного документооборота в хозяйственной деятельности.

«Бизнес в целях адаптации своих информационных систем ожидает от госсектора регулирования и создания инфраструктуры машиночитаемых доверенностей. Отмечу инициативу и опережающую работу в этом направлении Федеральной налоговой службы. Ими в короткие сроки был подготовлен и запущен пилотный проект по машиночитаемым доверенностям на основе цифровой платформы распределенного реестра. К пилоту присоединились операторы ЭДО, крупные банки и Федеральное казначейство. Считаю целесообразным ФОИВам изучить пилотный проект ФНС и присоединяться к его проведению для получения единой распределенной системы управления доверенностями и полномочиями», - приводятся в сообщении слова **Чернышенко**.

В аппарате вице-премьера отметили, что со следующего года участники взаимодействия начнут применять машиночитаемую доверенность при обмене электронными документами. Уточняется, что Минцифры РФ в начале октября выпустило три приказа, устанавливающие требования к доверенностям и формированию классификатора полномочий. В ближайшее время должны быть утверждены три постановления правительства, устанавливающие порядок предоставления машиночитаемых доверенностей, а также технические требования к порядку их хранения. Таким образом, будет сформирована вся необходимая нормативная правовая база.

В свою очередь глава ФНС Даниил Егоров сообщил, что в рамках эксперимента в роли владельцев узлов уже выступают девять операторов электронного документооборота, шесть банков и Федеральное казначейство, а в качестве клиентов более 500 организаций.

В декабре ФНС подведет итоги эксперимента и представит доклад в кабмин с предложениями по нормативному и организационному обеспечению технологии.

Об электронном документообороте

Вице-премьер также назвал электронный документооборот инструментом снижения рисков и затрат бизнеса.

«Электронный документооборот - инструмент снижения рисков и затрат бизнеса. В рамках рабочей группы при участии предпринимателей уже сейчас найдены решения по унификации подходов при разработке форматов электронных документов, определены правила общения в цифре между хозяйствующими субъектами. По последним исследованиям, крупные компании видят потребность в переводе на ЭДО, считая это крайне эффективным механизмом развития бизнеса и повышение производительности в целом», - отметил **Чернышенко**.

Вице-премьер добавил, что развитие электронного документооборота является одной из 42 стратегических инициатив, утвержденных правительством.

По словам **Чернышенко**, в Госдуму внесен законопроект, предусматривающий установление правил хранения электронных документов, создания дубликатов бумажных документов в электронной форме, а также конвертации электронных документов из одного формата в другой. Данный документ позволит систематизировать работу с уже созданными электронными документами и отказаться от хранения большого объема бумаги после перевода ее в цифру.

Уточняется, что в заседании приняли участие Даниил Егоров, замминистра цифрового развития, связи и массовых коммуникаций Олег Пак, представители МВД, Минздрава, Минкультуры, Минпромторга, других органов власти, общественных организаций и бизнес-сообщества.

https://tass.ru/ekonomika/12642987

К аннотации

Российская газета (rg.ru), Москва, 12.10.2021

ЧЕРНЫШЕНКО РАССКАЗАЛ О ПРЕИМУЩЕСТВАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ДЛЯ БИЗНЕСА

Автор: Кошкин Василий

Развитие электронного документооборота (ЭДО), которое является одной из 42 стратегических инициатив правительства, позволит снизить риски и затраты бизнеса. Об этом заявил вице-премьер **Дмитрий Чернышенко** во время заседания межведомственной рабочей группы.

«В рамках рабочей группы при участии предпринимателей уже сейчас найдены решения по унификации подходов при разработке форматов электронных документов, определены правила общения в цифре между хозяйствующими субъектами. По последним исследованиям, крупные компании видят потребность в переводе на ЭДО, считая это крайне эффективным механизмов развития бизнеса и повышение производительности в целом», - отметил **Чернышенко**.

По его словам, в Госдуму внесен законопроект о правилах хранения электронных документов, создания дубликатов бумажных документов в электронной форме, а также конвертации электронных документов из одного формата в другой. Это один из ключевых нормативных правовых актов, который позволит систематизировать работу с уже созданными электронными документами и позволит отказаться от хранения большого объема бумаги после перевода ее в цифру.

В рамках проведения реформы электронной подписи было введено понятие «машиночитаемая доверенность». Уже со следующего года участники взаимодействия начнут применять этот инструмент при обмене электронными документами.

«Отмечу инициативу и опережающую работу в этом направлении Федеральной налоговой службы. Ими в короткие сроки был подготовлен и запущен пилотный проект по машиночитаемым доверенностям на основе цифровой платформы распределенного реестра. К пилоту присоединились операторы ЭДО, крупные банки и Федеральное казначейство», - заявил вице-премьер.

«Создаваемая инфраструктура не только может в короткие сроки удовлетворить потребности участников информационного взаимодействия, но и позволит создать единую среду с актуальными сведениями о машиночитаемых доверенностях. Сейчас в рамках эксперимента в роли владельцев узлов уже выступают 9 операторов электронного документооборота, шесть банков и Федеральное казначейство, а в качестве клиентов более 500 организаций», - пояснил глава Федеральной налоговой службы Даниил Егоров.

https://rg.ru/2021/10/12/chernyshenko-rasskazal-o-preimushchestvah-elektronnogo-dokumentooborota-dlia-biznesa.html

К аннотации

Парламентская газета (pnp.ru), Москва, 12.10.2021

ГРАЖДАНЕ ПОЛУЧАТ ВОЗМОЖНОСТЬ ДЕЛАТЬ КОМПЛЕКСНЫЙ ЗАПРОС В ПФР

Пенсионный Фонд России (ПФР) разработал проект постановления, устанавливающий форму и порядок комплексного запроса гражданина, а также перечень госуслуг, предоставляемых на его основании. Документ опубликован на портале проектов нормативных правовых актов.

Сейчас в ПФР можно получить только одну услугу за одно обращение через личный кабинет на сайте фонда, при личном посещении отделения Пенсионного фонда или через МФЦ.

Проектом предлагается реализовать возможность запросить сразу несколько услуг. Подать комплексный запрос гражданин может лично или через законного представителя в территориальный орган ПФР либо по почте. При подаче запроса можно будет указать удобные способы информирования о результатах предоставления госуслуг ПФР.

Документом утверждается примерная форма комплексного запроса, порядок его приема должностным лицом и предоставления госуслуг на основании такого запроса, а также список госуслуг, которые ПФР предоставляет на основании комплексного запроса.

В частности, за один раз можно получить следующие услуги и информацию: подать заявление на установление страховых пенсий, накопительной пенсии и пенсий по государственному пенсионному обеспечению; получить данные о выплате пенсий, получить сведения о трудовом стаже; подать заявление на ежемесячную выплату на ребенка в возрасте от восьми до 17 лет.

Также можно подать заявление на установление дополнительного ежемесячного материального обеспечения за выдающиеся достижения и особые заслуги перед РФ; узнать о предоставлении государственной соцпомощи в виде набора социальных услуг; получить информацию о размере маткапитала или его оставшейся части и другие. Всего в перечень планируется включить 25 госуслуг.

В случае принятия документ вступит в силу с 1 января 2022 года.

К 2023 году в России должны перевести в электронный формат массовые социально значимые государственные и муниципальные услуги. Такое поручение в октябре прошлого года дал президент Владимир Путин.

До 1 декабря 2022 года кабмину поручено завершить централизацию информационных ресурсов ПФР, МВД, Росреестра и других органов власти, которые используются для подтверждения данных, предоставляемых заявителями для получения госуслуг. Также должен быть завершен переход на обработку межведомственных запросов и предоставление этих сведений в системе межведомственного взаимодействия в режиме реального времени.

Как сообщал глава Минцифры **Максут Шадаев**, к 2024 году около 300 государственных услуг будут представлены в новом формате.

https://www.pnp.ru/politics/grazhdane-poluchat-vozmozhnost-delat-kompleksnyy-zapros-v-pfr.html

К аннотации

Экспертный центр электронного государства (d-russia.ru), Москва, 12.10.2021

ФАС СОГЛАСОВАЛА НОВУЮ МЕТОДИКУ РАСЧЕТА ТАРИФА НА ДОСТУП ОПЕРАТОРОВ СВЯЗИ К ИНФРАСТРУКТУРЕ КОМПАНИИ «РОССЕТИ»

Во всех дочерних обществах группы «Россети» с конца 2021 года будет применяться согласованная ФАС методика расчета стоимости услуг на размещение волоконно-оптических линий связи (ВОЛС) на объектах сетевого комплекса, сообщает ФАС во вторник.

Методика соответствует требованиям антимонопольного законодательства, учитывает дополнительные затраты на обслуживание и ремонт ЛЭП, на которых размещены ВОЛС, расходы на обеспечение целостности линий связи при переустройстве сетевой инфраструктуры, говорится в сообщении «Россетей».

Методика устанавливает прозрачный механизм формирования тарифа, что позволит решить задачи по облегчению доступа телекоммуникационных компаний к объектам электросетевой инфраструктуры для размещения линий связи. Также это позволит оптимизировать капитальные и операционные затраты операторов на развитие и, как следствие, активнее решать задачи по ликвидации «цифрового» неравенства.

Также по поручению президента ФАС совместно с Минэнерго и Минцифры подготовлены изменения в Правила недискриминационного доступа к инфраструктуре для размещения сетей электросвязи, согласно которым устанавливается закрытый перечень расходов, включаемых в тариф на доступ. По мнению ФАС, принятые изменения обеспечат благоприятные условия для развития сетей связи по всей стране.

Напомним, в августе глава Минцифры **Максут Шадаев** отмечал, что что ключевым барьером для создания инфраструктуры связи вдоль дорог является стоимость подключения базовых станций к электричеству. Также энергетики зачастую пользуются своим монопольным положением, устанавливая иногда необоснованные тарифы на использование своей инфраструктуры операторами связи для подключения населенных пунктов и для строительства инфраструктуры мобильного Интернета, сказал министр.

Обсуждение вопроса об использовании операторами энергетической инфраструктуры обнаружило тогда разногласия Минцифры и вице-премьера Александра Новака (курирует энергетику), который утверждал, что в сетевых компаниях тарифы регулируются государством, и у них дополнительных источников для финансирования нет.

Справка

«Россети» - одна из крупнейших электросетевых организаций мира (в управлении - более 2,4 миллиона км ЛЭП). «Россети» предоставляют объекты для размещения ВОЛС сторонних компаний.

https://d-russia.ru/fas-soglasovala-novuju-metodiku-raschjota-tarifa-na-dostup-operatorov-svjazi-k-infrastrukture-kompanii-rosseti.html

К аннотации

Российская газета (rg.ru), Москва, 12.10.2021

РОСТРУД ПЛАНИРУЕТ РАЗВИВАТЬ ДИСТАНЦИОННЫЙ НАДЗОР

Автор: Манукиян Елена

Трудовые инспекторы будут проверять работодателей в том числе - дистанционно. Об этом рассказал руководитель Роструда Михаил Иванков.

«Сегодня цифровизация - это важнейший тренд, который затрагивает все сферы жизни и надзор не может быть в стороне. У нас много новых задач, в числе которых дистанционный надзор и дистанционное взаимодействие с работодателями», - сказал он на открытии VI Всероссийского форума инспекторов труда.

Роль дистанционного надзора возрастает в условиях цифровизации, подчеркнул замминистра цифрового развития **Максим Паршин**. По его словам, рынок трудовых отношений изменился. Так, стало возможным дистанционное заключение трудового договора, когда работодатель и работник не встречаются, но при этом между ними возникают трудовые отношения.

«Важно обеспечить соблюдение прав работника и работодателя в этом цифровом дистанционном взаимодействии», - пояснил замминистра.

Между тем, сегодня дистанционно работают около 3 млн россиян, следует из данных Минтруда. Как ранее отметил министр труда и социальной защиты Антон Котяков, до пандемии в России удаленно работали около 30 тысяч человек, а во время - до 11% от трудоспособного населения. Дистанционный формат занятости остается востребованным до сих пор.

https://rg.ru/2021/10/12/rostrud-planiruet-razvivat-distancionnyj-nadzor.html

К аннотации

ТАСС, Москва, 12.10.2021

ЭКСПЕРТ: ДОСТУП ОПЕРАТОРОВ СВЯЗИ К ЛЭП ПОЗВОЛИТ УСКОРИТЬ РАЗВИТИЕ РЫНКА СВЯЗИ

Операторы также нуждаются в отсутствии бюрократических проволочек и возможном сокращении издержек, отмечает глава TelecomDaily Денис Кусков

МОСКВА, 12 октября. /ТАСС/. Доступ телекоммуникационных компаний к линиям электропередачи (ЛЭП) для размещения на них волоконно-оптических кабелей, а также формирование группой «Россети» единой методики определения стоимости доступа позволят ускорить развитие рынка связи. Об этом ТАСС сообщил генеральный директор TelecomDaily Денис Кусков.

«Россети» заинтересованы в исполнении поручения президента по решению вопроса устранения цифрового неравенства», - говорит Кусков. При этом операторы нуждаются в облегчении процедур, отсутствии бюрократических проволочек и возможном сокращении издержек, добавляет он.

Вопрос развития инфраструктуры связи обсуждался на совещании президента РФ Владимира Путина с правительством 5 августа. В частности, министр цифрового развития, связи и массовых коммуникаций **Максут Шадаев** на нем заявил, что решение вопроса стоимости размещения кабелей связи вдоль линий электропередачи позволит увеличить число пользователей мобильного интернета в России с нынешних 80 млн до 100 млн человек уже к 2024 году.

Ранее «Россети» (работают в 81 регионе РФ, управляет сетевыми компаниями «Россети ФСК ЕЭС», «Россети Центр», «Россети Центр и Приволжье», «Россети Московский регион», «Россети Ленэнерго» и др.) сообщали ТАСС, что компания разрабатывает методику расчета цен для операторов связи при размещении ВОЛС на линиях электропередачи, которая будет применяться всеми компаниями группы с конца 2021 года.

В настоящее время единая методика на предоставление доступа утверждена и согласована с Федеральной антимонопольной службой (ФАС) РФ. Она будет учитывать дополнительные затраты на обслуживание и ремонт линии электропередачи, возникающие вследствие размещения на ней

ВОЛС, расходы на обеспечение целостности ВОЛС при переустройстве линии электропередачи. В дальнейшем индексация цены предполагается не выше уровня инфляции.

Кусков также добавил, что принятие новой методики поможет цифровому и технологическому развитию страны. При этом он пояснил, что говорить о конкретных показателях оптимизации и сокращении затрат операторами связи можно будет после ее публикации.

С этим мнением согласны в «Билайне» и Tele2. При этом в Tele2 подчеркнули, что основная проблема заключается в различной степени доступности сетевой инфраструктуры в зависимости от региона. «Важно, чтобы их [сетевых компаний] представители были заинтересованы в предоставлении операторам доступа к своим сетям для размещения ВОЛС, поэтому для эффективной работы требуется вовлечение и поддержка региональных властей», - сообщили там.

В свою очередь, в МТС ждут снижения действующих тарифов на размещение волоконно-оптических линий связи после формирования единой методики. «Единые тарифы позволят сделать процесс ценообразования более прозрачным, что также должно положительно сказаться на деятельности операторов», - подытожили в МТС.

https://tass.ru/ekonomika/12640405

К аннотации

3DNews.ru, Москва, 12.10.2021

ПРИНЦИПЫ OPEN SOURCE - КЛЮЧ К СОЗДАНИЮ ВЫСОКОНКУРЕНТНОГО IT-РЫНКА

Автор: Мироненко Владимир

В Москве 1 октября прошел саммит Russia Open Source Summit, посвященный вопросам развития и внедрения Open Source технологий в России, а также теме снижения зависимости отечественного IT-рынка от зарубежных вендеров.

Организатором саммита, который входит в деловую программу московского финала международного чемпионата ICPC (International Collegiate Programming Contest), выступил Российский фонд развития информационных технологий, а одним из партнеров стала компания Huawei.

В рамках саммита прошла панельная дискуссия «Корпорации как контрибьюторы: вклад корпораций в OS-проекты», в которой приняли участие **Максим Паршин**, заместитель министра цифрового развития, связи и массовых коммуникаций, Александр Павлов, генеральный директор РФРИТ, Эдуард Лысенко, министр правительства Москвы, Михаил Комков, вице-президент по развитию экосистемы Huawei в регионе Евразия, Владимир Рубанов, главный технический директор по разработке программного обеспечения R&D-подразделения Huawei в России, а также представители российских партнеров Huawei - ВТБ, Тинькофф, Сбер, Яндекса.

В ходе дискуссии Михаил Комков рассказал об опыте Huawei по внедрению технологий открытого программного обеспечения. Совершенствование собственной Open Source-платформы позволило компании выстроить независимую от сторонних производителей и монополистов рынка ПО стратегию развития. «Нам был необходим альтернативный путь, в противном случае, дальнейшее развитие компании было бы сильно осложнено», - сообщил Комков.

Он отметил, что современному российскому IT и телеком-бизнесу также необходимо развивать Open Source-технологии. «Ощутимая часть доходов IT-индустрии концентрируется в руках компаний - монополистов (в основном американских). Российским производителям это крайне невыгодно. Нам нужно создавать высококонкурентную среду», - подчеркнул вице-президент Huawei.

На вопрос о дальнейших планах Huawei на российском рынке Михаил Комков ответил: «Мы стремимся развивать независимую экосистему компании HarmonyOS, в том числе, привлекая к работе локальных разработчиков. Мы ценим совместный опыт и итоговые продукты нашего сотрудничества. Кроме этого, компания Huawei развивает партнерство с российским госструктурами. Одним из примеров такого партнерства является как раз проведение российского Open Source Summit».

https://3dnews.ru/huawei/news/1050917

К аннотации

Российское образование (edu.ru), Москва, 12.10.2021

СТУДЕНТЫ АЛТАЙСКОГО ПЕДУНИВЕРСИТЕТА ПРОВЕЛИ «УРОК ЦИФРЫ» В СЕМИ ШКОЛАХ РЕГИОНА

Студенты Алтайского государственного педагогического университета провели «**Урок цифры**» в семи школах региона. Об этом сообщает пресс-служба вуза.

В проекте участвовали будущие учителя информатики.

«Они узнали о возможностях использования учебно-методических материалов «**Урока цифры**» в работе учителя, которые в дальнейшем будут использовать в школах», - уточняется в информационном релизе.

Очередной онлайн-урок прошел с 27 сентября по 10 октября в рамках Всероссийского проекта «**Урок цифры**», он был посвящен теме «Искусственный интеллект».

Урок несет просветительскую направленность, способствует развитию цифровых навыков и раннему профессиональному самоопределению. Несмотря на технологическую направленность, урок можно было провести на любом предмете и в любом классе, в том числе и в начальной школе.

http://www.edu.ru/news/pedagogicheskoe-obrazovanie/studenty-altayskogo-peduniversiteta-proveli-urok-c/

К аннотации