ГАЗЕТА

МАЯК

№3/2019

РУБРИКА: КАПИТАНСКИЙ МОСТИК

ОБОРОТ «АКТИВА» ВТОРОЙ ГОД ПОДРЯД ПРЕВЫШАЕТ 1 МЛРД РУБЛЕЙ

Константин Черников,

генеральный директор компании «Актив», обозреватель

Прошлый год стал для компании годом значимых событий, результаты которых окажут долговременное влияние на стратегию и динамику развития «Актива». Завершена разработка новых продуктов, расширилась партнерская сеть, новых проектов стало больше — вот далеко не полный перечень наших достижений. Второй год подряд оборот компании превышает 1 млрд руб. За 2018 год бизнес вырос на 24,2%. Значительно возросло количество проектов в корпоративном сегменте, стали больше продавать смарт-карт. Технологически мы стали совершеннее. Компания в течение года продолжала расширять партнерское сотрудничество, как количественно, так и качественно.

Сформирован существенный задел на 2019, юбилейный для нас, год. Компании исполнится 25 лет. Мы остаемся верны себе и продолжаем как следует делать наше дело. Мы всегда делали ставку на высокое качество продукции и на стабильные отношения с клиентами и партнерами. И сегодня мы последовательно создаем флагманские решения в области информационной безопасности. Надеемся, что наши продукты, решения и подходы к обеспечению безопасности будут и дальше позитивно восприняты рынком.

Дмитрий Горелов,

коммерческий директор компании «Актив», обозреватель

Я считаю, что в продуктовой компании во главе угла должно быть построение команды. Без людей с уникальными компетенциями и навыками сложно сделать что-то действительно серьезное на рынке информационной безопасности. Второе — это создание, выращивание технологий, которые трудно повторить и которые долго проживут. И только потом финансовые вопросы, эффективное управление. Без коллектива и технологий остальное не работает. И что еще очень важно: люди не должны работать в вакууме, в хрустальном замке своего понимания рынка, потребностей клиентов и партнеров. «Нервные окончания» должны простираться далеко за пределы компании.

Любой серьезный продукт на рынке информационной безопасности — это как ребёнок, его нельзя быстренько вырастить и воспитать. Иногда трудно определить момент «зачатия» и даже рождения, но трудности взросления и поиска своего места в мире пропустить невозможно. Все наши значимые продукты «выстреливали» только после многих лет упорной работы и значимых инвестиций. И во всех наших флагманских продуктах есть влияние наших коллег и друзей, наших технологических и бизнес-партнеров. Если продолжить аналогию с ребенком, наши партнеры — это дяди и тети наших продуктов, они внесли неоценимый вклад в их воспитание. Пользуясь возможностью, хочу их поблагодарить за это.

БОРТОВОЙ ЖУРНАЛ

25 ЛЕТ НА РЫНКЕ

ДОХОД ВЫРОС НА 24% И ДОСТИГ 1,3 МИЛЛИАРДА РУБЛЕЙ

ПРОИЗВЕДЕНО 2,3 МИЛЛИОНА УСТРОЙСТВ В 2018 ГОДУ

КОМАНДА 160 ЧЕЛОВЕК

СОТНИ ПАРТНЕРОВ, МИЛЛИОНЫ ПОЛЬЗОВАТЕЛЕЙ

СТРАТЕГИЯ НА 3–4 ГОДА

- ✓ РАСШИРЕНИЕ ЗА СЧЕТ НОВЫХ НАПРАВЛЕНИЙ
- ✓ ВЫХОД НА ЗАРУБЕЖНЫЕ РЫНКИ
- ✓ АКТИВНАЯ РАБОТА С ГОСОРГАНАМИ
- ✓ УСЛУГИ И КОНСАЛТИНГ В ОБЛАСТИ ИБ
- ✓ ПОЛНЫЙ ПОРТФЕЛЬ РЕШЕНИЙ

РУБРИКА: ПОДЗОРНАЯ ТРУБА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ

Мария Грудева,
руководитель отдела маркетинговой аналитики компании «Актив»

Цифровизация и ИБ

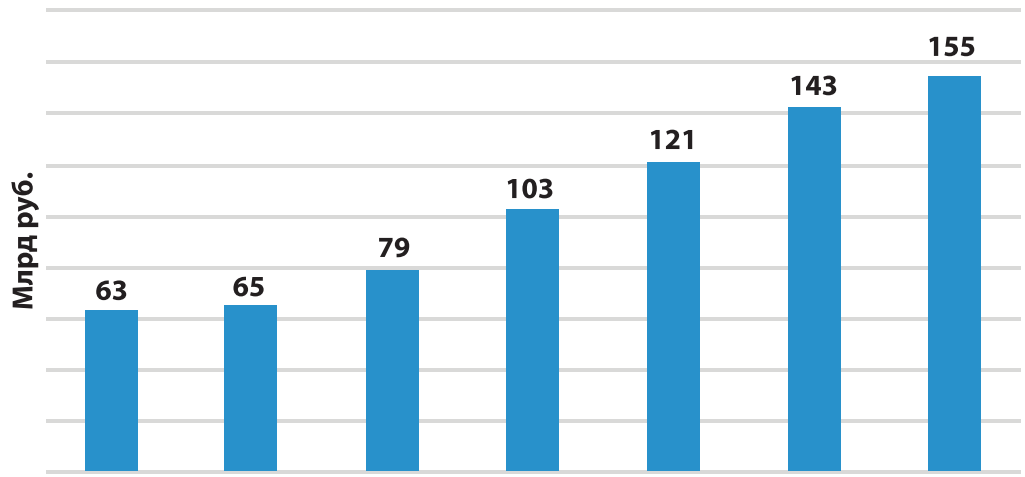
Мы живем в эпоху глобальной и интенсивной трансформации — изменяется все, начиная от привычных повседневных действий, заканчивая критически важными процессами на производстве и в бизнесе. Цифровизация и автоматизация — вот два основных тренда текущей трансформации. А чем больше оцифрованной, а значит, где-то хранимой информации, тем выше необходимость ее защиты. Одним из трендов цифровизации становится усиление роли информационной безопасности (ИБ). Это подтверждают и цифры. Рынок ИБ демонстрирует позитивную динамику. За последние 4 года он почти удвоился и, согласно прогнозам, рост продолжится в долгосрочной перспективе.

Идентификация и аутентификация как базис

Любая безопасность, будь то физическая или информационная, начинается с идентификации и/или аутентификации, роль которых сложно переоценить особенно при текущем уровне киберугроз. Идентификация и аутентификация — это первые шаги человека в системе и одновременно первые шаги к созданию и практике информационной безопасности.

Подробнее в материале Андрея Игнатова (стр. 3).

Диаграмма 1. Российский рынок информационной безопасности и темпы его роста

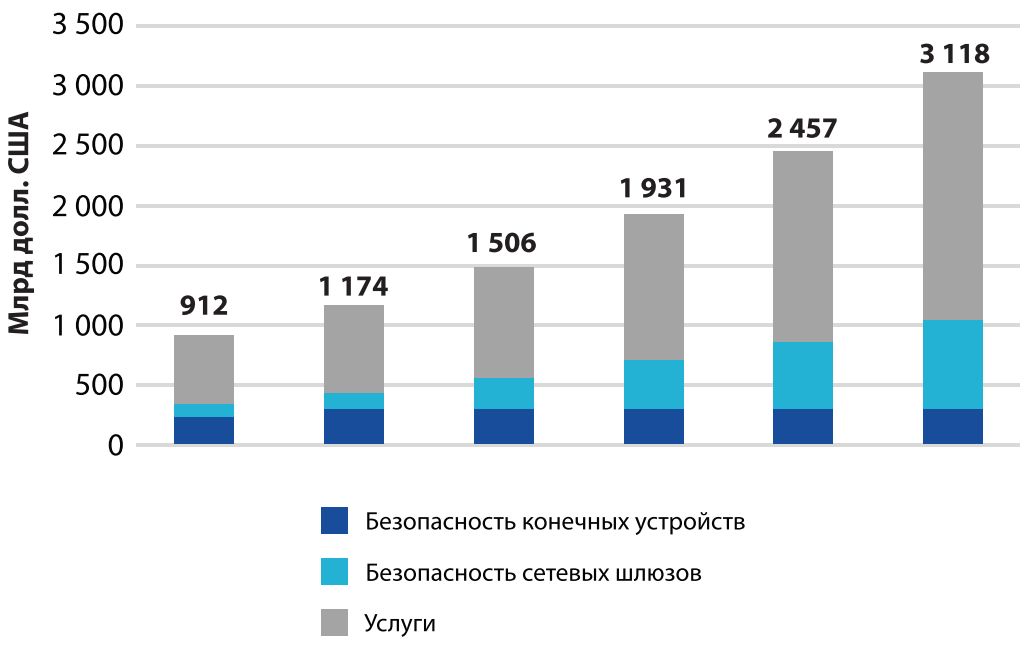


IoT и межмашинное взаимодействие

Прямо на наших глазах формируются новые рынки, которые насквозь пропитаны технологиями ИБ. Сегодня автоматизируются и протекают без участия человека множество критически важных производственных и бизнес-процессов, которые еще недавно невозможно было себе представить без участия людей. Речь идет об IoT-технологиях.

IoT постепенно охватывает все новые области, в которых существует и развивается общество. Те, кто сегодня тесно связан с проблемами кибербезопасности, полагают, что удавшиеся атаки на IoT-инфраструктуру в будущем могут привести к катастрофическим последствиям как для бизнеса, так и для людей. И финансовые убытки здесь — не самое страшное. Поэтому такие аспекты, как аутентификация, конфиденциальность, защита канала связи по-прежнему актуальны. Идентификация и аутентификация являются фундаментальным базисом в сфере IoT и межмашинного взаимодействия. По данным Gartner, на безопасность IoT в настоящее время в мире тратится $1,5 млрд, к 2021 году эта сумма увеличится вдвое.

Диаграмма 2. Мировой рынок безопасности интернета вещей



ЭКСПЕРТНОЕ МНЕНИЕ

Алексей Лазарев,
ведущий менеджер проектов компании «Актив»

Рынок интернета вещей находится на начальной стадии своего развития. Это дает нам шанс заранее заложить основы для обеспечения безопасности в данной сфере, разработать ключевые принципы и методы. Недостаточное или несвоевременно оказанное внимание к вопросам безопасности может дорого обойтись. Поэтому необходима тщательная проработка методологии обеспечения всесторонней защиты. Это особенно актуально, если принять во внимание возможности и потенциал сегодняшних злоумышленников.

Диаграмма 3. Российский рынок услуг безопасности по сегментам

Рост сегмента услуг

Уже сегодня сегмент услуг занимает бÓльшую часть мирового рынка безопасности и с течением времени будет расти интенсивнее других.

Согласно данным IDC, российский рынок услуг безопасности будет полностью следовать тренду мирового рынка без отставания. На текущий момент эксперты оценивают его объем почти в $80 млн, разделяя на три сегмента и прогнозируя наиболее интенсивный рост сегменту консалтинговых услуг. Основным драйвером для него служит дефицит квалифицированных кадров в области безопасности.

Выводы

Накладывая два тренда друг на друга (критическая важность идентификации и аутентификации и рост сегмента услуг в области безопасности) можно прогнозировать, что рынок, на котором сегодня работает компания «Актив» и ее партнеры, будет развиваться интенсивно, и драйвером дальнейшего роста послужит развитие направления услуг — интеграция, консалтинг, сопровождение, обучение как в области безопасности, так и конкретно в сфере идентификации и аутентификации.

Именно услуги будут составлять основу бизнеса в не столь отдаленной перспективе при сохраняющейся актуальности аппаратных средств идентификации и аутентификации. Уже сегодня и компания «Актив», и многие ее партнеры начали постепенное, но уверенное движение по этому пути.

ИССЛЕДОВАНИЕ:

ЧТО БУДЕТ С АУТЕНТИФИКАЦИЕЙ И ПАРОЛЯМИ?

Андрей Игнатов,
Менеджер по продуктам компании «Актив»

ДЕЛИМСЯ С ВАМИ РЕЗУЛЬТАТАМИ ИССЛЕДОВАНИЯ «THE STATE OF STRONG AUTHENTICATION 2019» И ДЕЛАЕМ ВЫВОДЫ.

Начиная с 2017 года резко возрос процент использования строгой аутентификации.

С ростом числа уязвимостей, затрагивающих традиционые решения для аутентификции, организации усиливают свою защиту. Количество предприятий, использующих двухфакторную аутентификацию с использованием криптографии, утроилось с 2017 года для потребительских и увеличилось почти на 50% для корпоративных приложений.

Тут мы видим иллюстрацию поговорки «пока гром не грянет — мужик не перекрестится». Пока эксперты предупреждали о ненадежности паролей, никто не торопился внедрять двухфакторную аутентификацию. Как только пароли начали красть — внедрение 2ФА резко ускорилось.

Пароли находятся на грани вымирания.

За прошедший год зависимость от паролей значительно снизилась как для потребительских, так и для корпоративных приложений (с 44% до 31%, и от 56% до 47% соответственно).

Но в целом по-прежнему преобладают ранее скомпрометированные и уязвимые способы аутентификации.

Для пользовательской аутентификации около четверти организаций используют одноразовые пароли из SMS вместе с секретными вопросами. В результате для защиты от уязвимости приходится внедрять дополнительные средства защиты, что увеличивает затраты.

В эпоху фишинга злоумышленники могут использовать корпоративную электронную почту для мошенничества, чтобы обманным путем получить доступ к данным, учетным записям (с соответствующими правами доступа) и даже чтобы убедить сотрудников выполнить денежный перевод на его счет. Поэтому учетные записи корпоративной почты и порталов должны быть особенно хорошо защищены.

Google усилил свою защиту, внедрив строгую аутентификацию.

Google опубликовал отчет о внедрении двухфакторной аутентификации на базе криптографических ключей безопасности по стандарту FIDO U2F, сообщив о впечатляющих результатах. По данным компании, против более чем 85 000 сотрудников не было проведено ни единой фишинговой атаки.

РЕКОМЕНДАЦИЯ

Используйте строгую аутентификацию на предприятии.

Ряд систем являются наиболее привлекательными целями для преступников. К ним относятся такие внутренние и подключенные к Интернету системы, как, например, бухгалтерская программа или хранилище корпоративных данных. Строгая аутентификация не дает злоумышленникам получить несанкционированный доступ, а также позволяет точно установить, кто именно из сотрудников совершил злонамеренную деятельность.

Криптографические токены и смарт-карты надежно защищены PIN-кодом. Перед началом работы пользователь подключает свой токен к устройству с помощью USB, Bluetooth, NFC или через SmartCard Reader. Далее, он вводит PIN-код, который разблокирует доступ к защищенной памяти токена и позволяет выполнить аутентификацию. PIN-код не передается на сервер, а значит не может быть перехвачен при передаче. В отличие от пароля он может быть простым и лёгким для запоминания. Этот PIN-код является фактором знания, что позволяет достаточно просто организовать двухфакторную аутентификацию с помощью криптографических токенов / смарт-карт.

Таким образом, практически любой способ аутентификации имеет изъяны, за исключением криптографических токенов.

Прочитать полную версию статьи можно в нашем блоге на Habr. Подписывайтесь:

https://habr.com/ru/company/aktiv-company/

Ждем ваших комментариев!

НОВИНКИ NEW

«ЖЕЛЕЗНАЯ» ЗАЩИТА АККАУНТОВ АУТЕНТИФИКАТОРАМИ РУТОКЕН

В 2019 году компания «Актив» начала серийное производство аппаратных аутентификаторов: генераторов одноразовых паролей Рутокен OTP и токенов стандарта U2F (Universal 2nd Factor) — Рутокен U2F.

Рутокен OTP и Рутокен U2F являются действительно безопасными средствами для входа в личные кабинеты и учетные записи web-сайтов и порталов. Специалисты Минкомсвязи и зарубежные эксперты из Национального института стандартов и технологий США (NIST) подтверждают это, указывая на ненадежность SMS, и рекомендуют не использовать пароли и SMS для входа на ресурсы. По сравнению с программными генераторами одноразовых паролей, аппаратные аутентификаторы работают, даже если в телефоне сел аккумулятор, при плохом качестве мобильное связи, когда извлечена сим-карта, случилась поломка или телефон забыт или украден.

Не важно, какой именно аутентификатор будет использоваться: защитив Рутокеном самые важные аккаунты (к примеру, основную почту, к которой привязаны остальные учетные записи) — можно быть уверенным, что никто и никогда не получит доступ к учетной записи без этого токена. Благодаря второму фактору — владению токеном — сам пароль от учетной записи можно сделать сильно проще, так как перебор или перехват такого пароля ничего не даст злоумышленнику.

Аппаратный аутентификатор — устройство размером с обычную флешку, которое удобно носить с собой и которое подключается к компьютеру через USB-порт. С точки зрения пользователя, использовать аутентификатор очень просто, так как нет необходимости в инфраструктуре открытых ключей (PKI), сертификатах и дополнительном дорогостоящем программном обеспечении.

РУТОКЕН U2F

Рутокен U2F работает по открытому стандарту универсальной двухфакторной аутентификации, разработанному FIDO Alliance, где первый фактор — пароль от аккаунта, а второй — обладание аппаратным токеном с ключом. Ключ с аппаратного токена не может быть извлечен, поэтому он не может утечь через интернет. Один токен может использоваться для доступа к различным сайтам.

Использование универсального второго фактора можно настроить как на популярных интернет-сервисах и платформах: сервисы Google (gmail, drive, cloud и т.п); Youtube; Facebook; LastPass; Dropbox; Evernote; WordPress; Github, так и в корпоративных публичных и закрытых сервисах.

РУТОКЕН OTP

С генератором одноразовых паролей Рутокен OTP для входа на сайт нужно не только знать логин и пароль, но и предъявить уникальный одноразовый пароль, который вводится автоматически в экранную форму при нажатии кнопки на Рутокен OTP. Не нужно больше запоминать и вводить вручную длинные пароли.

Одноразовый пароль создается с помощью криптографических алгоритмов на основе секретного ключа и счетчика количества нажатий на кнопку генерации паролей. Злоумышленник не может получить этот секретный ключ, поскольку он не может быть перехвачен или считан из устройства Рутокен.

Использование генераторов одноразовых паролей удобно для однократной аутентификации и единого входа (Single Sign-On), доступа в дистанционный банк-клиент и популярные системы управления сайтами.

Ввиду своей простоты использования генераторы одноразовых паролей чаще всего используются в корпоративном секторе и особенно в сегменте SOHO.

НОВЫЙ РУТОКЕН ДЛЯ ГАДЖЕТОВ С РАЗЪЕМОМ USB TYPE-C

В 2019 году компания «Актив» запустила серийное производство токенов с разъемом USB Type-C.

В компьютерной индустрии USB-C — новый тренд, потому что это не только усовершенствованный разъем для зарядки, но и способ отказа от большого набора специфических портов в пользу одного универсального разъема.

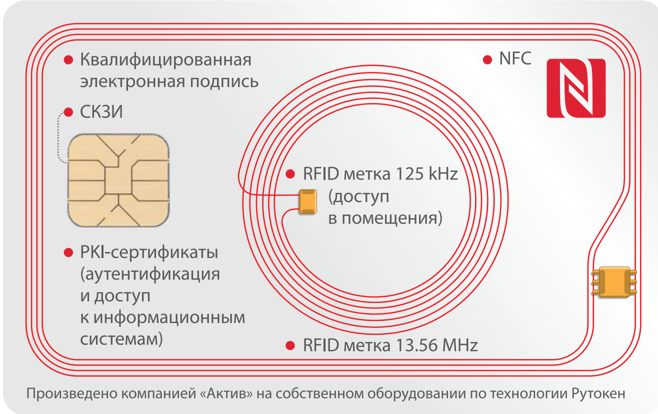
Рутокен ЭЦП 2.0 и Рутокен ЭЦП PKI — первые токены с разъемом USB Type-C на российском рынке аутентификации и электронной подписи.

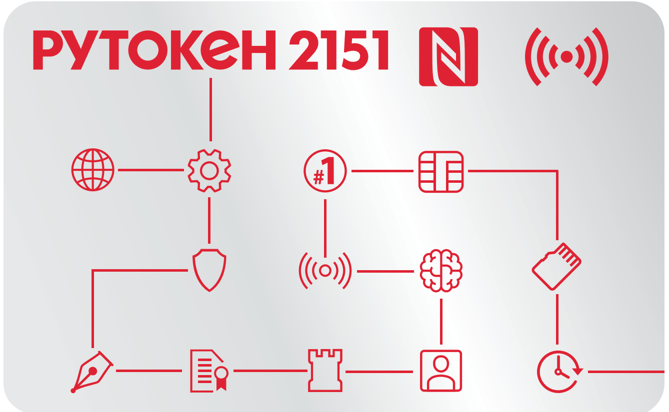
Рутокены с интерфейсом USB Type-C отлично справляются со своими традиционными задачами: Рутокен ЭЦП 2.0 безопасно хранит и подписывает квалифицированной электронной подписью, а Рутокен ЭЦП PKI — решает проблемы парольной защиты, защищает документы и удаленный доступ в корпоративной среде.

Рутокен ЭЦП с USB Type-C подсоединяется без переходников или USB-хабов к компьютерам iMac и Mac mini последнего поколения, ноутбукам MacBook Pro, MacBook Air и MacBook, а также к другим планшетам, смартфонам и ноутбукам иных производителей, оснащенных разъемом USB Type-C или Thunderbolt 3*.

НОВИНКА

ДУАЛЬНАЯ СМАРТ-КАРТА РУТОКЕН 2151 С ВОЗМОЖНОСТЬЮ РАБОТЫ ПО NFC





За 5 лет, с момента запуска в производство первого в России беспроводного мобильного средства электронной подписи Рутокен ЭЦП Bluetooth мы накопили богатый и уникальный опыт применения мобильной подписи. В начале 2019 года инженеры и разработчики компании «Актив» придумали еще один способ работы с подписью на мобильных устройствах — новую дуальную смарт-карту Рутокен 2151.

За исключением возможности работы карты по NFC в остальном карточки сохранили полную функциональность USB-токенов и смарт-карт Рутокен ЭЦП 2151 и так же как и они, построены на отечественном микроконтроллере MIK51 производства «Микрон».

Беспроводной канал NFC позволяет получить полноценное рабочее место на телефоне или планшете на Android с возможностью электронной подписи документов, хранящихся на мобильных устройствах, по новому ГОСТ Р 34.10 2012.

Для этого достаточно приложить смарт-карту к задней поверхности телефона или планшета, где обычно находится считыватель NFC — и за считанные секунды на смарт-карту передается электронный документ, подсчитывается подпись и возвращается обратно в приложение.

Посмотрите минутное видео, как это работает:

Для удобства встраивания дуальных смарт-карт в прикладные приложения разработчиками компании «Актив» созданы превосходные инструменты: комплект разработчика SDK и каркасное приложение мобильного банка в исходных кодах с уже реализованными модулями обработки подключения карты и подписания платежных документов.

С их помощью очень легко разработать новые и доработать существующие системы мобильного электронного документооборота для сотрудников, работающих вне офиса с мобильных устройств на Android. КриптоАРМ, ЭОС mobile и приложение Directum Solo — уже работают с NFC-картами Рутокен.

РУБРИКА: КАЮТ-КОМПАНИЯ

ЧТО ЗВЕЗДЫ ГОВОРЯТ ПРО ИЮНЬ

ОВЕН
У вас будет шанс увеличить доход и заработать во второй декаде месяца.

ТЕЛЕЦ
Постарайтесь этот месяц посвятить карьере, он обещает порадовать в материальном плане.

БЛИЗНЕЦЫ
Новые знакомства обещают быть полезными и приятными.

РАК
Месяц пройдет под знаком информации. Вы легко будете вступать в любые коммуникации.

ЛЕВ
Переговоры с партнерами и деловые встречи будут проходить с выгодой для вас.

ДЕВА
В первый месяц лета вас будут привлекать новые идеи и проекты.

ВЕСЫ
Финансовое положение значительно улучшится.

СКОРПИОН
Вы сумеете расширить свой бизнес, заключив сделки с партнерами.

СТРЕЛЕЦ
Повысить свой доход вы сможете с помощью совместных проектов.

КОЗЕРОГ
Вы будете с легкостью завязывать деловые знакомства и находить общий язык с разными людьми.

ВОДОЛЕЙ
В рабочих моментах наступает благоприятный период, когда вы будете хорошо ориентироваться в любой незнакомой ситуации.

РЫБЫ
В деловых отношениях с партнерами будет царить гармония и полное взаимопонимание.

ЯПОНСКИЙ КРОССВОРД

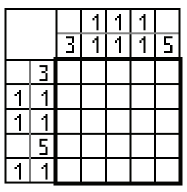
Column clues (35 columns, top to bottom):

																						2												
					2					2												1								2	2			
				3	1	2		2	2	1		2	2	2		2	2	2	2		2	1	2							2	2			
		3	2	5	1	5	2	5	2	3	2	1	5	1	2	5	1	1	5	2	5	1	5	2			2	2	2	2	2	2		
7	9	3	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	13	13	2	2	2	2	2	2	11	11

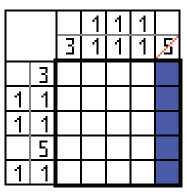
Row clues (15 rows, left to right):

											0
											23
											33
										4	10
									3	2	2
	2	3	1	1	3	1	1	3	2	2	2
2	1	1	2	1	1	1	1	1	2	2	2
		2	1	1	3	1	1	2	3	2	2
2	3	1	1	1	2	1	1	1	2	2	2
2	1	1	1	1	1	1	1	3	2	2	2
									3	2	2
										4	10
											33
											23
											0

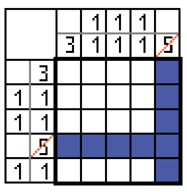
1 Имеем исходный японский кроссворд. Для простоты его размеры 5х5 клеток.



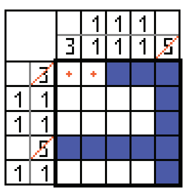
2 Обратим внимание на большие числа. Сверху стоит число 5. Поскольку в столбце 5 клеток, то весь столбец можно закрасить.



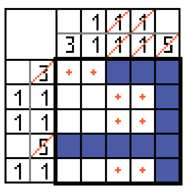
3 Слева тоже есть число 5. Закрасим целиком четвертую сверху строчку кроссворда. Не забываем зачеркивать отработанные числа.



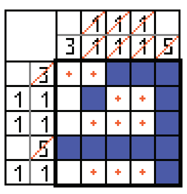
4 Слева нашли число 3. Видим, что крайняя правая клетка строки закрашена, то закрашиваем 2 соседние, а остальные помечаем пустыми.



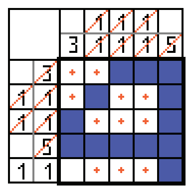
5 3 и 4 столбцы имеют по две одиночные клетки. И они уже закрашены, значит помечаем остальные клетки как пустые. И зачеркиваем числа.



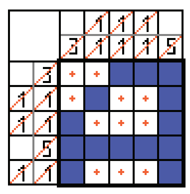
6 Второй столбец имеет закрашенную клетку и 2 пустые выше. Закрашенные клетки не соприкасаются, значит, красим клетку из второй строки.



7 Автоматически получили готовую вторую строку, а в третьей — единственный вариант. Закрашиваем и эту клетку.



8 Последний шаг — красим последнюю клетку. Зачеркиваем тройку из первого столбца и две единицы из пятой строки. Кроссворд разгадан!



Газета «Маяк», № 3/2019. Зарегистрировано в службе по надзору в сфере связи, информационных технологий и массовых коммуникаций «Актив». Для лиц старше 16 лет. Распространяется бесплатно.

Главный редактор: Виктория Чирва
Над номером работали: Андрей Игнатов, Мария Грудева, Анастасия Птуха, Кирилл Мещеряков, Павел Анфимов
Дизайн и верстка: Сергей Дементьев

Тираж: 1000 шт.
Дата выхода в свет: 4.06.2019
Отпечатано в типографии «MaxPress»

Адрес редакции: 115088, Москва, Шарикоподшипниковская ул., 1
Тел.: +7 495 925-77-90
www.aktiv-company.ru, www.rutoken.ru, www.guardant.ru

https://habrahabr.ru/company/aktiv-company/
https://www.facebook.com/aktivsoft/