CIS
Современные Информационные Системы
№ 3 (9) / 2019

В «Сколково» объявили победителей

Стр. 4

Cybersecurity Challenge

Электронная подпись со смартфона

Стр. 64

Дарья Верестникова, коммерческий директор компании SafeTech

Витаем в облаках

Стр. 60

Какие облачные решения выбрать для бизнеса?

Криптозащита информации

Стр. 54

Актуальные вопросы законодательства

ПРЕДИСЛОВИЕ

СКОЛКОВО

ОПЫТ

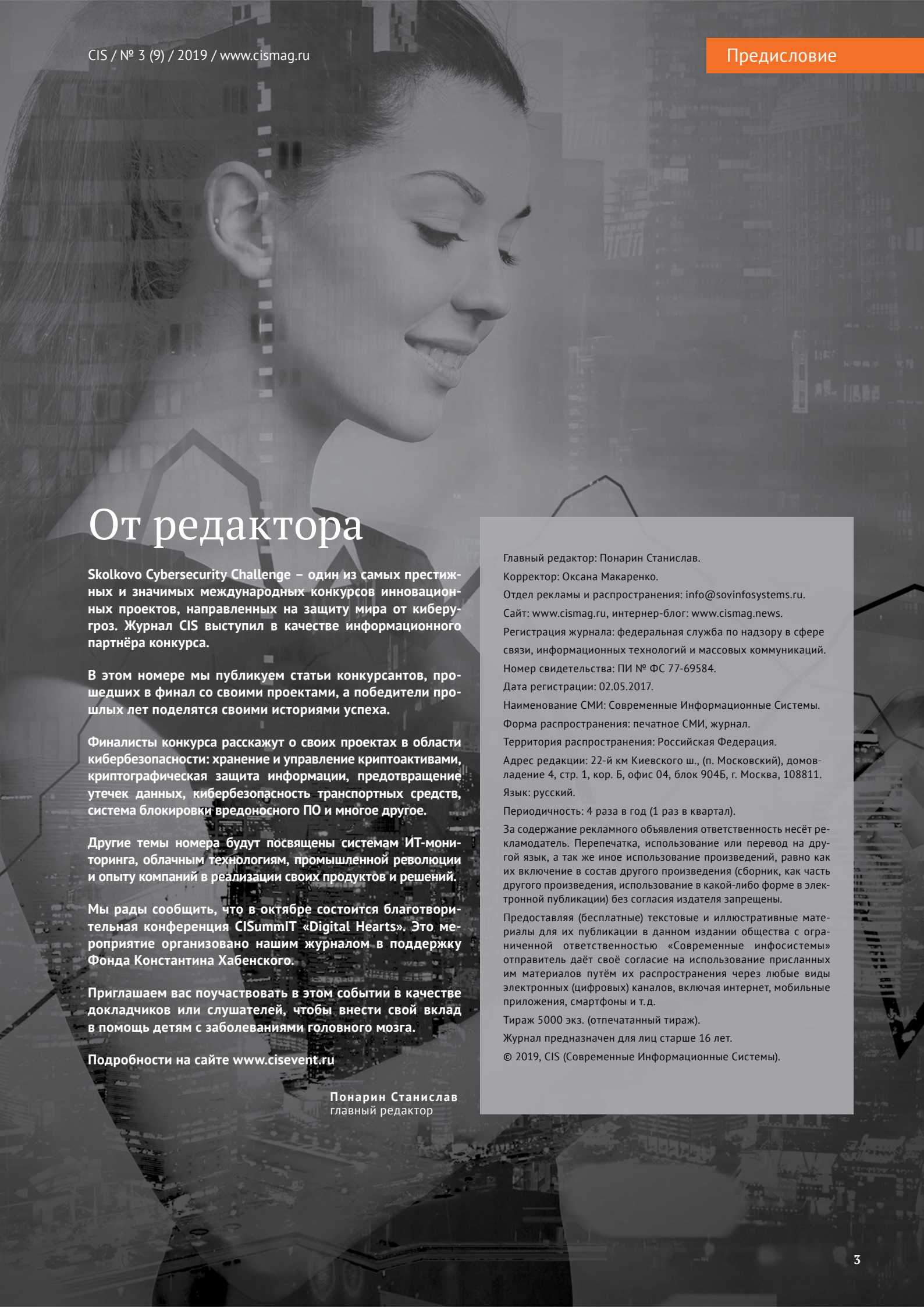
РЕШЕНИЯ

КУЛЬТУРА

ФОТООТЧЁТ

КРОССВОРД

КАЛЕНДАРЬ



От редактора

Skolkovo Cybersecurity Challenge – один из самых престижных и значимых международных конкурсов инновационных проектов, направленных на защиту мира от киберугроз. Журнал CIS выступил в качестве информационного партнёра конкурса.

В этом номере мы публикуем статьи конкурсантов, прошедших в финал со своими проектами, а победители прошлых лет поделятся своими историями успеха.

Финалисты конкурса расскажут о своих проектах в области кибербезопасности: хранение и управление криптоактивами, криптографическая защита информации, предотвращение утечек данных, кибербезопасность транспортных средств, система блокировки вредоносного ПО и многое другое.

Другие темы номера будут посвящены системам ИТ-мониторинга, облачным технологиям, промышленной революции и опыту компаний в реализации своих продуктов и решений.

Мы рады сообщить, что в октябре состоится благотворительная конференция CISummIT «Digital Hearts». Это мероприятие организовано нашим журналом в поддержку Фонда Константина Хабенского.

Приглашаем вас поучаствовать в этом событии в качестве докладчиков или слушателей, чтобы внести свой вклад в помощь детям с заболеваниями головного мозга.

Подробности на сайте www.cisevent.ru

Понарин Станислав
главный редактор

Главный редактор: Понарин Станислав.

Корректор: Оксана Макаренко.

Отдел рекламы и распространения: info@sovinfosystems.ru.

Сайт: www.cismag.ru, интернер-блог: www.cismag.news.

Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Номер свидетельства: ПИ № ФС 77-69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

Адрес редакции: 22-й км Киевского ш., (п. Московский), домовладение 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.

Язык: русский.

Периодичность: 4 раза в год (1 раз в квартал).

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

В «Сколково» объявили победителей конкурса Cybersecurity Challenge

В рамках конференции Startup Village 2019 состоялся финал международного конкурса инновационных проектов в сфере кибербезопасности Skolkovo Cybersecurity Challenge.

«Мы запустили конкурс Cybersecurity Challenge для того, чтобы найти высокотехнологичные и перспективные стартапы в отрасли информационной безопасности. Многие проекты конкурса уже являются резидентами ИТ-кластера «Сколково», а многие становятся резидентами по результатам совместной работы после конкурса. Приятно видеть, что интерес к теме информационной безопасности каждый год только растёт. Если на прошлый конкурс нам подалось около 70 стартапов, то сейчас таких заявок было уже больше сотни. Большинство проектов имеют весомый бекграунд в части фундаментальных и прикладных исследований, это темы искусственного интеллекта для автоматизации различных процессов ИБ, искусственные иммунные системы, поведенческая аналитика и пр. Думаю, решения многих участников конкурса мы сможем увидеть в лидерах рынка через пару лет».

С уважением, Михаил Стюгин, руководитель направления «Информационная безопасность» Кластера информационных технологий Фонда «Сколково».

В Skolkovo Cybersecurity Challenge приняли участие индивидуальные исследователи, независимые команды, технологические компании, малые и средние инжиниринговые компании и представители научного сообщества.

Заключительный этап конкурса включал три трека:

- финал по основному конкурсу Skolkovo Cybersecurity Challenge;
- финал совместного конкурса с Фондом перспективных исследований (ФПИ) «Лучшее решение в области создания интеллектуальной технологии поведенческого анализа сетевых устройств»;
- финал совместного конкурса с компанией «Цезарь-Сателлит» по поиску идей и технологий в направлениях видеоаналитики и телеметрии в задачах безопасности.

В жюри вошли руководители Сбербанка, Почты России, компаний «Ростелеком», «Инфосистемы Джет», «Лаборатория Касперского», «ИнфоТеКС», «Норникель», InfoWatch и Фонда перспективных исследований.

«Считаю очень важной поддержку создания новых технологических решений в области кибербезопасности, развития передовой экспертизы и компетенций. В этом году для участия в конкурсе было подано более 140 заявок. В условиях высокой конкуренции звёздным составом жюри были отобраны лучшие проекты. Несмотря на то, что конкурс Skolkovo Cybersecurity Challenge прошёл в четвёртый раз, в числе конкурсантов было много новых решений, и это особенно приятно. В мире, где киберугрозы представляют критические риски для растущего количества бизнесов, мы считаем необходимым поддерживать новые решения, чтобы в России появлялось всё больше успешных компаний в области кибербезопасности, примеры которых вдохновляли бы следующее поколение».

Сергей Ходаков, директор по операционной работе Кластера информационных технологий Фонда «Сколково».

Победители Skolkovo Cybersecurity Challenge:

- 1-е место – **«Автовизор»**, комплекс обеспечения защиты автомобиля от несанкционированных атак;
- 2-е место – **«АТРЕТЕК-ТАФС»** (резидент «Сколково»), самообучающаяся система выявления мошенничества на финансовых рынках;
- 3-е место – **UserGate** (резидент «Сколково»), высокопроизводительные UTM-решения (англ. Unified threat management, шлюз безопасности).

Все победители могут претендовать на грант в размере 5 млн рублей (при условии прохождения определённых процедур в соответствии с регламентами Фонда «Сколково»).

В специальных номинациях от партнёров конкурса победителями стали:

- от **Почты России – Security Vision Incident Response Platform [IRP]** (резидент «Сколково»), система управления полным жизненным циклом инцидентов информационной безопасности с автоматическим реагированием на них;
- от компании **«Инфосистемы Джет»** – платформа **AppSec. Hub** для автоматизированного управления и контроля сквозных процессов разработки защищённого программного обеспечения;
- от компании **InfoWatch – «АТРЕТЕК-ТАФС»** (резидент «Сколково»), самообучающаяся система выявления мошенничества на финансовых рынках;
- от **ПАО «Ростелеком»** – платформа **Bishop**, решение для динамического анализа защищённости мобильных приложений;
- от компании **«ИнфоТеКС» – H1CORE**, системы безопасности домашних сетей и устройств «Интернета вещей».

Группа компаний «Цезарь Сателлит», индустриальный партнёр Кластера информационных технологий Фонда «Сколково» и ключевой поставщик рынка телематических услуг и комплексной безопасности на территории РФ, в рамках стратегии технологического развития также учредила конкурсную номинацию. Лучшие решения планируется внедрить в компании для повышения качественного уровня и расширения сервисов и услуг.

В треке совместного конкурса с «Цезарь Сателлит» победили:

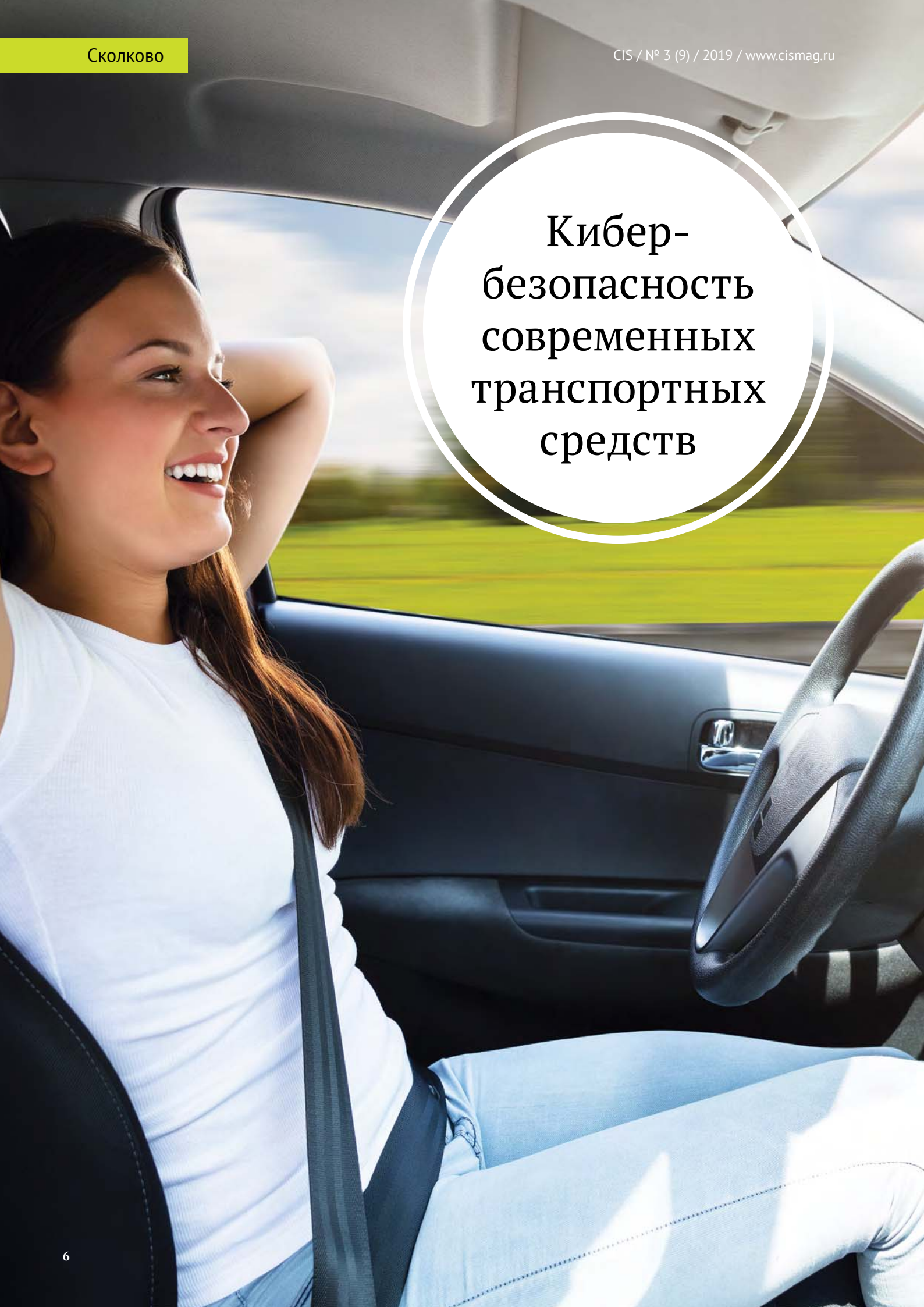
- 1-е место – **«БИЭЙ»**, проект «Технологические решения по оценке вероятности происхождения тревожного события для объектов охраны с использованием технологий Big Data, ML и AI»;
- 2-е место – **«Орион Система»**, проект «Видеоаналитика Orion»;
- 3-е место – **Академия ФСО РФ**, проект «Подход к маркированию текстовых электронных документов».

Победители получили от компании денежные призы: 100 тыс. рублей – первое место, 75 тыс. рублей – второе место и 50 тыс. рублей – третье место.

В треке Фонда перспективных исследований финалистами стали ЗАО «АСТ», АО «Инфосистемы Джет» и Санкт-Петербургский государственный университет аэрокосмического приборостроения. Победители будут определены позже.

Журнал CIS «Современные Инфосистемы» стал информационным партнёром мероприятия и решил опубликовать доклады победителей конкурса Skolkovo Cybersecurity Challenge в этом номере.

Кибер-безопасность современных транспортных средств



В статье рассмотрены вопросы обеспечения кибербезопасности современных транспортных средств с целью поиска путей нивелирования киберугроз. Проводится анализ современного состояния угроз информационной безопасности современных автомобилей в контексте широкого проникновения мультимедиа систем и тенденции к внедрению технологий беспилотного управления автомобилем.

Авторами проанализированы и приведены материалы ряда исследований, посвящённых актуальным проблемам кибербезопасности автомобилей. На основании проведённого анализа авторы приходят к выводам об актуальных способах защиты современных и перспективных автомобилей от киберугроз в рамках современного положения дел в сфере кибербезопасности автомобильного движения.

Введение

В век стремительно развивающихся технологий, сопровождающийся увеличением роли информации в жизни общества, весьма значимое место занимают вопросы обеспечения безопасности информационно коммуникационных технологий, к основным рискам которых относятся кибератаки. Угрозы кибератак становятся фактически повсеместны в связи с широким распространением информационных технологий и всеобъемлющего их проникновения во все сферы жизни человека. Такие угрозы зачастую выходят за рамки кибербезопасности и несут в себе угрозу кибер-физического характера.

В настоящее время все системы управления современных автомобилей становятся более автономными. Почти всеми системами в автомобиле управляет электроника: двигатель, тормоза, круиз-контроль, подушки безопасности, климат-контроль, стеклоочистители, зажигание и т.д. Без сложной электроники невозможно было бы реализовать всё это. Однако современные системы автомобиля имеют серьёзный недостаток – значительное количество программных и аппаратных уязвимостей. Несанкционированное вмешательство в обмен данных по шине управления может быть выполнено как со стороны шины управления (например, подключение «жучка»), так и со стороны мультимедийных систем и систем связи (USB-порт, Bluetooth, Wi-Fi, 3G и т.д.).

Стоит отметить, что подобные инциденты уже не являются историями из будущего или чем-то отдалённым от ежедневной жизни. Хакеры уже сегодня наносят определённый ущерб транспортным системам, ставя под угрозу не только жизнь водителей, но и безопасность общественного транспорта.

На сегодняшний день актуальность таких угроз становится всё выше и выше. К сожалению, кибератаки на различные объекты жизнедеятельности уже становятся привычным делом и в традиционных сферах (банковское дело, промышленные системы, транспортные системы) уже воспринимается как объективно существующий риск с высоким значением. Ещё одной негативной тенденцией является расширение деятельности террористических организаций, которые начинают практиковать, в том числе и кибертерроризм. Так, если автопроизводители вовремя не обеспокоятся безопасностью транспортных средств, то террористам достаточно будет провести кибератаку на транспортную систему, для того чтобы направить автобус или грузовик в толпу или в подземный переход, как они пока делали, предположительно, только физическим путём.

Как и любая система передачи данных и управления, шина контроллеров автомобиля имеет свои уязвимости. Исследования в данной области выявили целый ряд возможных атак на шину управления, направленных на вторжение и оказание воздействия на контроль транспортного средства. Основные системы автомобиля, подверженные угрозе вторжения, – передача, безопасность транспортного средства, комфорт, информационные/развлекательные и телематические системы.

В настоящее время нет системы, которая была бы способна защитить шину передачи данных транспортных средств от вторжения и вмешательства на аппаратном уровне. Принимая во внимание вышесказанное, можно сделать вывод об актуальности использования такого рода устройств для обеспечения безопасности шин управления.

Как и любая система автоматического управления, сеть контроллеров автомобиля (CAN, LIN-шина) имеет свои уязвимости. Соответственно, способ и система для защиты шины передачи данных транспортного средства от атак-вторжений и ошибок весьма желательны. Особенно это актуально для VIP лиц.

В соответствии с исследованием Navigant Research»s Energy Technologies к 2020 году на земле в активном использовании будет не менее 188 млн так называемых «подключённых» автомобилей, которые могут быть объектами кибератак, а к 2025 году 15% всех машин будет иметь полные или частичные функции

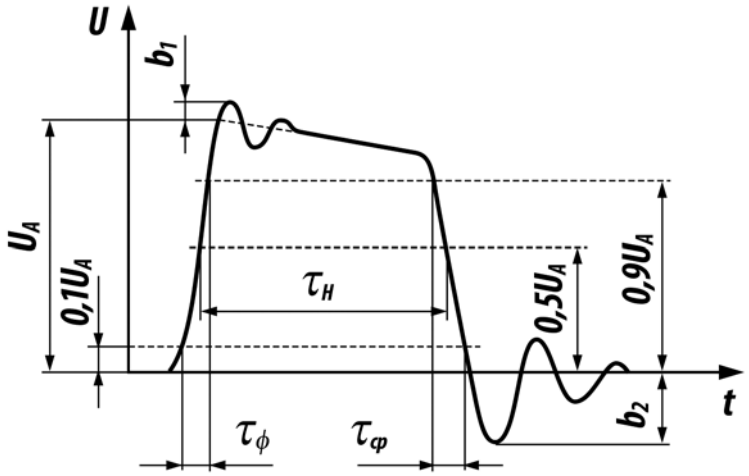


Рисунок 1. Форма искажённого прямоугольного сигнала в шине CAN.

автопилота. В последние годы наблюдается активное распространение технологий помощи водителю Advanced Driver Assist Systems (ADAS), особенно таких как автономное экстренное торможение автомобиля (Automatic Emergency Braking, AEB) и удержание автомобиля на полосе (Lane departure warning system LDW). Хакерам доступна возможность управления этими системами удалённо, что ставит под угрозу жизни участников дорожного движения.

Национальная администрация безопасности дорожного движения США (NHTSA) в 2016 году выпустила в этой связи весьма тревожный предупреждающий документ. В этом документе рассказывается о зафиксированных попытках взлома автомобилей и используемых при этом каналах связи. Американскими чиновниками на публичном уровне было продекларировано, что доступ к CAN может быть получен через модем сотовой связи, по Wi-Fi, по каналу Bluetooth и даже через USB подключение к мультимедиа системе автомобиля. Всё это очевидным образом свидетельствует о факте уязвимостей к кибератакам и уже существующих автомобилей без масштабных систем компьютерного управления (в том числе без доступа центрального компьютера к рулевому управлению и тормозной системе).

На международном уровне продолжается работа по разработке и пересмотру стандарта ISO 26262 Функциональная безопасность автомобиля (Automotive Functional Safety), а объединение рабочих групп ISO (21434) и SAE (J3061) приступило к разработке стандарта информационной безопасности автомобиля (Automotive Cyber-Security Standard). Этот стандарт будет содержать описание процессов, обеспечивающих информационную безопасность, что поможет компаниям обеспечить кибербезопасность транспортных средств на протяжении всего жизненного цикла продукции. В то же время эта тема обсуждается в Целевой группе ООН по вопросам кибербезопасности в ОТА в рамках группы WP29/ITS-AD (неофициальная рабочая группа по интеллектуальным транспортным системам – автоматизированное вождение (ITS/AD), 2017). Столь высокий уровень внимания к проблематике предполагает появление в настоящем и ближайшем будущем ряда технических решений, обеспечивающих кибербезопасность автомобилей.

В рамках проведённых исследований нами было подготовлено программно-аппаратное решение, которое позволяет обеспечивать кибер-физическую безопасность современных транспортных средств как частных автомобилей, так и грузовых и иных коммерческих машин (в том числе автобусов). В его основе лежит технология спектрального анализа CAN-шины, позволяющая отслеживать и нивелировать любые угрозы процессу нормальной работы автомобиля.

Спектральный анализ автомобильной шины CAN производится с целью определения изменения активного и реактивного сопротивления шины, что позволяет сделать вывод о типе и конфигурации нагрузок на ней (количество устройств, отклонение от стандартов и норм).

Данный метод позволяет выполнять измерение в момент непосредственного обмена сообщениями по шине. Данные в шине CAN передаются в виде цифровых последовательностей, которые на уровне сигналов имеют форму меандра (последовательные прямоугольные импульсы). При различных резистивных параметрах шины форма сигнала искажается и становится отличной от прямоугольной (рис. 1), где на передних фронтах формируются выбросы b1, а на задних – завалы b2. Длительность и амплитуда этих выбросов и завалов даёт возможность для расчёта активного и реактивного сопротивления сети. Однако непосредственный анализ формы выбросов и завалов цифрового сигнала в шине CAN требует высокой частоты дискретизации АЦП (сотни МГц) и, соответственно, высокой производительности микропроцессор.

Однако оценивать различные изменения сигнала во времени более удобно в спектральной области, тем более если сигнал имеет периодический характер. Цифровой сигнал в шине CAN имеет характеристику, приближённую к периодической, это значит, что, имея даже более низкую частоту дискретизации АЦП (десятки МГц), можно уловить изменения фронтов сигнала, произведя достоянное накопление отсчётов во времени и произведя их анализ в частотной области. Суть анализа спектра заключается в исследовании амплитудных соотношений высокочастотной части спектра: чем более искажённую форму имеет цифровой сигнал, тем выше амплитуда высокочастотного спектра (рис. 2, 3).

Обозначенная технология запатентована и имеет свою практическую реализацию, которая на сегодняшний день и в перспективе имеет возможность обеспечивать кибер-физическую безопасность автомобилей. При этом особенности технологии в том, что благодаря разработанному устройству может быть обеспечена безопасность

Рисунок 2. Форма сигнала при двух устройствах на шине CAN.

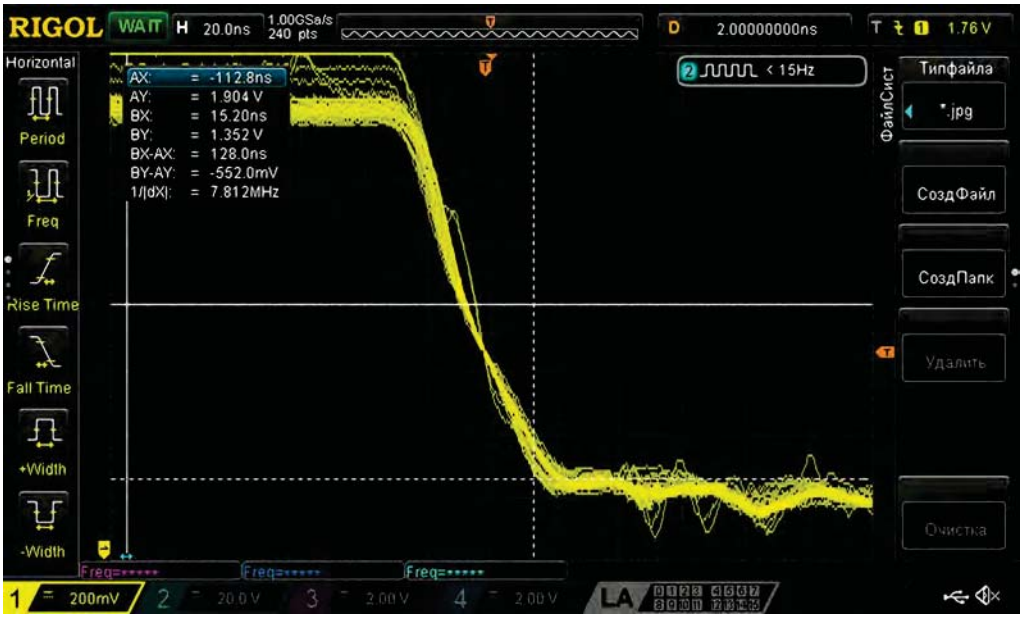
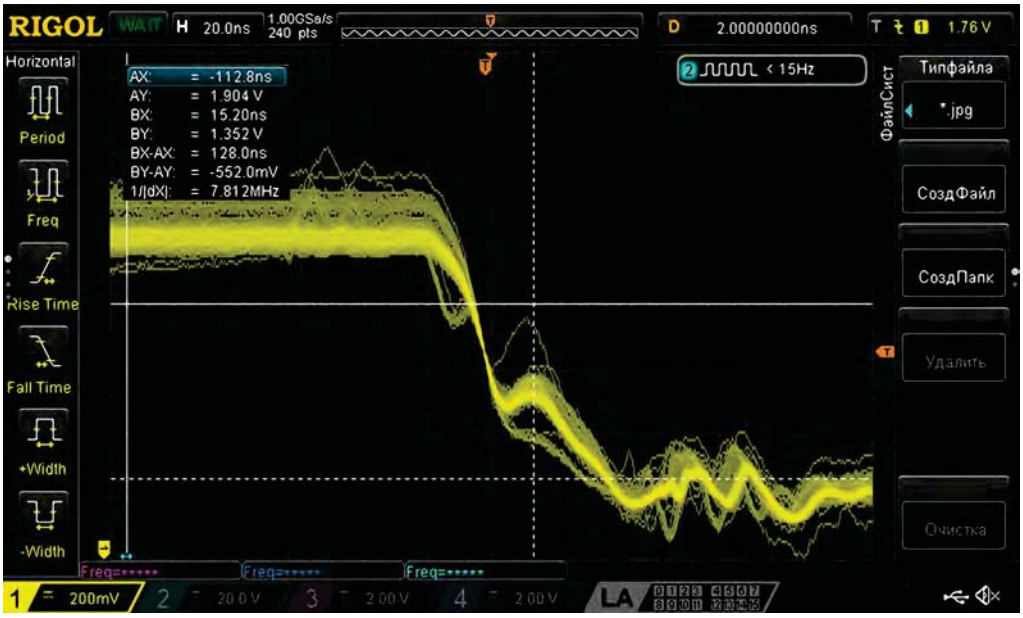


Рисунок 3. Форма сигнала при трёх устройствах на шине CAN.



не только современных автомобилей, в которые данное устройство внедряется на этапе разработки и сборки, но и машины, уже находящиеся в эксплуатации довольно значительное количество времени. Благодаря простоте использования разработанного нами устройства возможно обеспечение безопасности значительной части автомобилей, произведённых позднее 2007 г.

В заключение представляется важным отметить, что найденное в ходе исследований обозначенной проблематики эффективное решение может в полной мере обеспечивать кибербезопасность транспортных средств на современном этапе. Представляется, что внедрение систем кибербезопасности для транспортных средств в целом должно стать логичным продолжением системной работы по повышению безопасности дорожного движения в рамках страны и мира. Отмечается также, что существует возможность установления требований по установке систем кибербезопасности транспортного средства для операторов автопарков (операторы такси и каршеринга, операторы общественного транспорта и так далее), что в свою очередь вполне соотносится с работой, которая ведётся в России по обеспечению безопасности критической информационной инфраструктуры.

AutoVisor

Михайлов Дмитрий Михайлович
д.т.н., доцент, Руководитель ГК «Инжиниринговые технологии»

esc-center.ru

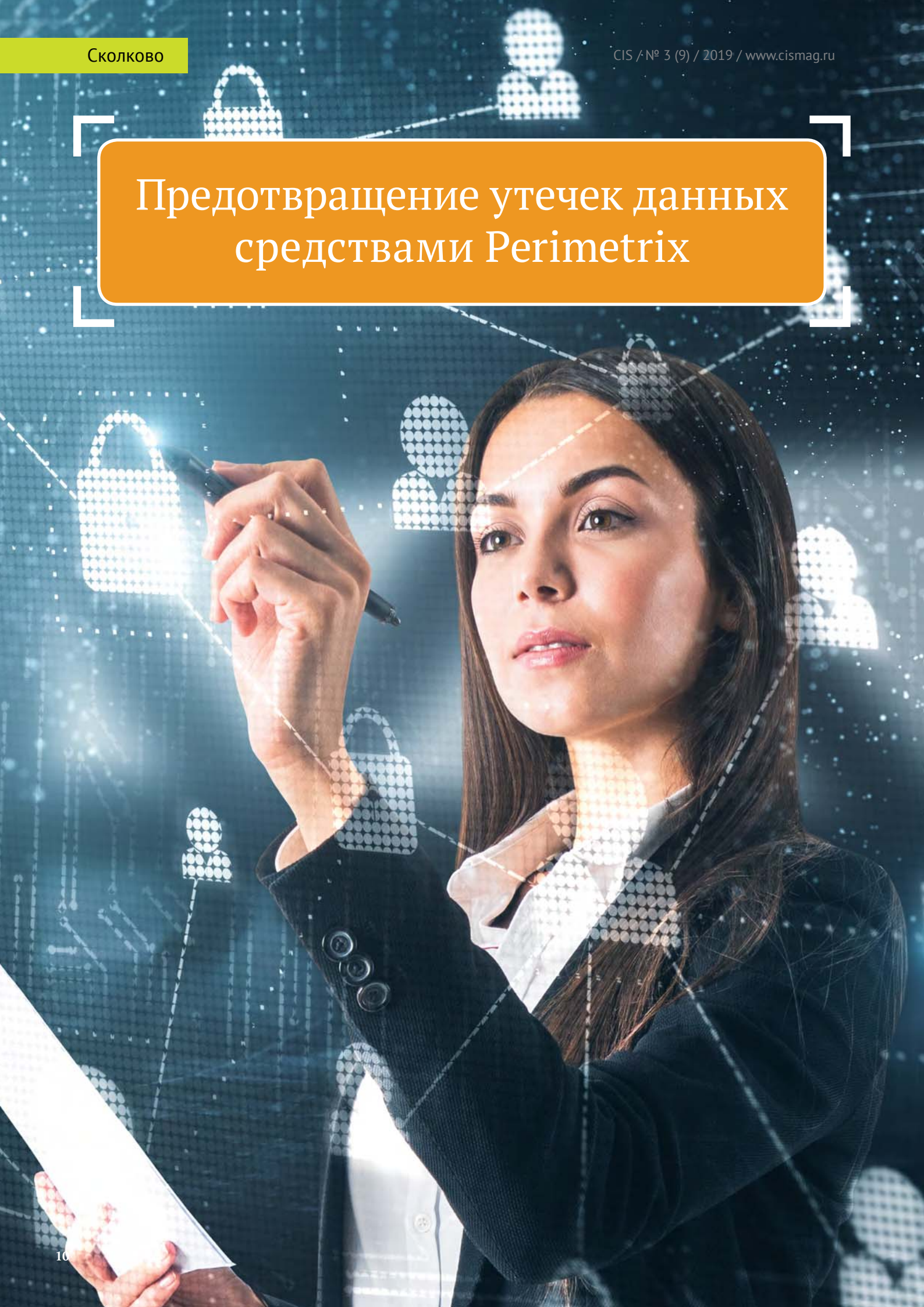
Педанов Владимир Александрович
Генеральный директор «Технологии безопасности транспорта»

autovisor.sg

Багров Сергей Валерьевич
Руководитель развития бизнеса AutoVisor Pte. Ltd.

autovisor.sg

Предотвращение утечек данных средствами Perimetrix



Главный источник конкурентоспособности бизнеса сегодня – эффективное использование передовых технологий, создающих дополнительную ценность для клиентов, генерирующих новые потоки доходов.

Для компаний, осознавших это, безопасность и конфиденциальность данных значит больше оптимизации затрат, поскольку становится драйвером дохода и роста бизнеса. Постоянные утечки данных заставляют потребителей с сомнением относиться к бизнесам, пренебрегающих киберугрозами. Пытаясь защитить свои данные, компании приходят к пониманию, что основанный на защите сетевого периметра подход к безопасности **«Perimeter-based security»** (PBS) уже не соответствует современным угрозам.

С позиции PBS утечка происходит в тот момент, когда конфиденциальные данные покидают периметр компании. Поэтому системы предотвращения утечек первоначально фокусировались на контроле над каналами, по которым информация может покинуть корпоративный периметр. Но в цифровой организации подход PBS не способен защитить от нарушителей, действующих внутри «доверенной» сети, противостоять угрозам, связанным с использованием технологий цифровой мобильности (BYOD, коворкинг, работа дома и т.п.).

Отличным от «Perimeter-based security» и более перспективным является информационно-центричный подход к обеспечению безопасности (**«Data-centric security»**, DCS), при котором фокус контроля переносится с содержимого каналов передачи данных на действия, выполняемые с данными. Следование такому подходу позволяет идентифицировать и защитить ценные информационные активы, строго контролировать доступ к конфиденциальным данным, обеспечить эффективное выполнение бизнес-процессов компании внутри защищённой цифровой экосистемы на протяжении всего жизненного цикла данных. DCS позволяет в полной мере использовать преимущества развитой логики ABAC (Attribute-Based Access Control), формулировать политики безопасности в терминах, понятных бизнес-владельцам данных. Использование DCS требует высокой степени осознанности бизнес-процессов и квалифицированного менеджмента информационной безопасности.

Наиболее популярные сегодня технологии, решающие задачу предотвращения утечек данных двумя различными способами – это DLP и IRM.

DLP-решения традиционно являются одним из компонентов подхода PBS. Блокировка нежелательной передачи данных на основе анализа содержимого каналов, реализуемая DLP, с определённой вероятностью позволяет предотвратить утечку, но может и помешать нормальному выполнению бизнес-процессов. Зачастую основной задачей, возлагаемой на DLP, становится мониторинг с целью проведения расследований. Основные ограничения DLP-систем связаны с невозможностью отслеживания всех возможных каналов утечки и форматов данных, а также с необходимостью соблюдения норм информационного права. Кроме того, при использовании DLP возникают серьёзные проблемы при контроле шифрованного трафика, запароленных архивов, файлов, хранящихся в облаках и передаваемых контрагентам. Самое сложное при внедрении DLP – определение данных, которые необходимо защищать, и выявление всех возможных каналов утечки. Кроме того, приходится ограничивать использование программ, протоколов и типов данных, которые не обрабатываются DLP-решением.

В основе решений класса **IRM (Information Rights Management)**, позволяющих контролировать действия с данными, сочетание нескольких технологических приёмов: неотрывная классификация контента, шифрование защищаемых данных, обязательная аутентификация пользователя и гранулярные политики безопасности, определяющие допустимые действия с данными в зависимости от полномочий пользователей.

Благодаря использованию IRM неавторизованные пользователи не смогут распорядиться защищаемой информацией, при этом все попытки доступа протоколируются. С помощью IRM можно не только запретить или разрешить доступ пользователя к файлу, но обеспечить контроль того, как именно пользователи работают с ценными цифровыми объектами – документами, письмами, чертежами, изображениями и т.д.

С учётом сегодняшнего ландшафта угроз информационной безопасности речь не идёт о выборе между DLP и IRM, наоборот, требуется их совместное применение в рамках подхода «Data-centric security». Интеграция DLP и IRM – передовой метод борьбы с утечками данных. DLP – по-прежнему хорошее решение для мониторинга коммуникаций, опознавания конфиденциального содержимого с последующим оповещением или блокировкой передачи данных. IRM – для обеспечения безопасного документооборота, в который вовлечено ограниченное число ответственных сотрудников организации и, возможно, внешних контрагентов.

Если использование DLP в российских компаниях уже стало обычной практикой, то готовность к внедрению IRM показывают лишь флагманы цифрового бизнеса. В ближайшем будущем нас ждёт рост количества инсталляций IRM-систем и с учётом импортозамещения российским производителям этого ПО открываются возможности роста продаж.

Perimetrix SafeSpace™ – комплексное программное решение управления электронными данными, позволяющее обеспечить конфиденциальность и целостность электронной информации ограниченного доступа при её хранении, обработке и передаче. В основе решения – концепция управления жизненным циклом информации ограниченного доступа и уникальная технология контроля перемещений электронной информации. Решение позволяет обеспечить защищённое исполнение пользователем и приложениями рабочего процесса, ограничивая при этом всю другую, не относящуюся к выполнению бизнес-процесса, активность пользователей, приложений и процессов. Применение политик «режима» хранения, обработки и передачи классифицированных данных происходит динамически в момент доступа к классифицированным электронным данным. Программный комплекс сертифицирован ФСТЭК России (Сертификат №3658 от 15.11.2016 г. действителен до 15.11.2019 г., соответствие РД, ТУ и НДВ4). Внедрение Perimetrix SafeSpace™ позволяет выполнять требования №149ФЗ от 27.07.2006 «Об информации, информационных технологиях и защите информации» и №98ФЗ от 29.07.2004 «О коммерческой тайне»..

Андрей Рыбин,
директор по развитию PERIMETRIX

PERIMETRIX

*Компания **PERIMETRIX** – российский разработчик информационно-центричных систем безопасности.*
www.perimetrix.ru

Как следует подходить к хранению криптоактивов?

Получение потенциальных выгод от инноваций в финансовых услугах в значительной степени зависит от нормативно-правовой среды. Конечно же, получение выгод от новых технологий должно быть сначала разрешено регуляторами. Если говорить о технологиях на основе blockchain и криптоактивах в частности, то в коридоре от 10-15 лет мир адаптирует свою нормативную базу и откроет возможности для широкого их применения. И следующей проблемой станут особенности по непосредственному использованию, хранению и управлению, криптоактивов.

Владение активом влечёт за собой элемент риска, и хранение криптоактивов не является исключением, хотя непосредственные угрозы несколько отличаются от тех же у традиционных активов. Главная особенность – полная ответственность пользователя за сохранность закрытых ключей. Ключи могут быть похищены злоумышленником как непосредственно из кошелька пользователя, так и биржи подвержены хакерским атакам. С другой стороны, ключи могут быть потеряны самим пользователем. В таком случае доступ к активам также будет утрачен полностью. Частным случаем такого исхода событий может быть смерть владельца криптоактивов, если он заранее не передал копии закрытых ключей кому-либо.

Одна из проблем заключается в том, что безопасное хранение ключей и управление ими является обременительной и сложной задачей, которая все ещё требует высокого уровня технических знаний. Следовательно, эта задача часто передаётся специализированным сторонним сервисам-депозитариям, которые берут на себя обязанность за хранение криптовалют. Но по статистике за 2018 год только 32% из них фактически берут на себя ответственность за сохранность активов. Это вновь вводит посредника во взаимоотношения пользователя криптоактивов. Главным же преимуществом технологии блокчейн является отсутствие необходимости доверять сторонам сделки друг другу, и в то же время исключается необходимость в использовании посредника-гаранта, которому также необходимо проявлять доверие. Таким образом, наличие посредника в хранении и управлении криптоактивами прямо противоречит самой идеи технологии блокчейн и снова вводит дополнительные неконтролируемые риски для конечного пользователя. Более того, выбор сервисов-посредников по хранению криптоактивов существенно ограничивается ассортиментом предлагаемых криптовалют, так как около трети крупных кастодиальных сервисов поддерживают или планируют поддерживать от двух до трёх криптовалют.

Также на некоторых этапах работы с криптоактивами чаще всего появляется необходимость взаимодействовать с биржами криптовалют, что также подвергает владельцев чрезмерным рискам.

Лучшие практики на сегодня подразумевают использование multi-signature кошельков с применением третьих лиц (депозитариев в т.ч.), при которой несколько сторон должны подтвердить транзакцию или являются хранителями резервных ключей. Таким образом рождаются новые системы, которые позволяют размыть риски.

Но по статистике 62% самых крупных кастодиальных сервисов криптоактивов имеют полный контроль над средствами пользователей. Хотя у более мелких эта доля составляет 30%. При этом необходимо отметить, что индустрии чрезвычайно не хватает прозрачности: более 80% отчётов аудитов безопасности как внутренних, так и внешних не раскрывается публично.

Нельзя не упомянуть о масштабах потерь лишь только от действий злоумышленников: на сегодня около 1,5 млрд. долл. украдены в 58 официальных документированных эпизодах краж криптоактивов у бирж и кастодиальных сервисов, которые являются основными целями хакерских атак как носители самых больших объёмов криптовалют. В эту категорию также можно включить крупных майнеров криптовалют.

Сегодняшние наработки пионеров индустрии уже позволяют утверждать, что большая часть пути по созданию доступных средств управления криптоактивами как минимум для физических лиц и малого/среднего бизнеса пройдена и не подразумевает существенных накладных расходов, предоставляя при этом разумный допустимый уровень сохранности криптоактивов.

В таких условиях индустрии необходимо предложить пользователю средства управления активами с сопоставимой простотой

использования, с одной стороны, и надёжностью, которая по крайней мере не уступает современным требованиям к методам защиты активов, хранимых в электронном виде, а также разного рода корпоративных и государственных реестров, – с другой.

Поэтому мы поставили перед собой цель – создать продукт, к которому будет минимум необходимости «доверять». Весь исходный код проекта, а также список используемых компонентов будет доступен сообществу. Индустрия уже давно пришла к выводу, что концепция «безопасность через неясность» (Security through obscurity) безнадёжно устарела. В то же время только 11% кастодиальных сервисов на сегодня предоставляют исходный код своих продуктов, и чем больше фирма, тем меньше процент «раскрываемости» кода.

Наш продукт «Криптокошелёк», как и ряд других на рынке, представляет из себя мобильное аппаратно-программное средство с цветным сенсорным дисплеем. Главной особенностью комплекса является использование съёмной защищённой смарт-карты формата SIM, имеющей сертификацию на соответствие ISO 15408 Common Criteria EAL 6+ в качестве носителя закрытых ключей. В настоящее время такой подход признан самым надёжным, и фактически на рынке нет альтернатив с сопоставимым уровнем безопасности без существенных денежных инвестиций в дорогие интеграционные решения. Более того, сам комплекс представляет из себя кошелёк типа «cold-storage», то есть «холодный». Это означает, что он не имеет доступа в Интернет, другими словами, отрезаются все векторы атак с применением сетей, оставляя возможность злоумышленнику только лишь на физический доступ к хранилищу ключей. Таким образом достигается максимальная защищённость содержимого на устройстве. По состоянию на 1 кв. 2018 г. в среднем 82% всех криптоактивов были защищены в «холодных» хранилищах.

Как мы выяснили выше, большинство кастодиальных сервисов чаще всего поддерживают не более трёх самых популярных криптовалют (coins). В нашем же случае устройство поддерживает 10 таковых, а также все без исключения валюты (tokens), выпущенные на базе блокчейна Ethereum (ERC-20, ERC-721). При этом следует учитывать два положения. Во-первых, говоря о поддержке валют, мы строго имеем в виду поддержку нашим собственным приложением без учёта сторонних продуктов от других разработчиков. В то время как конкурентные решения, заявляя о поддержке сотен и тысяч криптовалют, фактически выполняют это посредством именно сторонних приложений, что существенно повышает конечные риски для пользователя. Во-вторых, архитектура нашей экостистемы позволяет вводить новые криптоактивы в очень сжатые сроки, не превышающие 3-4 недель.

Также действительно уникальным средством противодействия от физического проникновения в устройство является защита корпуса от вскрытия посредством самоуничтожения MCU. Таким образом устанавливается конечный барьер для злоумышленника от подмены собственных компонентов печатной платы, так как именно такой метод атак активно набирает обороты (атаки, как правило, происходят в период доставки продукта до конечного потребителя).

Помимо непосредственных преимуществ для работы с криптоактивами, наш продукт позволяет существенно улучшить пользовательский опыт и в повседневной деятельности. Так «Криптокошелёк» будет поддерживать двухфакторную авторизацию посредством международного стандарта FIDO U2F. Это открытый бездрайверный протокол для двухфакторной авторизации, основанный на вызов-ответной аутентификации с помощью электронной цифровой подписи. Другими словами, пользователь получает защиту физическим токеном сразу к целому ряду популярных сервисов в Интернете, среди которых Google, Github, Wordpress, Dropbox, Evernote, Facebook и криптобиржа Bitfinex. Для остальных сервисов, не поддерживающих данный стандарт, наш продукт включает менеджер паролей. При этом, помимо возможности легко создавать уникальные пароли с высокой энтропией любым не самым технически подготовленным пользователем, мы не навязываем своего облачного сервиса для резервирования паролей. Пользователь сам выбирает метод резервирования, не будучи зависимым от нас. Например, рекомендуемая нами схема в связке с 2FA для облачных сервисов Google и Dropbox является крайне простой и надёжной конфигурацией для широкого потребителя.

В планах на будущее – дополнение устройства картой памяти SD-формата для возможности хранения любых пользовательских файлов в зашифрованном виде. Вторым расширением функционала станет возможность создания сложных смарт-контрактов в качестве хранилища криптоактивов, где «Криптокошелёк» будет лишь одним из факторов управления этим хранилищем. Это позволит совместить удобство использования индивидуального решения, а также добавит ещё один слой надёжности, как в случае с сервисами-кастодинами при нестандартных транзакциях, а также простоту передачи прав на активы в экстренных случаях, таких как тяжёлая болезнь, физическое вымогательство или смерть. То есть пользователь сам сможет конфигурировать, например лимиты на транзакции, как мы сейчас это делаем в своём интернет-банке; позволить временно отзывать транзакции; добавлять пользователей или устройства в качестве дополнительного фактора и политики перехода прав наследования, например с задействованием доверенных лиц, включая нотариуса, без прямой передачи копий ключей. Причём всё это возможно будет делать на ходу буквально в несколько кликов на устройстве, что не усложнит работу, а наоборот, сделает управление интуитивно понятным.

Stéphane Autelli,
генеральный директор
ООО «Центр Умных Технологий»

Gemalto, компания группы Thales

ВАШ ГИД В МИРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

180+
Стран с нашим представительством

30 000+
Клиентов по всему миру

2 млрд.
Людей, использующих наши решения

$1 трлн.
Защищенных межбанковских переводов ежедневно

200+
Государственных программ по всему миру

150+
eSIM разработок

Мы предоставляем две основные технологии, которые позволяют организациям предлагать защищенные цифровые услуги миллиардам людей

DIGITAL **IDENTITY**

DATA PROTECTION

Обслуживание организаций на 6 рынках

Банковское дело и Оплата

Информационная безопасность предприятий

Правительство

Интернет вещей

Мобильная связь

Монетизация программного обеспечения

С помощью следующих решений

Обеспечение граждан одним из самых технически продвинутых электронных паспортов.

Добавление системы Octopus payment & travel card в Samsung Pay.

Обеспечение Telefonica Deutschland технологией более быстрого распознавания ID.

Предоставление компании OnKöl технологии для обеспечения безопасности пожилых пациентов и их связи с теми, кто за ними ухаживает.

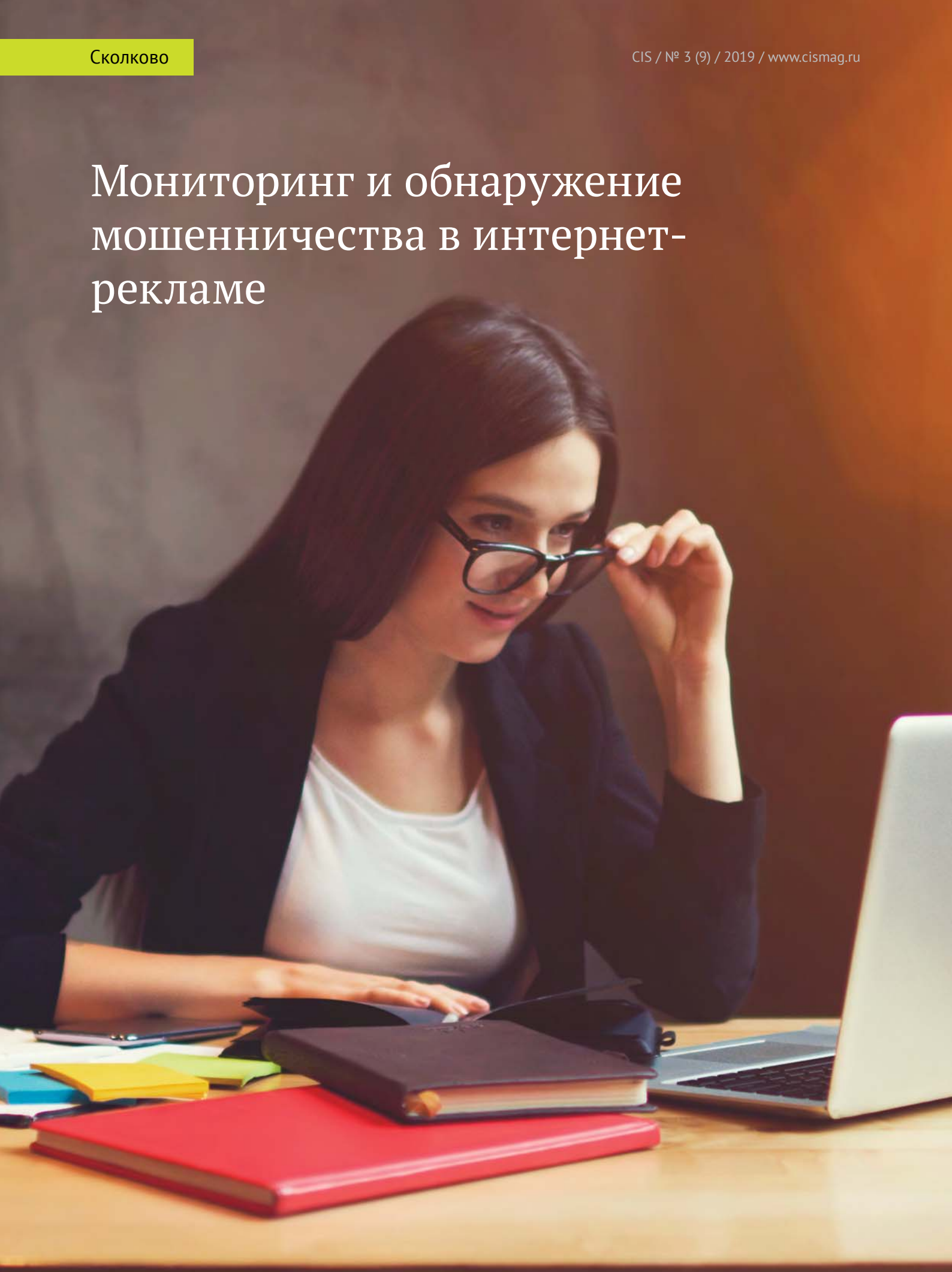
THALES

Gemalto является частью группы Thales, организации с оборотом в **€ 19млрд.**, персоналом в **80 000** человек в 68 странах по всему миру.

gemalto
a Thales company

CIS / № 3 (9) / 2019 / www.cismag.ru

Мониторинг и обнаружение мошенничества в интернет-рекламе



Коротко о важном

Сегодня интернет-реклама – один из главных каналов коммуникации рекламодателя со своими клиентами. Однако с её развитием в цифровом пространстве активизировался и фрод. С каждым годом его схемы усложняются и становятся всё менее очевидными.

Рынок интернет-рекламы растёт на 10-20% в год. Доля потерь от мошенничества уже составляет более 50% (58 млрд долл/год) и продолжает расти (рис. 1).

Постоянно мутируют существующие и изобретаются новые способы мошенничества.

Объединив 10-летний опыт работы в digital и экспертизу в области борьбы с интернет-мошенничеством, в 2015 году мы создали компанию Admon, которая осуществляет независимый фрод-мониторинг, определяет уязвимости сайта и защищает от недобросовестных подрядчиков. С первых дней мы доказали свою эффективность, сэкономив рекламный бюджет наших клиентов, который в разы превышал стоимость наших услуг.

Нам доверяют

Уже спустя три месяца после основания компании мы стали официальным партнёром и экспертом Ассоциации компаний интернет-торговли, в которую входят крупнейшие интернет-магазины России. В 2018 году мы официально вошли в число резидентов Фонда «Сколково» в кластере ИТ и информационной безопасности.

Свою защиту от фрода в рекламе нам доверяют ведущие российские и международные бренды – FMCG, банки, телеком-операторы и интернет-магазины.

Как мы работаем

Прозрачность, подтверждённые данные и контроль 24/7 – главное в нашей работе и коммуникации с клиентами. Мы предоставляем бесплатный тестовый период, оперативную техподдержку, а также еженедельный детальный отчёт о выявленных нарушениях. Это позволяет своевременно обнаружить перерасход рекламного бюджета, очистить рекламу от мошенников и тем самым значительно повысить эффективность или сэкономить средства рекламодателя.

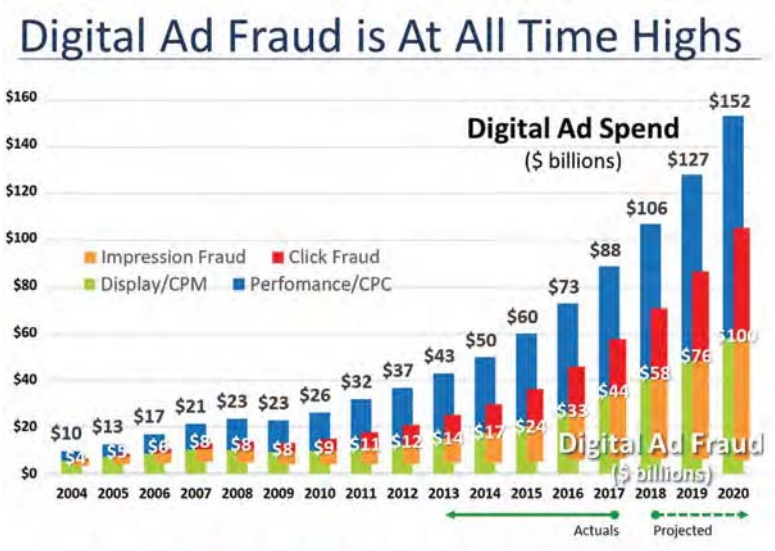


Рисунок 1. Цифровое мошенничество с рекламой всегда было и остаётся на высоком уровне.

Каждому клиенту мы предлагаем индивидуальное решение с учётом специфики бизнеса. В отличие от рекламных агентств, мы работаем за фиксированную плату, что исключает конфликт интересов с нашей стороны и искажение данных.

Мы оцениваем все риски, несём полную ответственность за сбор доказательств фрода и выступаем в качестве независимого эксперта, который помогает эффективнее развиваться вашему бизнесу.

Удачные кейсы

Недавно мы обнаружили массовый неочевидный фрод в медийной рекламе. Зачастую крупные бренды, размещаясь на площадках партнёров, даже не подозревают о том, что большая доля просмотров рекламы осуществляется не людьми, а ботами. При такой схеме мошенничества рекламодатель может терять огромные суммы, а обнаружение фрода осложняется отсутствием доступа к коду сайта-партнёра. Для выявления таких потерь, в частности, и привлекают Admon.

Примером эффективной работы нашей компании стало выявление мошенничества на 11 миллионов рублей за три месяца для одного из наших клиентов.

Команда

Мы привлекаем талантливых разработчиков и digital-экспертов со всей страны. Сердце нашей компании находится в Москве, однако активное участие в работе принимает и наш офис в Новосибирске. Расстояние не мешает нам эффективно решать задачи наших клиентов. Мы регулярно встречаемся, проводим выходные вместе и устраиваем корпоративные мероприятия. Сплочённость команды напрямую влияет на качество нашей работы и достижение высоких результатов.

Участие в CyberSecurity Challenge 2019

Весной 2019 года нам предложили принять участие в конкурсе «Сколково», из более 250 компаний мы вошли в число 15 финалистов.

Однако выиграть в конкурсе нам так и не удалось. По фидбеку, полученному от жюри конкурса, состоящего в основном из представителей служб безопасности крупных компаний и поставщиков систем безопасности, наша тематика для них оказалась незнакомой. Этим и пользуются недобросовестные поставщики интернет-рекламы.

Поэтому мы надеемся привлечь внимание уважаемого сообщества к проблеме, поскольку растущие объёмы рекламных бюджетов с одной стороны и безнаказанность мошеннических действий в той сфере – с другой, привлекает всё больше мошенников.

admon.ai
ECOLOGY IN DIGITAL

Admon *– профессиональный мониторинг и обнаружение мошенничества в интернет-рекламе.*

www.admon.pro

CIS / № 3 (9) / 2019 / www.cismag.ru

Система блокировки вредоносного программного обеспечения Safenvi

Safenvi – инновационная система блокировки вредоносного программного обеспечения. Safenvi блокирует основной канал внедрения вредоносного программного обеспечения через офисные документы и фото/видео файлы.

Даже в тех случаях, когда пользователи открывают заражённый документ из почтового сообщения, Safenvi блокирует действия опасной программы. При этом блокируются вирусы, которые не обнаруживаются антивирусами и другими средствами защиты.

Частота кибератак, уровень их сложности и масштабы существенно выросли за последние годы. При этом растёт количество атак, в ходе которых используются высокотехнологичные, устойчивые к обнаружению средствами защиты инструменты. Современные целенаправленные атаки представляют собой спланированные операции. Чаще всего за целенаправленными атаками стоят не злоумышленники-одиночки, а организованные преступные сообщества с чётко определёнными ролями. Практически во всех компаниях применяются средства защиты информации. Однако при этом кибератаки не становятся менее результативными. При целенаправленных атаках применяются неопубликованные методы, использующие неизвестные на тот момент уязвимости операционных систем и прикладного программного обеспечения. Злоумышленники активно разрабатывают методы обхода средств защиты, что приводит к тому, что и модифицированные методы, использующие известные уязвимости, также не обнаруживаются.

Известным фактом является то, что самым слабым звеном при обеспечении информационной безопасности является пользователь. Человеческий фактор сегодня остаётся одной из самых больших уязвимостей в киберзащите. Соответственно, и злоумышленники рассматривают пользователей как основной канал проникновения в сети компании.

Для того чтобы проникнуть в любой компьютер, злоумышленникам необходимо доставить пользователю заражённый файл и заставить его запустить данный файл. Несмотря на проводимые работы по повышению осведомлённости, пользователи всё равно открывают вложения или ссылки из фишинговых писем. При этом достаточно хотя бы одного запуска вредоносного вложения для успешного заражения. В большинстве случаев заражение происходит через офисные документы, а также архивы и аудио, видео файлы. Существенно реже для заражения используются исполняемые файлы. И если запуск неизвестных исполняемых файлов можно запретить и ограничить запуск аудио/видео

файлов, то работу с офисными документами запретить нельзя.

Большинство атак используют для проникновения в компьютер и выполнения вредоносного кода те или иные уязвимости операционных систем и программного обеспечения. Практически в любом программном обеспечении присутствуют уязвимости. Количество обнаруженных и закрытых уязвимостей год от года не снижается. Необходимо признать, что они были, есть и будут... В среднем от момента начала эксплуатации обнаруженной уязвимости до закрытия её вендором проходит от полугода до года. Всё это время компьютеры и сети компаний остаются незащищёнными от воздействия вредоносного программного обеспечения, использующего данные уязвимости.

Таким образом, невозможно запретить пользователям использовать офисное программное обеспечение, нельзя исключить возможность открытия вредоносного вложения и с высокой долей вероятности определить, что открываемый файл является опасным. Одним из вариантов исключения возможности заражения при работе с офисными файлами является создание контролируемой среды выполнения программного обеспечения, обрабатывающего эти файлы.

Safenvi позволяет создать такую среду выполнения и обеспечивает контроль офисного программного обеспечения. В продукте реализована технология виртуализации приложений для блокировки возможных путей внедрения вредоносных программ.

Safenvi не пытается определить являются ли открываемый файл или операции, выполняемые после открытия документа, аномальными или похожими на операции вредоносного характера. Все действия, которые могут привести к внедрению вредоносного программного обеспечения, выполняются только в виртуальной среде.

Реализованная технология позволяет блокировать большинство видов вредоносного программного обеспечения, в том числе использующих для проникновения неизвестные уязвимости офисного программного обеспечения и не обнаруживаемые антивирусными средствами. Блокировка вредоносного программного обеспечения производится на этапе его внедрения. Все действия с файлами и реестром будут производиться в виртуальной среде и не смогут повлиять на работу операционной системы и других процессов. Также будут заблокированы попытки обратиться к памяти других процессов и попытки запуска дополнительных. Таким образом, вредоносное программное обеспечение не сможет выполнить действия, которые приводят к заражению компьютера и выйти из виртуальной среды выполнения программы.

Safenvi для каждого контролируемого программного обеспечения при запуске и в процессе работы:

- Создаёт виртуальные ветки реестра.
- Создаёт виртуальные папки для работы с файлами в файловой системе.
- Контролирует работу приложения с памятью.
- Контролирует запуск дополнительных процессов.

Контролируемое программное обеспечение работает так же, как и без применения Safenvi. Но все данные, которые возникают в процессе работы приложения (ключи реестра и их значения, файлы), сохраняются в виртуальной среде. Только документы, сохранённые пользователем во время работы, автоматически и прозрачно выгружаются из виртуальной среды в реальную файловую систему. Все исполняемые файлы, библиотеки и т.д., полученные во время работы приложения, остаются в виртуальной файловой системе и не видны операционной системе и другим процессам. Все изменения реестра остаются в виртуальном реестре и не видны операционной системе и другим процессам.

Для пользователя работа Safenvi абсолютно прозрачна. Все действия он выполняет точно так же, как и раньше: работает в тех же офисных программах, видит все свои папки и файлы, может сохранять и открывать документы, видит историю открытых документов, может работать со всеми шаблонами и т.д. После внедрения нашего продукта для пользователей остаются доступны все шаблоны и расширения. Не нужно предпринимать никаких дополнительных действий для запуска приложения в безопасном режиме. Все действия на компьютерах выполняются в автоматическом режиме и не требуют действий администратора безопасности.

Safenvi контролирует работу следующего программного обеспечения:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Adobe Acrobat Reader
- WinRAR
- Microsoft Windows Media Player

Использование Safenvi позволяет:

- Существенно снизить риск проникновения в контролируемую сеть.
- Снизить риски остановки деятельности компании из-за вирусов-вымогателей.
- Снизить нагрузку на антивирусные средства.
- Обеспечивать защиту без изменения алгоритма работы пользователей.
- Обеспечивать защиту без снижения производительности компьютеров.

В результате открытие заражённого документа из почтового сообщения не приводит к заражению компьютера пользователя и сети в целом. Действия вредоносного программного обеспечения будут заблокированы. Таким образом существенно снижается влияние человеческого фактора на защиту корпоративной сети.

Safenvi легко внедряется. В процессе эксплуатации не требует постоянного обновления каких-либо правил. Все действия выполняются в автоматическом режиме. От пользователей не требуется дополнительных знаний и действий.

Защищаем просто, надёжно, безусловно.

SAFENVI

«Safenvi» – многопрофильный системный интегратор, поставщик корпоративных ИТ-сервисов.

www.safenvi.ru

CIS / № 3 (9) / 2019 / www.cismag.ru

Security Vision на защите информационных активов: как была реализована автоматизация управления инцидентами в СДМ-Банке

Банки играют ключевую роль в функционировании не только финансового, но и других секторов экономики, являясь важнейшим фактором её развития. Более того, стабильность работы банковской системы напрямую связана с финансовым состоянием государства и является основным фактором национальной безопасности. Поэтому важность максимально надёжной защиты информационных активов крупнейших банков сложно переоценить.

Резидент «Сколково» компания «Интеллектуальная безопасность» является разработчиком уникальной ИТ-платформы Security Vision, которая позволяет роботизировать исполнение программно-технических функций офицера безопасности с долей автоматизации до 95%. Система выполнена на уровне лучших мировых аналогов, получила широкое признание экспертного сообщества и уже обеспечивает в глобальных масштабах информационную безопасность многих государственных органов и коммерческих структур, среди которых ФСО России, ГК «РОСТЕХ», АО «Гознак», ФАУ «Главгосэкспертиза России», АО «Газпром-Медиа Холдинг», Корпорация «МСП». Особую роль Security Vision играет в обеспечении кибербезопасности банков, защищая информационные активы Сбербанка – крупнейшего банка в России, а также в Центральной и Восточной Европе, банка «Открытие», СДМ-Банка и других крупнейших «игроков» финансовой отрасли.

Проект автоматизации процессов управления инцидентами кибербезопасности в СДМ-Банке закончился совсем недавно – в середине июля. Он был направлен на повышение уровня информационной безопасности банка, обеспечение оперативного реагирования на инциденты кибербезопасности и нивелирование их воздействия, а также на снижение риска человеческого фактора и ошибок персонала, привлекаемого к реагированию на инциденты.

В рамках проекта были реализованы следующие задачи:

1. Расширена система мониторинга банка:
   - установлены и настроены новые узлы инфраструктуры мониторинга;
   - подключены ключевые источники событий информационной безопасности;
   - реализованы правила выявления инцидентов информационной безопасности.
2. Сформирован и автоматизирован процесс обработки инцидентов информационной безопасности с учётом специфики бизнес-процессов банка.

3. Реализована база активов банка с ролевым разделением доступа к информации об активах.
4. Реализован процесс управления активами банка.
5. Реализованы операционные и аналитические отчётные материалы.

Олег Владимирович Илюхин, заместитель председателя правления – директор департамента ИТ СДМ-Банка: *«СДМ-Банк входит в ТОП-100 крупнейших российских банков и продолжает стабильно развиваться. Вопросы обеспечения информационной безопасности банка, надёжная защита его информационных активов от всех видов внешних и внутренних угроз входят в число наших приоритетных задач, качественное и своевременное решение которых является залогом устойчивого функционирования банка. СДМ-Банк неукоснительно соблюдает требования и рекомендации банка России, платёжных систем МИР, Visa и MasterCard, является участником информационного взаимодействия с ФинЦЕРТ Банка России. Качественно организованный мониторинг является одним из столпов правильной работы всей системы управления информационной безопасностью. А чтобы обеспечить оперативное реагирование на инциденты кибербезопасности, мы выстроили процесс управления активами как отправную точку в вопросах защиты информации».*

Владимир Николаевич Солонин, Директор по информационной безопасности СДМ-Банка: *«Автоматизация в вопросах кибербезопасности выходит на первый план, поскольку роботизированные инструменты реагирования позволяют в режиме 24x7 обеспечивать должный уровень защиты информации. Одним из важных шагов в направлении автоматизации стало выстраивание процесса, охватывающего базовые принципы управления инцидентами кибербезопасности, с целью дальнейшего снижения риска человеческого фактора и ошибок сотрудников, вовлечённых в реагирование на инциденты кибербезопасности, а также с целью высвобождения времени квалифицированного персонала от рутинных операций для выполнения более экспертных задач».*

Руслан Рахметов, генеральный директор компании «Интеллектуальная безопасность»: *«Благодаря командной работе с банком удалось построить рабочий процесс управления инцидентами кибербезопасности и управления активами. Это основополагающие факторы работоспособности центра мониторинга и начало его успешного развития в вопросах обеспечения соответствия стандартам кибербезопасности и лучшим практикам в этой области».*

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

«Интеллектуальная безопасность»

www.securityvision.ru

AppSec.Hub – платформа оркестрации DevSecOps-процессов

29 мая 2019 состоялся финал международного конкурса проектов в сфере кибербезопасности Skolkovo Cybersecurity Challenge. Одним из финалистов конкурса стал проект «Платформа AppSec.Hub». По результатам конкурса проект получил специальный приз ИТ-интегратора «Инфосистемы Джет» за самое перспективное решение в направлении DevSecOps.

Платформа AppSec.Hub – это решение для автоматизированного управления и контроля всеми сквозными процессами разработки защищённого ПО, которое позволяет кардинально сократить время на запуск инициативы Application Security в целом и обеспечить максимально оперативный перевод инженерных процессов из DevOps в DevSecOps, а также повысить эффективность команд разработчиков в рамках общей трансформации инженерных процессов и перехода к концепции Shift Left.

Почему это так важно? Одним из основных вызовов современного времени с точки зрения разработки ПО является сокращение Time To Market (T2M). При этом подразумеваются следующие факторы: сокращение длительности релизных циклов, ускорение вывода новых продуктовых фич в промышленную эксплуатацию и обеспечение максимальной гибкости любых внедрений в целом. Эти инженерные задачи успешно решаются инструментальным стеком DevOps. Однако практики обеспечения информационной безопасности крайне сложно интегрируются в DevOps и, по сути, являются бутылочным горлом для разработки, а значит, и для бизнеса.

Как это работает сейчас: есть инструментальный стек информационной безопасности (ИБ), куда входит большое количество инструментов; есть инструментальный стек разработки, куда входит ещё большее количество инструментов. Некоторые из них более-менее интегрируются, но реализация технологического процесса – это в целом ручной труд в рамках сложных консалтинговых проектов.

Большинство существующих продуктов для автоматизации (DefectDojo, SecurityRAT, ThreadFix, XebiaLabs, Code DX, Cybric, Veracode, Fortify SSC, Orchestron и др.) направлены на решение точечных проблем, в частности на задачу корреляции и агрегации информации о дефектах (рис. 1).

AppSec.Hub – это более комплексный подход. Платформа позволяет реализовать бесшовную интеграцию инструментального стека ИБ с инструментами разработки; организовать полностью автоматизированное управление и настройку конвейера сервисов безопасности (security pipelines) в рамках циклов непрерывной интеграции (CI/CD); обеспечить контроль процесса безопасной разработки с помощью набора метрик.

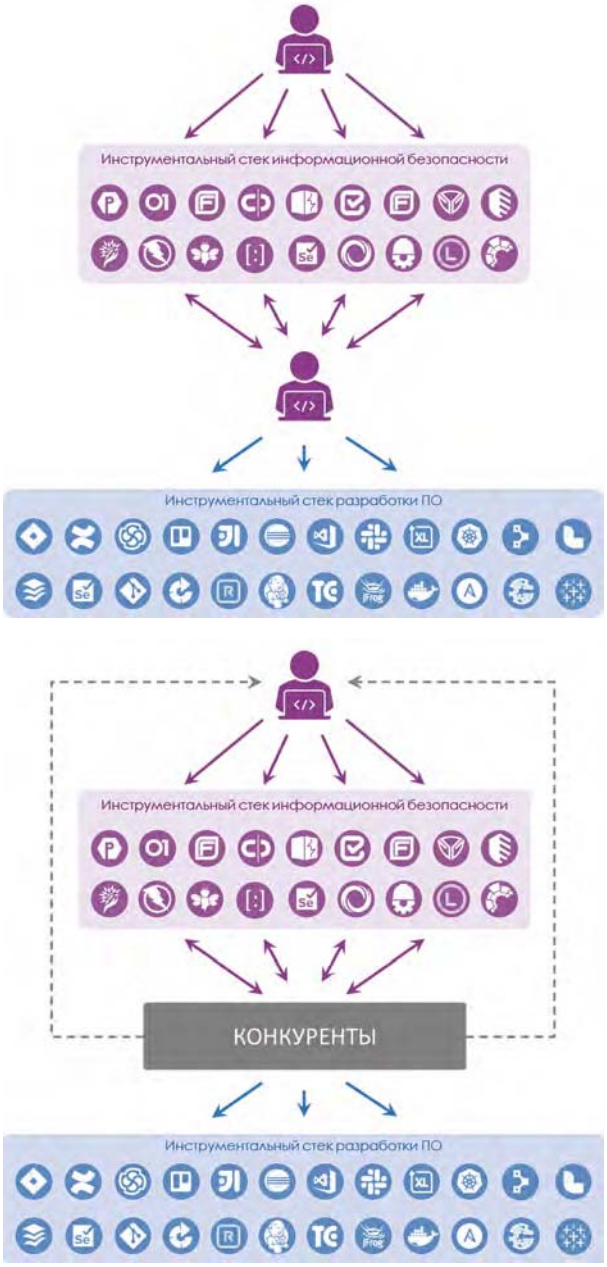


Рисунок 1.

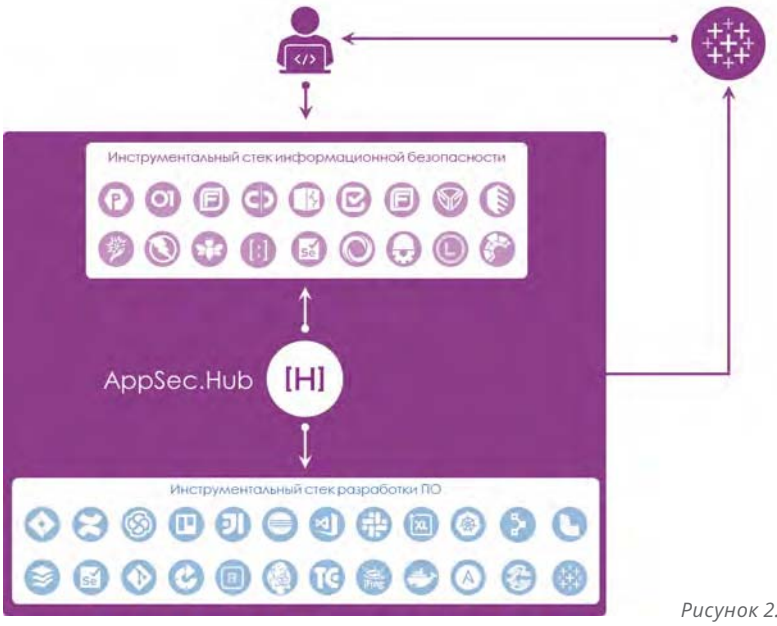


Рисунок 2.

Юрий Сергеев,
генеральный директор компании AppSec Solutions

Эксперт в области внедрения практик DevSecOps в рамках программ цифровой трансформации крупнейших организаций финансового сектора с общим опытом более 15 лет в индустрии разработки ПО и информационной безопасности.

Что, по сути, реализует на практике включение процессов ИБ в непрерывный процесс разработки, а это и есть DevSecOps (рис. 2).

С точки зрения интеграции инструментального стека AppSec.Hub, по сути, является единым окном для:

- включения инструментов ИБ в цикл разработки и их настройки;
- контроля портфеля проектов разработки в контуре DevSecOps;
- агрегации данных о статусе и результатах работы практик информационной безопасности.

На данный момент платформа поддерживает полноценную интеграцию с 16 сторонними продуктами, такими как GitLab, Jenkins, TeamCity, Confluence, Jira, Checkmarx, Fortify, Sonatype Nexus, Synopsis BlackDuck и др. И этот список быстро растёт (рис. 3).

Если говорить про платформу с точки зрения оркестрации, то для каждого проекта в контуре DevSecOps AppSec.Hub создаёт security-pipelines с необходимыми проверками ИБ, автоматически поддерживает их в актуальном состоянии для каждой ветки разработки, а в случае добавления ветки разработки автоматически создаёт пул проверок и для неё (рис. 4).

AppSec.Hub также позволяет контролировать процессы DevSecOps в реальном времени благодаря комбинации алгоритмов сбора и консолидации данных, интеграции с BI инструментом Tableau и уникального подхода к анализу данных. Интеграция с Tableau позволяет максимально эффективно визуализировать метрики процессов DevSecOps, консолидировать данные в любые конфигурации дэшбордов (разного уровня гранулярности) с минимальными трудозатратами (рис. 5).

Реализованный уникальный подход к анализу данных в прошлом году был отмечен наградой компании Sonatype как лучший инновационный проект за интеграцию решения AppSec.Hub с платформой Sonatype Nexus IQ в рамках задачи консолидации данных и мониторинга метрик для контроля и анализа рисков применения компонент с открытым исходным кодом.

У платформы уже есть несколько кейсов опытно-промышленной эксплуатации как на локальном, так и на международном рынках. Решение ещё не идеально, но проработав детально ожидания пользователей, разработчики успешно двигаются к целевому состоянию в рамках плана развития технологических и бизнес-функций продукта (расширение пула поддерживаемых инструментов класса SAST / SCA / DAST / IAST / WAF, реализация поддержки GSuite/OAuth 2.0, реализация автоматизированного процесса управления требованиями и рисками ИБ, реализация поддержки сервиса нотификации на базе корпоративных мессенджеров, реализация полноценной интеграции с платформами Bug-Bounty, интеграция с платформами геймификации и обучения).

На данный момент в рамках одного из ключевого направления развития платформы AppSec.Hub

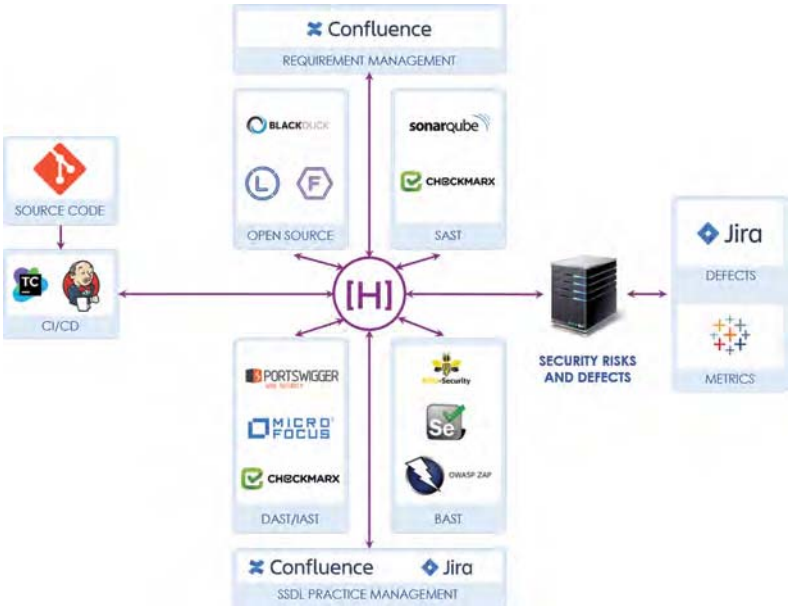


Рисунок 3.

Рисунок 4.

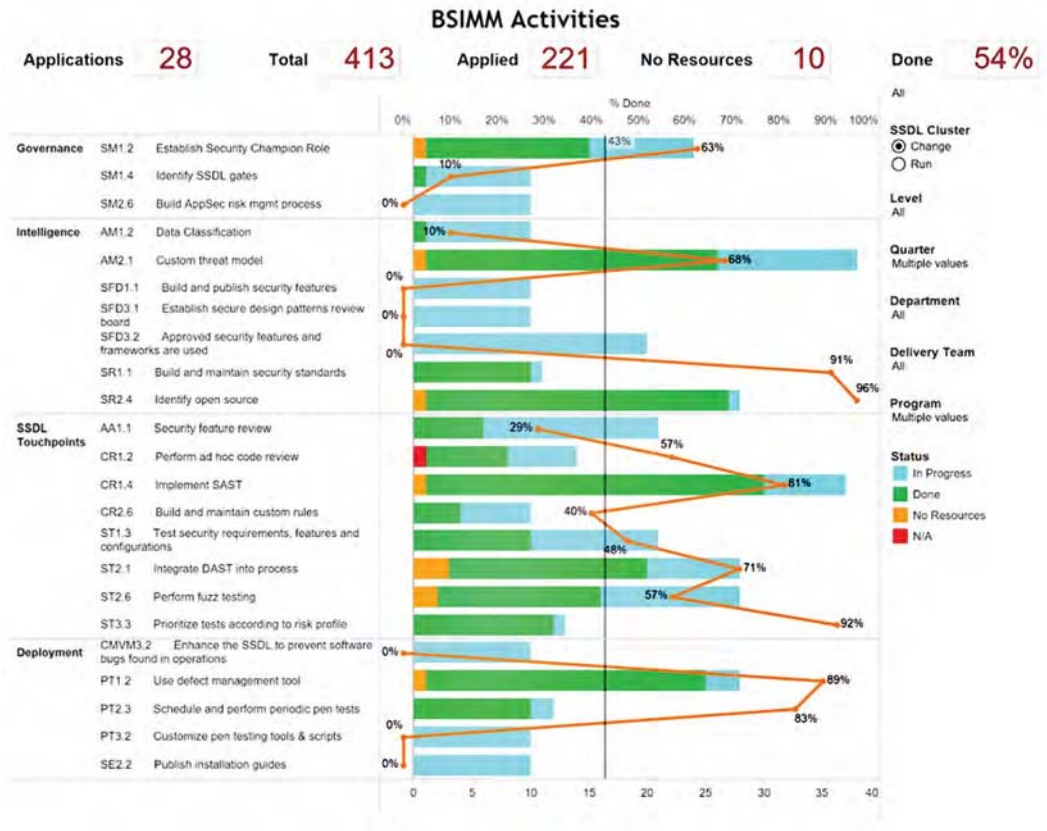
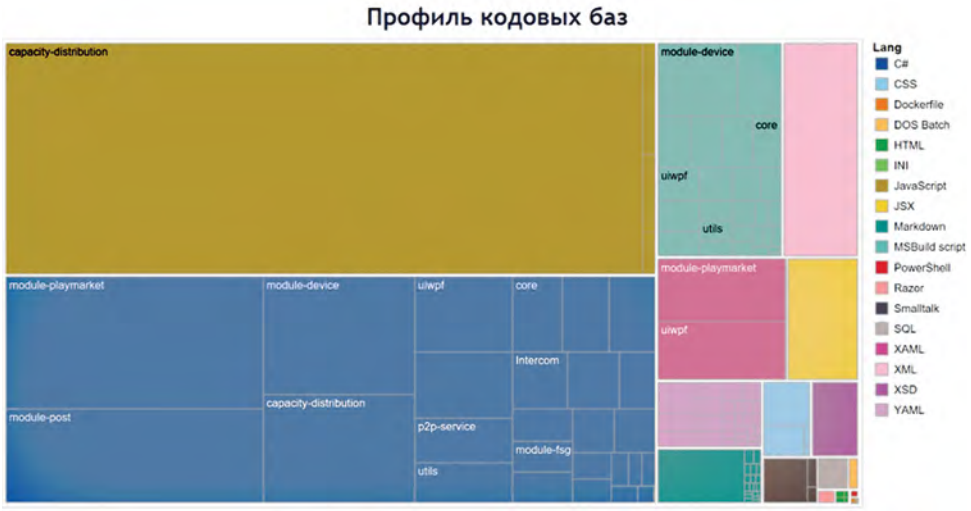


Рисунок 5.



проводится пилотирование технологий машинного обучения. Разрабатываемые алгоритмы в первую очередь направлены на решение задач корреляции результатов сканирования и обнаруженными дефектами ИБ, выявления наиболее уязвимых участков кода и наиболее уязвимых приложений и сервисов.

Если же говорить о коммерческом потенциале платформы, то команда проекта ориентируется на мировые тенденции и прогнозы. В 2018 году Gartner выделил новый сегмент – Application Security Testing Orchestration (ASTO) в дополнение к сложившемуся уже на данный момент сегменту Application Release Orchestration (ARO). В обоих сегментах согласно прогнозам есть очень сильный потенциал роста и ожидания к консолидации этих сегментов в перспективе. В планах у разработчиков платформы AppSec.Hub войти в ТОП-3 продуктов этого консолидированного сегмента ASTO/ARO, который, по данным Markets & Markets (MarketsAndMarkets.com), уже к 2022 году составит 10% от всего рынка Application Security.

[AppSec SOLUTIONS

*Компания **AppSec Solutions** специализируется на разработке решений в области автоматизации непрерывного процесса производства защищённого программного обеспечения (DevSecOps).*

hub.appsec.global
+7 (495) 721-37-76 | inbox@appsec.global

Платформа динамического анализа защищенности мобильных приложений – Bishop

Юрий Шабалин,
Главный архитектор и руководитель проекта «Платформа Bishop».

Application Security – эксперт с опытом более 8 лет в области внедрения практик безопасной разработки, построения процессов DevSecOps. Аналитик мобильных приложений, участник программы Bug-Bounty Google/Android.

Финалист международного конкурса проектов в сфере кибербезопасности Skolkovo Cybersecurity Challenge – «Платформа Bishop» получила специальный приз компании «Ростелеком-Солар».

Платформа Bishop – это инструмент для анализа защищённости мобильных приложений во время их работы на устройстве. В ходе анализа применяются методы динамического, интерактивного и поведенческого анализа приложения. Во время работы пользователя с приложением или запуске автоматических тестов, собирается вся возможная информация о поведении приложения, на основе которой проводится последующее тестирование, позволяющее выявлять более 30 типов дефектов безопасности и определять детальные рекомендации по устранению и недопущению подобных дефектов в дальнейшем.

Необходимость такого всестороннего тестирования защищённости приложений обусловлена глобальным трендом, заключающимся в переходе пользователей на мобильные платформы вместо веб-версий, что подтверждается статистикой крупнейших цифровых Банков. В связи с этой популярностью существенно растёт число мобильных приложений и компаний разработчиков. По данным компании Google, ежедневно в магазин Google Play загружается более 5000 приложений. При этом безопасность этих приложений находится всё ещё на достаточно низком уровне, что подтверждается отчётами компаний по анализу защищённости, согласно которым более 75% Android приложений банковского сектора содержат уязвимости критического уровня. Таким образом, важнейшим вызовом для поддержания конкурентоспособности является сокращение времени выпуска новой функциональности на рынок (Time To Market) при сохранении качества и повышении защищённости, что порождает определённые проблемы, а именно:

1. При появлении новой функциональности в приложении или при исправлении выявленного дефекта, необходимо пройти полное тестирование приложения и убедиться, что изменения в коде не затронули остальной функционал приложения. С точки зрения анализа защищённости необходимо проделать ту же самую работу, но по поиску новых уязвимостей. Учитывая, что приложения становятся сложнее и приобретают всё больше функциональности – сложность тестирования возрастает.
2. При текущей скорости разработки и переходе на непрерывный цикл разработки ПО (DevOps), время, затрачиваемое на выпуск обновлений, сокращается. В связи с этим необходимо проводить функциональное тестирование и анализ защищённости быстрее, чтобы сохранять конкурентоспособность.
3. Во многих приложениях присутствует функционал оплаты или взаимодействие с персональными данными пользователей. Приложения хранят и обрабатывают всё большее количество данных, в том числе критических, с точки зрения безопасности. Некоторые приложения попадают в область действия регуляторных требований, таких как PCI DSS или GDPR и должны им соответствовать. Так же, в компаниях возможен свой собственный стандарт безопасности, который также необходимо соблюдать.

Все эти проблемы решает платформа Bishop, которая помимо обнаружения дефектов безопасности, умеет определять соответствие отраслевым стандартам безопасности, регуляторным требованиям ИБ (GDPR, PCI DSS, СТО БР ИББС, OWASP Mobile Top-10, OWASP MASVS и др.), а также поддерживает возможность создания внутреннего стандарта, в который возможно включить кастомизированные требования ИБ.

Так как платформа Bishop является аппаратно-независимой, отсутствует необходимость в создании и поддержании физических аппаратов для тестирования, а также, появляется возможность протестировать приложения на различных версиях операционных систем, просто выбрав необходимую из интерфейса. Платформа предоставляет простой и понятный интерфейс для настроек и проведения сканирования, что позволяет проводить анализ защищённости приложений и изменять правила анализа и поиска уязвимостей под конкретное приложение, не имея экспертных знаний в программировании. При необходимости дальнейшего ручного анализа или модификации правил поиска уязвимостей платформа Bishop предоставляет пользователю всю собранную информацию по всем отслеживаемым действиям в удобном формате с возможностью экспорта всех данных (рис. 1).

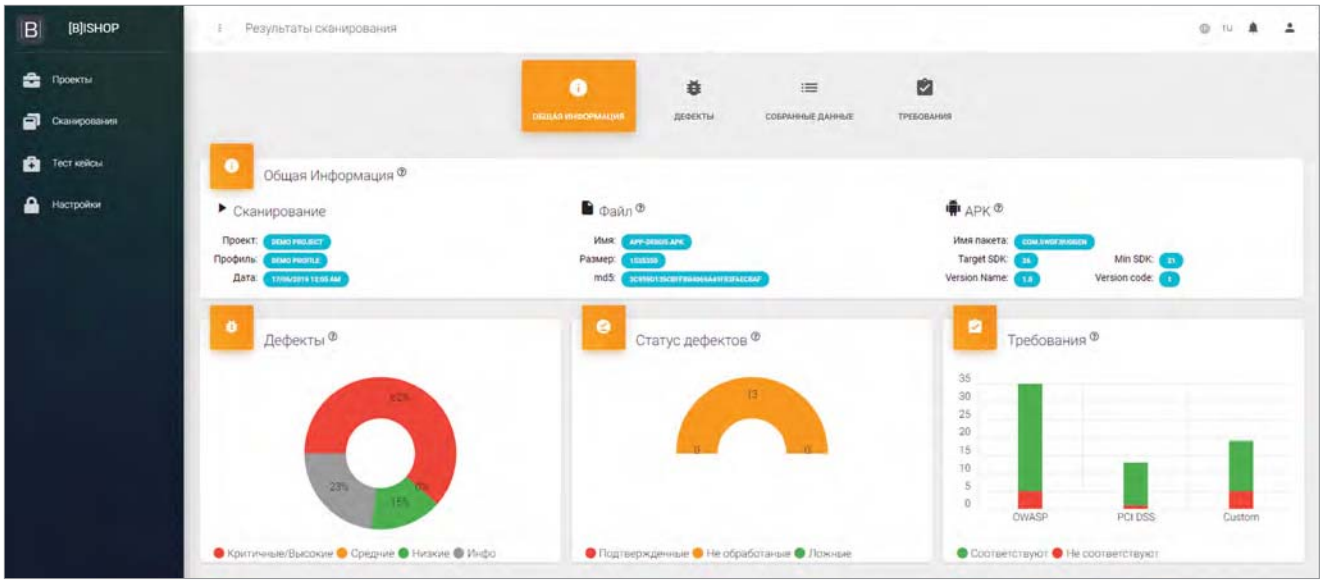


Рисунок 1.

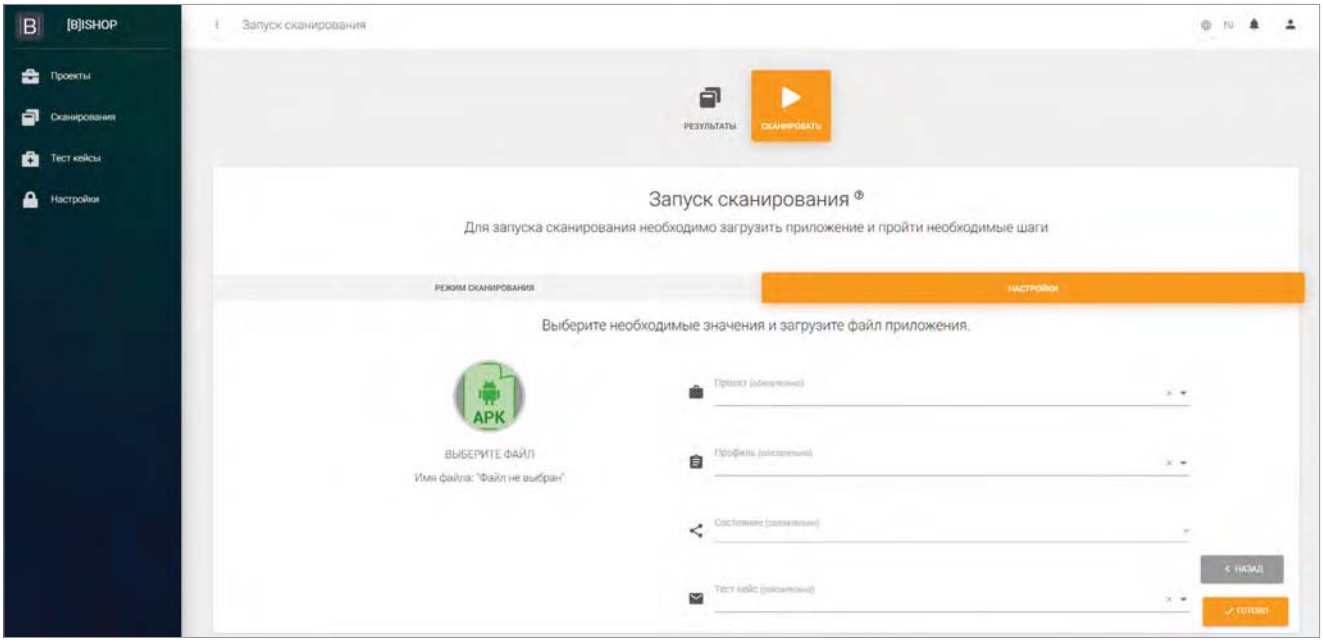


Рисунок 2.

Помимо упомянутого функционала, важной особенностью, выделяющей Bishop на фоне конкурентов, является уникальный механизм записи сценариев поведения пользователя и дальнейшее их воспроизведение без участия человека (создание автоматических тестов на основе работы пользователя с приложением). При этом платформа отслеживает изменение интерфейса в последующих версиях приложения при помощи методов машинного обучения и автоматически корректирует записанные сценарии, что позволяет существенно снизить трудозатраты и время на проведение анализа защищённости и уменьшить срок выхода новых версий на рынок. Благодаря этой функциональной возможности процесс тестирования защищённости мобильных приложений может быть встроен в непрерывный процесс разработки (DevOps), что позволяет обеспечить раннее обнаружение уязвимостей и проверку их устранения до публикации в магазин приложений без влияния на Time To Market (рис. 2).

Платформа Bishop представлена в нескольких сегментах рынка:

- как SaaS решение, для компаний, которые хотят проводить тестирование вне контура организации;
- так и как решение в модели on-premise, что позволяет разворачивать платформу внутри закрытого контура организации.

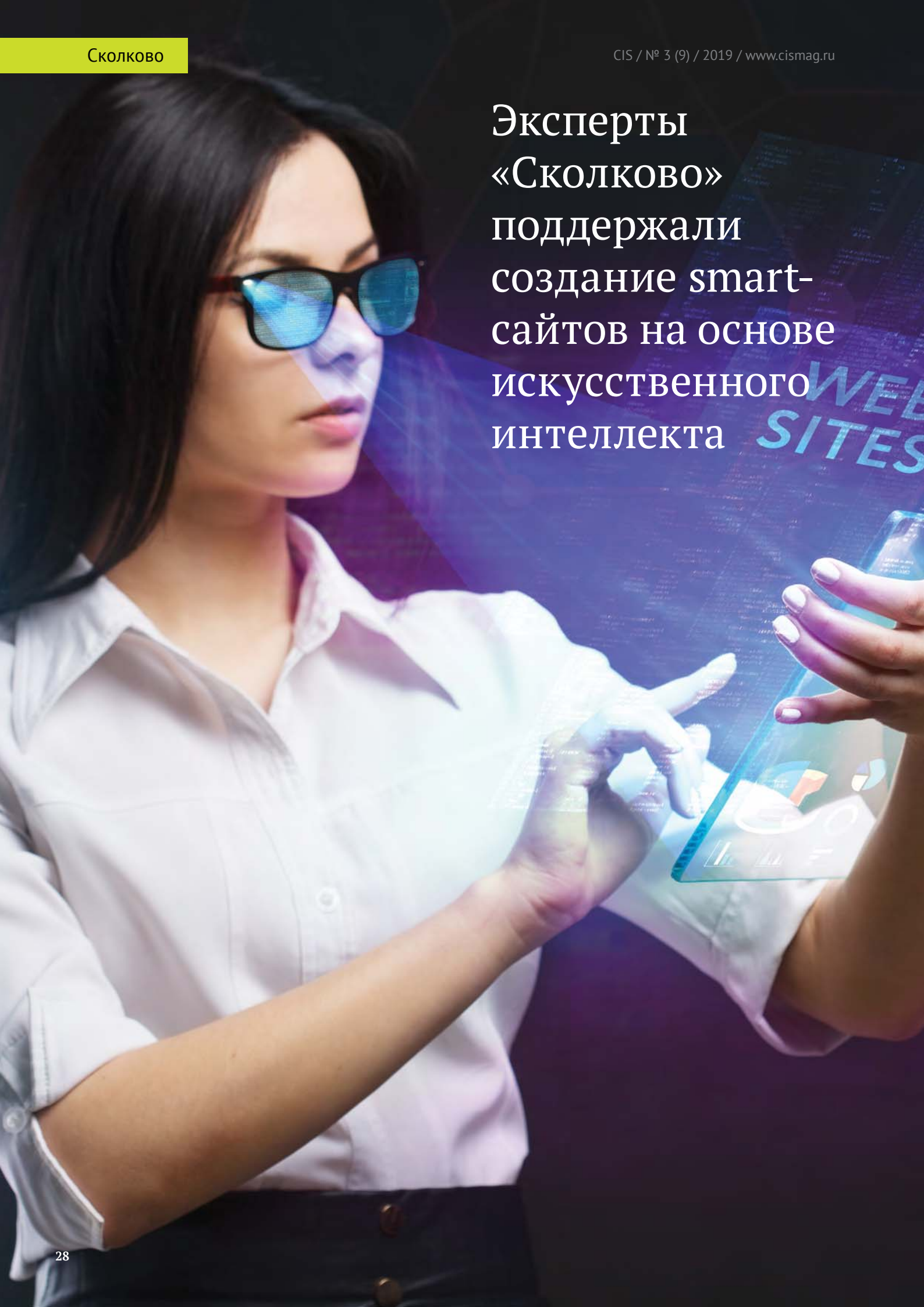
Развитие платформы базируется на пожеланиях и потребностях клиентов. На данный момент решение проходит опытно-промышленную эксплуатацию в нескольких крупных компаниях РФ.

[A]ppSec SOLUTIONS

[B]ishop *– уникальное решение для динамического анализа защищенности Android приложений на базе технологий IAST и BAST.*

bishop.appsec.global

Эксперты «Сколково» поддержали создание smart-сайтов на основе искусственного интеллекта



Веб-студия Aiger в ближайшее время станет новым резидентом инновационного центра «Сколково» с проектом создания «умных сайтов».

Smart-сайты, способные понимать и анализировать свою аудиторию, стали новой разработкой веб-студии Aiger. Проект получил широкую поддержку среди российских и зарубежных экспертов. Smart-сайты на основе ИИ были признаны лучшей разработкой по итогам акселератора технопарка «Русский». Создатели проекта удостоились гранта «Фонда Бортника» и получили приглашение стать резидентами центра «Сколково». По словам разработчиков, «умные сайты» помогут в разы увеличить конверсию и число заявок на продающих ресурсах.

Особенностью работы веб-студии Aiger является создание сайтов на основе ценностных карт, являющихся частью трендовой зарубежной модели Business Model Canvas. В основе такого подхода – определение страхов и выгод клиентов, которые может решить тот или иной продукт. «Умные сайты» стали продолжением работы по налаживанию взаимопонимания между поставщиком продукта и потребителем.

«Мы уже давно работаем с клиентами по принципу создания сайтов на основе ценностных карт и убедились в эффективности такого подхода. Когда сайт создан на основе потребностей и выгод аудитории, он становится отличным инструментом для продвижения продукта и наращивания клиентской базы. Однако при составлении ценностной карты мы основываемся только на представлении нашего клиента о его аудитории. Искусственный интеллект позволяет проверить объективность этого взгляда и даёт реальное представление об интересах посетителей сайтов», – разъяснил руководитель веб-студии Aiger Роман Бабеев.

Он пояснил, что, работая в рамках smart-сайта, ИИ делит всю аудиторию на группы посетителей и определяет, какая именно информация заинтересовала тот или иной сегмент пользователей.

«Все страницы сайта размечены с точки зрения изначальной ценностной карты. Затем в процессе работы ресурса искусственный интеллект определяет разные группы посетителей в зависимости от того, какая именно информация стала триггером, мотивирующим совершить целевое действие, то есть сделать заказ. Для одной части аудитории важна скорость доставки, для другой – цена, для третьей – отзывы клиентов. Искусственный интеллект считывает это поведение и даёт рекомендации по изменению структуры сайта в соответствии с интересами и потребностями пользователей», – рассказал Роман Бабеев.

Он добавил, что smart-сайты не только будут анализировать интересы пользователей, но и самостоятельно подстраиваться под их интересы. Такой сайт будет менять заголовки и часть контента на странице в зависимости от того, с какого объявления или запроса пришёл пользователь. Попадая на «умный сайт», посетитель первым будет видеть раздел именно с той информацией, которую искал.

Соответствие контента запросу, персонализация информации под каждого конкретного посетителя дают кратное увеличение конверсии продающего сайта и значительный рост числа заявок. Что, соответственно, позволяет компании экономить свой маркетинговый бюджет и иметь мощное преимущество перед конкурентами.

Таким образом, smart-сайт становится эффективным работающим инструментом, адаптированным под реальные потребности аудитории, отражающим интересные именно ей смыслы.

В веб-студии сообщили, что создание таких сайтов возможно как при личном контакте с клиентом, так и дистанционно. Компания Aiger работает в 18 городах России и создаёт более 100 сайтов в год. Суммарная аудитория разработанных веб-студией ресурсов уже превышает 1,6 млн человек. По словам программистов, smart-сайты станут только первым этапом реализации проекта «Искусственный интеллект». В дальнейшем веб-студия планирует анализировать поведение аудитории на группах сайтов определённой специфики, чтобы наиболее точно определять интересы потребителей продуктов.

Веб-студия Aiger *работает на рынке ИТ-услуг Дальнего Востока с 2012 года. Особенностью работы компании является разработка сайтов на основе трендовой зарубежной модели Business Model Canvas, которая успешно используется крупнейшими компаниями мира: Coca-Cola, Airbnb, GeneralElectrics, MasterCard, Lego, Procter&Gamble.*

Секрет эффективности сайтов от Aiger заключается в определении проблем и выгод клиента, разработке карт ценностного предложения, которые в дальнейшем служат базой для создания эффективного сайта.

Клиентами веб-студии уже стали известные в регионе бренды, такие как ДНС, Slavda Group и окна «Эталон».

www.aiger.ru

CIS / № 3 (9) / 2019 / www.cismag.ru

За гранью облака: Edge computing для киберзащиты веб-ресурсов

Цифровизация экономики приводит к непрерывному росту объёма передаваемых через интернет данных, а требования к их защищённости постоянно повышаются. Это вынуждает ИТ-индустрию искать новые подходы к созданию надёжных и быстрых веб-ресурсов. Как интернет-бизнесу надёжно защититься от кибератак и при этом ускорить работу веб-ресурсов?

Владельцы веб-сайтов постоянно вынуждены балансировать между высоким уровнем защищённости и производительностью сетевых ресурсов. До недавнего времени интернет-площадкам приходилось либо мириться со снижением скорости работы при повышении уровня защищённости, либо «ослаблять гайки» и надеяться, что хакеры их не атакуют. Однако активность киберпреступников из года в год растёт, а атаки становятся всё масштабнее и технологичнее. Вместе с этим повышается активность интернет-пользователей, увеличиваются объёмы информации, всё больше используется тяжёлый мультимедийный контент. Бизнесу и государству остро нужны решения, которые одновременно и защищали бы сайты, и ускоряли бы их работу.

На что жалуетесь?

DDoS-атаки стали элементом повседневной реальности для большинства компаний, бизнес которых связан с интернет-сервисами. Система анализа угроз NETSCOUT международной ИБ-компании Arbor Networks в 2018 году зафиксировала более 6,13 млн атак по всему миру[1]. Причём если ещё в «нулевых» мощность DDoS не превышала десятков Гбит/с, то в 2016 году мощность атак впервые перешагнула отметку в 1 Тбит/с. При этом доля DDoS, длящихся не часы, не дни, а недели, достигает 10%.

Кроме того, растёт количество кибератак на уровне приложений с целью несанкционированного доступа к веб-ресурсам и конфиденциальным данным посетителей. Злоумышленники всё активнее используют специально обученных программных ботов, которые сканируют веб-ресурсы на уязвимости, воруют контент, «скликивают» рекламные объявления, собирают информацию о пользователях.

Индустрия информационной безопасности непрерывно выводит на рынок новые аппаратные и программные средства защиты веб-ресурсов от DDoS-атак и хакерских вторжений. Однако их внедрение требует серьёзного бюджета на кибербезопасность, включая постоянные затраты на апгрейд инфраструктуры и обучение персонала.

Облачные решения по защите от кибератак, хотя и упрощают задачу, тоже не идеальны: они используют выделенные центры очистки трафика, что удлиняет сетевые маршруты до защищаемых веб-ресурсов и, соответственно, замедляет их загрузку.

Security & Performance из облака

Как сбалансировать защищённость и производительность в облаке? Ответ может дать новая концепция облачной защиты веб-ресурсов – умная маршрутизация трафика с использованием машинного обучения (Machine Learning) и фильтрация запросов распределённой сетью Edge-серверов.

Облачная платформа NGENIX – это территориально распределённый программно-аппаратный комплекс, состоящий из серверного и сетевого оборудования, и управляемый ПО собственной разработки.

Доступ к ресурсам платформы осуществляется через интернет. Узлы платформы размещаются в местах концентрации трафика интернет-пользователей, в частности в точках межоператорского обмена трафиком (Internet eXchange, IX), в сетях крупных телеком-провайдеров, а также в дата-центрах, которые обеспечивают одновременное подключение к нескольким операторам связи.

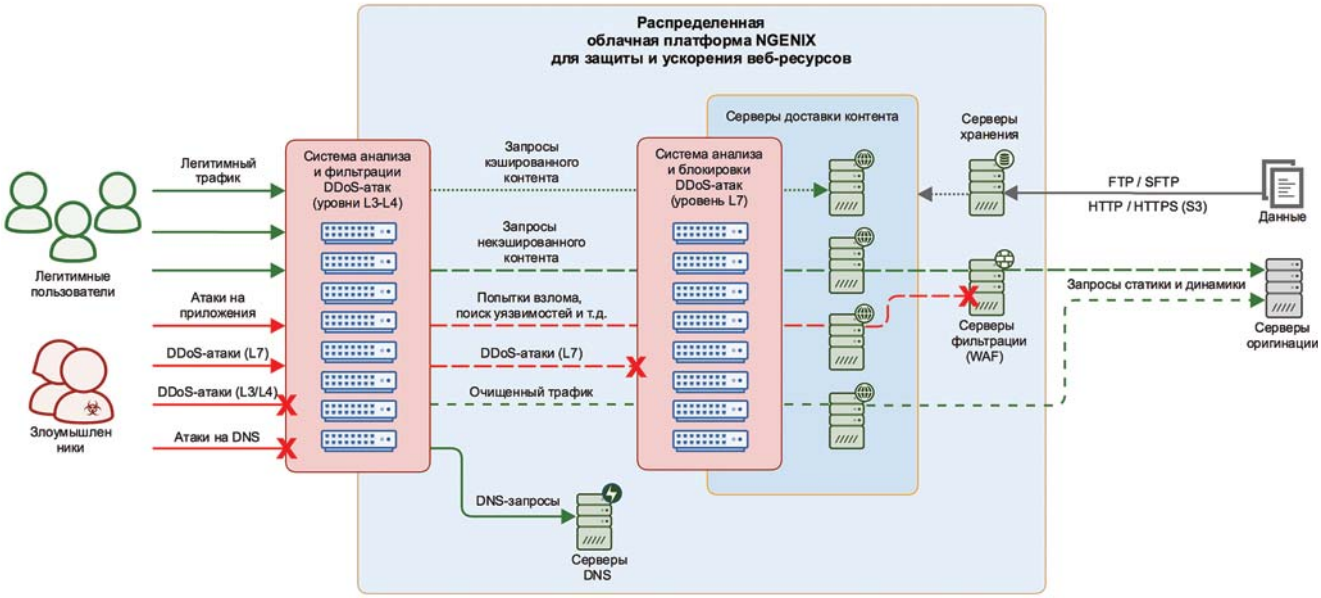
Сегодня платформа NGENIX состоит из 38 узлов – от Хабаровска до Франкфурта. Она стыкуется с сетями более 1000 интернет-провайдеров, работающих в РФ, странах СНГ и Европы. В течение многих лет платформа остаётся самой быстрой в России: согласно данным мониторингового сервиса Cedexis Radar, среднее время отклика на запрос пользователя 17 мс.

Облачное решение сочетает в себе функции фильтрующего экрана и распределённой сети доставки контента, обеспечивая веб-ресурсу защиту от DDoS-атак и взломов без снижения производительности. Очистка трафика производится на распределённой сети Edge-серверов, а контент веб-ресурса кэшируется и доставляется с ближайшего к пользователю Edge-сервера с помощью интеллектуального балансировщика.

Алгоритм балансировки при построении сетевого маршрута учитывает до 40 параметров и использует машинное обучение (Machine Learning), обеспечивая выбор оптимального сервера для каждого пользовательского запроса. Это означает отсутствие потерь пакетов между пользователем и сервером, а также высокую скорость транзакций.

Константин Чумаченко, генеральный директор провайдера облачных сервисов NGENIX.

[1] https://www.netscout.com/report/



Открытая архитектура

Платформа NGENIX обеспечивает широкие возможности интеграции с внешними системами, в том числе для развёртывания на сторонней инфраструктуре. Например, решение по защите от DDoS-атак позволяет подключать по API системы анализа трафика и SOC на стороне конечного клиента. Кроме того, возможна быстрая интеграция с платформой партнёрских ИТ-решений.

На платформе реализованы сервисы защиты на сетевом (Layer 3), транспортном (Layer 4) и прикладном (Layer 7) уровнях, включая защиту систем DNS. Уникальная особенность платформы NGENIX – защита от атак на уровне приложений (Layer 7), которая работает на географически распределённой сети Edge-серверов как с раскрытием, так и без раскрытия SSL-трафика, защищённого криптографическим шифрованием. Это позволяет отражать атаки эффективнее и быстрее, чем при традиционном подходе с помощью центров очистки трафика.

Система анализа веб-трафика включает три основных блока: динамический анализ трафика, построение статических правил и фильтрация. Такая архитектура позволяет отделить логику анализа трафика от механизмов управления трафиком. Это, во-первых, обеспечивает возможность подключения на стороне клиента собственной системы анализа. Во-вторых, позволяет быстро обучать систему новым сочетаниям типичных и аномальных профилей поведения пользователей. И, в-третьих, даёт возможность детектировать и фильтровать атаки и трафик зловредных ботов с минимальной задержкой.

В режиме управляемых сервисов

Платформа NGENIX может быть развёрнута по модели управляемого сервиса (Managed Service) на инфраструктуре компании-партнёра, а именно: облачного провайдера, сервис-провайдера, оператора связи. Модель подразумевает, что NGENIX выступает в качестве поставщика технологий, предоставляя их с различными уровнями интеграции для выделенной партнёром инфраструктуры.

После внедрения платформы партнёр получает возможность оказывать своим конечным пользователям (владельцам веб-ресурсов) облачные услуги защиты и ускорения веб-ресурсов и веб-приложений. Клиент получает защиту от киберугроз «по подписке» без инвестиций в собственную инфраструктуру и персонал.

При необходимости партнёры или владельцы веб-ресурсов могут подключать к платформе по API собственные системы анализа трафика и корпоративные Центры мониторинга и обработки инцидентов информационной безопасности (SOC). Это позволит им самостоятельно реагировать на атаки.

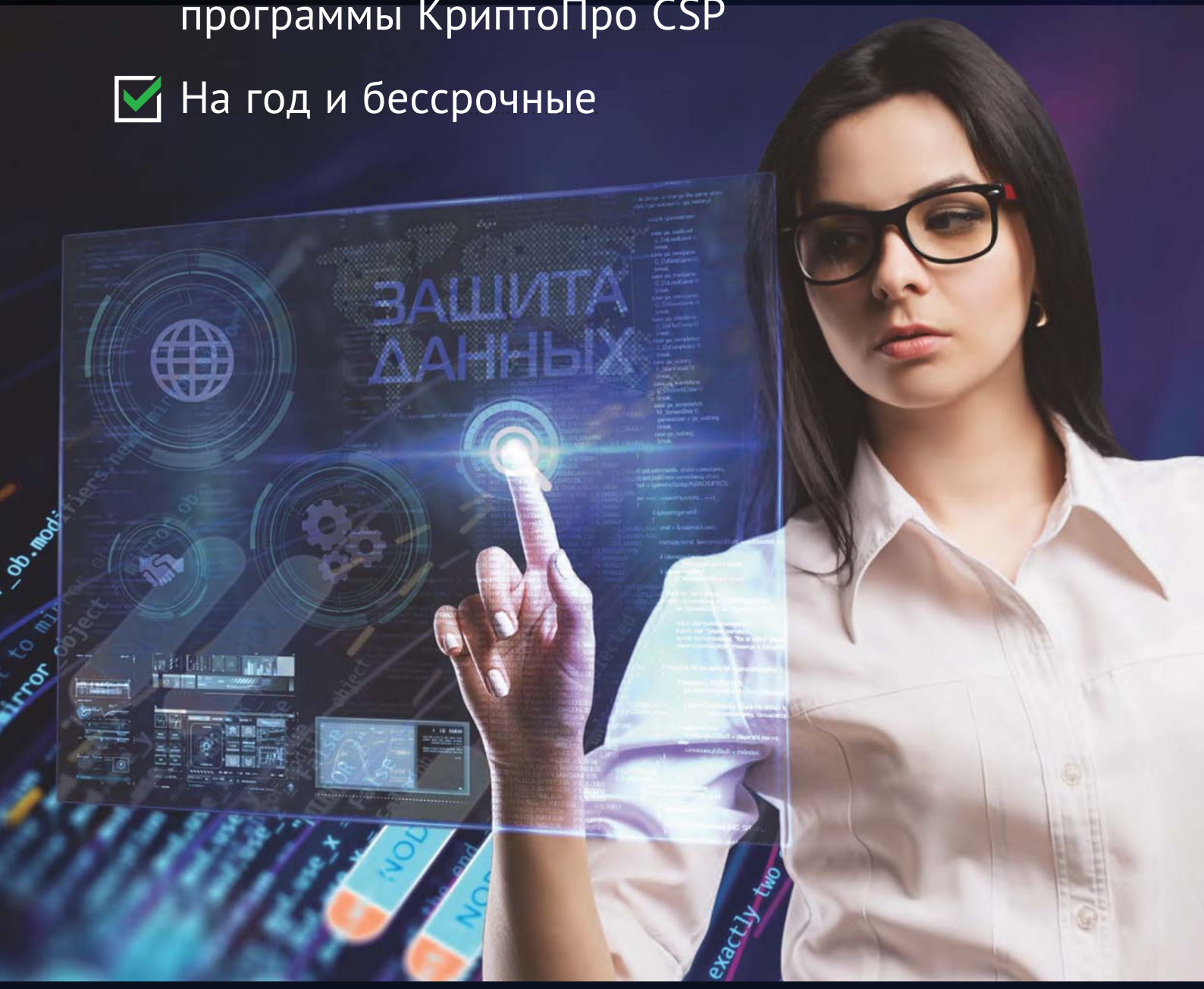
Интеллектуальная платформа NGENIX на практике воплощает наиболее современные и удобные для клиентов и партнёров бизнес-модели. По нашей оценке, платформа обладает большим экспортным потенциалом и может стать одним из актуальных российских продуктов на международном рынке ИБ.

NGENIX

www.ngenix.net

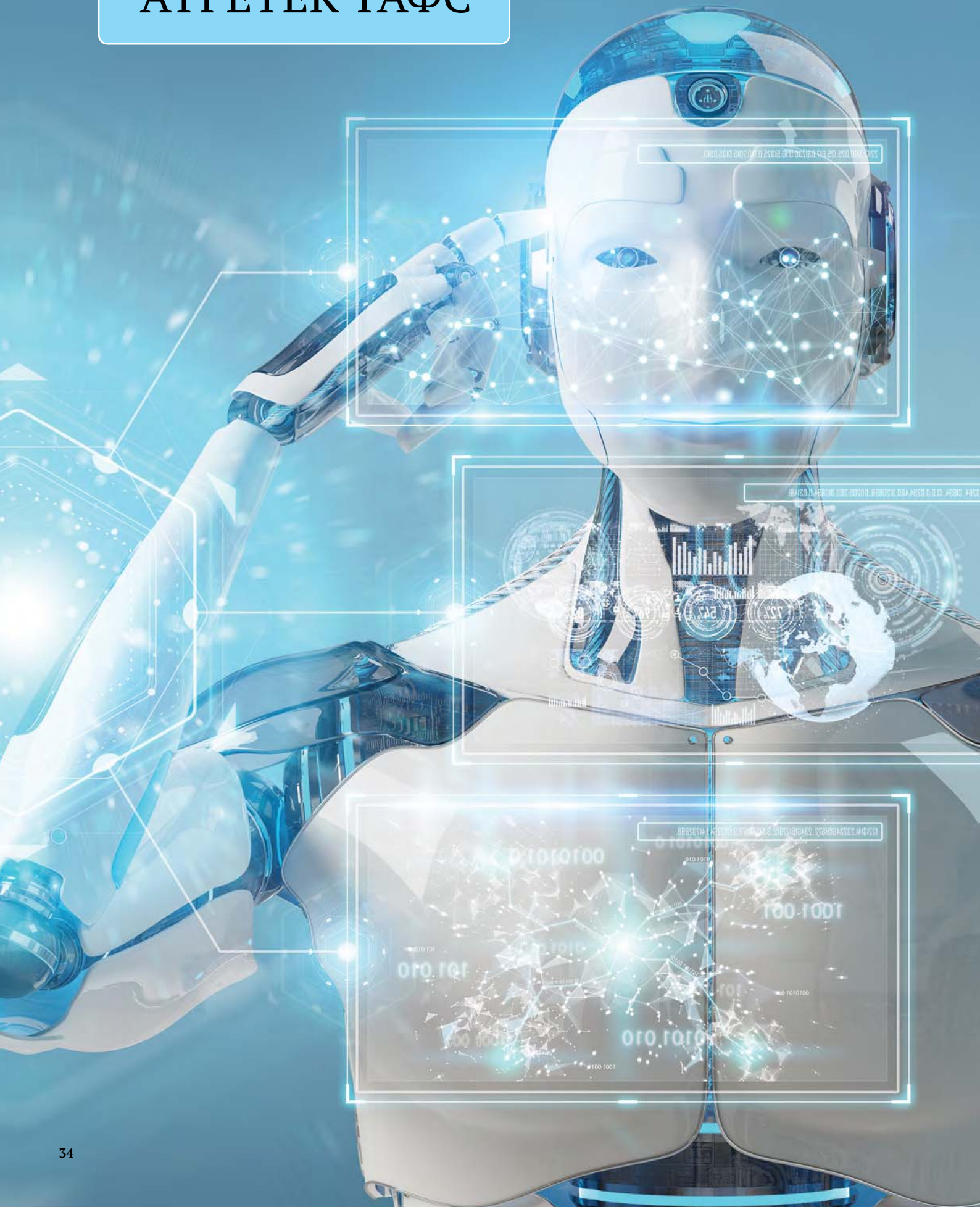
КРИПТОПРО CSP

- ☑ Электронные ключи и коробочные лицензионные программы КриптоПро CSP
- ☑ На год и бессрочные



КРИПТО ПРО
ЗАЩИТА ВАШЕЙ ИНФОРМАЦИИ

АТРЕТЕК ТАФС



АТРЕТЕК ТАФС – инновационное решение для противодействия мошенническим операциям на финансовых рынках с использованием искусственного интеллекта.

На вопросы редакции отвечает генеральный директор ООО “Атретек», Геннадий Белов:

- опыт на глобальных финансовых рынках более 20 лет;
- 1991–1997 гг. – Финансовая академия (МЭО) и Оксфордский Университет;
- 1994 г. – начало профессиональной карьеры во Внешторгбанке (bullion desk, fixed income desk);
- 1999–2005 гг. – руководил трейдинговыми подразделениями в международных финансово-банковских группах (American International Group, Raiffeisenbank);
- 2006–2015 гг. – управлял инвестиционными фондами в Сингапуре, Гонконге, Шанхае, Сайгоне, Москве;
- 2016 г. – управляющий директор Корпорации Развития Северного Кавказа (группа Внешэкономбанк).

Чем вызвана необходимость появления данного продукта?

Основная причина – ужесточение требований регуляторов во всём мире к повышению прозрачности банковских операций. Это не просто слова, это суммы гигантских штрафов. За последние 7 лет суммы этих штрафов, выплаченные банками США и Европы, превысили 320 миллиардов долларов США. И это тренд, который не закончится через пару лет. Ответом на эти колоссальные суммы штрафов стало появление на свет в 2015 году новой индустрии, которая называется RegTech (Regulatory Technology).

Профессиональные участники финансовых рынков тоже вынуждены выплачивать значительные суммы регуляторам из-за мошеннических действий сотрудников трейдинговых подразделений.

Вторая не менее важная причина заключается в несанкционированных действиях трейдеров, которые также приводят к скандальным многомиллиардным убыткам. Вспомните, например, трейдера по имени Жером Кервьель из французского банка Societe Generale. Более года он скрывал несколько сотен тысяч несанкционированных сделок на финансовых рынках, что привело к убытку для банка в 7 миллиардов долларов США. Или другой пример, когда несколько трейдеров Банка «Открытие» в 2011 году украли 150 миллионов долларов США. Такие инциденты случаются в мире регулярно. Банки стараются их замалчивать и иногда просто увольняют целиком трейдинговые подразделения (как это было пару лет назад в одной европейской банковской группе). Но проблема от этого не исчезает (табл. 1).

Наше программное обеспечение помогает автоматизированным образом решать обе проблемы: и снижение штрафов регуляторам, и своевременное пресечение схем, которые практикуют профессиональные трейдеры для «выкачивания» денег работодателя в свой карман или для сокрытия убытков.

Расскажите о предыстории возникновения ТАФС. Кто был инициатором появления этого решения?

Я начинал свою карьеру на финансовых рынках ещё в 1994 году на золотом деске (bullion desk, global markets) во Внешторгбанке России. После этого был многолетний опыт руководства трейдинговыми подразделениями международных и российских банковских групп. Владелец одной из таких банковских групп (человек, которому я глубоко обязан в понимании успешных бизнес-стратегий) однажды заметил: «Геннадий, я считаю, что за спиной каждого трейдера должен постоянно находиться сотрудник службы безопасности». Тогда, в 2006 году, это было шутливое, но очень прозорливое замечание. Оно отпечаталось в памяти, и я об этом долго размышлял. Через 8 лет я предложил тему «автоматизации контроля трейдинговых подразделений банков» партнёру одной из ведущих международных компаний, специализирующихся на банковском анти-фроде. Он поддержал идею, выделил несколько программистов, и мы начали разрабатывать и тестировать алгоритмы. Но в то время интерес к этой тематике со стороны банков был скорее отрицательный и тема постепенно сошла на нет. С небольшой командой единомышленников мы несколько лет уже самостоятельно продолжали разработку алгоритмов.

В начале 2018 года мне удалось собрать уже свою небольшую, но очень профессиональную команду молодых амбициозных программистов и специалистов по искусственному интеллекту, которые запрограммировали нашу библиотеку алгоритмов на Java/Scala и помогли разработать систему обработки и визуализации многомерных данных об инцидентах.

Какие задачи решает продукт?

ТАФС (Trading Anti-Fraud Solutions) помогает банкам, управляющим активами, страховым компаниям, другим финансовым институтам и промышленным компаниям улучшать свои финансовые показатели за счёт своевременного предотвращения:

1) штрафов регуляторов за манипулирование и инсайд, отмывание средств;
2) схем мошенничества недобросовестных сотрудников на финансовых рынках;
3) несанкционированных сделок таких сотрудников;
4) схем отмывания средств клиентами банков через финансовые рынки.

Таблица 1.

Организация	Трейдер	Убыток $ млрд
JPMorgan	Bruno Iksil	9,0
Morgan Stanley	Howie Hubler	9,0
SOCIETE GENERALE	Jérôme Kerviel	7,2
Sumitomo Corporation	Yasuo Hamanaka	3,4
ARACRUZ	Isac Zagury, Rafael Sotero	2,5
UBS	Kweku Adoboli	2,0
CITIC PACIFIC	Frances Yung	1,8

ТАФС помогает также выявить неэффективность операций трейдеров и повысить общую прибыльность организации.

Что ТАФС считает мошенническими действиями? (Примеры задач, которые решает продукт ТАФС)

1. **СХЕМЫ ВЫВЕДЕНИЯ СРЕДСТВ СДЕЛКАМИ «ВНУТРИ» РЫНОЧНЫХ ЦЕН**
   Выявление сделок, произведённых внутри рыночных цен, когда прибыль выводится из финансовых организаций в пользу неформально-аффилированных структур трейдеров или для отмывания доходов.
2. **ПРОСТЫЕ ВНЕРЫНОЧНЫЕ СДЕЛКИ**
   Выявление таких внерыночных сделок, по которым есть справочная информация о ценах.
3. **СЛОЖНЫЕ ВНЕРЫНОЧНЫЕ СДЕЛКИ**
   Выявление внерыночных сделок, по которым нет прямой информации о ценах на заданные дату и время, но можно сделать расчёт цен, используя специальные алгоритмы (внебиржевые опционы, сделки СВОП, РЕПО, IRS, CIRS).
4. **МАСКИРОВКА БИРЖЕВЫХ СДЕЛОК ПО ВНЕРЫНОЧНЫМ ЦЕНАМ ПОД РЫНОЧНЫЕ**
   Выявление биржевых рыночных сделок в периоды низкой ликвидности рынка с неформально-аффилированными контрагентами.
5. **ФРАНТ-РАННИНГ и ИНСАЙДЕРСКАЯ ТОРГОВЛЯ**
   • Выявление франт-раннинга на одном или нескольких рынках, включая внебиржевые;
   • Торговля перед событиями;
   • Выявление инсайдерской торговли перед выходом важных новостей;
   • Сделки корпоративных инсайдеров.
6. **МАНИПУЛИРОВНИЕ ЦЕНАМИ И ОБЪЁМАМИ**
   • Манипулирование заявками;
   • Выталкивание цены на уровни срабатывания клиентских стоп-лоссов;
   • Фиксирование референтной цены;
   • Зеркальные биржевые и внебиржевые сделки для раскрашивания ленты.
7. **ПАРКОВКА ПОЗИЦИЙ**
   • Выявление парковки убыточных позиций трейдерами с целью получения бонуса;
   • Выявление парковки убыточных позиций трейдерами с целью сокрытия рисков;
   • Выявление парковки прибыльных позиций трейдерами с целью нарушения лимитов для получения дополнительной прибыли.
8. **ВЫВОД СРЕДСТВ ИЗ ФИНАНСОВО ОСЛАБЛЕННЫХ ИЛИ БАНКРОТЯЩИХСЯ БАНКОВ**
   Выявление схем использования организации для вывода средств из третьих банков.
9. **НЕЗАКОННЫЕ ОПЕРАЦИИ ПО ВЫВОДУ КАПИТАЛА**
   Выявление схем незаконного вывода капитала из страны через финансовые рынки.
10. **НЕЭКОНОМИЧЕСКИЕ СДЕЛКИ**
    Сделки с целями, отличающимися от целей при обычной экономической деятельности.
11. **ВЫЯВЛЕНИЕ СВЯЗЕЙ НЕФОРМАЛЬНОЙ АФФИЛИРОВАННОСТИ СОТРУДНИКОВ С КЛИЕНТАМИ И КОНТРАГЕНТАМИ**

Рисунок 1.

Решение направлено против спекулятивных сделок трейдеров в пользу банков?

Ни в коем случае. Профессия трейдера как раз подразумевает проведение спекулятивных сделок. Это суть профессии. Для этого трейдеру формально устанавливаются лимиты на размер открытых позиций и иные лимиты, в рамках которых трейдер имеет право открывать спекулятивные позиции.

Решение направлено лишь на устранение асимметрии информации. Ведь сотрудники Казначейства и трейдеры не всегда информируют руководство обо всех реальных рисках своих и клиентских сделок и схем (рис. 1).

Руководство видит только отчёты о формальном отсутствии нарушения лимитов и о размерах открытых позиций. При этом трейдеры практикуют различные схемы хищений, растрат, вывода и отмывания средств, схемы по сокрытию позиций, рисков, сокрытию прибыли или убытков, схемы по манипулированию и инсайду. Проверяющие сотрудники подразделений внутреннего аудита, риск-менеджмента и комплаенс несут ответственность, но не всегда замечают скрываемые от них финансовые схемы.

Программа представляет собой инновационное автоматизированное решение с использованием машинного обучения (градиентный бустинг на деревьях решений / регрессия и калибровка вероятностей на большом наборе данных) по противодействию мошенническим действиям на финансовых рынках: выявление манипулирования рынками, инсайдерской торговлей, несанкционированных сделок трейдеров и растрат средств организации трейдерами в сговоре с клиентами и контрагентами.

Регулярные проверки активности на финансовых рынках обычно проводятся подразделениями внутреннего аудита и комплаенс. При этом традиционные проверки осуществляются так: из 1 миллиона транзакций выбирается несколько сотен

и проверяется вручную в Excel. Элемент случайности при таком подходе очень высок. Наш программный продукт проверяет все сделки без исключения, обрабатывая каждую с помощью многих десятков алгоритмов.

Что поменяется для финансовых институтов (банков, управляющих активами, страховых компаний) после введения решения ТАФС, и что изменится для игроков финансового рынка – трейдеров?

Профучастники финансовых рынков получают «волшебный» инструмент, позволяющий одним прикосновением сделать прозрачной любую активность трейдеров и клиентов на финансовых рынках. Этот инструмент позволит проверять не только «манипулирование и инсайд», но и несанкционированные сделки трейдеров (в международной терминологии применяется особый термин – rogue trading), хищения и отмывание средств через сделки на финансовых рынках.

Образно говоря, наша команда разработала такой «чемоданчик», при помощи которого внутренние и внешние аудиторы могут прийти и проверить любые сделки на финансовых рынках (например, Казначейство банка). До сих пор аудиторы в принципе не могли полноценно осуществлять проверку сделок Казначейств банков из-за недостатка узкоспециализированных компетенций и отсутствия автоматизированной возможности обрабатывать миллионы сложнейших схем и транзакций с валютами, акциями, облигациями, драгметаллами и производными инструментами. Такой «чемоданчик» позволяет на ранней стадии выявлять подозрительные схемы, минимизировать суммы штрафов, репутационные риски, скрытые рыночные риски, убытки от несанкционированных действий трейдеров, включая хищения.

Для трейдеров не изменится ничего. Но уже само наличие такого программного продукта заставит многих отказаться от противоправных действий (рис. 2).

Какие данные будет использовать ТАФС для противодействия мошенническим операциям на финансовых рынках?

Это традиционные данные о сделках, заявках, рыночных ценах и объёмах. Это та информация, которая ежедневно накапливается и хранится во фронт-офисных системах профучастников (таких как Murex, Kondor+, Callypso).

ТАФС – это нишевое решение для противодействия специфическим видам неправомерных операций на финансовых рынках, основывающееся на технологиях загрузки, обогащения, обработки и визуализации больших массивов данных. Система использует методы распознавания шаблонов (pattern recognition) для анализа больших массивов данных сделок на финансовых рынках, а затем восстанавливает логику принятия решений трейдерами для выявления потенциально мошеннических сделок и схем.

Насколько рискованно доверять системе корпоративные данные, если говорить про безопасность?

Это очень хороший вопрос, решению которого мы посвятили много времени.

Во-первых, система не требует реальных имён клиентов, контрагентов или сотрудников. Все данные могут загружаться в систему в замаскированном виде. Например, клиент ООО «Ромашка» попадает в систему как Client_231, трейдер Иванов – как Trader_14, контрагент Центральный Банк РФ – как Coounterparty_27 и т.д.

Во-вторых, организация-приобретатель лицензии на систему ТАФС может полностью ограничить её связь с внешним миром. Система устанавливается на внутренний сервер, и потоки данных не выходят за пределы организации.

Недавно мы получили грант от компании Microsoft, которая хочет разместить наш программный продукт в Azure. При поддержке её специалистов сейчас мы разрабатываем защищённое облачное решение, которым можно будет пользоваться для обработки и анализа замаскированных (по примеру выше) данных. Это будет вариант, альтернативный традиционному «разворачиванию» системы на внутренних серверах заказчиков.

Какой этап внедрения ТАФС самый сложный и почему?

Самый сложный этап – это обогащение данных и маппинг (автоматизированное сопоставление) полей фронт-офисной системы клиента с полями системы ТАФС. Зачастую во фронт-офисной системе не хвата-

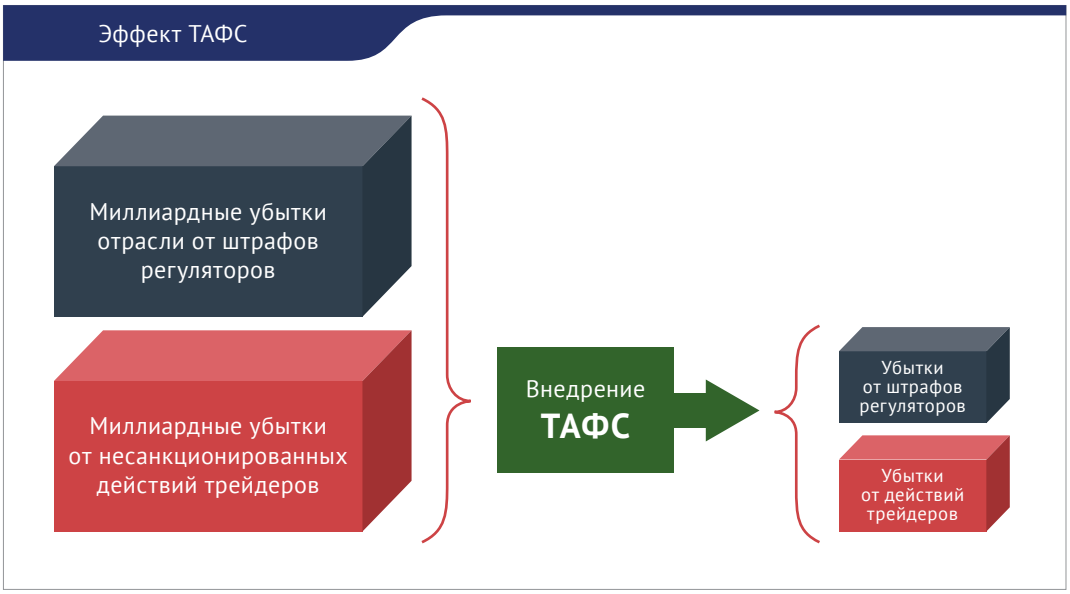


Рисунок 2. Внедрение ТАФС снижает убытки от штрафов и хищений.

ет данных по многим полям и требуется креативный подход для расчёта недостающих полей на основании тех, которые имеются в наличии. Обычно это может занимать несколько недель.

Почему конкуренты не спешат или не хотят активно занимать нишу по выявлению мошенничества на финансовых рынках в отличие от ТАФС?
Во-первых, конкуренты есть, и их немало. Но основные конкуренты сфокусированы на манипулировании/инсайде. Наш продукт, помимо модулей автоматизации, требований 224-ФЗ и требований европейского MAR (Market Abuse Regulation), имеет встроенную библиотеку алгоритмов по выявлению схем «намеренно упущенной прибыли», схем отмывания средств через финансовые рынки по выявлению несанкционированных сделок. В перспективе система сможет осуществлять мониторинг эмоционального состояния трейдеров.

Во-вторых, продукт является достаточно сложным для реализации и требует глубоких компетенций.

Выявление неправомерных сделок внутри любой организации – это очень «чувствительная» тема как к скелетам в шкафу, так и к текущей активности. Поэтому на начальном этапе руководители некоторых банков просто отказывались с нами разговаривать, узнав, что именно умеет делать наш продукт. Поэтому мы внедрили в систему «несколько уровней доступа». Аналитик видит только то, что ему «позволено». Руководитель видит то, что позволено ему. И только собственник видит полную картину.

Может ли ТАФС интегрироваться с «самодельными» системами банков или использовать их хранилище данных по инцидентам?
Да, это является дополнительным преимуществом системы ТАФС. Она может работать без сложной промышленной интеграции, а в качестве дополнения и усиления уже существующей самодельной инфраструктуры по хранению и обработке сделок. Таким образом, система не конкурирует с самодельными продуктами, а эффективно усиливает их узкоспециализированными компетенциями и суперпродвинутой библиотекой алгоритмов.

Важным моментом в этой связи является возможность снизить количество ложных срабатываний при помощи ТАФС. Это позволяет нашим клиентам снижать расходы на количество аналитиков, которые требуются для анализа вручную каждого срабатывания (инцидента).

Какая задача перед командой ТАФС стоит сейчас?
Наше решение сейчас включает в себя удобный пользовательский интерфейс и встроенную библиотеку алгоритмов.

Дальнейшая разработка программы ТАФС ведётся по направлению инновационных методов машинного обучения, включая глубинные нейросети:

- выявление новых шаблонов поведения трейдеров;
- новые методы детектирования аномалий и подозрительного, нехарактерного поведения;
- улучшение качества скоринга инцидентов;
- визуализация многомерных данных об инцидентах.

В перспективе будет реализована технология превращения ТАФС в самообучающуюся систему на базе машинного обучения, глубинных нейросетей, теоретико-игрового подхода (Game Theory).

Какое развитие продукта Вы видите в дальнейшем?
В первую очередь это развитие на российском рынке. Ведь с 1 мая 2019 года автоматизированное детектирование подозрительных операций на финансовых рынках стало обязательным для всех участников финансовых рынков в России (224-ФЗ Статья 11, параграф 2, пункт 2). Теперь требования Регулятора делают установку систем класса ТАФС обязательной для всех профучастников.

Практический интерес к решению ТАФС мы видим со стороны руководителей подразделений Банков:

1. **Служба Комплаенс:**
   - модуль «224-ФЗ» (Манипулирование и инсайдерская торговля) + MAR (Market Abuse Regulation);
   - модуль «Отмывание денежных средств на финансовых рынках».
2. **Службы внутреннего аудита и внутреннего контроля:**
   - модуль «Несанкционированная торговля» + «Отмывание денежных средств на финансовых рынках» (несанкционированные сделки трейдеров и клиентов на финансовых рынках, направленные на растрату средств финансовой организации);
   - модуль «Необычная активность» + «Эффективность» (необычная подозрительная активность на финансовых рынках + сделки с намеренно сниженной экономической эффективностью).

В ноябре 2018 года мы демонстрировали первую версию системы ТАФС на Wall Street в Нью-Йорке в рамках New York RegTech Summit 2018. Со стороны американских банков восприятие было достаточно высокомерное, и на текущем этапе им было просто интересно узнать «теоретически», что умеет ТАФС. А вот со стороны банков из Пакистана, Бангладеша, Индии интерес был значительный и практический.

Европейское законодательство также требует автоматизированного детектирования сделок на финансовых рынках. Европейским клиентам мы предлагаем в основном модуль MAR (Market Abuse Regulation), модуль Rogue Trading и AML на финансовых рынках.

Расскажите о Вашей команде и компании.
ООО «АТРЕТЕК» является резидентом технопарка «Сколково» и участником инновационного центра «Сколково».

Ядром нашей амбициозной команды являются специалисты по искусственному интеллекту, теории вероятности и математической статистике. В основном это выпускники Мехмата МГУ и Бауманского Университета.

Особенность нашего продукта, заключается ещё и в том, что библиотека алгоритмов разрабатывается специалистами по финансовым рынкам, каждый из которых имеет опыт работы трейдером свыше 10 лет в трейдинговых подразделениях международных банков. Это позволило нам смотреть на проблематику не снаружи (глазами внутреннего аудита или комплаенс), а изнутри – глазами трейдеров. Поэтому мы объективно считаем библиотеку алгоритмов ТАФС уникальной с точки зрения глубины проработки.

AUTRETECH

www.tafs.pro
gennady.belov@tafs.pro

«Инфосистемы Джет» протестирует решение для DevSecOps

ИТ-интегратор «Инфосистемы Джет» – официальный партнёр международного конкурса проектов в сфере кибербезопасности Skolkovo Cybersecurity Challenge, отметил среди финалистов компанию AppSec Solutions за наиболее перспективное решение в направлении непрерывного обеспечения безопасности на всех этапах разработки ПО – DevSecOps.

Почти из 100 проектов, защищавшихся на конкурсе, специалисты «Инфосистемы Джет» выделили платформу AppSec. Hub, предназначенную для управления практиками DevSecOps в процессе разработки ПО. Интегратор протестирует решение в собственной демолаборатории и по результатам испытаний рассмотрит возможность включения платформы в свой продуктовый портфель.

В 2019 году направление DevSecOps стало одним из наиболее перспективных для Центра информационной безопасности «Инфосистемы Джет». Реализация подобных проектов предполагает комплексный подход, учитывающий как встраивание практик ИБ в существующие у компаний циклы разработки, так и классическую защиту инфраструктуры (контроль доступа, безопасную настройку, анализ защищённости и т. д.).

«Крайне важным является встраивание безопасности в процесс разработки софта так, чтобы она не замедляла бизнес наших заказчиков. Именно этот фактор компании часто называют среди причин, сдерживающих интеграцию безопасности в направление DevOps, что понятно, т. к. во главе угла традиционно стоит показатель time-to-market. Автоматизация и оркестрация – естественный способ для ускорения процессов. В ближайшее время мы планируем запустить тестирование выбранной нами платформы, и, надеюсь, его результаты станут стартом продуктивного сотрудничества, которое расширит наши возможности в части реализации проектов по созданию непрерывной безопасности разработки», – отметил **Павел Волчков, начальник отдела консалтинга Центра информационной безопасности «Инфосистемы Джет»**.

*Компания **«Инфосистемы Джет»** – один из крупнейших российских системных интеграторов – образована в 1991 году. Входит в ТОП-10 крупнейших поставщиков ИТ-услуг России (Эксперт РА, 2017 г.), ТОП-5 компаний страны в сфере защиты информации (CNews Analytics 2018 г.), ТОП-3 крупнейших поставщиков в области комплексных проектов построения инфраструктуры ЦОД (CNews Analytics, 2017 г.) и т.д. Основные направления деятельности компании: бизнес-решения и программные разработки, ИТ- и телекоммуникационная инфраструктура, информационная безопасность, ИТ-аутсорсинг и техническая поддержка, управление комплексными проектами и др. Компания располагает 13 офисами и представительствами на территории РФ и СНГ.*

www.jet.su

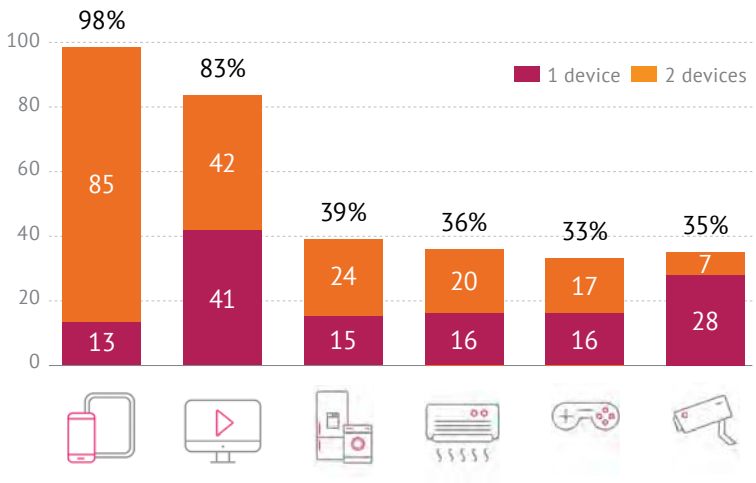
CIS / № 3 (9) / 2019 / www.cismag.ru

НМ CORE – платформа безопасности IoT для дома и малого офиса

«УМНЫЙ ДОМ» – БЕЗОПАСНЫЙ ДОМ?

Опрос потребителей

Количество домашних устройств интернета-вещей (IoT) среди опрошенных*



83%
Как минимум 1 IoT устройство, кроме ПК, Смартфонов, Планшетов

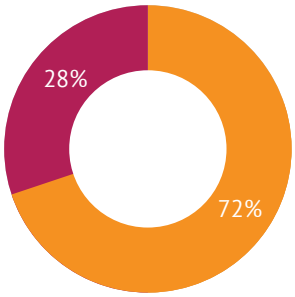
25%
Более 10 IoT устройств, кроме ПК, Смартфонов, Планшетов

Что беспокоит потребителей?*

33% – нарушение частной жизни (Приватность)
22% – кибератаки
26% – зависимость от технологий
18% – сложность технологий
6% – стоимость

По возрастным группам
18-60 лет – приватность и кибератаки
60 лет и более – зависимость от технологий и кибератаки

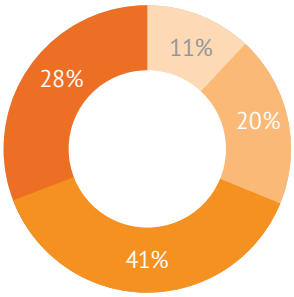
Готовы ли потребители платить за безопасность IoT?*



ДА
НЕТ

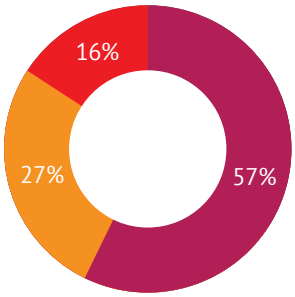
72%
готовы платить за безопасность IoT.

Сколько вы готовы заплатить за безопасность в месяц IoT?*



1-2$
До 5$
До 10$
До 15$

Кому вы доверите защиту вашего «подключённого» дома?*



Интернет-провайдер
Без разницы
Поставщики решений безопасности AV и пр.

* Исследование Allot Connected Home Cybersecurity: consumer perspective Teleco Security Trends Q3 2018.
Опрос 1261 респондента в 10 странах мира от 18 до 60 лет.

Решение: платформа безопасности IoT для дома

Для чего нужно решение?

Мы разработали простое и доступное для домашних пользователей решение, основанное на мобильном приложении и дополнительных облачных сервисах, которое позволяет провести оперативную диагностику и получить ответы на следующие вопросы:

- Какие устройства подключены к моей домашней сети?
- Есть ли среди них неавторизованные или незнакомые устройства?
- Какие проблемы безопасности обнаружены?
- Что делать, чтобы их устранить?

Если пользователь заинтересован в повышении уровня безопасности своей сети, он с помощью нашего приложения сможет подключить дополнительные сервисы безопасности и управления устройствами в своей сети.

Наше решение – HM CORE – преследует простую цель – привнести в жизнь обычного человека, окружённого огромным количеством различных ИТ-решений от смартфона до «умного» тостера, удобную и быструю безопасность. Достаточно нажать одну кнопку в мобильном приложении, установленном на вашем телефоне, и наше решение позаботится о:

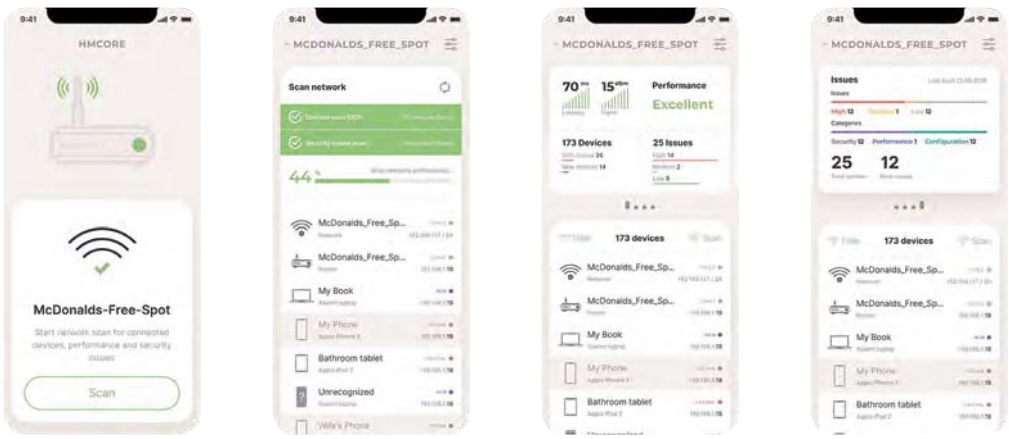
- выявлении уязвимости во всех «железках», которые стоят дома;
- своевременном устранении уязвимостей или их скрытии от хакеров;
- фильтрации опасного контента в интернете для каждого устройства в доме;
- блокировке рекламы;
- приватности работы в интернете (VPN, Tor и пр.);
- управлении всеми устройствами «умного дома» (IoT) с обычного телефона.

---

* Независимость от производителя и оборудования.
Поддерживаемые модели: MikroTik, в разработке Linksys, TP-Link, D-Link, ASUS, ZTE, Netgear и другие WRT маршрутизаторы, а также все устройства, поддерживающие CWMP/TR069 и другие протоколы управления CPE.

Выход на рынок: осведомлённость (как канал продаж)

2019 рынок B2C, распространение через AppStore и Google Play Market
Цель на конец года более 10000 активных пользователей, из которых более 15% используют подписку.
Мобильный сканер безопасности для SOHO (Small Office Home Office) сетей и IoT.



Основные подходы к реализации решения:

- решение делается строго в виде мобильного приложения, которое можно будет поставить на основные мобильные платформы (iOS, Android);
- все сервисы будут поставляться по подписке из облака, для этого достаточно будет подключить свой роутер к нашему облаку или заказать услугу у провайдера.

Технологические и рыночные преимущества:

- отсутствие необходимости покупать отдельное аппаратное устройство;
- гибкое управление услугами и необходимым функционалом. Так каждую конкретную услугу можно будет купить с телефона.

Выход на рынок: управление и безопасность

B2C

2019-2020
Мобильное приложение, агент и облачный сервис

Домохозяйства и малый бизнес – распространение через AppStore и Google Play Market.

2020-2021
B2C Мобильное приложение, собственно устройство и облачный сервис

Домохозяйства и малый бизнес – распространение через e-commerce и приложение.

B2B

2020-2022
Интернет-провайдеры – возможность расширить спектр услуг для клиентов (Прямые продажи).

Производители оборудования – возможность партнёрства для развития сервиса и улучшения безопасности оборудования.

Основные рынки сбыта:

В качестве основных и первоочередных рынков сбыта рассматриваются Северная и Южная Америка. Наши опросы показывают, что на текущий момент жители США и обладают большим количеством IoT устройств дома, осведомлены о существующих угрозах и в значительной степени обеспокоены безопасностью своей частной жизни. На российский рынок компания планирует выходить не ранее чем через несколько лет после запуска продукта в Америке.

Широта пользовательского охвата будет достигаться через одновременный запуск сразу двух каналов распространения. По модели B2C приложение будет распространяться через App Store и Google Market и станет доступным во всех магазинах по всему миру. Это означает, что любой пользователь платформы iOS или Android будет иметь возможность воспользоваться приложением и подписаться на дополнительные услуги. Также продажи будут осуществляться через телеком-провайдеров (первый и основной рынок – США, затем Южная Америка и Европа).

Рынок безопасности «Интернета вещей» (IoT) для дома

Поставщики решений ИТ-безопасности (Security vendors)	**Производители домашних сетевых устройств** (SOHO WiFi router vendors)	**Новые игроки** (New players)
«Безопасные» WiFi маршрутизаторы (Secure WiFi router)	**Маршрутизаторы, интегрированные с платформами безопасности от MacAfee и TrendMicro**	**Производство «безопасных» маршрутизаторов Secure WiFi router**
Avast Smart Home Security – not release yet **Trend Micro** Home Network Security – Авг 2018 **Bitdefender** Box 2 – Декабрь 2017 **F-secure** SENCE – Осень 2017 **Norton** Core Secure WiFi Router – Весна 2017	**Trend Micro Smart Home Network™** • ASUS + AiProtection powered by Trend Micro • NTT DOCOMO Hikari Router 01 **McAfee Secure Home Platform** • Arris • скоро для новых D-Link роутеров	**Fing:** FingBox **Cujo:** AI Smart Internet Security Firewall **Dojo:** Dojo Smart internet security and privacy solution **Roqos:** Core VPN Router – Next Generation UTM Firewall **Firewalla:** Cyber Security Firewall for Home & Business **Gryphon Connect**

Пример схемы работы с Secure WiFi router

WiFi роутер и/или модем
(собственный и/или провайдера)

«безопасный» роутер
Межсетевой экран

мобильное приложение
для управления

Рынок безопасности IoT и домашних сетей относительно молодой, можно сказать, что данная проблема находится в фокусе внимания, начиная с 2014 года. Существует два основных подхода к защите IoT устройств, первый из которых «агентский» (endpoint security), второй – «сетевой» (security gateways). В первом случае это установка на каждое IoT устройство агентского решения (аналогично антивирусу). Такую технологию продвигает MacAfee, разработав свой антивирусный агент для «умных» телевизоров MacAfee Security for TV. Второй подход заключается в установке дополнительного сетевого устройства, аналогичного UTM (Unified Threat Management), для защиты домашней сети и устройства «Интернета-вещей». Этим путём идёт большинство производителей решений безопасности и управления IoT.

Мы ориентируемся на второй подход. Однако наше принципиальное отличие состоит в максимальном использовании уже имеющегося оборудования (Wi-Fi маршрутизатор) и устройства пользователя – смартфон (iOS или Android).

Пользовательский опыт

Сканируй

- Установи приложение
- Запусти сканирование
- Узнай
  - кто использует твою сеть
  - какие проблемы есть
  - что делать, чтобы их решить

Регистрируйся

- Зарегистрируйся и предоставь доступ
- Мы упрощаем управление;
- Ты решаешь самому управлять или пользоваться нашими услугами
- Мы помогаем:
  - конфигурировать устройство
  - обеспечивать безопасность
  - обеспечивать поддержку.

Управляй

- Управляй из любой точки мира
- Получай отчеты и уведомления
- Контролируй скорость, производительность и безопасность, подключенные IoT устройства
- Блокируй атаки, устройства, пользователей и Интернет-ресурсы
- Управляй умными устройствами IoT

Коммерческие услуги

Кибербезопасность

- Обнаружение угроз
- Кибеpразведка и аналитика
- Виртуальные патчи и обновления
- Фильтрация вредоносного контента
- Защита от хакеров и вредоносного ПО

Родительский контроль

- Пауза (Время для семьи)
- Время сна и уроков
- Контентный фильтр
- История посещений
- Безопасный поиск и YouTube

Приватность и VPN

- Блокировка рекламы и трекеров
- VPN для домашней сети
- Приватный веб-серфинг
- Интеграция с TOR и I2P

«Умные дома» и IoT

- Управление домашними IoT из приложения
- Интеграция устройств от различных производителей
- Отчётность с устройств в одном месте

Маршрутизаторы и DSL модемы, доступные через интернет

SHODAN

censys

Total results: 1,787,905

Top countries

Brazil	396,453
United States	253,698
Russian Federation	108,633
Pakistan	69,338
Canada	59,635

Top services

HTTP	600,283
Telnet	285,282
HTTP (8080)	278,155
SNMP	157,606
SMB	88,296

Top organizations

Vivo	66,250
Oi Velox	62,417
Algar Telecom	52,840
Oi Internet	46,675
Rostelecom	13,094

IPv4 Hosts

Page: 1/314,842 Results: 7,871,036
Time: 327ms

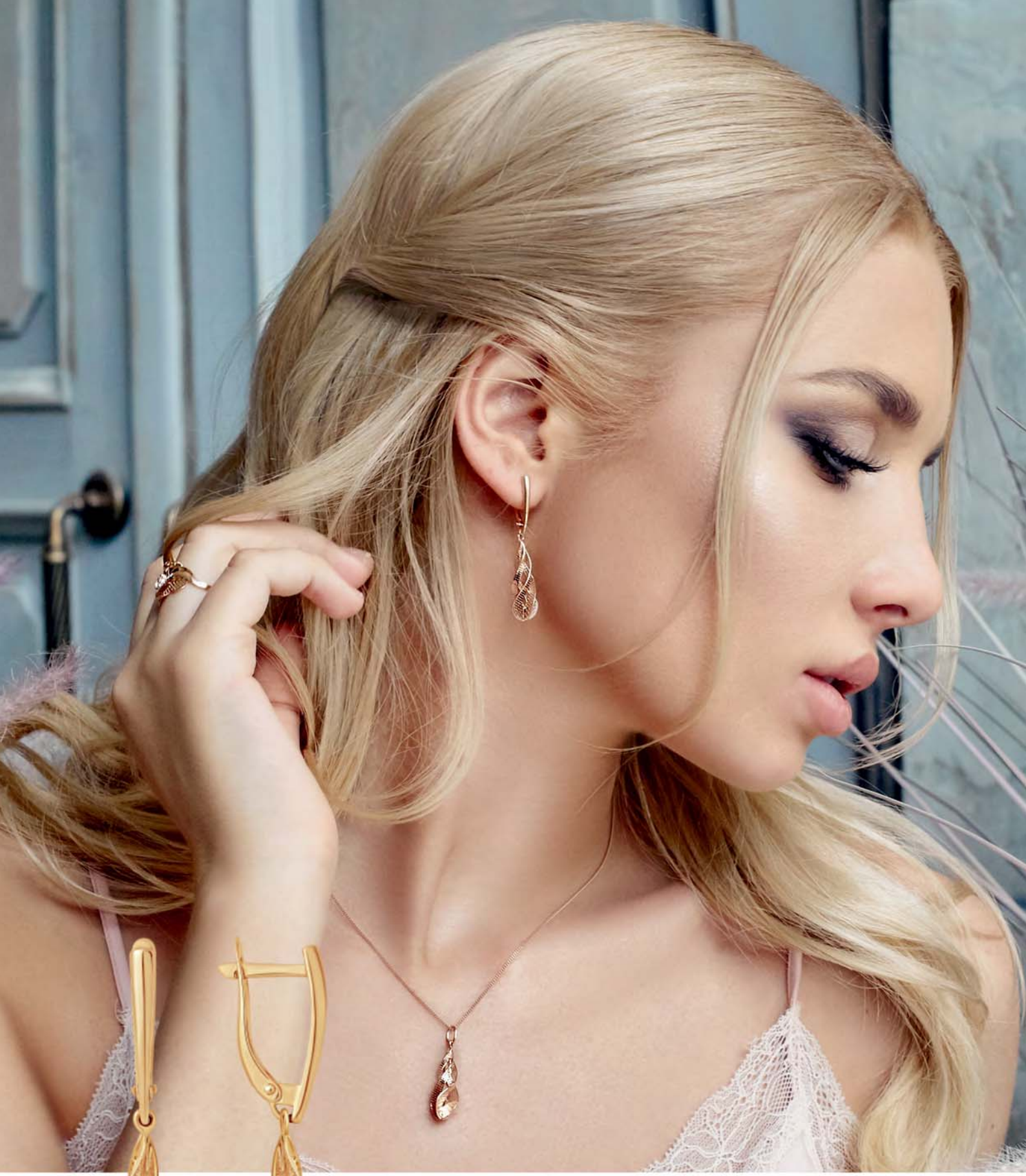
Country Breakdown

Country	Hosts	Frequency
United States	2,953,064	37.52%
Brazil	464,440	5.9%
United Kingdom	317,667	4.04%
Poland	309,362	3.93%
Russia	192,397	2.44%
Spain	191,318	2.43%
Vietnam	190,564	2.42%
Canada	179,153	2.28%
China	174,734	2.22%
Venezuela	169,872	2.16%

Количество маршрутизаторов и модемов напрямую, доступных через Интернет.

Маршрутизатор – центр сети и центр проблем безопасности

- Стандартные пароли (default passwords)
- Открытые сервисы управления через Telnet / HTTP / SSH / WinBox
- Открытый UPnP позволяет удалённую настройку
- Обновления прошивок (Firmware updates)
- Политики безопасности;
- Мониторинг и анализ
- Управление и поддержка
- Фильтрация сетевого трафика
- Управление IoT устройствами
- Обнаружение атак по WiFi



Бренд EFREMOV — это современные утончённые ювелирные украшения, настоящий европейский стиль на российском рынке!

EFREMOV

Бренд EFREMOV эксклюзивно для конкурса «Мисс CIS» создал главный приз — корону победительницы.

«Мисс CIS» — всероссийский ежегодный конкурс красоты среди девушек, работающих в ИТ-сфере, организованный журналом CIS.

Миссия конкурса — выявить самых красивых девушек на звание «Мисс CIS» и сделать из обладательницы короны символ информационной безопасности России.

efremov.gold

CIS / № 3 (9) / 2019 / www.cismag.ru

Необходимость создания информационной экосистемы «Роскосмос 2.0» в условиях антикризисного управления в ракетно-космической отрасли России

Переход к этапу четвёртой промышленной революции и к «Индустрии 4.0» в России начался и продолжается на фоне серьёзных кризисных процессов в различных отраслях экономики, в том числе в ракетно-космической отрасли.

От когда-то сильной административно-командной и научно-производственной систем, сформированных ещё при Сергей Павловиче Королёве, осталась крайне деформированная система, характеризующаяся низкой эффективностью работы предприятий. Структурные и управленческие диспропорции, ставящие первоочередными задачи «псевдо или цифрового бизнеса», а не развитие космической отрасли, отсутствие стимулов развития производства, низкая управленческая и информационная культура, проблемы сбыта отечественной продукции, отсутствие опыта работы большинства руководителей предприятий в рыночных условиях (т.е. не на рынке гособоронзаказа, а, как говорят, «реальном» внутреннем и внешних рынках) и полное непонимание процессов формирования «Цифровой экономики» Российской Федерации ведут к потере управляемости и рентабельности многих предприятий в ракетно-космической отрасли.

На сегодняшний день уровень эффективного управления отраслью определяется не только величиной социально-экономических показателей, но и в большей степени уровнем и числом внедряемых технологий эры четвёртой промышленной революции, таких как робототехника, искусственный интеллект, исследования, разработка и развитие новых вычислительных и информационных технологий (ИТ), концепция «цифровой экономики», которая включает Интернет вещей и ценностей, а также технологии производства передовых материалов и многомерной печати, био- и нейротехнологии, виртуальная и дополненная реальность и многие другие.

На конференции «Стратегия развития информационных технологий Госкорпорации «Роскосмос», прошедшей в конце 2018 года в НПО «Энергомаш», генеральный директор Госкорпорации «Роскосмос» Дмитрий Рогозин отметил: «Весь мир вступает в эпоху цифрового бизнеса, и это порождает волну инноваций во многих отраслях, в том числе прежде всего в ракетно-космической». Здесь, конечно, хочется акцентировать внимание на словах «цифровой бизнес» и «инновации» в ракетно-космической отрасли, которые вызывают недопонимание, и задать вопрос: «Бизнес» и «космос» в России – вещи совместимые?» На мой взгляд, уместнее было бы обратить внимание на взаимосвязь и развитие «космоса» и «цифровой экономики» Российской Федерации. О каком «бизнесе» может идти речь?

Но в то же время нельзя не согласиться с Дмитрием Олеговичем в том утверждении, что: «Чтобы колонизировать и развивать страну, надо создавать принципиально новую государственную экономическую инфраструктуру… Всё это нужно делать с помощью космических технологий…»

Как говорил Сергей Павлович Королёв: «То, что казалось несбыточным на протяжении веков, что вчера было лишь дерзновенной мечтой, сегодня становится реальной задачей, а завтра – свершением». И как мне представляется, «космос» сегодня – это не только «реальная задача» – это «свершение»!

Тем не менее в ракетно-космической отрасли мы имеем не только проблемы менеджмента, но и серьёзные проблемы в направлении создания и развития единой информационной платформы как основы цифрового пространства или цифровой экосистемы отрасли «Роскосмос 2.0».

Как известно, с введением нового управления на предприятиях отрасли одной из основных задач антикризисных менеджеров является реинжиниринг и реализация бизнес-процедур организаций с целью выведения их из финансового кризиса. И, как мы все понимаем, успешное достижение поставленных целей и реализация задач на сегодняшнем этапе невозможно осуществить без использования новых информационных технологий и технологий четвёртой промышленной революции, которые способствовали бы развитию научно-производственной базы и принятию своевременных и оптимальных управленческих решений в условиях формирования «цифровой экономики».

В текущих условиях антикризисным управляющим в области информационных технологий, или, проще говоря, новым руководителям ИТ-служб предприятий ракетно-космической отрасли, необходимо уже решать в кратчайшие сроки ещё одну важную задачу – реорганизацию бизнес-процедур предприятия на уровне большого числа разрозненных информационных систем, т.е. на фоне отсутствия и необходимости создания единой отраслевой цифровой платформы.

И здесь мы имеем явное управленческое упущение, которое может повлечь серьёзные финансовые и репутационные риски для отрасли, заключающиеся в том, что подобные виды работ хоть и предусмотрены Стратегией развития информационных технологий Госкорпорации «Роскосмос», но относятся к так называемому второму этапу её реализации в 2022-2026 годах, который *«является базовым с точки зрения перехода на уровни «наглядность», «проницаемость» «Индустрии 4.0»…»*

Говоря о Стратегии, невольно задаёшься вопросом: что это за слова «связанность», «наглядность», «проницаемость», «оптимизация», «предсказуемость» и «самоорганизация», обозначающие основные этапы реализации Стратегии «Роскосмоса»? И кто это писал? Возможно, господам «маркетологам» нужно было посоветоваться со специалистами? Или, например взять на вооружение слово «перфекционизм». Тому есть наглядный пример, когда всем известное решение оптимизируется, становится легче, потребляет меньше топлива, стоит в разы дешевле и позволяет зарабатывать в разы больше.

Согласно официальному пресс-релизу «Роскосмоса» от 26.12.2018 на предприятиях ракетно-космической отрасли существуют две полярные ситуации использования и развития информационных систем и цифровых платформ. Первая связана с отсутствием, например информационных систем управления жизненным циклом продукции (Product Lifecycle Management, PLM) или управления ресурсами предприятия (ERP). Где-то только сейчас происходят процессы их внедрения и комплексное переоснащение рабочих мест конструкторов и технологов и так далее. При второй ситуации на предприятиях накоплен богатый фонд хорошо отработанных программных и аппаратных решений «под ключ», поставщики которых обеспечивают комплекс услуг по выбору, инсталляции, адаптации, обучению и технической поддержке используемых систем. Это даёт нам понимание того, что относительно быстрое и требующее меньших затрат решение задачи

реорганизации ИТ и создания единой распределённой цифровой платформы отрасли и соответствующих центров компетенций по таким направлениям, как «Искусственный интеллект», «Интегрированная система управления», «Цифровизация производства и жизненного цикла изделий», «Система математического моделирования», «Big Data», «Ситуационно-аналитический центр» и другим, возможно лишь на базе данных предприятий.

Ещё раз хочется обратить ваше внимание на тот факт, что реорганизация и дальнейшее успешное функционирование предприятий ракетно-космической отрасли и корпорации «Роскосмос» невозможно без использования новых информационных технологий и технологий четвёртой промышленной революции.

Вне зависимости от одной из выше описанных критических ситуаций руководители ИТ-служб предприятий ракетно-космической отрасли, в текущих условиях выступающие, по сути, как антикризисные менеджеры, должны знать современные методы разработки, внедрения или реорганизации цифрового пространства и создания цифровой экосистемы отрасли, чтобы способствовать правильной организации работ связанных с её созданием. К числу таких методов можно отнести подход нового системного проектирования, центральной задачей которой станет формирование и оптимизация единого технологического ядра корпоративного облака с целью реализации возможности «сквозной» автоматизации процессов конструирования, производства и управления предприятиями, а также формирование инфраструктуры «больших данных» с целью обеспечения работы «сквозных» виртуализированных сервисов массового сбора и обработки данных на основе технологий индустриального интернета вещей (так называемый Industrial Internet of Things, IIoT), больших данных (Big Data) и искусственного интеллекта (Artificial Intelligence, AI).

Нужно отметить, что в значительной степени именно новейшие достижения в области информационных технологий дают новые возможности для развития предприятий в период формирования «цифровой экономики», а также информационные технологии являются основой формирования технологической платформы реальной реорганизации цифрового бизнеса на предприятии и цифровой платформой для формирования новых доверительных отношений и возможностей людей.

Для того чтобы создать эффективную цифровую экосистему «Роскосмос 2.0», нужно понимать и принять следующее:

1. Всегда существует двунаправленное воздействие между научно-техническими, производственными процессами и цифровыми платформами, которые должны лечь в основу создания цифровой экосистемы отрасли.
2. Если научно-технические, производственные процессы или цифровые платформы меняются, то маловероятно, что соответствующая наследуемая ИТ-архитектура (в том числе серверная инфраструктура центров обработки данных) сохранится. Это должно учитываться непосредственно в Стратегии развития информационных технологий Госкорпорации «Роскосмос», особенно при реализации её первого этапа в 2019-2021 годах, а также при разработке проекта создания Национального космического центра.
3. Соответствие между научно-техническими, производственными процессами и цифровыми платформами является решающим фактором успеха, но на его достижение может уйти значительное время. Опыт последних двадцати лет в области ИТ подсказывает, что весь объём работ, который запланирован в Стратегии развития информационных технологий Госкорпорации «Роскосмос» в период с 2019 по 2030 годы, можно реализовать за три-пять лет или увеличить объём выполняемых работ в рамках того же срока в три-пять раз.

Накопленный за последние двадцать лет научный потенциал, определяющий методологию, методы и методики создания цифровых платформ, позволяют в текущих условиях достаточно быстро найти нужный оптимальный путь, который позволит достигнуть качественно новых результатов в управлении и развитии высокотехнологичного производства продукции и услуг в ракетно-космической отрасли.

Текущие события на предприятиях «Роскосмоса» свидетельствуют о том, что многие из них по тем или иным причинам не вписываются в рамки текущих рыночных условий. Это вынуждает многие из них произвести реинжиниринг основных видов деятельности и, как следствие, изменить научные и производственные процессы на предприятиях. Как было указано выше, изменение бизнес-платформы влечёт за собой не только изменение ИТ-архитектуры, но и её платформы. Успешный переход на новую эффективную цифровую экосистему «Роскосмос 2.0», построение новой ИТ-архитектуры способствует успешному решению задач реорганизации бизнес-процедур любого из предприятий «Роскосмоса».

В результате к классическим методам разработки цифровых платформ предъявляется ряд принципиально новых требований. Новые методы проектирования данных платформ должны обладать повышенной гибкостью для обеспечения живучести предприятия в условиях общего бизнес-реинжиниринга предприятия и формирования взаимоотношений в «цифровой экономике». И, как следствие, к классическим методам проектирования добавляются новые со своими наборами методов и математическим аппаратом.

Интеграция подходов бизнес-реинжиниринга, новых информационных технологий, социопсихологических методов и технологий четвёртой промышленной революции позволяют создавать уникальные цифровые экосистемы.

Важно отметить, что точка пересечения этих технологий представляет собой область формирования инновационного цифрового производства в рамках развития концепции «Промышленность 4.0».

Подводя итог, хочется отметить ещё раз столь значимое для нашей страны и экономики событие, а именно появление Стратегии развития информационных технологий Госкорпорации «Роскосмос», по сути, являющейся новым толчком развития как ракетно-космической отрасли, так и рынка новых и информационных технологий Российской Федерации, и закончить словами Сергея Павловича Королёва: «Можно сделать быстро, но плохо, а можно – медленно, но хорошо. Через некоторое время все забудут, что было быстро, но будут помнить, что было плохо. И наоборот».

Александр Чесалов
Директор по развитию ООО «Программные Системы Атлансис»,
Член Совета ТПП РФ по развитию информационных технологий и цифровой экономики, д. т.н., Член-корр. РАЕН

eToken

Продукты линейки eToken –
основа инфраструктуры информационной
безопасности современного предприятия

etokenstore.ru

CIS / № 3 (9) / 2019 / www.cismag.ru

Первый в России корпоративный турнир по киберспорту «Киберлига Корпораций» пройдёт при поддержке «Ростеха»

Всероссийское физкультурно-спортивное общество «Трудовые резервы» презентовало самый масштабный в истории России чемпионат по киберспорту.

«Киберлига Корпораций» состоится осенью текущего года при поддержке Госкорпорации «Ростех» – стратегического партнёра «Трудовых резервов». Об этом было объявлено в ходе IV конференции «Цифровая индустрия промышленной России», которая проходит в эти дни в Иннополисе (Татарстан). Киберспортсмены будут бороться за первенство в пяти дисциплинах, являющихся наиболее популярными во всём мире: Dota 2, Counter-Strike, World of Tanks, FIFA 19 и HearthStone. Регистрация на турнир продлится до 13 сентября. Желающие смогут принять участие в корпоративной лиге как в составе команды, так и в индивидуальном зачёте. «Киберспорт – одно из самых быстроразвивающихся направлений спортивной индустрии. По итогам 2018 года Россия занимает 3 место в мире по размеру аудитории киберспортивных мероприятий, она составила более 22,3 млн человек. Это современный вид спорта, связанный с высокими технологиями. Он развивает командный дух, учит ставить цели и добиваться их. Новая лига объединит сотрудников промышленных предприятий России из самых разных отраслей – такого в отечественном киберспорте ещё не было», – сообщила директор по коммуникациям «Ростеха» Екатерина Баранова. В течение первых двух месяцев турнира пройдут отборочные игры. Для удобства участников лига разделена на три дивизиона: Запад, Центр и Восток. Киберспортсмены будут соревноваться друг с другом в режиме онлайн по субботам и воскресеньям. Лучшие команды и индивидуальные участники сыграют в финале, который пройдёт 22-24 ноября в Москве на одной из лучших киберспортивных арен страны Cyberspace. «Спорт постоянно трансформируется, появляются новые дисциплины и целые направления, которые привлекают всё больше участников и зрителей. Первые корпоративные киберспортивные игры позволят найти единомышленников, сплотят коллективы и позволят проявить себя с неожиданной стороны любому представителю компании: от рядового сотрудника до топ-менеджера», – считает президент ВФСО «Трудовые резервы» Илья Галаев.

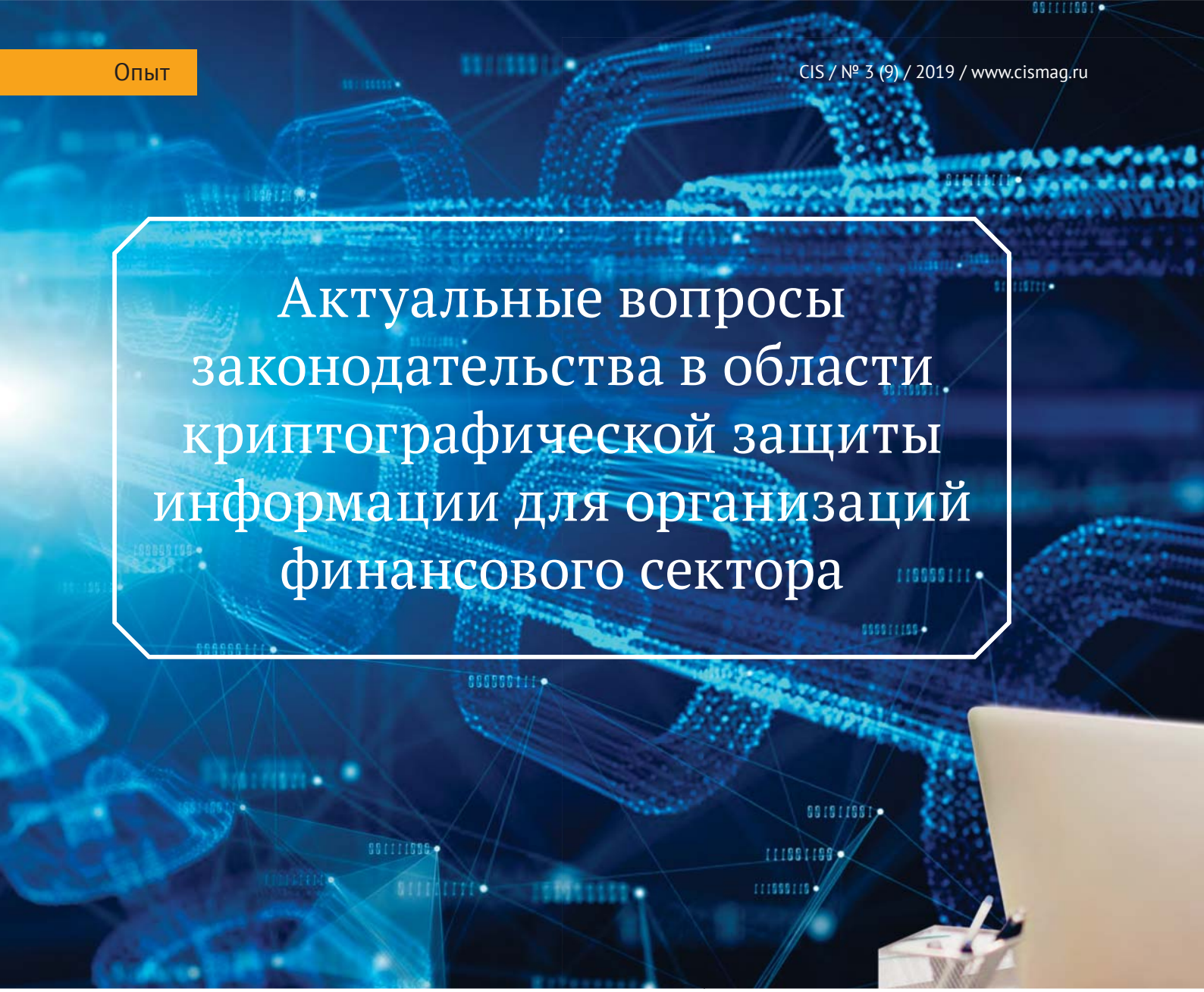
Конференция «Цифровая индустрия промышленной России – 2019» проходит с 22 по 24 мая в городе Иннополис (Республика Татарстан). ЦИПР-2019 традиционно объединяет руководителей федеральных, региональных ведомств, представителей крупного бизнеса и стартапов, частных инвесторов и государственные институты развития, предпринимателей-практиков и представителей научного сообщества. В конференции принимают участие более 5000 делегатов и 370 спикеров. ЦИПР-2019 посвящён сквозным цифровым технологиям и перспективам их развития в России. **ВФСО «Трудовые резервы»** воссоздано по поручению Президента РФ в марте 2018 года и объединяет предприятия промышленного, оборонно-промышленного и энергетического комплексов страны. Основная цель проекта – развитие корпоративного спорта и массовое привлечение работников российской промышленности к занятиям физкультурой. Стратегическим партнёром общества является Госкорпорация «Ростех». Под эгидой ВФСО проводятся знаковые любительские спортивные соревнования: Российские и Мировые корпоративные игры, Фестиваль дрон-рейсинга Rostec Drone Festival, региональные турниры по командным видам спорта. Среди дисциплин, которые проводятся под эгидой «Трудовых резервов», есть как командные (мини-футбол, баскетбол, волейбол), так и индивидуальные виды спорта (бильярд, большой теннис, шахматы) – всего 27 дисциплин. **Госкорпорация «Ростех»** – одна из крупнейших промышленных компаний России. Объединяет более 700 научных и производственных организаций в 60 регионах страны. Ключевые направления деятельности – транспортное машиностроение, электроника, медицинские технологии, химия и инновационные материалы. Холдинги «Ростеха» формируют три кластера: радиоэлектроника, вооружение и авиация. В портфель корпорации входят такие известные бренды, как АВТОВАЗ, КАМАЗ, Концерн Калашников, «Вертолёты России», «Уралвагонзавод» и др. «Ростех» активно участвует в реализации всех 12 национальных проектов. Компания является ключевым поставщиком технологий «Умного города», занимается цифровизацией государственного управления, промышленности, социальных отраслей, разрабатывает планы развития технологий беспроводной связи 5G, промышленного интернета вещей, больших данных и блокчейн-систем. «Ростех» выступает партнёром ведущих мировых производителей, таких как Boeing, Airbus, Daimler, Pirelli, Renault и др. Продукция корпорации поставляется более чем в 100 стран мира. Почти треть выручки компании обеспечивает экспорт высокотехнологичной продукции.

Ростех

Партнер в развитии

Пресс-служба
тел. +7 (926) 911-28-36
Москва, ул. Усачева, д. 24

www.rostec.ru



Актуальные вопросы законодательства в области криптографической защиты информации для организаций финансового сектора

Как известно, банковская сфера да и в целом финансовый сектор являются одной из наиболее зарегулированных с точки зрения законодательства по информационной безопасности областью экономики нашей страны. С каждым годом появляется всё больше нормативных правовых актов, регулирующих вопросы защиты информации и требующих от банков и других организаций финансового сектора применения тех или иных организационных и технических мер защиты информации.

Поэтому финансовым организациям важно уметь ориентироваться во всём многообразии выпускаемых регуляторами документов. В настоящей статье речь пойдёт о некоторых актуальных вопросах законодательства в области криптографической защиты информации для финансовых организаций.

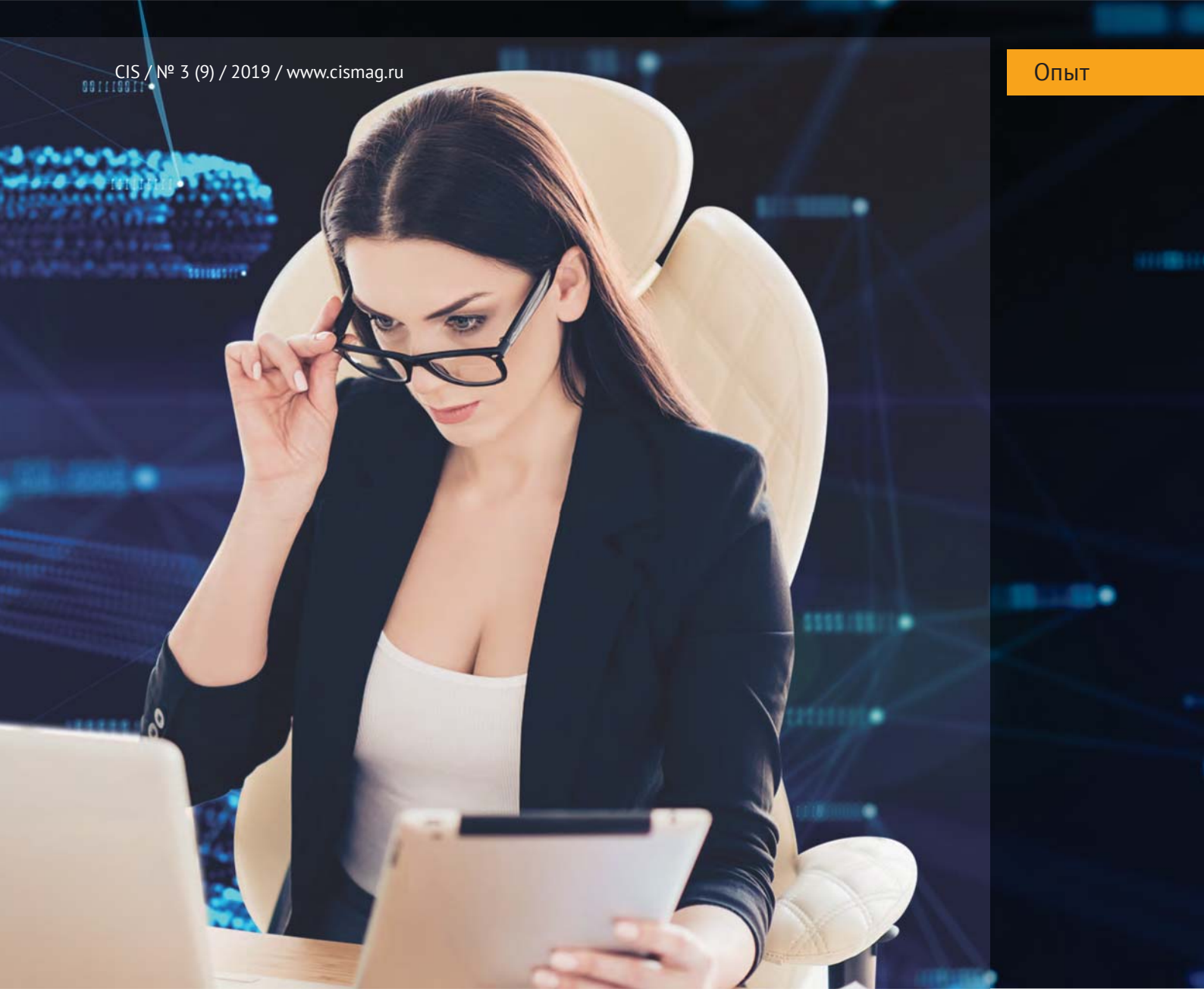
Единая биометрическая система (ЕБС)

С появлением Единой биометрической системы (ЕБС) любому клиенту банка (гражданину РФ) достаточно зарегистрироваться в данной системе один раз, после чего он сможет удалённо получать услуги в любом банке, подключённом к ЕБС.

В части взаимодействия банков с ЕБС положениями Федерального закона от 07.08.2001 № 115-ФЗ (№ 115-ФЗ), введёнными Федеральным законом от 31.12.2017 № 482-ФЗ (№ 482-ФЗ), установлено следующее:

- банки обязаны при личном присутствии клиента и с его согласия размещать биометрические персональные данные в ЕБС (регистрация биометрии);
- банки вправе предоставлять услуги без личного присутствия клиента после его успешной удалённой идентификации с использованием ЕБС.

Порядок проведения банками регистрации биометрии и удалённой идентификации пользователя с использованием ЕБС регламентируется статьёй 14.1 Федерального закона от 27.07.2006 № 149-ФЗ, введённой № 482-ФЗ. В том числе банки должны обеспечить и защиту от угроз безопасности, предписанную Указанием Банка России и ПАО «Ростелеком» от 09.07.2018 № 4859-У/01/01/782-18 (Указание № 4859-У). Кроме этого, банки должны придерживаться методических рекомендаций Банка



России по нейтрализации банками соответствующих угроз безопасности (4-МР от 14.02.2019).

Согласно информационному письму от 28.06.2018 № ИН-03-13/40 Банка России все подразделения банков должны соответствовать указанным требованиям до конца 2019 года.

Регистрация биометрии и требуемые классы защиты

Пользователь лично приходит в филиал банка для регистрации своих биометрических данных в ЕБС. Далее оператор производит сбор биометрии пользователя и передаёт данные в защищённом виде в головной офис банка. При этом биометрия заверяется сотрудником и отправляется по защищённому каналу с использованием средств криптографической защиты информации (СКЗИ) класса КС3.

На стороне банка биометрические данные проходят проверку на соответствие требованиям, установленным Приказом Минкомсвязи от 25.06.2018 № 321. В случае успешного прохождения контроля качества пользовательская информация подписывается усиленной квалифицированной электронной подписью (ЭП) банка и направляется в ЕБС. На стороне ЕБС биометрические данные также проходят контроль качества, и в случае успеха на их основе формируется биометрический контрольный эталон пользователя.

Согласно упомянутому Указанию Банка России биометрические данные пользователя должны передаваться банком по защищённому каналу, их защита от угрозы нарушения конфиденциальности осуществляется с использованием СКЗИ класса КС3.

Неизменность передаваемых данных подтверждается банком с помощью усиленной квалифицированной ЭП. Для этого банки должны использовать HSM, сертифицированный ФСБ России по классу КВ2/КВ. Для этих целей можно, например, использовать ПАКМ КриптоПро HSM, имеющий необходимые сертификаты ФСБ России.

Удалённая идентификация и требуемые классы защиты

Согласно Указанию № 4859-У ПДн пользователя и информация о степени соответствия должна передаваться в банк по защищённому каналу с использованием СКЗИ класса КС3. Для обеспечения защиты от подмены или удаления информации о степени соответствия биометрии пользователя банк должен проверять подпись данной информации с использованием СКЗИ класса КВ2/КВ. Как и при регистрации биометрии, для этих целей также можно использовать ПАКМ КриптоПро HSM.

Между банком и устройством пользователя устанавливается защищённое соединение с аутентификацией банка по протоколу TLS. Независимо от того, с какого устройства физическое лицо собирается провести удалённую идентификацию, оно должно иметь возможность использовать для этого СКЗИ, сертифицированное по классу не ниже КС1, а банк на своей стороне должен использовать СКЗИ, сертифицированное по классу не ниже КС3.

Если для удалённой идентификации физическое лицо использует мобильное устройство (смартфон или планшет), то оно обязано использовать СКЗИ, сертифицированное по классу не ниже КС1. Иначе банк должен будет отказать ему в удалённой идентификации.

Если для удалённой идентификации физическое лицо использует иное устройство (например, ПК с браузером) и при этом отказывается от использования сертифицированных СКЗИ, принимая соответствующие риски, то у физического лица должна быть возможность использовать несертифицированные СКЗИ (в том числе с использованием зарубежных криптографических алгоритмов). А банк со своей стороны, соответственно, должен обеспечить для физического лица такую возможность.

Таким образом, для обеспечения удалённой идентификации физического лица банк обязан одновременно обеспечить на своей стороне поддержку как TLS ГОСТ, так и зарубежного TLS. При этом СКЗИ, реализующее на стороне банка TLS ГОСТ, должно быть сертифицировано по классу не ниже КС3. Это в свою очередь накладывает ограничения на удовлетворяющий указанным требованиям перечень технических средств, которые можно использовать для решения постав задачи. Так, например, одновременная поддержка TLS ГОСТ и зарубежного TLS в настоящее время реализована в продуктах КриптоПро и уже несколько месяцев обеспечивается при доступе к сайту cryptopro.ru (можно попробовать самостоятельно, предварительно установив на своё устройство КриптоПро CSP 4.0 и, например, Яндекс. Браузер). В частности, КриптоПро NGate, сертифицированное по классу КС3, способно решить поставленную задачу по идентификации физического лица с соблюдением всех необходимых требований.

683-П и 684-П Банка России (замена SMS и PUSH-уведомлений)

Последние несколько лет в профессиональном сообществе по информационной безопасности активно обсуждается вопрос недостаточного уровня безопасности, предоставляемого SMS и PUSH-уведомлениями при проведении клиентами финансовых организаций соответствующих транзакций. При этом 17 апреля 2019 года Банк России утвердил два очень схожих положения, предъявляющих обязательные требования к обеспечению защиты информации в целях противодействия осуществлению переводов денежных средств без согласия клиентов (683-П – для кредитных организаций) и незаконных финансовых операций (684-П – для некредитных финансовых организаций).

Соответствующие пункты обоих положений (п. 5.1683-П и п. 10684-П) говорят о том, что финансовые организации должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом. Признание же электронных сообщений, подписанных электронной подписью, равнозначных документам на бумажном носителе, подписанных собственноручной подписью, должно осуществляться в соответствии со ст. 6, 63-ФЗ «Об электронной подписи». Данное требование регулятора многие специалисты трактуют как необходимость замены SMS и PUSH-уведомлений на более безопасные механизмы, способные обеспечить целостность и авторство отправляемых электронных сообщений. Это связано с тем, что, если факт составления электронного сообщения уполномоченным на это лицом (авторство) ещё можно как-то доказать, прописав в соответствующих соглашениях, то обеспечить целостность средствами SMS и PUSH-уведомлений (которые, по сути, представляют собой простую электронную подпись) без применения криптографических средств практически невозможно. Даже по определению из 63-ФЗ «Об электронной подписи» обеспечение целостности не является задачей простой электронной подписи.

Остаётся использовать либо усиленную неквалифицированную электронную подпись (НЭП), либо квалифицированную (КЭП). В данном случае при выборе между НЭП и КЭП есть всем известные за и против. Но в любом случае рекомендуется использовать именно сертифицированные ФСБ средства ЭП (в случае с КЭП – это обязательное условие), т. к. их использование существенно снижает риски организации по оспариванию подписи клиентом, в том числе в суде.

При этом и в случае с НЭП, и в случае с КЭП в качестве технических средств ЭП для решения поставленной задачи можно использовать, например, КриптоПро myDSS на базе программно-аппаратного комплекса облачной электронной подписи (ЭП) КриптоПро DSS. На данный момент КриптоПро myDSS является единственным на рынке сертифицированным ФСБ продуктом, способным решить указанную задачу.

Здесь важно ещё отметить, что указанные пункты 683-П и 684-П уже вступили в силу в 1 июня 2019 года.

ГОСТ Р 57580.1-2017 (Национальный стандарт по защите информации)

Положения настоящего стандарта распространяются на кредитные организации, некредитные финансовые организации, указанные в части первой статьи 76.1 Федерального закона «О Центральном банке Российской Федерации (Банке России)», а также на субъекты национальной платёжной системы. Таким образом, требования стандарта, кроме банков, также распространяются на некредитные финансовые организации, в частности на страховые и микрофинансовые компании.

Банк России сделал обязательным использование данного стандарта, сославшись на него в упомянутых выше положениях (683-П и 684-П). При этом требования данных положений по использованию стандарта вступают в силу с 1 января 2021 года.

Стандарт устанавливает три уровня защиты информации (и состав мер для каждого из них):

- уровень 3 – минимальный;
- уровень 2 – стандартный;
- уровень 1 – усиленный.

В части необходимости криптографической защиты информации стандарт говорит о том, что финансовая организация самостоятельно определяет необходимость использования средств криптографической защиты информации (СКЗИ), если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации, в том числе нормативными актами Банка России, стандартами, правилами профессиональной деятельности и (или) правилами платёжной системы.

Работы финансовой организации по обеспечению защиты информации с помощью СКЗИ должны проводиться в соответствии с требованиями законодательства РФ (63-ФЗ, ПКЗ-2005, 378-й приказ ФСБ) и технической документацией на СКЗИ.

При этом в случае, если финансовая организация применяет СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты или разрешения ФСБ России.

Применение СКЗИ, имеющих класс не ниже КС2, обязательно для 1 класса защиты при защите каналов связи и удалённого доступа в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определённых в модели угроз, и нарушителей безопасности информации финансовой организации.

Использование сертифицированных СКЗИ необязательно для обеспечения 2 и 3 уровня защиты при защите каналов связи и удалённого доступа (если это не противоречит другим нормативным правовым актам, в частности по защите персональных данных);

Кроме этого, стандарт требует от финансовых организаций проводить идентификацию, двухфакторную аутентификацию и авторизацию субъектов доступа после установления защищённого сетевого взаимодействия и выполнения двухсторонней взаимной аутентификации участников информационного обмена при передаче информации при осуществлении удалённого логического доступа.

Указанные выше задачи по защите удалённого доступа позволяет решить, например, VPN-шлюз КриптоПро NGate, имеющий сертификаты ФСБ России по классам КС1, КС2 и КС3. А в следующих версиях КриптоПро NGate сможет обеспечивать и защиту каналов связи по необходимому классу защиты.

Внесение изменений в положение Банка России 382-П

Изменения в 382-П вносятся в соответствии с указанием Банка России от 7 мая 2018 г. N 4793-У «О внесении изменений в 382-П». Далее приведены изменения в 382-П, касающиеся вопросов криптографической защиты информации.

Операторам значимых платёжных систем необходимо обеспечить использование:

- в аппаратных модулях безопасности информационной инфраструктуры платёжной системы (HSM) СКЗИ, реализующих иностранные криптографические алгоритмы, имеющих подтверждение соответствия требованиям, установленным ФСБ России. Это означает переход на сертифицированные ФСБ России HSM, реализующие иностранные криптографические алгоритмы. **Норма вступает в силу с 1 января 2024 года**.
- в HSM СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы РФ, имеющих подтверждение соответствия требованиям, установленным ФСБ России. Это означает переход на сертифицированные ФСБ России HSM, реализующие как отечественные, так и иностранные криптографические алгоритмы. **Норма вступает в силу с 1 января 2031 года**.
- СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы РФ, имеющих подтверждение соответствия требованиям, установленным ФСБ России, в иных технических средствах информационной инфраструктуры платёжной системы (т. е. исключая HSM), используемых при осуществлении переводов денежных средств, типы которых определяются Банком России по согласованию с ФСБ России. Это означает переход на сертифицированные ФСБ России СКЗИ (исключая HSM), реализующие как отечественные, так и иностранные криптографические алгоритмы. **Норма вступает в силу с 1 января 2031 года**.

Операторам национально значимых платёжных систем необходимо обеспечить использование HSM на базе иностранных криптографических алгоритмов и криптографических алгоритмов РФ, имеющих подтверждение соответствия требованиям, установленным ФСБ России, на основании требований 3342-У Банка России. Это означает переход на сертифицированные ФСБ России HSM, реализующие как отечественные, так и иностранные криптографические алгоритмы. **Норма вступает в силу с 1 января 2031 года**.

Операторы по переводу денежных средств, операторы услуг платёжной инфраструктуры вправе применять для обеспечения защиты информации при осуществлении переводов денежных средств СКЗИ иностранного производства в части, не противоречащей приведённым выше требованиям.

Обеспечение защиты информации с помощью СКЗИ осуществляется в соответствии с 63-ФЗ, Положением ПКЗ-2005 и технической документацией на СКЗИ. Обеспечение защиты персональных данных с помощью СКЗИ осуществляется в соответствии с 378-м приказом ФСБ России (то есть, если для защиты персональных данных используются СКЗИ, то они должны быть сертифицированы ФСБ России).

КРИПТОПРО

«КриптоПро» – разработка средств криптографической защиты информации.

info@cryptopro.ru
www.cryptopro.ru

Positive Technologies: небезопасное хранение данных – основной недостаток мобильных приложений

POSITIVE TECHNOLOGIES

Positive Technologies *– один из лидеров европейского рынка систем анализа защищённости и соответствия стандартам, а также защиты веб-приложений.*

Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

www.ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Эксперты протестировали мобильные приложения для iOS и Android и выяснили, что в большинстве приложений данные хранятся небезопасно, а хакеру редко требуется физический доступ к смартфону жертвы для их кражи.

По данным исследования, приложения для Android с критически опасными уязвимостями встречаются несколько чаще, чем программы для iOS (43% против 38%). Однако эта разница несущественна, считают эксперты, и общий уровень защищённости клиентских частей мобильных приложений для обеих платформ примерно одинаков.

Самой распространённой уязвимостью эксперты назвали небезопасное хранение данных, которое встречается в 76% мобильных приложений: в руках хакеров могут оказаться пароли, финансовая информация, персональные данные и личная переписка.

«Для кражи данных злоумышленникам редко нужен физический доступ к смартфону жертвы: 89% обнаруженных нами уязвимостей могут быть проэксплуатированы с использованием вредоносного ПО, – говорит **Яна Авезова, аналитик информационной безопасности Positive Technologies**. – Вероятность заражения увеличивается в разы на устройствах с административными привилегиями (root или jailbreak). Но вредоносное ПО может повышать права самостоятельно. Попав на устройство жертвы, вредонос может запрашивать разрешения на доступ к пользовательским данным, а получив разрешение, передавать данные злоумышленникам. Мы рекомендуем пользователям внимательно относиться к уведомлениям от приложений о запросе доступа к каким-либо функциям или данным. Не стоит предоставлять разрешение на доступ, если есть сомнение в его необходимости для нормального функционирования приложения».

Как показали результаты исследования, серверные части не менее уязвимы, чем клиентские: 43% имеют низкий или крайне низкий уровень защищённости, при этом 33% содержат критически опасные уязвимости. Среди самых распространённых недостатков высокого уровня риска в серверных частях – недостаточная авторизация и утечка информации.

SimbirSoft: помогаем спасти ИТ-продукт

Что делать, если ваше ИТ-решение не оправдало ожидания, не развивается и устаревает? Начать всё сначала или приложить усилия, чтобы «спасти» продукт? Мы в SimbirSoft помогли улучшить либо подготовить к релизу более 30 проектов и готовы поделиться опытом.

Бизнес обращается к ИТ-компаниям как за разработкой ПО с нуля, так и для усовершенствования своих продуктов. Бывает, что используемое решение нужно кардинально переработать. Мы в таких случаях обозначаем свою задачу коротко – «спасти» ИТ-продукт.

Чаще всего это необходимо в следующих ситуациях:

• Подготовка к срочному релизу

Как правило, на разработку выделяется достаточное количество времени. И всё же иногда компании обращаются к нам с «сырым» решением всего за несколько недель до релиза. Выход здесь очевиден – обеспечить работу наиболее важных функций.

Опираясь на наш опыт создания ПО для различных сфер, мы научились быстро приводить продукт в соответствие с бизнес-задачами нашего партнёра, находить и исправлять слабые места.

Из практики: Компания по оценке автомобилей обратилась к нам за три недели до релиза приложения, которое не смог закончить предыдущий разработчик. За 14 дней мы исправили ошибки и обеспечили выполнение основных функций. Приложение позволяет загрузить на сервер информацию об автомобилях, которые прошли оценку.

• Восстановление работоспособности продукта

Если ИТ-решение устарело, работает неправильно или утерян исходный код, рано ставить на нём крест. Зачастую для бизнеса неприемлемо отказаться от инструмента, в который вложены силы и средства. Понимая это, мы помогаем нашим партнёрам «спасти» тот продукт, которым они располагают:

- устранить ошибки;
- улучшить архитектуру, функциональность и UX;
- обеспечить регулярные релизы.

Вы хотите улучшить продукт?

Кейс: мобильный банк за 100 дней

Многие компании используют в своей работе готовые решения. В частности, в финтехе это «коробочные» системы дистанционного банковского обслуживания (ДБО): интернет-банк, мобильный банк и др. Минус «коробки» – необходимость доработки и постоянной модернизации под требования рынка.

Один из российских банков обратился к нам для интеграции готового ДБО – приложения для юридических лиц. Проанализировав задачи банка и пользователей, мы выяснили, что коробочное решение не обеспечит их выполнения. Совместно с нашим партнёром мы приняли решение разработать индивидуальный мобильный банк, сделав ставку на наиболее важные функции для пользователей. Следуя дорожной карте, мы всего за 100 дней выпустили мобильный банк, который впоследствии вошёл в ТОП5 банков для малого бизнеса.

Вашему приложению нужен современный UX?

Кейс: мобильное приложение для фудтеха

Сеть ресторанов японской кухни «НИЯМА» обратилась к нам для модернизации UX своего приложения. Мы провели юзабилити-анализ, обозначили слабые места, протестировали три варианта дизайна, что позволило повысить удобство приложения. В результате количество скачиваний приложения и положительных отзывов увеличилось в несколько раз.

«Когда к нам обращаются с просьбой «спасти» ИТ-продукт, мы выполняем приёмочное тестирование и определяем набор дальнейших шагов: от создания плана исправления дефектов до разработки и тестирования продукта, выпуска релиза и составления стратегии развития продукта. Мы в компании SimbirSoft таким образом «спасли» или помогли подготовить к срочному релизу уже более 30 систем».

Алексей Флоринский,
генеральный директор
SimbirSoft

Как мы спасаем продукт

- Изучаем систему: код, репозитории, документацию и др.
- Проводим аудит и тестирование
- Составляем план исправления дефектов
- Разрабатываем и тестируем продукт
- Выпускаем релиз
- Готовим план развития продукта

Что получает бизнес

- ИТ-продукт без ошибок
- Возможность регулярно выпускать релизы
- Исключительные права
- Исходный код и документацию

SimbirSoft

SimbirSoft *– глобальная ИТ-компания с опытом в разработке и тестировании ПО с 2001 года.*

www.simbirsoft.com
request@simbirsoft.com

CIS / № 3 (9) / 2019 / www.cismag.ru

Витаем в облаках: какие облачные решения для бизнеса выбрать и по каким критериям

Облачные системы хранения информации стали неотъемлемой частью бизнес-инфраструктуры. IT-разработчики уверяют, облака – качественная и надёжная система хранения данных. Консерваторы напоминают об утечке информации и взломах. Для каждого бизнеса – свои облака.

Седа Тороян,
проект-менеджер разработчика высоконагруженных интернет-проектов «РашенСофт»

Облачные системы – это высокотехнологичный онлайн-сервис, который позволяет быстро получить/вернуть вычислительные и программные данные. Использование облаков экономично. Всегда есть возможность использовать необходимые мощности под поставленные задачи, не брать дополнительные услуги или не покупать неподходящие тарифы.

Например, у владельца крупного портала число уникальных посетителей растёт еженедельно на 5% – нагрузка на сервер увеличивается. Мощность любого сайта не безгранична, её нужно наращивать для комфортного использования интернет-площадки. Можно взять дополнительный компьютер, подключённый к блокчейн-сети и распределить между ними нагрузку, повысить производительность действующего сервера или настроить облачную систему. Опираться стоит на финансовые возможности компании, прогнозы роста трафика посещаемости и самое главное, на соответствующую квалификацию технических специалистов.

Плюсы облачных систем:

- Скорость получения данных.
- Гибкость использования системы.
- Оптимизация расходов компании.

Недостатки облачных систем:

- Конфиденциальность и безопасность – возможны риски утечки информации, но многое зависит от квалификации IT-специалистов.
- Тонкая настройка программного обеспечения.
- Нужен стабильный интернет канал.
- Зависимость от поставщика облачных решений (если он один).

Где используются облачные решения

Облачные решения используются в любой отрасли, всё зависит от подходов и желания менять технологии бизнеса в лучшую сторону.

Схема работы:

1. Компания ставит перед разработчиками задачу.
2. Стороны согласовывают бюджет и детали.
3. Технические специалисты выбирают наиболее подходящее решение облачной системы.

Какими бывают облачные решения

Быстро разобраться в видах облачных систем:

№	Модель обслуживания в облачных системах	Что это	Для чего нужна заказчику
1.	IaaS	Инфраструктура как Услуга	Арендовать специализированное оборудование нужной мощности без дополнительного установленного сервиса.
2.	PaaS	Платформа как Услуга	Настроить алгоритм работы под задачи компании, автоматизировать регулирование, служит средством регулирования ПО.
3.	SaaS	Программное обеспечение как Услуга	Получить программные продукты, для примера CRM или Mail.
4.	CaaS	Коммуникация как Услуга	Предоставить обслуживание телефонии, текстовых и видео-мессенджеров.
5.	CaaS	Container as a Service — Контейнер как Услуга	Через приложение или пользовательский интерфейс аккумулировать информацию в веб- контейнере.
6.	DRaaS	Аварийное Восстановление как Услуга	Создать устойчивые к катастрофам облачные решения, в момент форс-мажора перезагружается уже в веб-хранилище.
7.	BaaS	Backup as a Service — Резервное Копирование как Услуга	Онлайн-кэш провайдера автоматически совершит создание копии на носителе.
8.	BaaS	Бэкэнд как Услуга	Предоставит возможность упростить работу техразработчиков, создаст площадку для оптимальной работы с компьютером.
9.	DBaaS	База Данных как Услуга	Подключит к информационным базам онлайн-хранилища.
10.	MaaS	Мониторинг как Услуга	Обеспечить аудит IT-инфраструктуры с централизованной точки доступа.
11.	DaaS	Рабочий стол как Услуга	Позволит работать удаленно от точки доступа с любого гаджета.
12.	STaaS	Хранилище как Услуга	Увеличить уровень безопасности информации, расширяя хранилищную нишу.
13.	NaaS	Сеть как Услуга	Организовать систему связи в хранилище провайдера.

Топ-6 критериев, по которым выбирают облачные решения

Существуют 6 основных критериев, которые надо учитывать при выборе облачной системы.

1. Надёжность компании поставщика

Важные проекты реализуются с использованием надёжных поставщиков облачных решений. Игнорирование этого критерия повлечёт проблемы в безопасности данных, технические сбои, слабый уровень поддержки – потерю лояльности клиента. Учитывайте возможности поставщика: рейтинг, инструменты и подходы.

2. Набор предлагаемых инструментов

Крупные проекты, которые сочетают в себе большое количество сервисов и задач, требуют соответствующих вычислительных мощностей и ресурсов. Поставщик облачных систем зачастую не может предоставить их все. Это негативно влияет на скорость принятия решения и производственные процессы, что сказывается на развитии бизнеса. Плохой поставщик с небольшим набором предлагаемых ресурсов – это как машина, которую надо постоянно чинить, далеко не уедешь. Чтобы избежать форс-мажоров, изучите коммерческие предложения, найдите максимально подробную информацию по всем видам решений.

3. Современность оборудования

Один из критериев поставщика услуг, который позволяет определить насколько развивается компания. Использование современного оборудования – это возможность получить хорошие вычислительные мощности.

4. Географическое расположение серверов

Актуально для международных проектов с высокой нагрузкой пользователей. Если компания использует неверный облачный сервис, потребители, географически далеко расположенные от центрального сервера вашего проекта, испытают проблемы с доступом к сайту или приложению. Если не учесть этот критерий, придётся сочетать в рамках одного проекта несколько разных поставщиков услуг. У каждого из них свои инструменты и возможности. Это создаёт проблемы с администрированием всей системы и приводит к дополнительным издержкам.

5. Компетентность и скорость техподдержки

Крупные и малые поставщики могут иметь проблемы с техподдержкой. У больших – слишком большой поток обращений сказывается на скорости реакции. У малых – менее компетентные сотрудники, не тренированные крупными клиентами и большим числом ситуаций. Стабильно работающая поддержка – тыл любого проекта. Если услуга настроена неверно, это приводит к перебоям в работе и потере доверия потребителя. Проверяйте службу поддержки поставщика до сотрудничества с ним.

6. Уровень цен

Выбор облачного решения для любого вида бизнеса напрямую связан с финансовыми возможностями компании. Большой бюджет не всегда гарантирует точный выбор услуги.

Прогноз развития облачных решений

1. Рынок облачных хранилищ продолжит расти

Bain&Company заявляет, сегмент облачных решений SaaS увеличится на 18% к 2020 году. Внедрение PaaS к 2020 году увеличится до 56%, сообщает KPMG. Согласно данным Statista, IaaS вырастет до $ 17,5 млрд.

2. Облака станут более гибкими в управлении и надёжными

- Распространится внедрение API для взаимодействия облачных решений между собой. Это позволит синхронизировать управление информацией, внедрить в облачные решения дополнительные инструменты. API позволит компаниям-потребителям соединить все процессы у одного поставщика.
- Компании начнут укреплять локальные решения с подключением облачных систем. Станет возможной гибкая настройка под любые потребности компании.

3. Управление облаками усовершенствуется

Основные игроки рынка облачных решений делают инвестиции в разработку искусственного интеллекта для максимальной оптимизации работы облаков с клиентами.

4. Разработчики обеспечат облачную безопасность

Крупные разработчики ищут способы обеспечить облака максимальной надёжностью, оптимизируют и объединяют их со службами безопасности хранилищ для предотвращения утечек информации.

5. IoT сделают облака популярными

Рост числа датчиков интернета вещей поднимет популярность облачных хранилищ.

6. Облачные системы станут бессерверными

Они помогают IT-специалистам выпускать обновления для техники, создавать и запускать новые приложения.

7. Данные станут виртуализированными

Технология позволит менять и восстанавливать данные, не используя техническую информацию (формат, местоположение).

8. На основе облаков разработчики создадут контейнерные системы

Станет возможным эффективно поддерживать большее количество приложений, защищая внутреннюю систему связи.

Системы ИТ-мониторинга

Как любому растущему предприятию с течением времени приходит понимание о необходимости автоматизации производственных процессов, так и его кровеносная система – ИТ-инфраструктура, разрастаясь, рано или поздно запросит мониторинг своих служб и подсистем.

Внедрение систем ИТ-мониторинга для компании ООО «МФМ-Интеграция» является если не ключевым, то историческим, и за долгое время у нас накопился богатый опыт внедрения почтиф всех современных систем ИТ-мониторинга.

В плане выбора решений для мониторинга наши заказчики не проявили большого желания экспериментировать с какими-то экзотическими решениями. Решение мирового ИТ-гиганта HPE Operations Bridge является самым популярным в мире, таким же оно стало и в России, и о нём мы сегодня хотим рассказать.

С 2017 года решение принадлежит компании Micro Focus в рамках программы диверсификации бизнеса HPE, отчего изначально неплохое решение стало только лучше.

Operations Bridge сегодня – это сложное и технологически насыщенное решение, где каждая компонента отвечает за свой участок мониторинга и может работать отдельно от остального пакета. Например, база данных конфигурационных единиц UCMDB опишет софтверное хозяйство заказчика, Asset Manager расскажет про оборудование, за каналы связи и их состояние отвечает компонента Operations Bridge – NNMi. Таких компонент очень много, но подробно мы сегодня остановимся на самой болезненной теме – как всё это собрать воедино и проанализировать.

Консолидация разнообразных данных – самая нелёгкая задача, стоящая перед системой мониторинга. Большая часть имеющихся решений имеют тенденцию к стерильному сбору данных согласно настройкам, тогда как ИТ-директор имеет противоположную задачу – собрать и проанализировать 100% данных и даже больше. В этом плане Operations Analytic вне конкуренции, она принимает всё: события, метрики, топологии, данные log-файлов, то есть неструктурированные данные, LOB и даже данные из бизнес-систем, например о продажах или о котировках.

Всё это OpsA группирует, сопоставляет во временном окне, проводит тренды и делает прогнозы, а также формирует удобные для пользования отчёты. При этом любое изменение ИТ-поля заказчика автоматически попадает в контур мониторинга.

Понятно, что при таком подходе собирается огромное количество данных, поэтому за хранение отвечает отдельный продукт – база данных колоночного типа Vertica, специально созданная для скоростной обработки больших данных. Она бесплатно входит в состав Operations Bridge и всех компонент.

Изюминкой OpsA является так называемая «машина времени» – то самое временное окно, упомянутое выше. Она позволяет устранить конфликтную ситуацию между подразделениями в процессе выяснения ответственных при возникновении сбоев.

Обычно каждое подразделение смотрит в свои инструменты мониторинга, часто не связанные с инструментами других подразделений, в результате у каждого из участников возникает иллюзия, что всё работает, но сбои всё равно случаются. Решение OpsA позволяет вывести на консоль метрики и данные от разных уровней ИТ (например, транзакции пользователей вместе с данными СХД, сети, серверами).

В случае конфликта консоль окрашивается в цвета, отличные от зелёного, а значит, вместо взаимных обвинений можно просто включить «машину времени», то есть начать отматывать время назад, как при просмотре фильма. При этом в консолях станут «перематываться» и данные (включая статусы, логи и так далее), таким образом можно будет фактически посмотреть фильм о сбое и увидеть, с какого объекта и момента всё началось. Такая машина времени работает без необходимости поиска и настройки фильтров – система сделает это за вас.

«Мобильная» электронная подпись

Как предоставлять удалённо любые услуги и выдать КЭП каждому жителю страны?

Дарья Верестникова,
коммерческий директор
компании SafeTech

С самого начала 2019 года в среде специалистов в области информационных технологий, а также представителей бизнес-подразделений, ответственных за дистанционные сервисы и электронный документооборот, возник повышенный интерес к мобильной аутентификации и подписи в смартфоне.

Это и понятно: в настоящее время возможность полноценной работы на мобильных устройствах, включая формирование подписи, стала неотъемлемым требованием к информационным системам и сервисам. Об особенностях «мобильной» подписи, её внедрении и перспективах использования мы поговорили с Дарьей Верестниковой, коммерческим директором компании SafeTech.

Дарья, расскажите, пожалуйста, зачем нужны средства электронной подписи и какие тенденции в их развитии сейчас существуют?

Вся жизнь современного человека неуклонно переходит в «цифровое» пространство. И проявляется это не только в социальных сетях, играх и развлечениях. Люди получают возможность удалённо совершать различные действия, делать покупки и получать услуги. И неважно, кто является клиентом прикладной системы – организация или человек, работа на мобильном устройстве стала обычным делом. При этом, как и на стационарных компьютерах, мобильному пользователю также необходимо пройти процедуру аутентификации (показать и доказать то, кем он является), а также подтвердить своё волеизъявление (сообщить и подтвердить то, что конкретно он хотел бы сделать). Самые современные инструменты решения первой задачи предоставляет Единая биометрическая система (ЕБС), а для решения второй задачи, по-прежнему, лучше всего подходит электронная подпись (ЭП), реализация которой на мобильных устройствах и стала требованием времени.

Конечно же, любая электронная подпись должна быть:

- безопасной;
- удобной;
- юридически значимой;
- не очень дорогой.

Вроде бы очевидно, но тем не менее эти факторы не всегда просто собрать в одном решении для смартфона или планшета. Классическим примером являются SMS-коды и USB-токены. Первые – абсолютно небезопасны и дороги, имеют низкий уровень юридической значимости, вторые – имеют не всегда достаточную мобильность и, к сожалению, ряд ограничений с точки зрения удобства использования.

Дарья, а в чём проблемы кодов, передаваемых пользователю в SMS или PUSH?

Привычная для всех SMS-ка имеет целый ряд ограничений, начиная с того, что она никак не гарантирует ни целостность, ни авторство «подписываемого» с её помощью документа. Она говорит лишь то, что кто-то, что-то, когда-то подтвердил. И если эти «кто-то» и «что-то» совпали с действительностью – это большое везение! Например, российская судебная практика сейчас всё чаще сводится к признаю SMS «неперсонифицированным» средством подтверждения. Помимо этого, использование SMS стало ещё и дорогим!

Это привело к тому, что бизнес-подразделения банков и компаний, оказывающих услуги через Digital-каналы, стали искать выход и начали использовать Push-коды. На первый взгляд, это казалось оптимальным, и все повсеместно начали переходить на эту технологию. На ваш смартфон пришло Push-уведомление, содержащее код для подтверждения операции, и вам даже не нужно его подставлять в интерфейс мобильного приложения – он сам «подставится» и подтвердит транзакцию. Удобно? Да! Но вот безопасно ли? Конечно нет! Эксперты в области безопасности называют такой вариант «профанация электронной подписи». Почему они так говорят? На сервере прикладной системы «сгенерировался» какой-то одноразовый пароль (OTP), он как-то был передан клиенту на смартфон, как-то сам за клиента «подставился» в интерфейс и сам «подписал» транзакцию. «Страшный сон» любого специалиста ИБ.

Также существует ещё и проблема социальной инженерии, и сколько бы банки не предупреждали пользователей об опасности, всё чаще мы слышим истории про то, как мошенник «выудил» у клиента код подтверждения и похитил деньги. Почему же так происходит? Потому что невозможно в одной SMS уместить все реквизиты платежа, чтобы человек сам видел, куда в действительности будут отправлены его деньги. Поэтому вопрос обеспечения безопасности транзакций по-прежнему остаётся сложным, и его необходимо решать комплексно.

Но ещё хуже, что находятся банки, которые вообще перестали предусматривать какие бы то ни было процедуры подтверждения операций. То есть вы просто отправляете платёж, и для его проведения «подставляется» некий ID установленной сессии, даже без SMS и Push-кодов! Конечно же, такое «подтверждение транзакций» совсем не подходит для развития дистанционных услуг.

Благо, регулятор отрасли старается задавать правильный вектор обеспечения безопасности удалённых пользователей. В частности, Положение Банка России от 17 апреля 2019 г. N 683-П «Об установлении обязательных для кредитных организаций требований...» значительно повышает уровень безопасности транзакций, требуя от банков находить такие способы подтверждения, которые бы смогли обеспечить контроль целостности и авторства подписываемого документа. На данный момент это делает такие небезопасные способы подтверждения, как SMS и Push, неприменимыми при работе в дистанционных каналах.

Дарья, расскажите, пожалуйста, что такое подпись в смартфоне? Чем она отличается от «обычной», и в чём преимущество её использования для клиента?

Несколько лет назад мы представили рынку подпись в смартфоне PayControl, призванную закрывать все риски, существующие в SMS- и PUSH-подтверждениях, и позволяющую «превратить» мобильное устройство в аналог USB-токена с таким же высоким уровнем безопасности и очень простым пользовательским сценарием.

Сейчас PayControl – это полноценная платформа мобильной аутентификации и электронной подписи. При её использовании обеспечивается эффективное противостояние наиболее распространённым атакам на клиентов систем ЭДО («перевыпуск» SIM-карты, фишинг, подмена документа, социальная инженерия и т. д.). Главный принцип – клиент видит реквизиты платежа на своём смартфоне и подтверждает их одним нажатием кнопки.

Сценарий работы пользователя очень прост:

- Информация о об операции приходит непосредственно в мобильное приложение банка. Клиент проверяет информацию и подтверждает её буквально «одним касанием» к экрану. Волеизъявление клиента (действие, электронный документ, финансовая транзакция) подписывается в смартфоне и передаётся в прикладную систему.
- Если на смартфоне пользователя доступ к сети Интернет отсутствует (при нахождении, например, в роуминге, на промышленной территории, на складе, в подвале, и прочее), то в интерфейсе Интернет-банка генерируется QR-код, отражающий детали конкретной операции, который пользователь сканирует в мобильном приложении на своём смартфоне. На основе полученных данных на смартфоне генерируется «усиленный» код, которым клиент подтверждает свой платёж в Интернет-банке.
- В основе PayControl лежит ассиметричная криптография. Закрытый ключ «рождается», «живёт» и «умирает» в конкретном смартфоне – попытки воспроизведения ключа на другом устройстве ни к чему не приводят. Подпись формируется как функция от 4-х аргументов: реквизиты конкретной операции, ключ клиента, момент времени и «отпечаток» смартфона пользователя. Решение PayControl может быть полностью встроено в мобильное приложение банка или другого провайдера услуг.

Решение PayControl может быть полностью встроено в мобильное приложение банка. Подпись формируется как функция от 4-х аргументов: реквизиты конкретной операции, ключ клиента, момент времени и «отпечаток» смартфона пользователя. Даже если предположить, что злоумышленник как-то получит доступ к подписи, то он никак не сможет её использовать для другой операции, на другом устройстве, в другое время.

У Вас есть совместная разработка с Компанией «КриптоПро» под названием «myDSS». В чём отличие этого решения?

Нам удалось предложить рынку два решения для формирования «мобильной» подписи: «облегчённую» версию, основанную на неГОСТ-овых криптоалгоритмах, которое идеально подходит для обслуживания физических и небольших юридических лиц, а также «самое полновесное» решение, востребованное в тех областях, где необходима квалифицированная электронная подпись (КЭП).

Решение для формирования КЭП называется «КриптоПро myDSS» и представляет собой совместную разработку компаний «КриптоПро» и SafeTech на базе программно-аппаратного комплекса облачной электронной подписи «КриптоПро DSS» и платформы PayControl. В прошлом году, 10 августа, на это решение был получен сертификат ФСБ России, и, по нашему мнению и мнению наших клиентов, – это настоящий прорыв для всего рынка информационной безопасности и цифровой экономики нашей страны.

Выбирая предложенные решения, очень важно понимать, что различным сегментам клиентов и наборам сервисов необходим разный уровень безопасности юридической значимости. Например, при дистанционном обслуживании физлиц или небольшого бизнеса простой или усиленной неквалифицированной подписи может быть вполне достаточно, но для предприятий с государственным участием или тех, кто взаимодействует с госструктурами (сдача налоговой отчётности, регистрация юридических лиц и прочее), необходимо использовать сертифицированные средства электронной подписи и усиленную квалифицированную электронную подпись. Именно поэтому мы постарались одним решением закрыть все категории клиентов.

Судя по тому, как Вы рассказываете, использование PayControl и myDSS выглядит для клиента очень просто. Разве может быть безопасность такой простой и почему это так сложно повторить?

Вы даже не представляете, насколько важный вопрос поднимаете! Очень часто, когда мы представляем свои технологии, возникает две типовые реакции потенциальных партнёров и заказчиков. Сначала говорят: «Это выглядит слишком просто, чтобы быть безопасным», а по мере ознакомления продолжают: «Действительно, очень простое решение – мы и сами такое же напишем за 2 недели».

Скажем честно, первая реакция нам даже нравится, она говорит об успешности наших разработчиков. Обычно безопасность накладывает свои ограничения, и удобство использования системы снижается. Есть даже расхожий стереотип, что «безопасность удобной быть не может». Тем не менее наши технологии разрабатывались с целью сделать работу пользователей и безопасной, и удобной. Для этого были затрачены отдельные усилия, и теперь простота использо-

вания наших решений – это конкурентное преимущество, которое выходит за рамки вопросов безопасности и вызывает неподдельный интерес со стороны бизнес-подразделений банков и компаний, оказывающих услуги через Интернет.

Фразы «напишем сами за 2 недели» говорят исключительно о поверхностном погружении в проблематику, поскольку кажется, что если выглядит просто для пользователя, то и сделать аналогичное решение не составит особого труда. Это глубоко ошибочное мнение. Специалисты, делающие такие заявления лишь по результатам первичного ознакомления с PayControl, вряд ли учитывают всю проблему целиком. За 2 недели нельзя даже сделать «видимость» PayControl, а уж разработать полноценное средство подписи – тем более. Поэтому я всегда призываю бизнес-подразделения и ИТ-подразделения банков смотреть «под капот». Не всё, что выглядит просто, является безопасным. Не всё, что выглядит как PayControl, позволит обеспечить ту же защиту дистанционных каналов. Если к вам приходит какой-либо разработчик и говорит, что сам произведёт похожее решение за короткий срок – не верьте сразу! Посмотрите внимательнее, отдайте это предложение на экспертизу своим специалистам по ИБ, отдайте своим юристам, посмотрите, как это будет работать в вашей инфраструктуре, соберите экспертное мнение. Обязательно! В платформе PayControl реализована полноценная электронная подпись на базе симметричной или ассиметричной криптографии, обеспечивается контроль целостности, контроль авторства и многое другое. Эта «простая» вроде бы технология лежит в основе решения MyDSS для мобильной аутентификации и формирования подписи с использованием «ГОСТ-овой» криптографии, которое имеет сертификат соответствия ФСБ России и досконально проверялось регулирующим органом.

Дарья, сейчас активно обсуждается Положение Банка России от 17 апреля 2019 г. N 683-П. Насколько PayControl «подходит» под данное постановление?

Выполнение требований этого Положения на данный момент вызывает много вопросов. Банки скрупулёзно анализируют и сами требования, и степень их выполнения в своих дистанционных каналах. В соответствии с пунктом 5.1., например: «Кредитные организации должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом». Решение PayControl, в частности, обеспечивает контроль целостности и авторства документа или транзакции. Выработка ЭП осуществляется с использованием закрытых ключей пользователей в их смартфоне на основе данных транзакции, значения времени и других опциональных параметров. При внесении изменений в подписываемые данные значение электронной подписи изменится. «Уполномоченное лицо» однозначно определяется соответствующим ему ключом и набором уникальных опциональных признаков, таких как отпечаток мобильного устройства.

Часто можно услышать, что PayControl не имеет аналогов. В чём уникальность?

PayControl – это платформа мобильной аутентификации и электронной подписи. Уже сейчас это не просто «подписалка», это действительно воплощение нового класса систем. Мы ещё 3 года назад говорили о том, что все «традиционные» и устаревшие способы аутентификации отойдут на второй план. Сейчас всё так и происходит. Теперь мы вновь смотрим на несколько лет вперёд и прекрасно понимаем, что «подписалки» даже с инновационными методами подписи скоро вновь окажется для заказчиков недостаточно. Поэтому мы активно развиваем решение, проводим интеграцию с различными системами обеспечения безопасности, в частности с биометрическими системами аутентификации и антифрод-системами. Это необходимо, например для предоставления банкам возможности «адаптивной аутентификации», а также возможности ещё большего повышения уровня безопасности и удобства для клиента. Интеграция с биометрическими системами позволит добавить дополнительные факторы аутентификации при совершении так называемых «высокорисковых» операций, а использование передовых антифрод-систем позволит «на лету» в момент совершения операции оценивать риск её подписи и работы пользователя на конкретном мобильном устройстве. Таким образом, PayControl – это, действительно, полноценная платформа, которая позволит банкам, как «кубики» собирать те функциональные возможности, которые им необходимо получить. Поэтому мы и говорим, что PayControl – это новый класс систем обеспечения безопасности транзакций, которые мы сейчас выводим на рынок, они будут развиваться в ближайшие несколько лет.

Дарья, Вы упомянули о биометрической и адаптивной аутентификации в PayControl. Расскажите, пожалуйста, об этих возможностях подробнее.

Постараюсь пояснить на примере. Если раньше смена номера телефона или самого мобильного устройства и, как следствие, смена ключа электронной подписи, словом, любая «высокорисковая» операция требовала жёсткого контроля и визита в офис банка с «физическим» подписанием бумаг, то сейчас это не требуется. Теперь в момент первичной регистрации с клиента «снимаются» биометрические данные, которые «складываются» в банк, и при каждой «высокорисковой» операции будет запрашиваться дополнительная идентификация, чтобы на всякий случай проверить клиента: он ли это совершает операцию или нет? Это и есть использование «дополнительных факторов биометрической аутентификации».

Адаптивная аутентификация – следующий шаг в развитии систем ДБО. Расскажу о ней на примере трёх сценариев подтверждения операций. Первый сценарий. Если проводится априори «хорошая» транзакция, например «типовая» или часто проводимая клиентом, то она подписывается без дополнительного подтверждения. Если транзакция так же «хороша», но по каким-то причинам требуется дополнительное

подтверждение (может быть актуально для юридических лиц), тогда это можно реализовать с помощью второго сценария, например дополнительного подтверждения Face ID или Touch ID. И третий сценарий – если операция очень рисковая или «Scoring» (интегральный показатель надёжности, выявленный антифрод-системой) у неё откровенно не заслуживает доверия, то проведение транзакции потребует формирования полноценной электронной подписи, причём пароль на использование ключа этой подписи задаётся в соответствии с очень жёсткими требованиями, так называемый «длинный пароль» – под стать риску этой операции. Таким образом мы закрываем риск того, что кто-то возьмёт ваше мобильное устройство, приложит ваш «пьяный палец» и похитит ваши средства.

Итак, когда мы анализируем поведение клиента в цифровом канале и решаем, можно или нельзя доверять его действиям, а затем в зависимости от результатов анализа просим его подписать транзакции различными способами, это и составляет суть адаптивной аутентификации. Тем не менее большинство бизнес-подразделений банков стремятся исключить запрос дополнительного подтверждения у физических лиц. Как это можно реализовать? Мы считаем, что это возможно только в интеграции с антифрод-системой. Если антифрод-система выдаёт свою оценку («Scoring»), которая подтверждает доверие этому человеку или этой операции, то возможно подписать эту операцию клиента или документ в автоматическом режиме. Причём это будет именно подпись, не подстановка какого-то непонятного идентификатора, а полноценная подпись. Только в таком случае мы можем быть уверенными, что противодействуем наиболее частым атакам злоумышленников.

Насколько это совместимо с использованием ЕБС?
Мы часто слышим про единую биометрическую систему. На использование ЕБС возлагают большие надежды. В банковской среде можно услышать даже такие «восторженные» ожидания: «У нас же есть Единая Биометрическая Система, теперь пользователям будет очень удобно – лицо приложил, и всё!» Особенность ЕБС на данный момент в том, что в составе этой системы нет средств электронной подписи. Поэтому возможности использования такой системы для подтверждения волеизъявления клиентов в настоящее время весьма ограничены. Как правило, речь идёт о предоставлении банкам возможности удалённой идентификации физических лиц с последующим удалённым открытием счёта. Но для того, чтобы дать даже такую возможность юридическим или физическим лицам проводить значимые транзакции, подписывать юридически значимые электронные документы и полноценно взаимодействовать с государством, нужна квалифицированная электронная подпись.

Многие эксперты предлагают использовать ЕБС для удалённой идентификации пользователей при выдаче квалифицированной электронной подписи. Сейчас по требованиям законодательства эта идентификация должна проходить очно, но уже есть соответствующие законопроекты. Когда мы технологически и законодательно придём к тому, что у каждого пользователя будет возможность получить на свой смартфон инструменты формирования квалифицированной электронной подписи удалённо, то использование ЕБС станет массовым, а удалённое получение цифровых услуг – действительно удалённым.

Какие ещё услуги банков становятся возможными на основе квалифицированной электронной подписи со смартфона?
Мы уже запустили ряд абсолютно новых удалённых услуг. Например, онлайн регистрация бизнеса с открытием расчётного счёта. Банк один раз встречается с клиентом, пока тот ещё «физик», выдаёт ему квалифицированную электронную подпись для смартфона, при помощи которой он подписывает все документы в налоговую на открытие бизнеса и «превращается в юрика». Ему «перевыпускают» ключ электронной подписи уже на юридическое лицо, он использует эту электронную подпись для открытия расчётного счёта, доступа в ДБО, для подписи документа – для чего угодно! С помощью этой же подписи он может отправить документы в налоговую, этой же подписью может пользоваться на госуслугах – где угодно! И вот этот идеальный «сквозной процесс», когда банк один раз посмотрел на клиента и предоставил ему все возможные сервисы, сейчас и реализуется.

На рынке уже представлены такие сервисы: удалённая регистрация бизнеса, сдача налоговой отчётности, система дистанционного банковского обслуживания, торги и Госзакупки прямо с мобильного телефона. Физические лица могут зарегистрировать недвижимость в Росреестре без необходимости установки дополнительного ПО и получения аппаратных средств ЭП.

Таких проектов с каждым днём появляется всё больше и больше. Если у нас совместно с регулятором отрасли, совместно с удостоверяющими центрами, совместно с ведущими производителями криптографических решений в России получится предоставить банкам технологии, которые помогут жителям страны экономить время, деньги, силы, то таких проектов станет ещё больше, и мы сможем «оКЭПить» каждого жителя страны, чтобы он стал полноценным участником безопасного электронного взаимодействия. Если мы не будем сбавлять темп, через несколько лет каждый житель страны сможет не только удалённо брать кредиты и подписывать трудовые договоры, но и расписываться о получении стола из «Икеи» прямо со смартфона без использования бумаги!

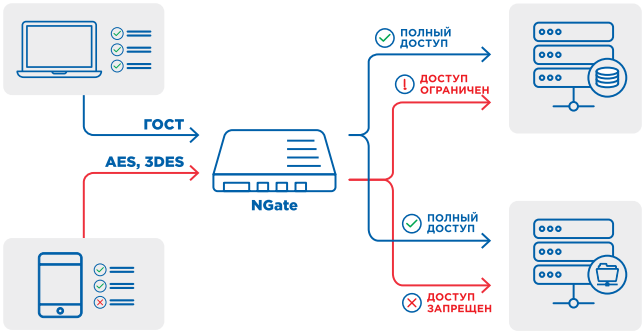
SafeTech
SAFETY TECHNOLOGIES

SafeTech *– российский разработчик инновационных решений для защиты систем дистанционного банкинга и электронного документооборота.*

www.safe-tech.ru

КРИПТОПРО NGate

Универсальный высокопроизводительный VPN-шлюз, позволяющий быстро и безопасно реализовать защищённый удаленный доступ к корпоративным ресурсам и информационным системам через незащищённые каналы связи.



Поддержка ГОСТ и зарубежных алгоритмов

NGate обеспечивает поддержку TLS-ГОСТ наравне с зарубежными криптографическими алгоритмами. Это позволяет реализовать плавный перевод защиты доступа к web-ресурсам на ГОСТ.

Выполнение требований регуляторов

Серверные и клиентские компоненты NGate сертифицированы по требованиям к СКЗИ и имеют соответствующие сертификаты ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать NGate для защиты персональных данных при передаче по незащищенным каналам связи, а также для защиты удаленного доступа к значимым объектам КИИ. Кроме этого NGate позволяет реализовать защищенные TLS-соединения при передаче биометрических ПДн в рамках соответствующих взаимодействий в ЕБС.

Три режима работы

NGate может работать в трех режимах — TLS терминатора, портального и VPN доступа. Режим TLS терминатора используется для снятия нагрузки по обработке TLS-соединений с бэкэнд-серверов и серверов доставки данных. Режим портального доступа — для организации персонального доступа пользователей к опубликованным на портале NGate веб-ресурсам в соответствии с корпоративными политиками ИБ. Режим VPN доступа — для подключения к произвольным ресурсам с помощью VPN-клиента, поддерживающего все популярные платформы (Windows, macOS, Linux, iOS, Android. Sailfish).

Простая реализация контроля доступа к ресурсам

NGate обладает широкими возможностями по управлению доступом удалённых пользователей со строгой многофакторной аутентификацией, а также гибким разграничением прав доступа к ресурсам.

Масштабируемость

Один узел NGate выдерживает нагрузку до 28000 одновременных соединений с обработкой информационных потоков до 10 Гбит/с в режиме TLS терминатора. Данные характеристики легко увеличить добавлением узлов в кластер.

КриптоПро NGate

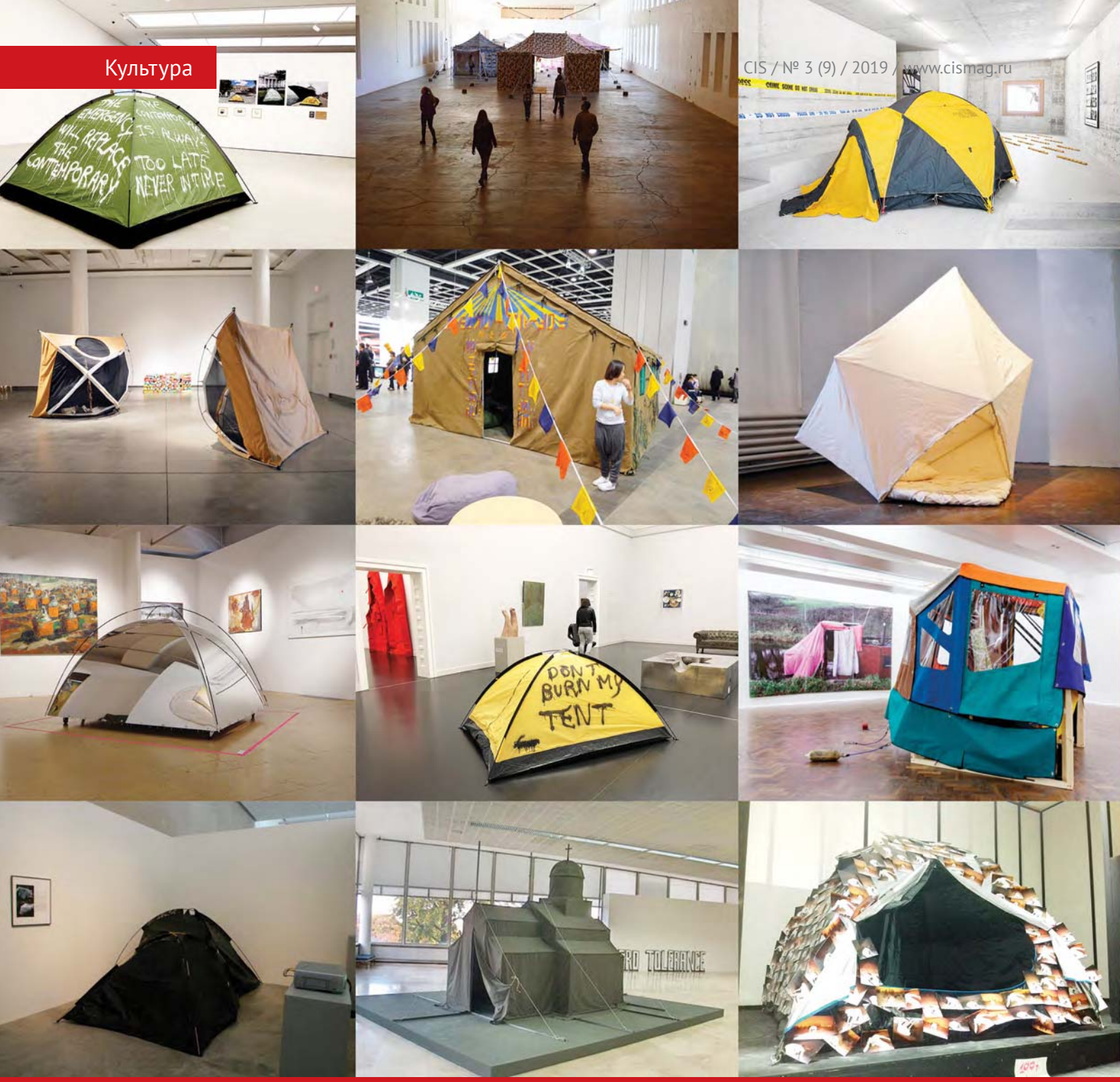
http://www.cryptopro.ru/products/ngate

КриптоПро CSP Lite

КриптоПро CSP Lite — это новый «облегченный» криптопровайдер на базе флагманского СКЗИ КриптоПро CSP 5.0, который представляет собой новое поколение криптопровайдера, развивающее три основные продуктовые линейки компании КриптоПро: CSP (классические токены и другие пассивные хранилища ключей), ФКН (неизвлекаемые ключи на токенах) и DSS (ключи в облаке).

Преимущества продуктов этих линеек не только сохраняются, но и преумножаются в КриптоПро CSP 5.0: шире список поддерживаемых платформ и алгоритмов, выше быстродействие, удобнее пользовательский интерфейс. Но главное — работа со всеми ключевыми носителями, включая ключи в облаке, теперь единообразна. Для перевода прикладной системы на поддержку ключей в облаке или на новые носители с неизвлекаемыми ключами не потребуется какая либо переработка ПО — интерфейс доступа остается единым, и работа с ключом в облаке будет происходить таким же образом, как и с классическим ключевым носителем.

КриптоПро CSP Lite предназначен для использования в браузерах в различных операционных системах, одновременно реализует функции КриптоПро CSP и КриптоПро ЭЦП Browser plug-in и не требует установки. Его использование сводит к минимуму настройки СКЗИ для пользователя. При этом набор поддерживаемых токенов и смарт-карт может быть динамически настроен под требования конкретного веб-ресурса (электронной площадки, системы ДБО и т.д.).

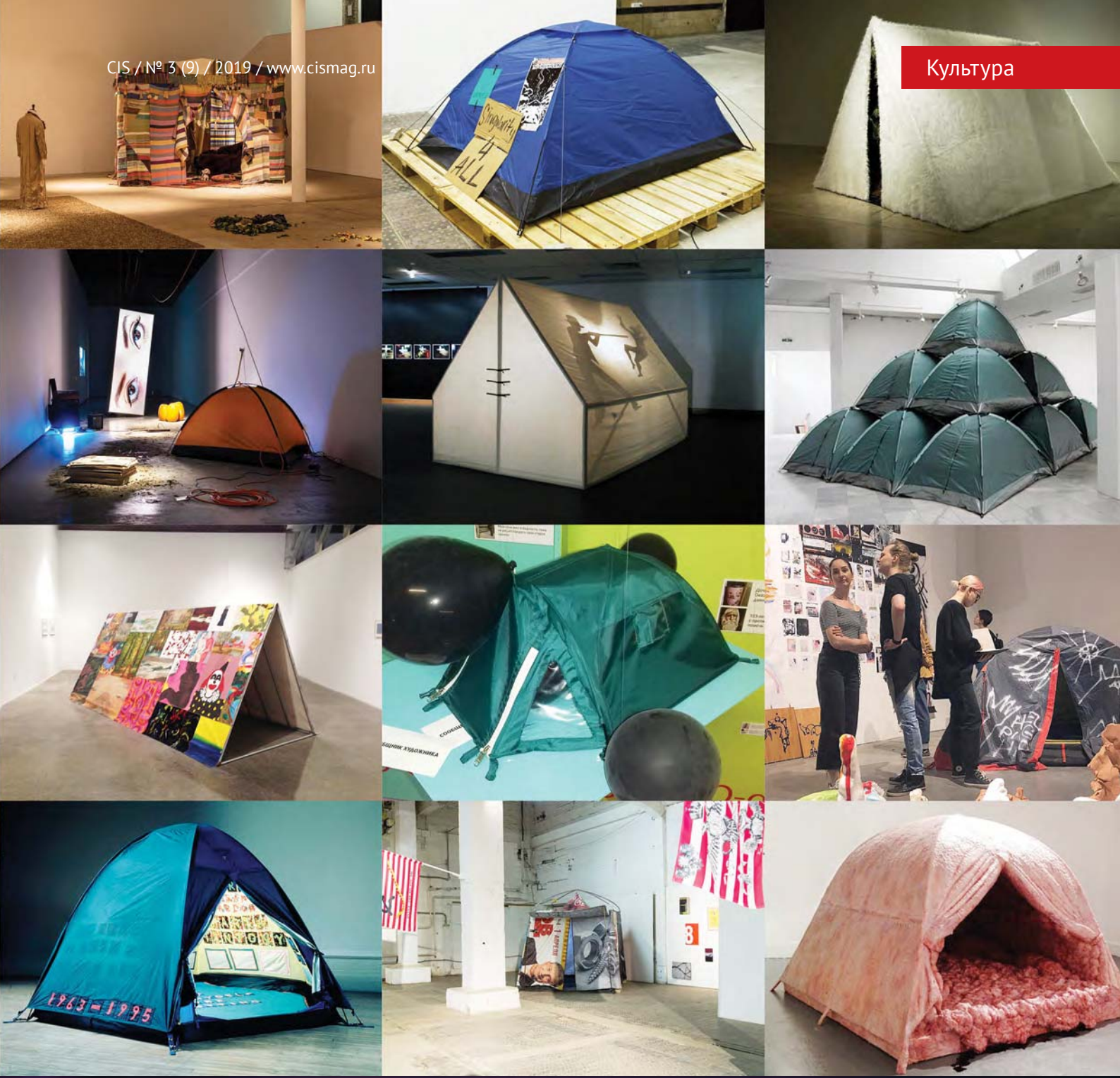


Выставка «Творческий метод» (Т.М.)

В галерее «Электромузей в Ростокино» Объединения «Выставочные залы Москвы» открывается выставка «Творческий метод» (Т. М.).

Принято считать, что современное искусство ограничено лишь физическим миром, технологическим прогрессом и фантазией автора – любой объект, субъект, действие, текст, компьютерный код или даже идея, может по праву считаться произведением искусства. Современный художник, в отличие от коллег из прошлого, не ограничен в выборе техник, практик и медиумов. Тем не менее, попадая в какую-нибудь галерею на выставку современного искусства, посетители часто испытывают эффект дежавю: обнаруживают работы, похожие на виденные раньше. Обнаруживаются некоторые закономерности, проявляющиеся в индивидуальных творческих методах и приёмах. Во мнимом разнообразии тем и возможностей выражения, их актуальное количество оказывается не таким уж и большим.

Существует ряд узкоспециальных приёмов, используемых в создании большого пласта произведений современного искусства. Таковыми, например, являются: надписи из неона; наборы одно-



типных предметов; перформансы современного танца; интерактивные проекции; сонифицированные объекты или процессы; фотосерии с однотипными персонажами в интерьерах и др.

В фокусе этой выставки – исследование и типологизация наиболее распространённых творческих методов при создании произведений современного искусства и их критическое осмысление.

Кураторы: Алексей Шульгин, Габбилен Галычев.

Участники: Михаил Марушкин, Константин Новиков, Габбилен Галычев, Яна Малиновская, Саша Пучкова и Кристина Вегера, Эмма Байер, Электробутик, Софа Скидан, Анатолий Осмоловский, Алек Петук, Маша Ротшильд, Софья Татаринова, Синие носы, Зоя Фалькова (Казахстан), Хенесси Янгман (США), Яспер Риголе (Бельгия), Николай Спесивцев (Белоруссия), Сергей Касич.

ВЫСТАВОЧНЫЕ ОБЪЕДИНЕНИЕ ЭЛЕКТРО МУЗЕЙ ЗАЛЫ МОСКВЫ

Место проведения:
«Электромузей в Ростокино» (Ростокинская ул., 1, м. ВДНХ, МЦК «Ростокино»)
Тел: 8 (499) 187-10-45;
electromuseum@vzmoscow.ru
www.vzmoscow.ru


May 21-22 2019
Positive
Hack
Days

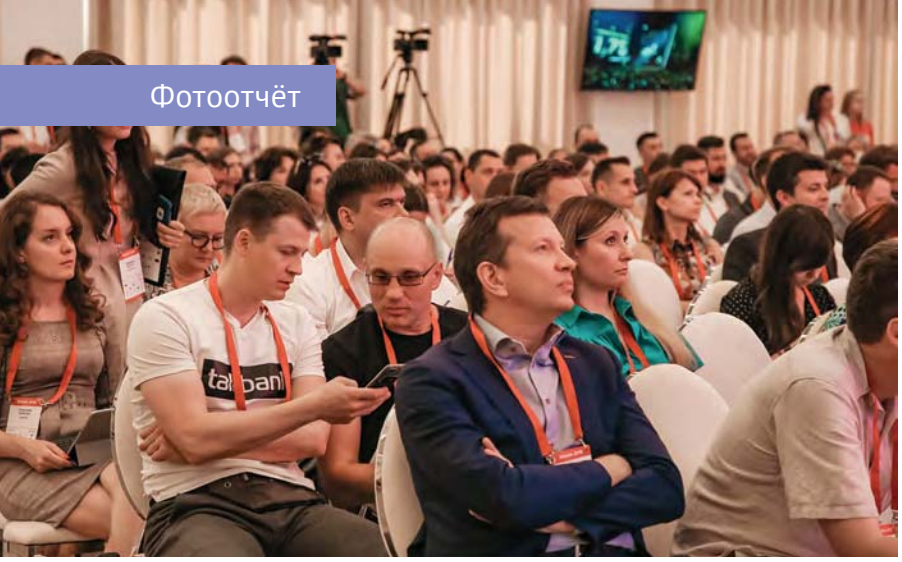

TELLING
STORIES


Positive Technologies


DPG
афиша
20 ЛЕТ
ПЯТНИЦА!
tvzavr
RIAMO.RU
TV BRICS
CIS
MEDIA BITCH
7ELLING STORIES

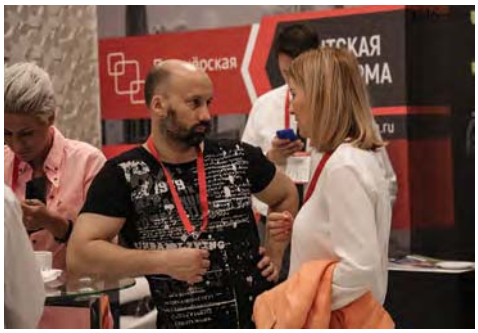

кибериграда
Ростелеком


phd




КЛИЕНТ 2020+


Клиентоцентричная модель вместо продуктовой модели
По типу компании в сегменте МСБ
Клиенты
ПРОДУКТ 1
ПРОДУКТ 2
ПРОДУКТ 3
ПРОДУКТ 4
ПРОДУКТ 5
ПРОДУКТ 6
ПРОДУКТ 7
>200
тыс. клиентов
>1
>50
тыс. клиентов
>5
Цифровые гиганты
Яндекс, Сбербанк, Mail.ru Group, Мегафон
Крупные компании
МТС, Билайн, Ростелеком ВТБ, Альфа Банк, Тинькофф Банк, 1С, Эвотор, Актион
Средние игроки
Банк Росбанк, Моё дело, Битрикс
Нишевые/локальные компании
Веста Банк, Мой склад



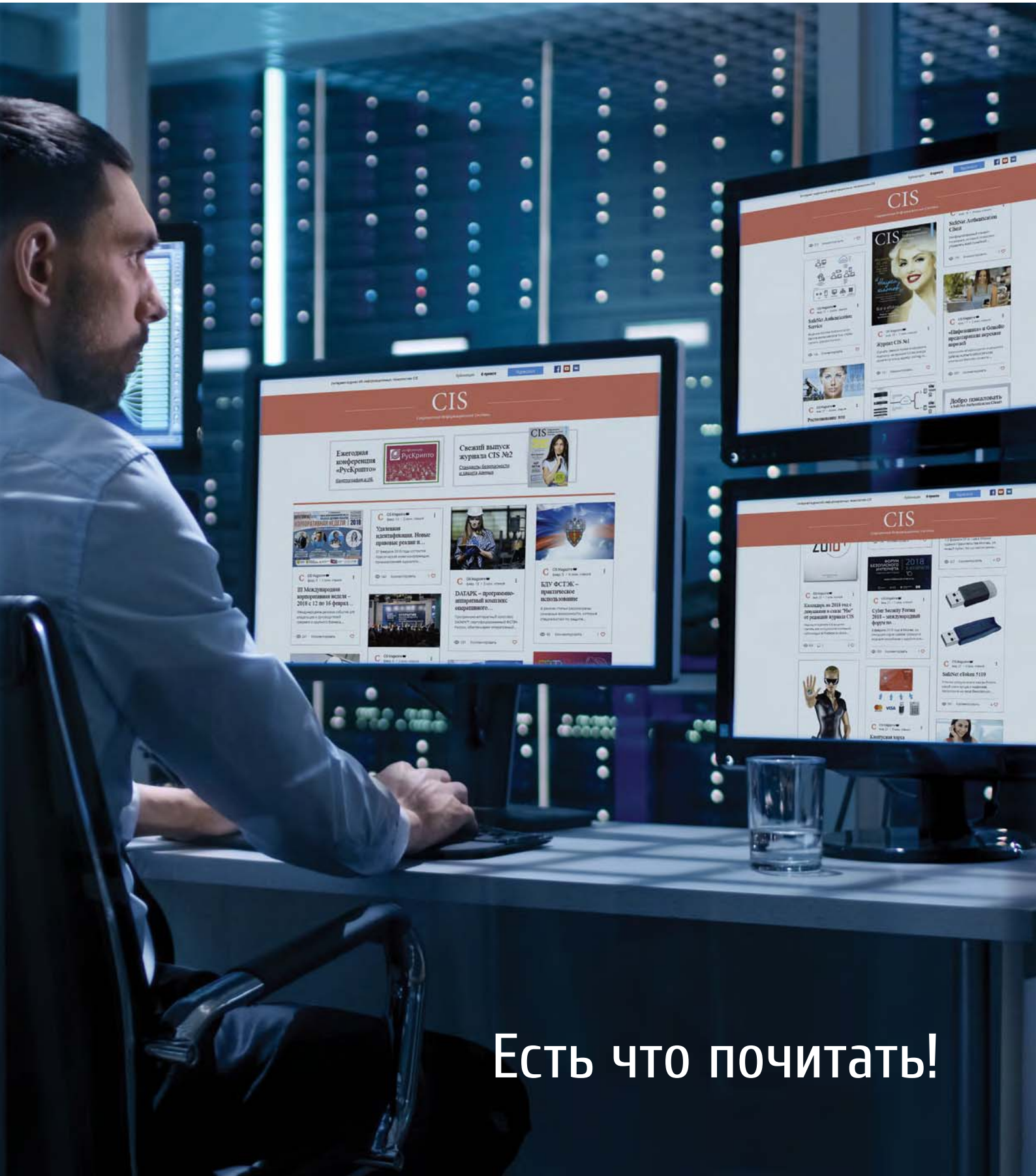

30+ сер
доступны в ма
470 000
«проголосова


Сбербанк
Бизнес Онлайн
Создать


Панельная дискуссия
«Outside the box»:
Максим Спиридонов
Нетология
Евгений Колбин
Сбербанк
Екатерина Фроловичева
Газпромбанк
Владимир Потапов
ВТБ
Динара Юнусова
Банки.ру
Владимир Урбанский
Почта России
Роман Гаврилов
Андрей Щенников
Банк Уралсиб

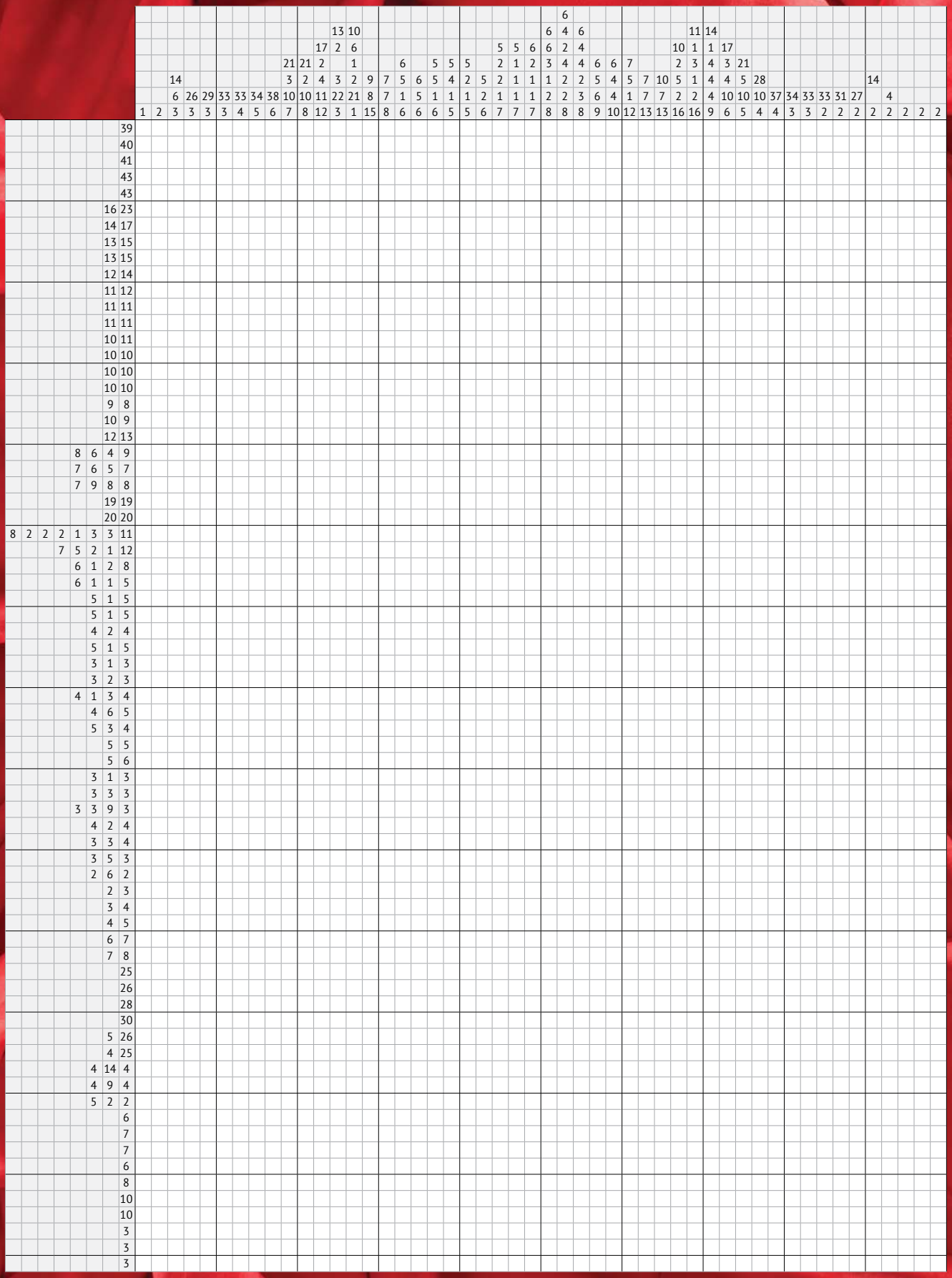
CIS news

www.cismag.news



Есть что почитать!

Японский кроссворд



Календарь мероприятий

5 сентября
Минск • Форум
Международный Гранд Форум «Вокруг ЦОД. Вокруг КЦ. Вокруг Облака. Вокруг IoT. Вокруг IP. Вокруг Безопасности» в Минске

7 сентября
Москва • Турнир
Велотурнир «IT Bike Fest Moscow 2019»

8 сентября
Москва • Турнир
Беговая эстафета «IT Run Moscow 2019»

10 сентября – 29 октября
Санкт-Петербург • Курс
Введение в автоматизацию тестирования ПО

11 сентября
Волгоград • Конференция
CRM И ПРОДАЖИ, Волгоград

11-13 сентября
Москва • Курс
BDAM: Большие данные Big Data для руководителей

12 сентября – 31 октября
Онлайн-трансляция • Курс
Фундаментальный курс по SEO

13-14 сентября
Киев • Тренинг
Data Science и машинное обучение для бизнес-аналитиков

14 сентября
п. Орехово • Турнир
Велотурнир «IT Bike Fest St. Petersburg 2019»

14 сентября
Белгород • Форум
БИФ-2019 – Белгородский IT-форум

17 сентября – 21 ноября
Санкт-Петербург • Курс
Обучающий курс «IT-рекрутер»

19 сентября
Москва • Конференция
Mobile Forensics Day 2019

19 сентября
Москва • Конференция
Biohacking Conference Moscow

20 сентября
Москва • Конференция
SAFe Russia

21 сентября
Киев • Конференция
Agile Rock Conference 2019

22 сентября
Киев • Конференция
AGILE COACH CAMP 2019

22 сентября
Санкт-Петербург • Турнир
Беговая эстафета «IT Run St. Petersburg 2019»

23-24 сентября
С.-Петербург • Онлайн-трансляция • Конференция
Saint TeamLead Conf

23-25 сентября
Москва • Курс
INTR: Основы Hadoop

23 сентября – 21 декабря
Москва • Курс
Digital Branding: Best Cases Learning. Полный курс digital маркетинга от лидеров рынка

24-25 сентября
Киев • Онлайн-трансляция • Конференция
Региональная конференция RIPE NCC

25 сентября
Воронеж • Конференция
Бесплатная бизнес-конференция CRM И ПРОДАЖИ, Воронеж

26-30 сентября
Токио • Хакатон
BizReach Hackathon in Tokyo 2019

26 сентября
Киев • Конференция
Kyiv iGaming Affiliate Conference

29 сентября
Москва • Турнир
Турнир по картингу «IT Race Moscow 2019»

30 сентября – 1 октября
Москва • Онлайн-трансляция • Конференция
DevOpsConf

1-2 октября
Казань • Конференция
Всемирный Цифровой Саммит об интернете вещей и искусственном интеллекте IoT & AI World Summit Russia

4-5 октября
Санкт-Петербург • Конференция
Linux Piter 2019

4-5 октября
Москва • Выставка
3D Print Expo 2019

5 октября
Москва • Онлайн-трансляция • Конференция
День интернет-рекламы: новый уровень

7 октября
Москва • Онлайн-трансляция • Конференция
GolangConf 2019

9 октября
Москва • Онлайн-трансляция • Конференция
MIXAR Conf++

9 октября
Калининград • Конференция
CRM И ПРОДАЖИ

10-13 октября
Таганрог • Конференция
8-ая Всероссийская молодёжная школа-семинар по проблемам информационной безопасности «ПЕРСПЕКТИВА – 2019»

12-13 октября
Казань Иннополис • Конференция
IT-конференция Стачка

13-14 октября
Москва • Онлайн-трансляция • Конференция
FrontendConf

18 октября
Москва • Онлайн-трансляция • Конференция
SEMconf 2019 – конференция по контекстной рекламе

19 октября
Москва • Турнир
Интеллектуальный турнир «IT Brain Battle Moscow 2019»

21-24 октября
Салехард • Хакатон
Хакатон на Полярном круге

22-25 октября
Москва • Конференция
25-я конференция пользователей Esri в России и странах СНГ

23-24 октября
Москва • Конференция
II Инновационно-технический форум «SAY FUTURE: MOSCOW-2019»

1 ноября
Санкт-Петербург • Конференция
Golang Piter 2019

1 ноября
Санкт-Петербург • Конференция
PiterPy 2019

5-8 ноября
Helsinki • Конференция
IEEE FRUCT 2019: 25th Conference of Open Innovations Association FRUCT

6-8 ноября
Москва • Курс
BDAM: Большие данные Big Data для руководителей

10 октября
Москва
Благотворительная IT-конференция CIS «Digital Hearts»

14-16 ноября
Санкт-Петербург • Конференция
15-я Научно-практическая конференция SECR / Разработка ПО 2019

14 ноября
Москва • Онлайн-трансляция • Конференция
INTERCOM»19

16 ноября
Москва • Турнир
Турнир по мини-футболу «IT Goal Moscow 2019»

CISummIT

Ежегодное мероприятие журнала CIS

Благотворительная ИТ-конференция «Digital Hearts»

10 октября

Площадка «Digital October»

Фонд Хабенского

Мероприятие журнала CIS
в поддержку Фонда Константина Хабенского

Заполните регистрационную форму для участия на мероприятии

Конференция CISummIT «Digital Hearts» объединит самых активных участников ИТ-рынка, ведущих производителей и экспертов, чтобы собрать средства для помощи детям с заболеваниями головного мозга.

CIS Современные Информационные Системы

www.cisevent.ru
www.cismag.news
www.cismag.news