CIS
Современные Информационные Системы
№ 4 (26) / 2023

Барби в мире ИТ

Стр. 72

знакомство с ИТ-конкурсом красоты «Beauty&DigITal»

Надежда Грибкова

ЧТО ВОЛНУЕТ ОБЩЕСТВО

Стр. 24

тематики сообщений в соцсетях

РОДИТЕЛЬСКИЙ КОНТРОЛЬ

Стр. 70

или стоит опасаться «большого брата»

КИБЕР-безопасность

Стр. 8

Будущее, риски, перспективы

ТЕХНОЛОГИИ

АНАЛИТИКА

СОБЫТИЯ

РЕШЕНИЯ

ОПЫТ

МИСС BEAUTY&DIGITAL

ИТ-ГОРОСКОП

КАЛЕНДАРЬ

КРОССВОРД

От редактора

Современный мир невозможно представить без информационных технологий, которые стали неотъемлемой частью нашей повседневности. Каждый день мы сталкиваемся с новыми достижениями в этой области, открывая перед собой широкие горизонты возможностей. И в этом быстром и захватывающем мире важно быть в курсе последних событий, тенденций и инноваций.

С гордостью представляем вам новый выпуск нашего ИТ-журнала, посвящённого современным информационным технологиям. В этом номере мы познакомим вас с разнообразными статьями, которые охватывают самые актуальные и интересные аспекты ИТ-мира.

Мы раскроем тему подтверждения возраста, понимая, что это широкий термин, который требует индивидуального подхода в каждом случае. В мире, где информация стала неотъемлемой частью нашей жизни, важно обеспечить адекватную защиту и доступ к контенту для каждого возраста.

Обратимся также к важному вопросу детской интернет-зависимости. Результаты исследования, проведённого «Лабораторией Касперского», помогут лучше понять, как цифровой мир влияет на молодое поколение и как обеспечить их безопасность в сети.

Современный цифровой мир обогатил нашу жизнь множеством новых возможностей, но вместе с тем появились и новые вопросы безопасности. На страницах журнала мы поговорим о родительском контроле и верификации возраста в интернете. Мы приглашаем вас задуматься о важности баланса между прозрачностью и приватностью в цифровой эпохе, где большие данные и искусственный интеллект играют всё более важную роль.

Сегодняшний мир программирования поражает многогранностью, и выбор языка программирования может быть непростой задачей. Статья нашего журнала поможет тем, кто стремится освоить язык программирования «с нуля», определиться с выбором. Наши эксперты расскажут, как сделать этот выбор максимально осознанным и адаптированным к вашим целям.

Опросы и исследования – это мощный инструмент для понимания текущих трендов и настроений в области ИТ. В этом выпуске вы найдёте обзоры и анализ таких тем, как восприятие биометрии, пользование интернетом, кибербезопасность и искусственный интеллект.

Также мы не могли обойти вниманием тему красоты и технологий. В статье о конкурсе «Beauty&DigITal-2023» мы представим интересные истории победительниц этого уникального конкурса, где красота сочетается с современными ИТ-технологиями.

Наша редакция уверена, что этот выпуск журнала станет для вас источником полезной информации, интересных открытий и новых пониманий в области информационных технологий. Желаем увлекательного чтения!

С наилучшими пожеланиями, редакция журнала CIS

Главный редактор: Станислав Понарин.
Директор по маркетингу: Валерия Рябинина.
Дизайн и вёрстка: Алексей Дмитриев.
Корректор: Оксана Макаренко.
Отдел рекламы и распространения: info@sovinfosystems.ru.
Сайт: www.cis.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), д. 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.
Язык: русский.
Периодичность: 4 раза в год (1 раз в квартал).

Фото на обложке: Надежда Грибкова
Тираж 5000 экз. (отпечатанный тираж).
Журнал предназначен для лиц старше 16 лет.

Восприятие биометрии

Опрос

Узнаем будущее по лицу

Биометрия, или система распознавания людей по уникальным физическим и поведенческим признакам, постепенно становится всё более привычным явлением. Открыть вклад голосом, пройти паспортный контроль по отпечатку пальца, оплатить проезд с помощью Face Pay – лишь малая часть предсказаний фантастов, воплотившихся в жизнь благодаря искусственному интеллекту. **На сегодняшний день с понятием «биометрия», по собственным оценкам, знакомы более половины россиян (55%)**. Среди тех, кто сталкивался с предложением сдать биометрические данные, показатель достигает 76%, что почти вдвое больше, чем среди россиян без соответствующего опыта (40%). Под этим термином информированные россияне понимают в первую очередь уникальные физические признаки человека (58% в группе осведомлённых). **В частности, речь идёт о биометрических данных в целом (35%), отпечатках пальцев (17%), внешности (9%) и сетчатке глаза (7%).** О том, что биометрия представляет собой систему распознавания человека, известно каждому третьему (31%), в том числе в единичных случаях упоминаются конкретные способы идентификации – распознавание голоса (3%) и анализ ДНК (2%). Чаще других верное определение биометрии («система идентификации личности») давала молодёжь: 18–24 лет – 41%, 25–34 лет – 36%.

Типичный россиянин, знакомый с понятием «биометрия»,– мужчина (59 % vs. 52 % женщин), 25–59 лет (25–34 лет – 66 %, 35–44 лет – 64 %, 45–59 лет – 60 %), с высшим или неоконченным высшим образованием (73 %), проживающий в одной из столиц (77 %) или городе-миллионнике (73 %) и пользующийся интернетом ежедневно (64 %).

Не имеют представления о биометрии 39% россиян. Чаще о ней ничего неизвестно женщинам (43%), старшему поколению 60+ лет (54%), гражданам с неполным средним образованием (70%), жителям сёл (58%) и активным телезрителям (68%).

Биометрические технологии: потенциал роста

Использование биометрических данных не ограничивается банковским сектором: помимо отделений банков, их можно сдать через специальное мобильное приложение. И, хотя некоторые эксперты отмечают, что в скором времени на смену бумажных паспортов придут биометрические данные, говорить о широком распространении последних пока не приходится. Согласно результатам опроса, **с предложением сдать биометрию в общей сложности сталкивались 42% россиян, в том числе 29% соглашались на сбор и обработку таких данных, не соглашались – 13%.**

Социально-демографический портрет подкованных в вопросе биометрии и сдававших её весьма схож. Опытом сдачи биометрических данных чаще обладают мужчины, нежели женщины (35 % vs. 24 % соответственно), россияне среднего возраста 25–59 лет (от 33 % до 36 %), высокообразованные граждане (38 %), москвичи / петербуржцы (50 %) и регулярные интернет-пользователи (33 %).

Никогда не поступало предложения сдать биометрические данные 56% россиян. Показатель выше среди активных телезрителей (83%), жителей сельской местности (68%) и Северо-Кавказского федерального округа (71%).

Сдача биометрии: за и против

Нынешний охват биометрическими сервисами может быть обусловлен не только слабой информированностью граждан о процедуре сбора данных и их возможностях, но и существующими предубеждениями на этот счёт. Результаты опроса показывают, что **среди россиян преобладает нейтрально-отрицательное отношение к сдаче биометрических данных: 34% относятся к ней безразлично (среди молодёжи 18–24 лет – 46%), 32% – негативно**. Анализ ответов тех, кто воспринимает данную практику негативно, позволил выделить следующие **четыре группы аргументов против сдачи биометрии:**

1. **Вторжение в частную жизнь** (в том числе «сбор личных данных/нарушение прав и свобод человека» – 25%, «контроль/слежка за человеком» – 7%, «государство использует против людей/цифровой концлагерь» – 4%).
2. **Нежелание и дефицит доверия** («плохо хранят данные/возможны утечки» – 11%, «не доверяю/не хочу/не нравится» – 11%, «возможны злоупотребления» – 8%, «могут попасть к мошенникам» – 6%, «небезопасно» – 3%).
3. **Отсутствие нужды** («нет смысла/не вижу необходимости /незачем» – 11%).
4. **Недостаточная информированность** (непонятно/непривычно/не понимаю, для чего это делается» – 5%).

Положительное отношение к сдаче биометрии декларируют 27% россиян. По мнению её сторонников, эта процедура обладает для пользователей такими преимуществами, как:

1. **Безопасность** («борьба с мошенничеством/помощь в поимке преступников» – 24%, «повышение уровня безопасности» – 8%, «защита данных» – 6%).
2. **Прозрачность** («идентификация человека» – 15%, «легче найти человека» – 11%, «больше информации о человеке» – 5%, «честному человеку нечего скрывать» – 3%).
3. **Простота** («удобно/проще пользоваться различными сервисами» – 19%, «упрощает систему опознания людей» – 5%, «сокращение бюрократизации» – 2%).
4. **Прогресс** («за этим будущее/развитие человечества» – 4%).
5. **Порядок** («повышение уровня контроля за людьми/дисциплина» – 4%, «контроль за людьми, пересекающими границу» – 2%).

Ещё 7% просто выразили поддержку без обоснования причин (в группе декларирующих положительное отношение).

ВЦИОМ
• Основан в 1987 году •

Всероссийский центр изучения общественного мнения (ВЦИОМ)

www.wciom.ru

CIS / № 4 (26) / 2023 / www.cis.ru

Пользование интернетом

Опрос

Кто в сети?

Представить современную жизнь без интернета невозможно: в сети совершают покупки, знакомятся, общаются, оплачивают коммунальные платежи, смотрят кино и слушают музыку, а также работают и учатся. Согласно опросу, **74% россиян ежедневно заходят в глобальную сеть, при этом доля heavy users – тех, кто в интернете проводит более четырёх часов в день,– составила 35%, это каждый третий.** За пять лет доля ежедневных пользователей выросла на 12 п. п. именно за счёт heavy users (2018 г.– 23%, 2019 г.– 27%, 2020 г.– 31%, 2023 г.– 35%), то есть пользование интернетом стало более интенсивным. **Не пользуются сетью совсем 16% (–3 п. п. к 2018 г.).**

- **Типичный heavy user** – молодой человек до 25 лет (86% vs. 35% среди всех россиян), с высшим и неполным высшим образованием (40%), с хорошим или очень хорошим материальным положением (39%), житель одной из столиц или города-миллионника (49% и 42% соответственно).
- **Типичный россиянин, проводящий в сети ежедневно менее четырёх часов в день,**– это россиянин среднего возраста 35–59 лет (48–47% vs. 39% среди всех россиян), с высшим образованием (44%), проживающий в городах (за исключением обеих столиц и миллионников) (42–44%).
- **Типичный россиянин, не пользующийся интернетом,**– представитель старшей возрастной группы 60+ (42% vs. 17% среди всех россиян), с неполным средним образованием (36%), житель села (33%).

С 2018 года процент ежедневных пользователей сети в молодёжной среде изменился несильно: среди 18–24-летних прирост составил 4 п. п. (2018 г.– 92%, 2023 г.– 96%), среди 25–34-летних – 7 п. п. (2018 г.– 85%, 2023 г.– 92%). В то же время интенсивность потребления интернета выросла в обеих группах, но в большей степени – среди младшей молодёжи до 25 лет, здесь доля heavy users достигает 86% (+24 п. п. к 2018 г.)

Наиболее заметный рост вовлечённости в интернет приходится на группу 45–59 лет – на 21 п. п. (2018 г.– 55%, 2023 г.– 76%). В этой же группе быстрее всего растёт доля heavy users (2018 г.– 14%, 2023 г.– 29%, в 2 раза). В целом рост пользователей глобальной сети в последние пять лет происходил за счёт старших возрастов (45+), но россияне старше 60 лет медленнее приобщаются к интернету (2018 г.– 32% еженедельных пользователей, 2023 г.– 44%). **Как и в 2018 году, сегодня именно старшая когорта в основном составляет группу тех, кто совсем не пользуется интернетом (2018 г.– 50%, 2023 г.– 41%).**

На активность пользования интернетом влияет уровень образования. Если среди россиян с высшим образованием ежедневно бывают в сети 84% и только 8% не пользуются интернетом совсем, то в группе имеющих неполное среднее образование доля ежедневных пользователей падает до 58%, а доля не бывающих в сети вырастает более чем в четыре раза – до 36%.

В меньшей степени маркером интернет-активности становится доход. Если пять лет назад доля ежедневных пользователей сети среди россиян с хорошим доходом составляла 72%, а в группе с плохим доходом – 59%, то сегодня эти различия сглаживаются, в обеих группах ежедневно пользуются сетью 73% и 70% соответственно. А вот **урбанизированность остаётся в числе факторов интернет-активности россиян:** среди жителей обеих столиц ежедневно проводят время в сети 84%, а на селе – 58%. Этот разрыв за пять лет даже увеличился (в 2018 г. показатели составляли 75% и 51% соответственно).

Абонент временно недоступен

Соцсети, мессенджеры, просмотр видео, игры, электронная почта – беспрерывный поток информации размывает границы между реальным и виртуальным и порой приводит к усталости.

Сегодня большая часть россиян убеждена, что нужно периодически «отдыхать» от интернета, на время ограничивать или полностью блокировать для себя доступ в сеть (66%).

Но разделяют эту точку наши граждане всё реже: 77% – в 2018 г., 73% – в 2020 г. Одновременно с этим **растёт доля тех, кто считает, в наше время в сети нужно быть всегда, так думает уже каждый четвёртый (2018 г.– 19%, 2020 г.– 24%, 2023 г.– 25%).**

- **Чаще о необходимости «отдыхать» от интернета** говорят те, кто активнее всего вовлекался в глобальную сеть в последние годы – 45–59-летние (70%), а также те, кто бывает в интернете редко – несколько раз в неделю (85%), несколько раз в месяц (81%) и реже (83%).
- **Группу сторонников «постоянного онлайна» отличает** молодой возраст (18–24 года – 36%) и высокая интенсивность пользования сетью, среди heavy users так думают те же 36%.
- **Интенсивность потребления интернета и цифровое воздержание связаны:** среди heavy users практикуют ограничение времени в сети 42%, а среди тех, кто проводит в сети ежедневно менее четырёх часов,– 36%. То есть аскеза зарождается среди утомлённых и пресыщенных.
- Среди молодёжи 18–34 лет в целом больший процент ограничивают себя во времени, проведённом в сети,– 46–45% vs. 31% в группе старше 60 лет. Но молодёжь чаще прибегает к таким ограничениям эпизодически – раз в полгода и реже (13–12%), а пользователи старшего возраста практикуют такое регулярно – еженедельно 21%.
- **Чаще других вынужденно оказывались без доступа к интернету** россияне 25–34 лет (60%), граждане с неполным средним образованием (69%), с плохим или очень плохим материальным положением (65%).
- **Не сталкивались с вынужденными ограничениями интернета** преимущественно пользователи с высшим образованием (48%), хорошим или очень хорошим материальным положением (47%) и жители городов в целом (44–47% vs. 37% среди жителей села).
- Определённую роль в привязке человека к виртуальному миру играет возраст: молодёжь 18–24 лет, вырвавшись из онлайна, испытывает положительные эмоции в два раза чаще, чем интернет-пользователи в целом (44% vs. 20%), это же характерно и для мужчин (24% vs. 16% женщин).
- Максимум тех, кто без интернета сталкивается с негативными эмоциями, приходится на жителей городов-миллионников (14% vs. 7% среди всех пользователей сети).

ВЦИОМ
• Основан в 1987 году •

Всероссийский центр изучения общественного мнения (ВЦИОМ)

www.wciom.ru

CIS / № 4 (26) / 2023 / www.cis.ru

Кибербезопасность: будущее, риски и перспективы в мире и в России

В настоящее время кибербезопасность является одной из самых важных и актуальных областей в информационных технологиях. С развитием цифровых технологий и Интернета вещей, а также увеличением количества кибератак и киберпреступлений защита от киберугроз стала приоритетной задачей для организаций и государств.

Будущее кибербезопасности выглядит перспективным, но и омрачено рисками. Одной из главных перспектив является развитие и применение искусственного интеллекта (ИИ) в области кибербезопасности. ИИ может значительно улучшить обнаружение и предотвращение кибератак, обеспечивая автоматическое распознавание аномального поведения и обработку большого объёма данных для выявления угроз. Также возможно использование ИИ для создания автоматических систем реагирования на кибератаки, что позволит сократить время реакции и минимизировать ущерб.

Однако с развитием технологий киберпреступники также совершенствуют свои методы. Они могут использовать ИИ для создания более сложных и совершённых атак, способных обмануть традиционные системы защиты. Это создаёт риск того, что в ближайшем будущем возникнет новое поколение угроз, с которыми будет сложно справиться существующими методами защиты.

В России кибербезопасность также имеет большое значение. С развитием цифровой экономики и постоянным ростом онлайн-сервисов и электронной коммерции обеспечение безопасности данных и защита от кибератак становятся особенно актуальными. Российское правительство придаёт этому вопросу высокий приоритет и предпринимает шаги для развития кибербезопасности в стране. Были созданы специальные структуры и центры, отвечающие за обнаружение и предотвращение кибератак, а также проводится работа по разработке новых законодательных актов в области кибербезопасности.

Кибербезопасность оказывает значительное влияние на множество сфер и индустрий. Одной из таких сфер является финансовый сектор. Киберпреступники часто нацеливаются на финансовые учреждения с целью кражи денежных средств и конфиденциальной информации клиентов. Защита финансовых данных и обеспечение безопасных банковских транзакций становятся основополагающими аспектами работы в этой индустрии.

Другая сфера, где кибербезопасность играет важную роль,– это медицина и здравоохранение. С развитием электронных медицинских записей и сетей обмена медицинской информацией, обеспечение конфиденциальности пациентов и защита медицинских данных становятся критически важными. Нарушение безопасности медицинской информации может иметь серьёзные последствия для пациентов и организаций здравоохранения.

Интеграция искусственного интеллекта со сферой кибербезопасности открывает новые перспективы и вызывает некоторые опасения. С одной стороны, использование ИИ может значительно повысить эффективность систем обнаружения и защиты от кибератак. ИИ может автоматически анализировать большие объёмы данных, идентифицировать аномальные шаблоны и обнаруживать новые виды угроз. Такие системы могут быстро реагировать на атаки и принимать соответствующие меры.

С другой стороны, интеграция ИИ также представляет угрозы. Киберпреступники могут использовать ИИ для создания более сложных и утончённых атак, которые традиционные методы защиты могут не распознать. Кроме того, существует опасность использования ИИ в качестве оружия для кибервойн и шпионажа. Разработка и применение правовых и этических норм и принципов, регулирующих использование ИИ в кибербезопасности, является важной задачей для мирового сообщества.

Чтобы человек мог воспользоваться всеми преимуществами кибербезопасности и быть максимально защищённым от злоумышленников в будущем, необходимо следовать нескольким ключевым подходам и мерам.

- Образование и информирование. Начинать следует с повышения осведомлённости и образования в области кибербезопасности. Это касается как обычных пользователей, так и специалистов. Необходимо проведение семинаров, вебинаров и мероприятий по кибербезопасности. Участие в таковых поможет развивать осознание угроз и учиться применять правила безопасного поведения в сети.
- Проактивная защита. Важно использовать передовые средства защиты и обновлять их регулярно. Это включает в себя использование антивирусного программного обеспечения, брандмауэров, защиты от фишинга и других атак. Также необходимо устанавливать обновления для операционных систем и программ, чтобы устранить известные уязвимости.
- Сильные пароли и многофакторная аутентификация. Использование сложных паролей и механизмов многофакторной аутентификации повышает уровень защиты учётных записей и усложняет задачу злоумышленникам при попытке несанкционированного доступа к аккаунтам пользователей.
- Регулярное резервное копирование данных. Систематическое резервное копирование данных на внешние носители или в облачное хранилище позволяет минимизировать потерю информации в случае успешной кибератаки.
- Осознанное поведение в сети. Не следует раскрывать личные данные, особенно на ненадёжных или незащищённых сайтах. Не открывайте подозрительные ссылки и не скачивайте файлы из недоверенных источников.
- Криптография. Использование криптографических методов для защиты данных и обмена информацией обеспечивает конфиденциальность и целостность данных.

- Киберстрахование. Для организаций, особенно крупных предприятий, страхование от киберугроз может представлять эффективный способ смягчения последствий кибератак и уменьшения финансовых потерь.
- Постоянное обновление знаний и инструментов. Поле кибербезопасности постоянно развивается, и злоумышленники ищут новые способы атак. Поэтому киберспециалисты и пользователи должны постоянно обновлять знания и инструменты, чтобы быть в шаге впереди угроз.

Чтобы рассмотреть влияние кибербезопасности на различные сферы и индустрии более подробно, рассмотрим некоторые ключевые области и их перспективы.

- **Промышленность и производство.** Промышленные предприятия, за счёт всё большей автоматизации, подключаются к сети, что повышает их уязвимость к кибератакам. Успешные атаки на промышленные системы могут привести к значительным простоям производства и финансовым убыткам. Развитие кибербезопасных промышленных систем и стандартов защиты становится необходимостью для обеспечения непрерывной и безопасной работы предприятий.
- **Здравоохранение.** Распространение электронных медицинских записей и медицинских устройств IoT создаёт больше точек входа для киберпреступников. Кибератаки на системы здравоохранения могут иметь катастрофические последствия, поскольку это затрагивает жизни людей и конфиденциальность их личных данных. Инвестирование в кибербезопасность в медицинской сфере помогает предотвратить утечки данных и гарантировать защиту жизненно важных систем.
- **Финансы и банковское дело.** Финансовые институты сталкиваются с постоянным ростом киберугроз, включая фишинг, DDoS-атаки, вредоносное программное обеспечение и кражу личных данных. Защита от кибератак для финансовых организаций является приоритетом, так как доверие клиентов и стабильность финансовой системы напрямую зависят от эффективной кибербезопасности.
- **Государственные и оборонные системы.** Кибератаки на государственные и военные системы становятся всё более угрожающими и разнообразными. Кибершпионаж, кибервойны и кибертерроризм представляют серьёзные угрозы для национальной безопасности. Интеграция ИИ и автоматизированных систем в вооружённых силах и разведывательных службах может улучшить обнаружение и реакцию на кибератаки.
- **Образование.** С развитием онлайн-образования и использованием технологий в учебном процессе кибербезопасность в образовательных учреждениях становится ключевой проблемой. Защита личных данных студентов и персональных сведений учителей – это важный аспект безопасности образовательных систем.
- **Энергетика.** Критическая инфраструктура, такая как энергосистемы, также подвержена растущему риску кибератак. Успешные кибератаки на такие системы могут привести к отключениям электроэнергии и серьёзным последствиям для экономики и общества. Обеспечение безопасности энергетических систем становится неотъемлемой частью их работы.

Интеграция искусственного интеллекта в сферу кибербезопасности обещает значительные преимущества, а также вызывает определённые опасения. При использовании ИИ в кибербезопасности следует учитывать многие факторы.

- **Усиление атак.** Киберпреступники могут использовать ИИ для создания более сложных и хитроумных атак, которые могут обходить традиционные методы обнаружения и защиты.
- **Улучшение обнаружения.** Применение ИИ позволяет обнаруживать аномалии и необычное поведение в сети, что помогает более точно выявлять угрозы и предотвращать их.
- **Автоматизация реакции.** Использование ИИ позволяет создать автоматизированные системы реагирования на кибератаки, что помогает сократить время реакции и минимизировать ущерб от атак.
- **Этические вопросы.** Развитие ИИ в кибербезопасности вызывает такие этические вопросы, как право на приватность и возможность автоматического принятия решений об атаке на противника.

В итоге будущее кибербезопасности зависит от объединения усилий со стороны государств, бизнеса и общества. Кибербезопасность является критической областью, определяющей безопасность и устойчивость нашего будущего, и только путём совместных усилий, развития новых технологий и образования пользователей можно достичь максимального уровня защиты от киберугроз и обеспечить безопасное и устойчивое цифровое будущее.

Искусственный интеллект

Бизнес. Оценка рынка ИИ, карта компаний и отраслей

Рынок ИИ — динамика

Динамика роста рынка искусственного интеллекта в России за 2001–2022 годы

Несмотря на то, что однозначно рынок ИИ оценить невозможно[1], мы всё же делаем оценку рынка «сверху», исходя из совокупного объёма выручки компаний, для которых искусственный интеллект даёт существенный вклад в их бизнес-модель и существенно влияет на их выручку.

Рынок ИИ России в 2022 году показывает рост 17%, тогда как ВВП России упал на 2%[2].

1. «Почему невозможно оценить рынок искусственного интеллекта?», Альманах «Искусственный интеллект» №2, 2019.
2. По данным Росстат ВВП России в 2022 году снизился на 2,1% относительно 2021 года.

647 млрд ₽
Рынок ИИ России 2021 г.

Размер ИИ рынка РФ, млрд ₽

Компании ИИ — карта

Компании работающие в области ИИ в России в 2021 г.

В 2021 г. в России насчитывается ~400 компаний, работающих в сфере искусственного интеллекта.

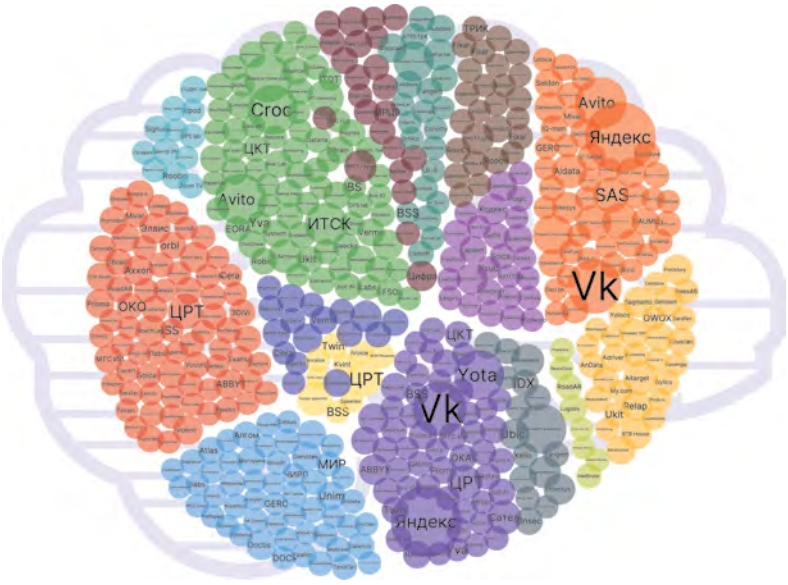
Все их можно посмотреть на интерактивной Карте компаний ИИ России (проект компании IP Laboratory).

Наиболее крупные сегменты, объединяющие 62% всех компаний на рынке (некоторые компании могут входить в несколько сегментов):

Сегменты	Кол-во компаний
Computer vision	76
Business Analytics	77
Healthcare	54
Natural language processing	55
Data Analysis	49

Подробнее на сайте aiRussia.online

Компании, работающие в области ИИ в России в 2021 г.



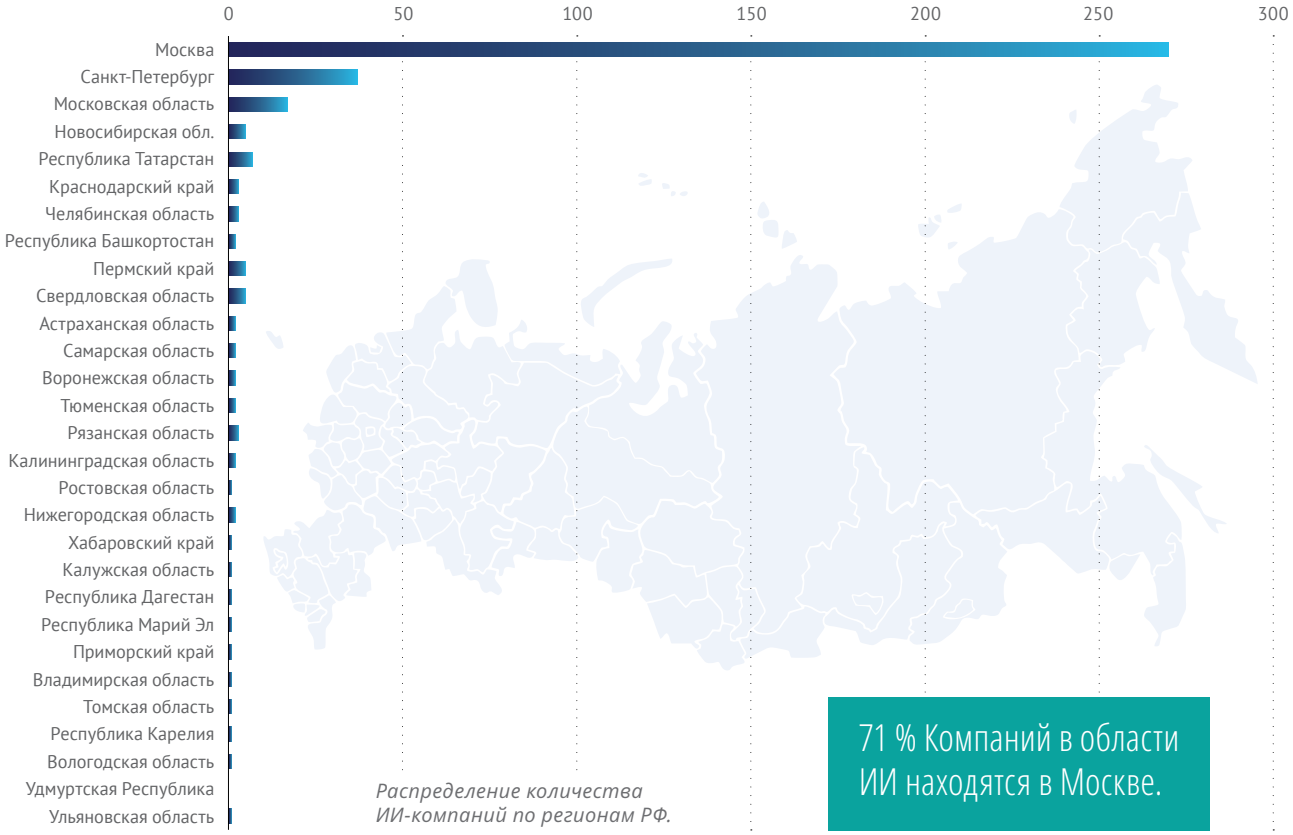
~400 компаний России активно применяют технологии ИИ

Компании ИИ — регионы

Региональная концентрация ИИ компаний в России в 2022 г.

С точки зрения региональной концентрации компаний в области ИИ, безусловным лидером является Москва, где сосредоточен 71% всех компаний рынка.

На втором месте находится Санкт-Петербург, там сосредоточено 10% компаний.



Распределение количества ИИ-компаний по регионам РФ.

71 % Компаний в области ИИ находятся в Москве.

Факторы в мире

Ключевые факторы, которые, на наш взгляд, оказывают сильное влияние на развитие ИИ в мире в 2023 году.

Позитивные +

ChatGPT

Модель ChatGPT, вышедшая в ноябре 2022 года, безусловно, стала событием года №1 и вызвала всплеск интереса бизнеса и общества к теме ИИ. Теперь многие компании пытаются сделать «свой» ChatGPT, что двигает отрасль вперёд.

ИИ, давай поговорим

Теперь ИИ может пользоваться каждый человек. Из сегмента B2B технологии ИИ стремительно перешли в B2C, и теперь журналисты, учёные, политики и другие желающие могут не только пользоваться, но и высказываться об использовании ИИ, тем самым влиять на его развитие. Общество перестало обсуждать ИИ и просто начало им пользоваться.

Негативные -

Вычислительный голод

С ростом размеров моделей по всему миру у компаний (за исключением нескольких гигантов) появилась сильная нехватка вычислительных мощностей. Она вызвана высокой ценой, а иногда и полной недоступностью оборудования.

«Гонка вооружений» в ИИ

Противостояние Китая и США продолжает во многом определять развитие ИИ в мире. К сожалению, эта гонка сильно затрудняет сотрудничество и влияет на качество работы, а значит, это, скорее, негативный фактор.

Факторы в России

Ключевые факторы, которые, на наш взгляд, оказывают сильное влияние на развитие ИИ в России в 2023 году.

Позитивные +

Рост выручки ведущих ИИ компаний

В 2022 г. пользователи начали больше использовать российские сервисы, что привело к росту выручки Яндекса, VK и других ИИ компаний. Это даёт компаниям больше ресурсов для R&D.

Государство стало заботиться

о своих ведущих компаниях в разных отраслях, в том числе ИИ. В первую очередь это связано с санкционными запретами и стратегической необходимостью собственных технологий. Отрасль стала получать повышенное внимание и поддержку.

Негативные -

Санкции на оборудование и технологии

Санкции, введённые из-за СВО, блокируют как покупку оборудования для ИИ, так и собственное производство чипов. Это мешает наращивать вычислительную мощность, необходимую для хранения, обработки данных и обучения моделей ИИ.

Разрушение сотрудничества

Научное международное сотрудничество, с трудом выстроенное за последние годы, стремительно теряет объемы. Международные компании, работавшие в России, закрываются, в том числе закрывают R&D. Глобальные рынки закрылись для российских компаний.

Отток кадров

Отток кадров в области ИИ в 2022 г. стал максимальным за последние годы, что в стратегической перспективе приведёт к ослаблению отрасли ИИ как в академии, так и в бизнесе.

Падение инвестиций

Как мы и предсказывали в 2022 г., инвестиционный рынок в России обрушился. Инвестиции требуют долгосрочного планирования, которое стало невозможно. Зарубежные инвестиции в Россию приостановлены на неопределённый срок.

Основные события ИИ в мире в 2022 г.

ChatGPT

Модель ChatGPT, вышедшая в ноябре 2022 года, безусловно, стала событием года № 1 и вызвала всплеск интереса бизнеса и общества к теме ИИ. Теперь любой человек за 20 $/мес может разговаривать с моделью ИИ от OpenAI.

Gato – шаг в направлении AGI

В 2022 году DeepMind выпустил модель Gato, которую обучили выполнять >600 самых разных заданий, правда не без «технических костылей». Но уже в начале 2023 года DeepMind выпустил модель DreamerV3 , которая обучается разным задачам уже без дополнительных ухищрений на чистом RL.

Mine RL

В 2022 г. Open AI выпустила модель, которая учится играть в Minecraft, обучаясь на неразмеченных видеоигр. На многих задачах эта модель демонстрирует результаты, сопоставимые с человеком.

ИИ как учёный

В 2022 г. с помощью ИИ было получено несколько новых научных результатов, например: новый матричного умножения или управление термоядерным синтезом. Можно уверенно сказать, что ИИ теперь ускоряет результаты научных исследований.

H100 – новая планка скорости

В 2022 г. был выпущен новый ускоритель H100 от компании NVIDIA, который был создан специально для обучения LLM моделей. Это вывело возможности обучения на новый уровень.

Снижение инвестиций в ИИ

Объём венчурных инвестиций в ИИ стартапы впервые за последние 10 лет упал и в мире, и в России. Это может характеризовать переход от инвестиций в ИИ-стартапы к инвестициям в зрелые компании, внедряющие ИИ.

Выводы

Наука

...российские исследователи сделали ~2,5 тыс. публикаций на разных конференциях. Благодаря этому Россия поднялась на 11-е место в мире по данному показателю. Мы почти вошли в десятку!

11 место

Стартапы и инвестиции

...на столько упал объём венчурных инвестиций в 2022 г. Это было ожидаемое, но драматическое падение.

–78 %

Бизнес

...рынок российского интеллекта в России составил ~650 млрд ₽.

650 млрд ₽

Гос. поддержка

...примерно в 3 раза за 2 года выросло государственное финансирование ИИ.

×3

Образование

...~3400 выпускников российских университетов вышли на рынок труда с необходимыми для компаний компетенциями.

3,4 тыс.

Тренды в мире

LLM

Большие языковые модели и ChatGPT, безусловно, являются главным трендом года. Благодаря ChatGPT необходимость своих LLM вышла на первый план и заставляет многие компании бросить все усилия на создание и обучение своей ChatGPT.

Диффузионки

Модели, генерирующие изображения, стали повседневно использоваться и в работе, и в частной жизни. Генерация изображений наряду с ChatGPT стала мощным трендом, который драйвит новые разработки.

Этика на практике

Вопросы этики ИИ поднялись в полный рост с появлением моделей, чья единственная задача — генерация текста. Open AI специально использовал алгоритм RLHF для обучения «этичности» ответов ChatGPT. Теперь каждой компании, разрабатывающей свой ChatGPT придётся 100 раз проверить этичность ответов модели перед выпуском на рынок.

Осторожно, двери закрываются

Похоже, что эра opensource может закончиться. Гонка и конкуренция в области ИИ приводят некоторые компании к выводу, что больше не нужно выкладывать результаты в opensource. Им противостоит коммьюнити, но тренд закрытия на лицо.

Новые ИИ специальности

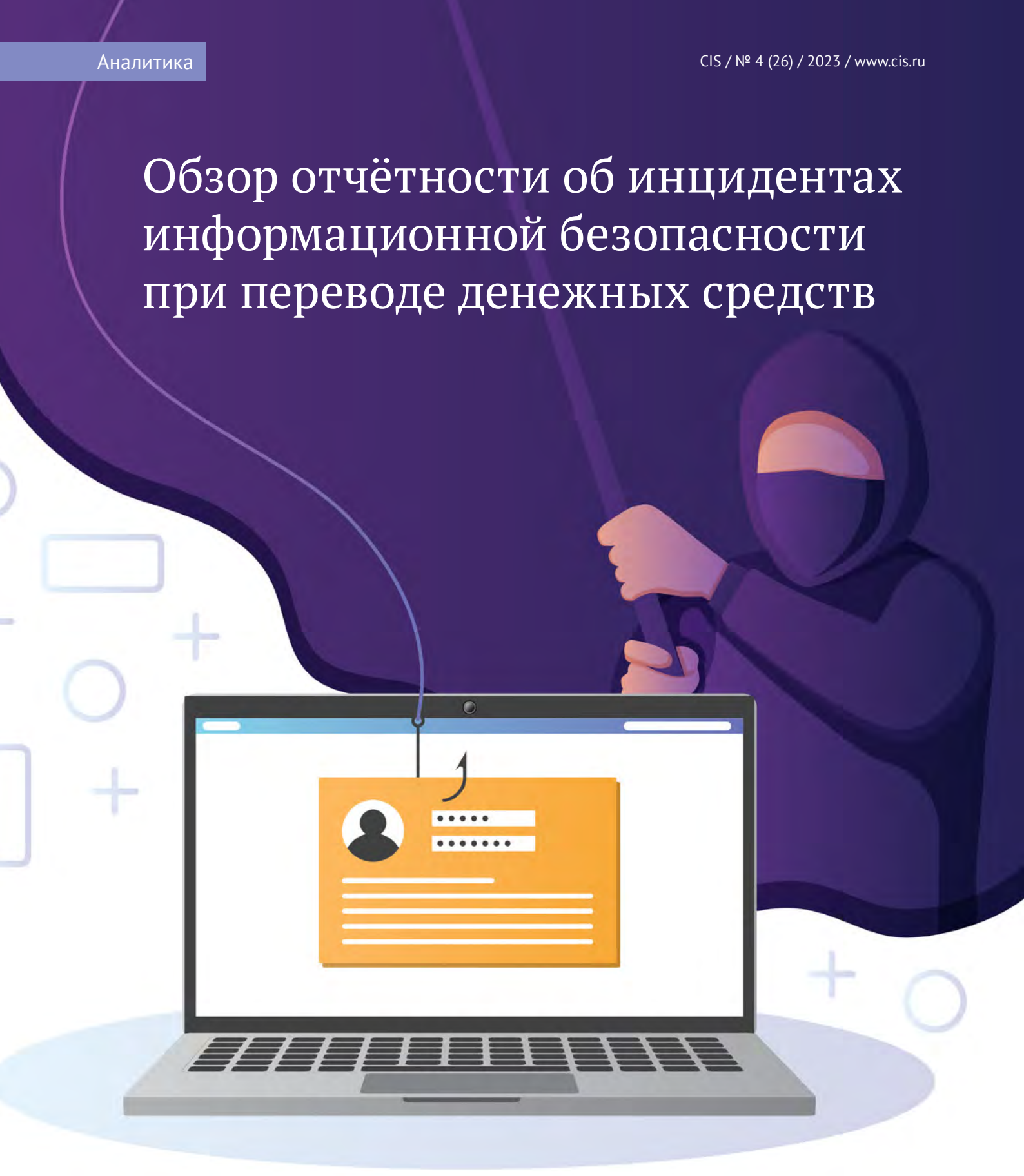
Как мы и предсказывали несколько лет назад, наступила эра, когда для обучения моделей появилась новая специальность – ИИ учителя, которые буквально «оценивают» ответы модели (RLHF). Другая новая специальность – prompt-engineering — специалисты, которые изучают, как правильно спрашивать LLM, чтобы добиться нужного результата.

«Новый интернет»

Теперь информацию можно искать не только в поисковых системах Яндекс или Google, но просто спрашивать ChatGPT. И многие считают это даже более удобным. Похоже, мы стоим в начале «нового интернета», где точкой входа будет не поиск, а диалог с LLM.

CIS / № 4 (26) / 2023 / www.cis.ru

Обзор отчётности об инцидентах информационной безопасности при переводе денежных средств



Банк России направил в адрес регистраторов доменных имен запросы на проверочные мероприятия и снятие с делегирования в отношении 1494 доменных имен сети Интернет, с использованием которых осуществлялась противоправная деятельность.

Кроме того, Банк России направил в Генеральную прокуратуру Российской Федерации информацию о **6805** доменах сети Интернет для проведения проверочных мероприятий и последующего ограничения доступа к ним в соответствии со статьей 15.3 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Ответственное структурное подразделение: Департамент информационной безопасности.

I квартал 2023 года / 31 мая 2023 года

Операции без согласия клиентов (ОБС): общая картина

	Количество ОБС, ед.	Объем ОБС,	Доля социальной инженерии, %	Доля возмещённых (возвращенных) средств (от объёма), %	Количество предотвращенных ОБС, ед.	Объём предотвращенных ОБС, тыс. руб.
Среднее значение за предшествующие четыре квартала	219 147	3 541 361,04	50,4	4,4	-*	-*
I квартал 2023	252 111	4 549 282,42	50,5	4,3	2 727 138	712 004 875,76

* Сбор информации осуществляется с 01.01.2023 г.

Физические лица

	Карты	Счета (Дистанционное банковское обслуживание, переводы)	СБП	Электронные кошельки	Без открытия счета
Количеств о ОБС, ед.	196 575	38 372	12 147	4 311	51
Доля социальной инженерии, %	51,8	35,5	64,0	92,4	72,5
Объём ОБС, тыс. руб.	1 363 735,83	2 489 788,90	552 526,15	28 242,29	9 173,86
Доля возмещённых (возвращённых) средств,%	5,6	1,5	11,6	0,0	0,0

Юридические лица

	Счета	СБП
Количеств о ОБС, ед.	642	13
Доля социальной инженерии, %	23,8	0,0
Объём ОБС, тыс. руб.	102 493,39	3 322,00
Доля возмещённых (возвращённых) средств,%	15,4	0,0

Основные типы компьютерных атак: выявлено (ед.), динамика (%)

Тип атаки	Среднее значение за предшествующие четыре квартала	I квартал 2023
Использование методов социальной инженерии	11538	19608 +69,94% ▲
Фишинговые атаки	1713	1889 +10,27% ▲
Атаки с использованием ВПО	89	75 –15,73% ▼
Атаки типа «отказ в обслуживании» (DDoS)	328	95 –71,03% ▼
Иные атаки	40	47 +17,50% ▲

Мошеннические телефонные номера: выявлено (ед.), динамика (%)

	Среднее значение за предшествующие четыре квартала	I квартал 2023
С использованием номеров 8800	476	683 +43,48% ▲
Городские телефонные номера	61676	9087 –85,30% ▼
Мобильные телефонные номера	126867	87146 –31,30% ▼

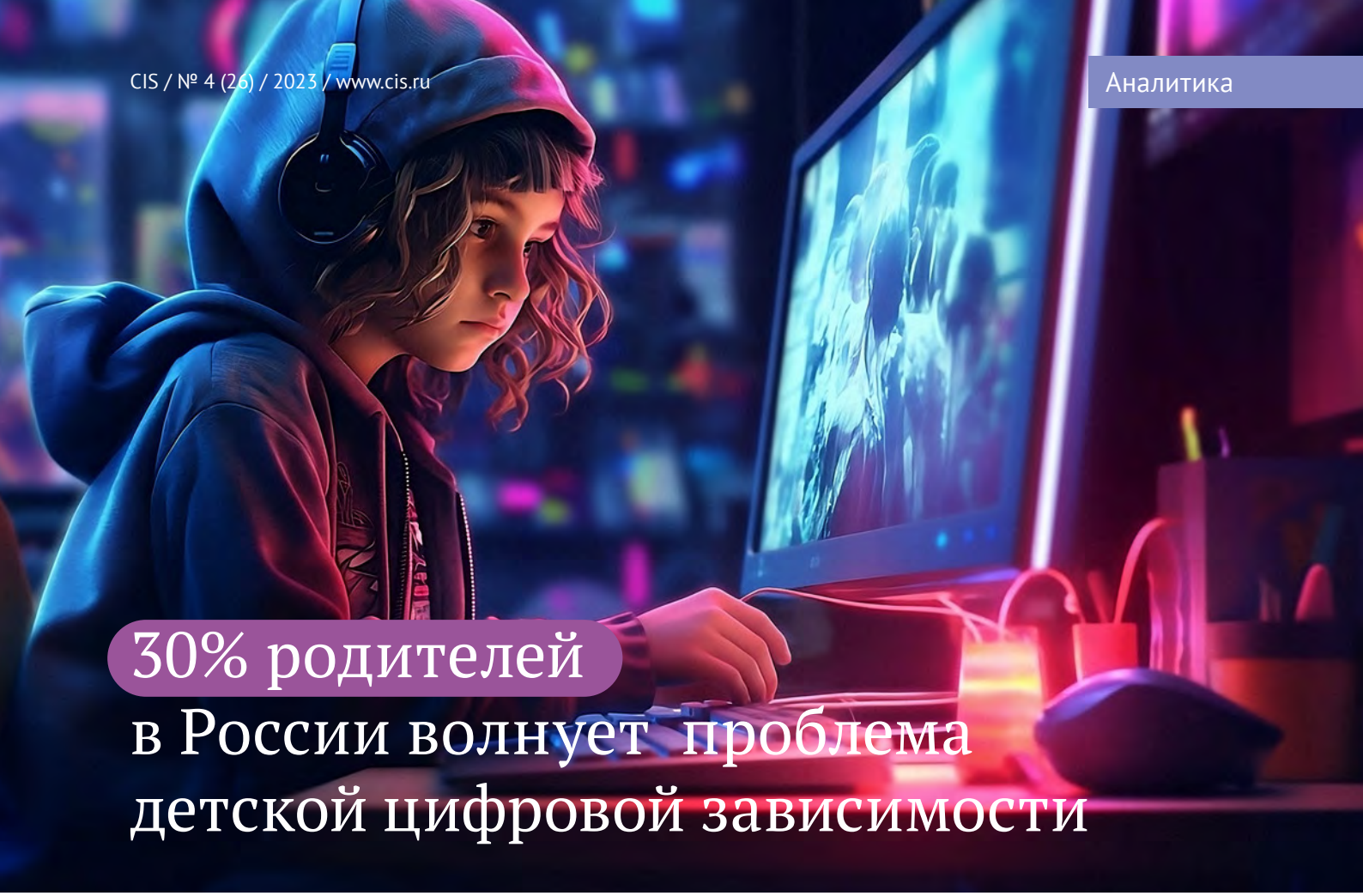
За отчетный период Банк России инициировал 96916 запросов операторам связи для принятия мер реагирования в отношении номеров телефонов, используемых в противоправных целях.

Мошеннические интернет-ресурсы: направлено на блокировку (ед.), динамика (%)

	Среднее значение за предшествующие четыре квартала	I квартал 2023
Безлицензионная деятельность	1314	1489 +13,31% ▲
Фишинг	1612	5462 +238,83% ▲
Финансовые пирамиды	1057	1348 +27,53% ▲

Банк России

www.cbr.ru



30% родителей в России волнует проблема детской цифровой зависимости

По данным нового исследования «Лаборатории Касперского»[1], почти треть (30%) опрошенных родителей в России волнует проблема детской интернет-зависимости.

Больше половины (54%) считают, что современные дети зависимы от гаджетов и интернета, то есть такого мнения о своём ребёнке придерживается каждый пятый. Эксперты по кибербезопасности подчёркивают, что такое заключение может дать только специалист, и, если опасение родителей подтвердится, семье необходимо обратиться за квалифицированной помощью.

Примерно каждый восьмой (13%) согласен, что зависимость от гаджетов и интернета проявляется не только в том, что ребёнок очень много времени проводит у экрана. Интересно, что больше половины детей (57%), также принявших участие в этом опросе, отметили, что, на их взгляд, родители много времени проводят в смартфонах или за компьютером.

Каждый четвёртый уверен, что зависимость от цифрового мира формируется не только из-за того, что дети много времени проводят за устройствами, а вследствие комплекса факторов. Однако взрослые не всегда понимают, как зависимость проявляется на самом деле. По мнению каждого десятого, то, что сегодня многие принимают за зависимость от гаджетов, не является таковой в классическом её проявлении.

Интернет и гаджеты – естественная среда для современных детей. Поэтому в большинстве случаев речь идёт не о зависимости, а о том, что они не представляют своей жизни без технологий. Такого же мнения придерживаются, по данным опроса, больше четверти родителей (27%).

«Конечно, случаи цифровой зависимости у детей встречаются, и это серьёзная проблема. Однако такое заключение может дать только квалифицированный специалист, он же поможет справиться с проблемой,– отмечает Андрей Сиденко, руководитель направления «Лаборатории Касперского» по детской онлайн-безопасности.– *Восприятие времени у детей часто отличается от того, как его ощущают взрослые. Поэтому родителям важно помогать детям развивать позитивные навыки цифрового поведения и привычки, учить их не злоупотреблять экранным временем. В этом могут помочь программы родительского контроля, благодаря которым можно составить расписание использования устройств, настроить лимиты для определённых приложений».*

В помощь родителям «Лаборатория Касперского» разработала решение для детской онлайн-безопасности Kaspersky Safe Kids – www.kaspersky.ru/safe-kids. Приложение обладает функциями мониторинга использования устройств и местонахождения, ограничения небезопасного контента, экранного времени и другими возможностями, которые помогут защитить детей в цифровом мире.

kaspersky

АО «Лаборатория Касперского»

www.kaspersky.ru

1. Опрос проведён компанией ОнИн по заказу «Лаборатории Касперского» в мае-июне 2022 года в России среди родителей и их детей школьного и дошкольного возраста. Всего опрошено 2032 человека: взрослых и детей.

CIS / № 4 (26) / 2023 / www.cis.ru

Реальные преимущества виртуального мира

Институт статистических исследований и экономики знаний НИУ ВШЭ проанализировал преимущества, которые получают российские пользователи интернета.

Согласно опросу, проведённому ИСИЭЗ НИУ ВШЭ в 2022 г., 82,5% россиян пользуются интернетом. Из них более половины (55,5%) извлекают те или иные выгоды, которые имеют отношение к следующим сферам:

1. **Коммуникации** (благодаря сети стало проще поддерживать связи с родственниками и друзьями, а также искать новых друзей или партнёров для отношений).
2. **Карьера** (люди в интернете ищут и находят более высокооплачиваемую работу, информацию, которая повышает их трудовые навыки; устанавливают профессиональные контакты; проходят курсы, которые невозможно пройти офлайн).
3. **Электронная коммерция** (покупают и продают вещи дешевле/выгоднее, чем офлайн).
4. **Финансы** (при использовании интернета люди выбирают более выгодные финансовые предложения, получают информацию о праве на льготу).
5. **Здоровье** (найденная в интернете информация помогает (начать) вести здоровый образ жизни или узнать больше о диагнозе, поставленном врачом).
6. **Социальная сфера** (интернет-пользователи получают консультацию или материальную помощь, которые невозможно или сложно получить офлайн).

Чаще всего пользователи интернета видят коммуникативные преимущества, связанные с расширением социальных контактов и поддержанием общения (74,5%). Это может быть обусловлено, с одной стороны, распространённостью цифровых практик, связанных с общением, а с другой – высоким уровнем развития соответствующих навыков у пользователей: по данным Росстата, цифровыми коммуникационными навыками владеют 91% из них (рис. 1).

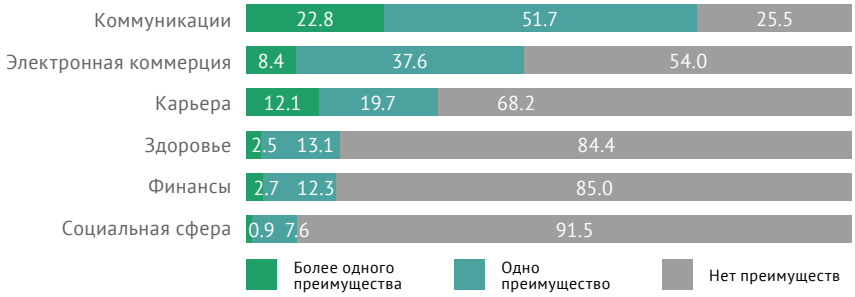
В частности, благодаря интернету 68% пользователей стало проще связываться с родственниками и друзьями; 25% нашли новых друзей; каждый 10-й завёл романтические отношения, а в возрастной группе 18–24 лет – почти каждый пятый (19,3%) (рис. 2).

Вторыми по распространённости среди российских пользователей интернета являются выгоды в сфере электронной коммерции (46%). Согласно опросу, 44% россиян, выходящих в сеть, благодаря онлайн-сервисам экономят, находя в сети товары дешевле, чем в ближайшем магазине. Популярность такого преимущества обусловлена высокой долей россиян, совершающих покупки онлайн (по данным Росстата, в 2022 г.– 50,1% населения в возрасте 15 лет и старше).

Почти треть пользователей используют преимущества интернета для карьерного развития (31,8%). При этом профессиональные контакты в сети находят 19%, а более высокооплачиваемую работу всего 5% пользователей.

Больше всего выгод во всех рассмотренных сферах получают активные пользователи, которые выходят в сеть каждый день или практически каждый. На эффективность использования сети влияет и уровень цифровых навыков: продвинутые пользователи ощущают больше положительных эффектов от своей деятельности в онлайне.

Рис. 1. Преимущества, когда-либо полученные респондентами от использования интернета, по группам: 2022 (в % от общей численности населения, использовавшего интернет за последние три месяца).



ИСИЭЗ НИУ ВШЭ

Рис. 2. Преимущества, когда-либо полученные респондентами от использования интернета: 2022 (в % от общей численности населения, использовавшего интернет за последние три месяца).

ИСИЭЗ НИУ ВШЭ[1]

1. Источники: расчёты ИСИЭЗ НИУ ВШЭ по данным репрезентативного опроса населения России (N=10021, от 14 лет и старше; время проведения: 4 августа – 7 сентября 2022 г.), организованного ИСИЭЗ НИУ ВШЭ; результаты проекта **«Мониторинг цифровой трансформации экономики и общества»** тематического плана научно-исследовательских работ, предусмотренных Государственным заданием НИУ ВШЭ.

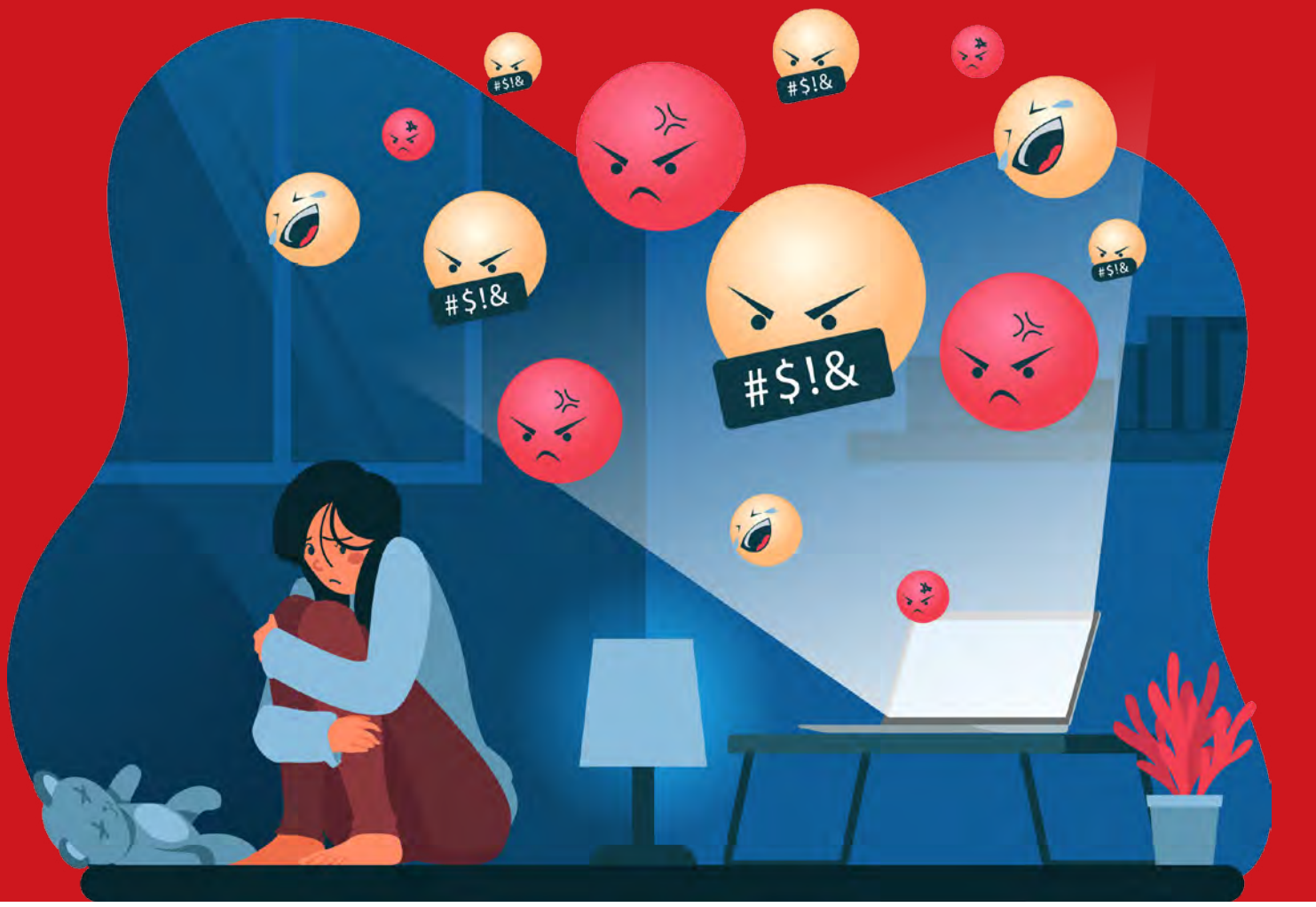
Авторы: сотрудники ИСИЭЗ НИУ ВШЭ Лилия Кузина и Евгений Попов

Материал перепечатан с разрешения ИСИЭЗ НИУ ВШЭ

Ссылка на первоисточник: issek.hse.ru/news/839773040.html

CIS / № 4 (26) / 2023 / www.cis.ru

Агрессия в соцсетях



Институт статистических исследований и экономики знаний НИУ ВШЭ на основе результатов опроса населения России изучил опыт столкновения с деструктивным поведением и способы противодействия ему в социальных сетях.

В цифровой среде довольно остро стоит проблема киберагрессии, проявления которой в диапазоне от навязывания общения до запугивания и травли оказывают негативное влияние на социальное самочувствие пользователей.

Особого внимания заслуживает агрессия в социальных сетях. На протяжении многих лет они значительно опережали по популярности прочие цифровые сервисы. Этот тренд сохранился и после 2019–2020 гг., на которые пришёлся резкий рост аудитории мессенджеров, обусловленный влиянием ограничительных мер, связанных с пандемией COVID-19.

По данным опроса ИСИЭЗ НИУ ВШЭ, в 2022 г. аккаунты в социальных сетях имели 71% россиян в возрасте от 14 лет и старше. Большинство из них (77%) зарегистрированы сразу в нескольких таких сервисах, в среднем – трёх. По популярности с большим отрывом лидирует «ВКонтакте» (аккаунт имеют 75% пользователей соцсетей). Следом идут Telegram (55%), который благодаря возможности создания каналов успел превратиться в полноценную социальную сеть, «Одноклассники» (48%), Instagram* (39%) и TikTok (27%) (рис. 1).

Почти треть (29%) пользователей соцсетей сталкивались с коммуникативной агрессией на этих сервисах за последние три месяца, предшествовавшие опросу. Её наиболее распространённая форма – нежелательное внимание (19%), включающее настойчивые попытки общаться несмотря на отказы (12%), бестактные вопросы от незнакомцев (9%) и нежелательные сообщения с предложениями сексуального характера (6%) (рис. 2).

Каждый десятый пользователь соцсетей подвергался враждебным нападкам (10%): получал оскорбительные комментарии (8%) или даже

* Принадлежит Meta, которая была признана экстремистской и запрещена в России.

сообщения с угрозами в свой адрес либо близких людей (2%), сталкивался с травлей или агрессивным преследованием со стороны группы лиц (3%). Около 10% видели в соцсетях агрессивные сообщения, адресованные другим людям.

Некоторые стали жертвами размещения недостоверной или компрометирующей информации о себе (2%). Особенно подвержены этой форме коммуникативной агрессии пользователи, которые становились объектами нежелательного внимания или агрессии.

Чаще сталкиваются с киберагрессией в соцсетях проявляющие в них большую активность молодые пользователи: в самой юной возрастной группе от 14 до 22 лет такой опыт имеют 43%; среди пользователей 23–29 лет их доля на 9 п. п. ниже (34%); в старших возрастных группах величина показателя ещё сильнее снижается. Девушки чаще юношей становятся объектами нежелательного внимания (34 против 22%).

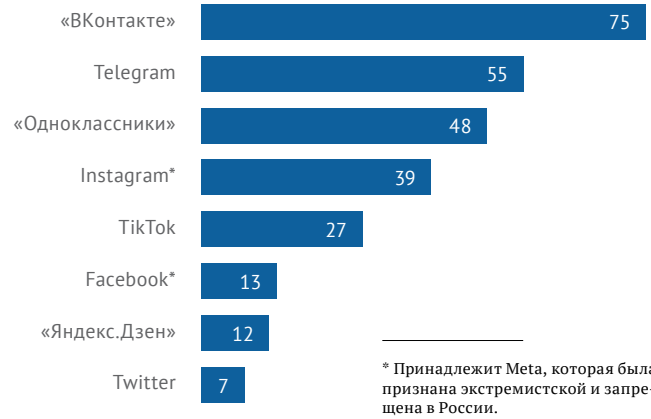
Характер пользования соцсетями также влияет на коммуникативные риски. Так, респонденты, которые «производят контент» (высказываются в личных сообщениях, постах или комментариях; размещают фотографии, делятся публикациями и др.), подвергаются киберагрессии чаще тех, кто этого не делает (32 против 11%). Выражение своей гражданской позиции (высказывания по общественным, политическим, экологическим и иным проблемам) также резко повышает соответствующие риски (57%). Ещё одна категория пользователей, притягивающих к себе агрессоров,– блогеры, причём даже те, которые публикуют контент нерегулярно, время от времени. Около 63% представителей данной группы сталкивались в соцсетях с какими-либо формами нежелательного поведения.

Функционал всех социальных сетей предусматривает стандартные инструменты для противостояния нежелательному поведению, но прибегают к ним только 34% пользователей. Среди столкнувшихся с проблемами менее трети (30%) добавляли кого-то в чёрный список и лишь 14% жаловались на комментарии.

Среди респондентов, выражавших в соцсетях гражданскую позицию по каким-либо вопросам, и блогеров свыше половины задействовали функции блокировки пользователей (53%) или жалоб на комментарии (51%). В то же время среди пользователей, наблюдавших киберагрессию исключительно в адрес других людей или групп, только 18% осуществляли хотя бы одно из этих действий.

Лучше защищают себя в соцсетях пользователи с высоким уровнем цифровых навыков: более половины из них, столкнувшись с нежелательным поведением, применяли какие-либо инструменты защиты. Среди пользователей с низким уровнем цифровых навыков таких вдвое меньше – 26%. Таким образом, слабая востребованность инструментов защиты от киберагрессии отчасти связана с дефицитом цифровых навыков аудитории рунета.

Рис. 1. Использование социальных сетей: 2022 (в % от опрошенных в возрасте 14 лет и старше, имеющих аккаунт в соцсетях).



* Принадлежит Meta, которая была признана экстремистской и запрещена в России.

ИСИЭЗ НИУ ВШЭ

Рис. 2. Столконовение с киберагрессией (за последние три месяца к моменту опроса) (в % от опрошенных в возрасте 14 лет и старше, имеющих аккаунт в соцсетях).

ИСИЭЗ НИУ ВШЭ[1]

1. Источники: расчёты ИСИЭЗ НИУ ВШЭ по данным репрезентативного опроса населения России (N=10021, от 14 лет и старше; время проведения: 4 августа – 7 сентября 2022 г.), организованного ИСИЭЗ НИУ ВШЭ; результаты проекта «Мониторинг цифровой трансформации общества» тематического плана научно-исследовательских работ, предусмотренных Государственным заданием НИУ ВШЭ.

Авторы: сотрудники ИСИЭЗ НИУ ВШЭ Валентина Полякова и Иван Юдин

Материал перепечатан с разрешения ИСИЭЗ НИУ ВШЭ

Ссылка на первоисточник: issek.hse.ru/news/843172295.html

Что волнует общество: тематики сообщений в социальных медиа

Система анализа соцмедиа и СМИ Brand Analytics представила результаты масштабного исследования тематик, которым посвящены сообщения пользователей в социальных медиа. С помощью нейросетей был проанализирован весь публичный поток сообщений в русскоязычных социальных медиа и потоки в каждой значимой социальной сети в отдельности. Разделены анализируемые потоки на тематики и определены самые популярные из них. О том, что важно обществу здесь и сейчас, в данном исследовании.

Социальные медиа стали важнейшим инструментом для общения и обсуждения: в них пользователи выражают мысли и чувства, делятся историями, фотографиями, видео и другими контентом. Это мощный инструмент для социального взаимодействия, отражающий культурные, социальные и политические тенденции. Это цифровой слепок общества, показывающий, чем оно живёт. Цель исследования – показать, что именно сейчас обсуждают люди в социальных медиа.

Как производился подсчёт

После исключения спама был проанализирован поток в 371 млн русскоязычных сообщений, опубликованных пользователями в социальных медиа с 1 по 14 июня 2023 года.

Для определения тематик из потока выделено 312 млн сообщений. Из анализа исключены короткие сообщения длиной менее 20 символов, не относящиеся ни к какой тематике. В результате анализа нейросети разделили сообщения на 62 тематики, 43% исследуемого массива было отнесено к одной из тематик.

Brand Analytics

www.br-analytics.ru

Самые обсуждаемые тематики в соцмедиа

СОЦМЕДИА 2023

топ-20 популярных тематик

1–14 июня 2023

	Количество сообщений	Доля тематики в потоке сообщений
Товары и услуги	23 979 678	7,7%
Одежда и обувь	9 603 287	3,1%
Военная тематика	8 008 850	2,6%
Вакансии	7 987 824	2,6%
Политика	6 965 763	2,2%
Красота	6 463 308	2,1%
Дети и воспитание	6 368 064	2,0%
Животные	6 012 502	1,9%
Психология и отношения	4 249 422	1,4%
Еда	3 807 030	1,2%
Музыка	3 773 908	1,2%
Культура и мероприятия	3 662 035	1,2%
Кино	3 646 398	1,2%
Автомобили	3 268 931	1,0%
Видеоигры	3 099 233	1,0%
Религия и духовность	3 044 011	1,0%
Спорт и киберспорт	2 917 535	0,9%
Природа	2 733 967	0,9%
Кулинарные рецепты	2 678 550	0,9%
Здоровье и медицина	2 628 751	0,8%

ВКонтакте

топ-15 популярных тематик

1–14 июня 2023

Доля тематики в публикациях на площадке

Товары и услуги	9,3%
Одежда и обувь	5,2%
Вакансии	3,2%
Дети и воспитание	2,8%
Животные	2,5%
Красота	2,4%
Культура и мероприятия	1,7%
Психология и отношения	1,5%
Кино	1,5%
Военная тематика	1,5%
Музыка	1,4%
Автомобили	1,3%
Политика	1,2%
Спорт и киберспорт	1,1%
Еда	1,1%

Telegram

топ-15 популярных тематик

1–14 июня 2023

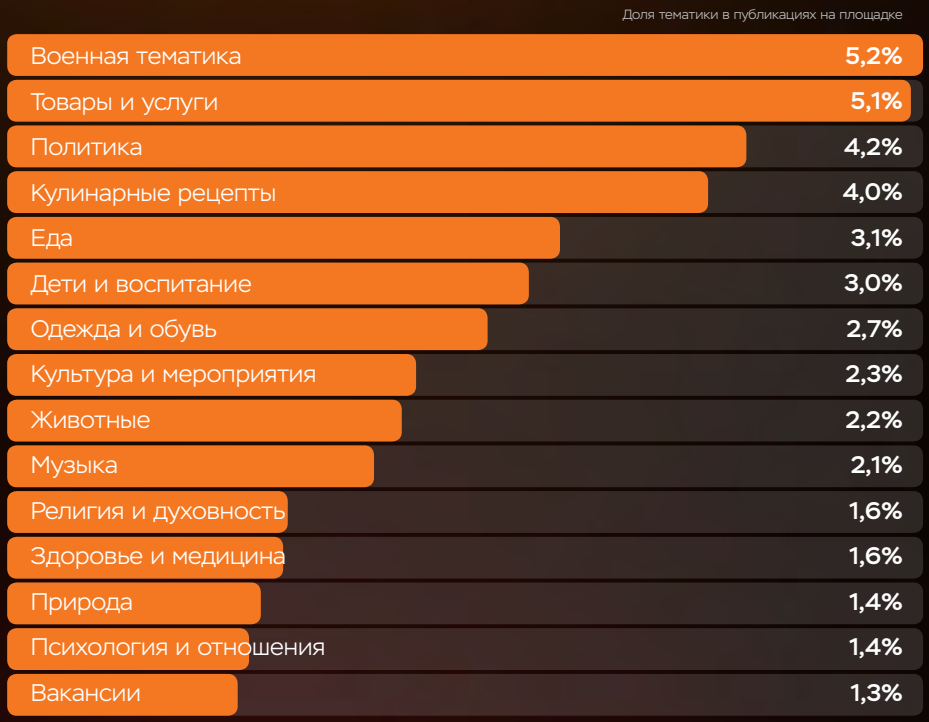
Доля тематики в публикациях на площадке

Товары и услуги	9,1%
Вакансии	3,4%
Военная тематика	2,7%
Политика	2,1%
Красота	2,0%
Видеоигры	1,3%
Одежда и обувь	1,2%
Животные	1,1%
Дети и воспитание	1,0%
Психология и отношения	0,9%
Спорт и киберспорт	0,9%
Эротический контент	0,9%
Еда	0,9%
Пиратский контент	0,8%
Автомобили	0,8%

Одноклассники

топ-15 популярных тематик

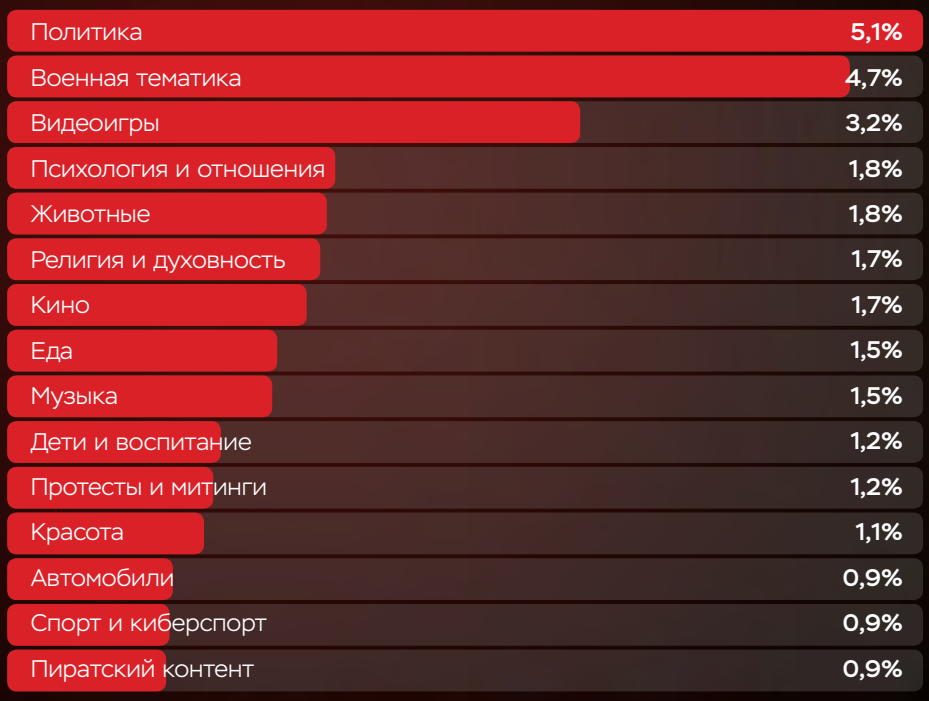
1–14 июня 2023



YouTube

топ-15 популярных тематик

1–14 июня 2023



Instagram*

топ-15 популярных тематик

1–14 июня 2023

Доля тематики в публикациях на площадке

* Социальная сеть Instagram запрещена на территории РФ.

Дзен

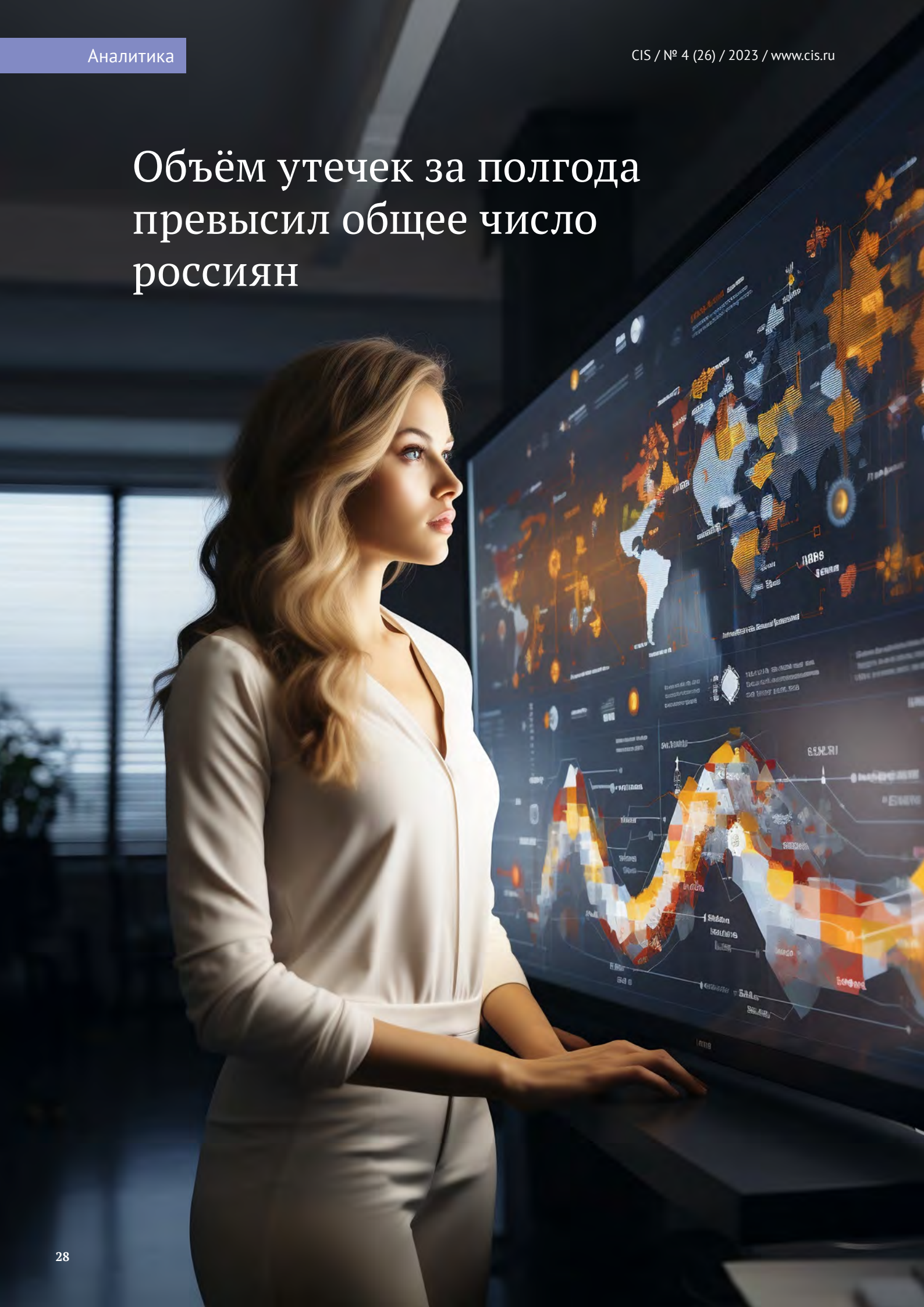
топ-15 популярных тематик

1–14 июня 2023

Доля тематики в публикациях на площадке

CIS / № 4 (26) / 2023 / www.cis.ru

Объём утечек за полгода превысил общее число россиян



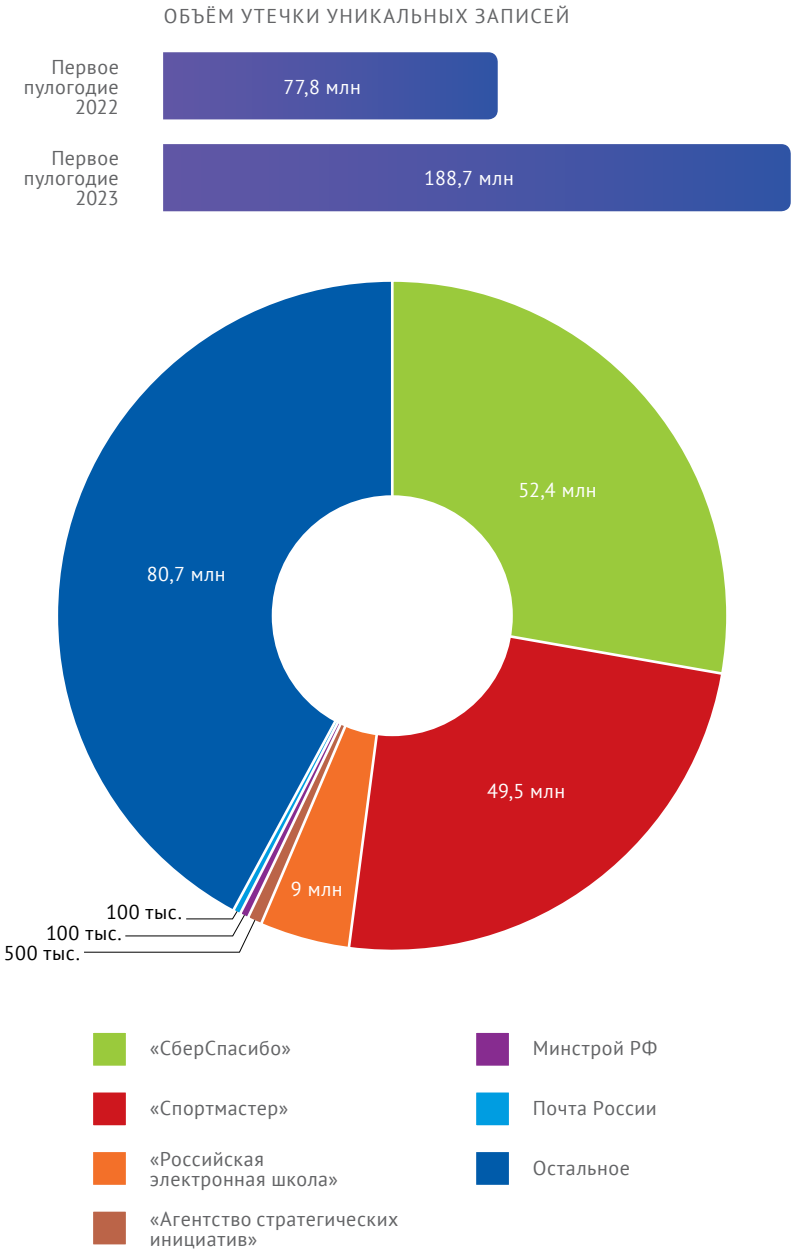
Российский сервис разведки утечек данных и мониторинга даркнета DLBI (Data Leakage & Breach Intelligence) проанализировал крупнейшие утечки данных, произошедшие в России за 6 месяцев 2023 года.

Всего за это время произошло 60 крупных утечек, содержащих 188,7 млн клиентских записей (содержащих уникальные клиентские e-mail или телефоны). При этом в первом полугодии прошлого года произошла 41 крупная утечка данных общим объёмом 77,8 млн уникальных записей, что позволяет говорить о росте на 46% по числу утечек и в 2,4 раза по их объёму.

Как и в первом квартале этого года, большинство утечек произошло из различных e-commerce проектов, а лидерами за полгода стали бонусная программа «СберСпасибо» (52,4 млн записей) и сеть «Спортмастер» (45,9 млн записей). Также среди крупнейших утечек можно отметить данные образовательной платформы «Российская электронная школа» (9 млн записей), Минстроя РФ (100 тыс. записей), «Агентства стратегических инициатив» (500 тыс. записей) и Почты России (100 тыс. записей).

При этом более 90% утечек, как и раньше, связаны с деятельностью украинских хактивистов и представляют собой дампы баз данных систем управления сайтом, в основном «1С-Битрикс», выгрузка которых могла стать возможной в результате взлома с использованием уязвимостей в компонентах CMS, которые не были обновлены вовремя.

Как отметил **основатель сервиса DLBI Ашот Оганесян**, мы имеем дело со сформировавшейся тенденцией тотального сканирования серверов в Рунете, поисках известных уязвимостей. «При этом, как мы видим по списку утечек, российские компании (и большие, и малые) продолжают игнорировать эту проблему, а регуляторы ограничиваются декларативным ужесточением законодательства, которое на практике не применяется»,– добавил он.



Методология исследования

В исследовании рассматривались утечки, обнаруженные сервисом DLBI и опубликованные на сайтах в даркнете, а также закрытых и публичных форумах и Телеграм-каналах в обычном интернете. В базу исследования включены как публикации массивов данных, так и сообщений о взломах с указанием объёма украденных данных, а также предложений о продаже данных. Размер утечки определялся по числу уникальных телефонных номеров или e-mail адресов. При наличии отдельных баз телефонов или адресов, учитывалась большая база, а не их сумма в силу возможностей пересечения.

О компании

DLBI (Data Leakage & Breach Intelligence) – российский сервис разведки уязвимостей и утечек данных, а также мониторинга мошеннических ресурсов в DarkNet. DLBI предлагает своим клиентам анализ внешней серверной инфраструктуры с выявлением недостатков реализации хранения, а также мониторинг предложений о продаже чувствительных данных на различных закрытых площадках, группах Telegram и мошеннических ресурсах в DarkNet.

CIS / № 4 (26) / 2023 / www.cis.ru

Исследование кибербезопасности АСУ ТП — новые подходы

Экспертно-аналитический центр группы компаний InfoWatch представляет отчёт по результатам исследования кибербезопасности АСУ ТП. В исследовании выявлен ряд изменений в подходах к защите АСУ ТП и КИИ за последний год, наиболее популярные и востребованные меры защиты, а также сопоставлены подходы к защите АСУ ТП в России и за рубежом.

Для отчёта использованы материалы анонимного опроса, проведённого путём целевых и массовых рассылок от имени группы компаний InfoWatch, Ассоциации по защите деловой информации (BISA), посетителей стенда InfoWatch на форуме PHDays 2023, а также отчёты ряда зарубежных и российских компаний.

Опрос проводился с мая по июнь 2023 г. Основную долю респондентов составили специалисты ИБ, ИТ и АСУ (АСУ ТП) из промышленного сектора.

Результаты исследования

Основную долю респондентов (70%) составили специалисты ИБ и АСУ (АСУ ТП) из промышленного сектора, в частности из нефтегазовой отрасли (15%) и электроэнергетики (13%). В опросе также приняли участие респонденты из оборонного сектора, атомной отрасли, приборостроения, транспорта и других.

Специалисты ИБ составили наибольшую долю опрошенных – 63%, специалисты АСУ – 7%.

89% опрошенных – представители крупных и средних компаний (55% и 34% соответственно). Все специалисты АСУ – из средних и крупных компаний (в большей мере крупных). Специалисты ИБ представили компании всех размеров, но большинство тоже из крупных.

Разница в подходах к обеспечению ИБ в зависимости от наличия объектов КИИ

Респондентам был задан вопрос: «Являются ли организации, в которых они работают, владельцами объектов КИИ?» Ответы распределились следующим образом:

Рисунок 1. Есть ли в организации объекты КИИ. Распределение ответов по всей выборке

Как видно из рисунка 1, 65% ответивших работают в организациях, являющихся владельцами объектов КИИ.

Рисунок 2. Есть ли в организации объекты КИИ. Ответы специалистов ИБ

Рисунок 3. Есть ли в организации объекты КИИ. Ответы специалистов АСУ

Картина по ответам специалистов ИБ в целом совпадает с общей выборкой: более чем в 2/3 организаций есть объекты КИИ. Почти единогласно о наличии объектов КИИ в их организациях заявили специалисты АСУ.

Стоит заметить, что несколько специалистов из оборонной, атомной металлургической, нефтегазовой отраслей промышленности ответили, что в их организациях нет объектов КИИ, хотя, согласно ст. 2187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017, организации, владеющие ИС, ИТКС, АСУ, функционирующие в вышеуказанных отраслях, являются субъектами КИИ. Возможно, отвечавшие специалисты рассматривали в качестве объектов КИИ только категорированные системы (значимые объекты КИИ).

Далее была рассмотрена **разница в подходах к защите на примерах групп организаций в зависимости от наличия или отсутствия у них объектов КИИ**. Респондентам был задан вопрос: «Есть ли регламенты или иные правила, явно отличающие подход к защите объектов КИИ и не КИИ внутри их компании?» Подробнее на рисунке 4.

Для большинства организаций-владельцев объектов КИИ видно однозначное разделение мер безопасности: **84% организаций разграничивают меры для защиты объектов КИИ и других объектов**. Ответы респондентов, не работающих в субъектах КИИ, разделились примерно пополам, но отсутствие у них объектов КИИ позволяет считать, что это их теоретические представления.

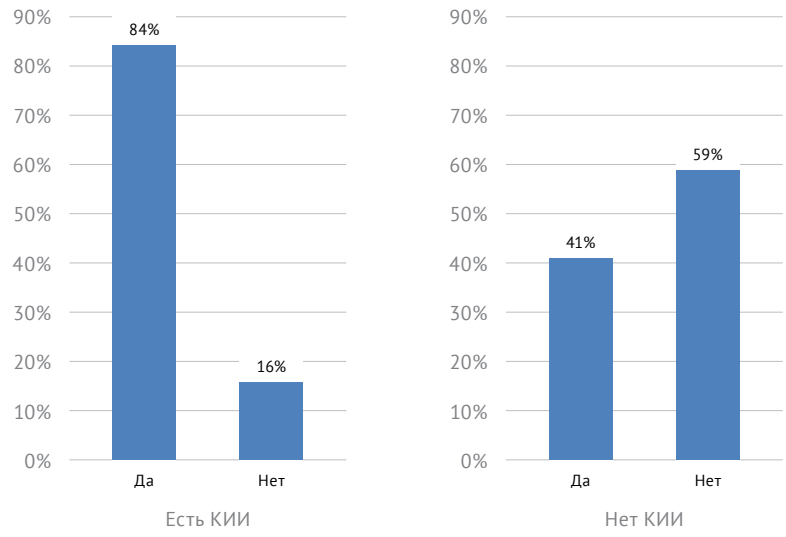


Рисунок 4. Различаются ли меры защиты объектов, относящихся к КИИ и не относящихся

Как отвечают на этот вопрос специалисты ИБ и АСУ:

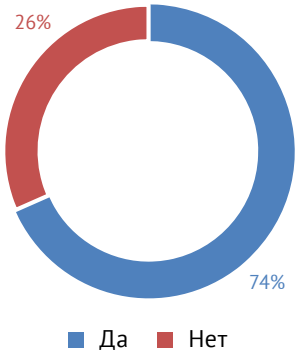


Рисунок 5. Различаются ли меры защиты объектов, относящихся к КИИ и не относящихся. Вся выборка

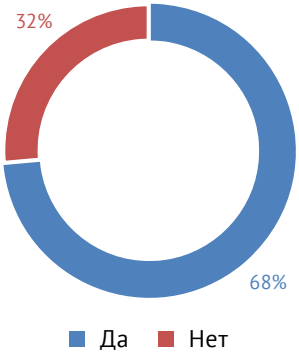


Рисунок 6. Различаются ли меры защиты объектов, относящихся к КИИ и не относящихся. Ответы специалистов ИБ

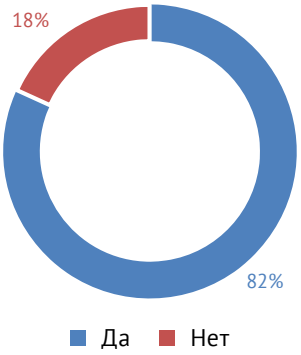


Рисунок 7. Различаются ли меры защиты объектов, относящихся к КИИ и не относящихся. Ответы специалистов АСУ

По ответам мы видим, что в более чем 74% организаций реализуется различный набор мер для обеспечения ИБ-объектов, относящихся к КИИ и не относящихся. Ту же тенденцию можно увидеть и по ответам специалистов ИБ и АСУ.

Одинаковые меры защиты всех категорий объектов (18% и 32%) применяются в основном в малых и средних компаниях.

Далее представлены сравнения в выборе мер ИБ для защиты рабочих станций для вышеуказанных

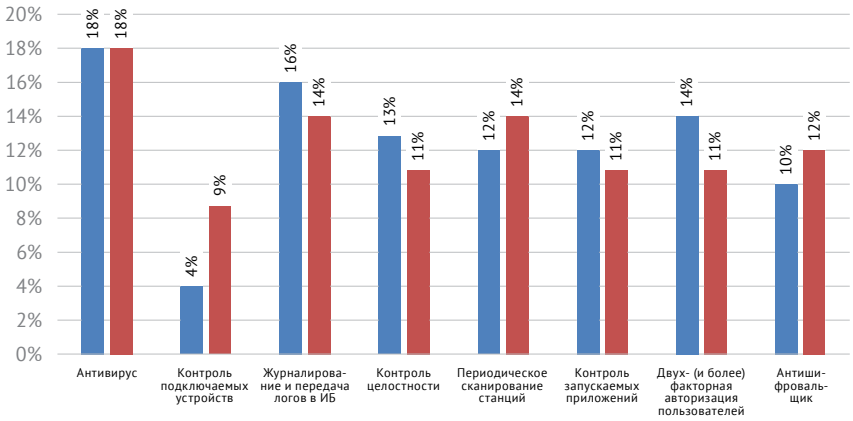


Рисунок 8. Меры ИБ, применяемые для защиты рабочих станций в условиях ухода с рынка западных вендоров

аудиторий в текущих условиях, в т. ч. связанных с уходом западных вендоров с российского рынка (рис. 8).

Разница прослеживается в распределении мер защиты.

Для владельцев объектов КИИ основными мерами защиты являются:

- антивирусная защита (18%);
- журналирование и передача логов в отдел информационной безопасности (16%);
- многофакторная аутентификация (14%).

Для организаций, которые не владеют КИИ:

- антивирусная защита (18%);
- журналирование и передача логов в отдел информационной безопасности (14%);
- периодическое сканирование станций (14%). Выделяются два вида ответов:
- «антишифровальщики» у обеих категорий стоят фактически на предпоследнем месте, хотя, например, согласно исследованиям и рекомендациям как CISA (США), так и «Лаборатории Касперского» и других компаний (см. далее), этот вид угроз выделен как один из основных;
- организации, не владеющие объектами КИИ, большее внимание уделяют контролю подключаемых устройств – 9% против 4%.

Наряду с вопросом о защите рабочих станций был задан вопрос о выборе функций безопасности для защиты промышленных сетей (рис. 9).

У обеих групп нет значимых различий в выборе ключевых мер защиты промышленных сетей, кроме WAF, который отметили 16% респондентов из организаций, не являющихся владельцами объектов КИИ.

Далее сравниваются подходы к **выбору средств защиты информации, прошедших официальную оценку соответствия требованиям безопасности информации**. Как правило, это сертифицированные СЗИ, гораздо реже – прошедшие такую оценку в ходе приёмо-сдаточных испытаний (рис. 10).

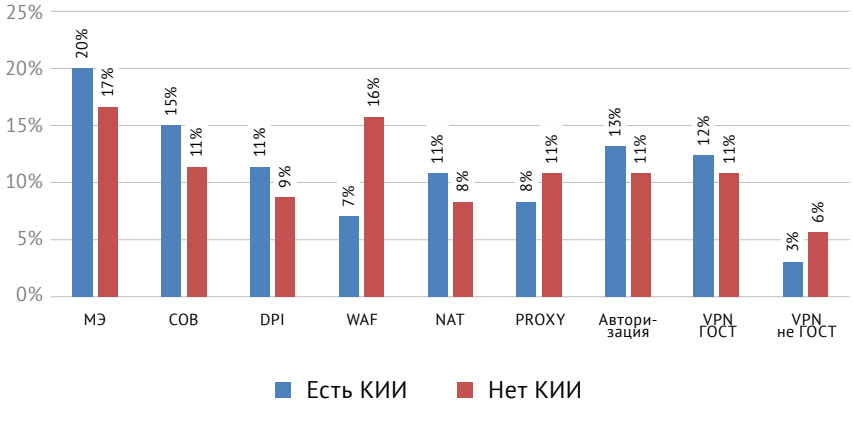


Рисунок 9. Ключевые меры защиты промышленных сетей.

Для организаций-владельцев объектов КИИ в большей степени имеет важное значение установка СЗИ, соответствующих официальным требованиям (ТУ от вендора, ФСТЭК России, ФСБ России), что объясняется требованиями НПА и ОРД, регулирующих безопасность КИИ.

В плане **допустимости установки СЗИ, рекомендованных производителем АСУ,** наблюдается такая картина (рис. 11).

Обе рассмотренные группы в большинстве случаев считают, что необходимо устанавливать СЗИ, рекомендованные производителем систем: такого мнения придерживаются более 60% ответивших. **При этом у специалистов АСУ такого мнения придерживается подавляющее большинство (91%).**

82% опрошенных представителей субъектов КИИ сообщили, что у них разделены корпоративная и промышленная сети. У организаций, не владеющих объектами КИИ, этот показатель составил 58% (рис. 12).

При этом подходы обеих групп похожи в реализации разделения сетей – 55% и 56% сетей разделены через СЗИ (рис. 13).

В связи с тем, что IIoT занимает рынок систем управления и постепенно вытесняет «традиционные» АСУ ТП, а обеспечение безопасности этих систем является одним из основных направлений кибербезопасности и имеет свою специфику, был задан вопрос о наличии и перспективах внедрения IIoT (рис. 14).

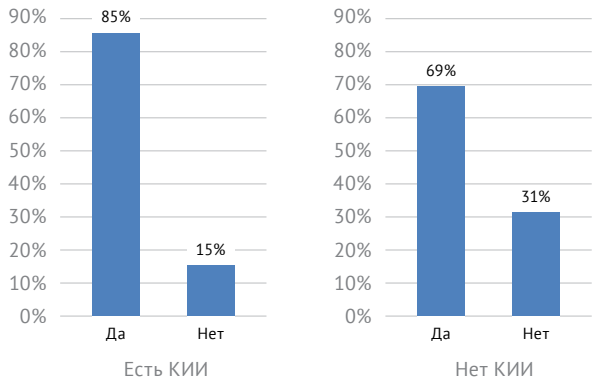


Рисунок 10. Важно ли соответствие СЗИ официальным требованиям

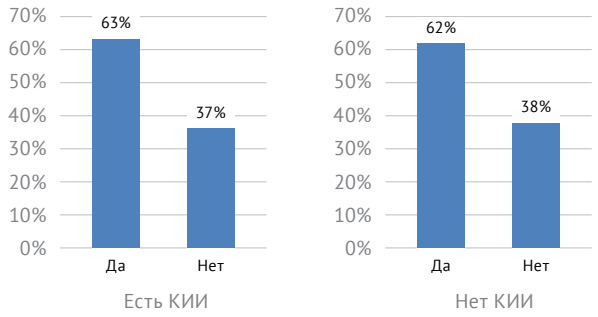


Рисунок 11. Допустимость установки только СЗИ, рекомендованных производителем АСУ

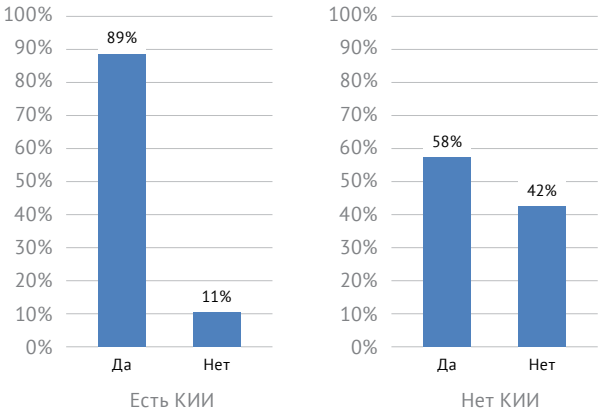


Рисунок 12. Разделены ли корпоративные и промышленные сети

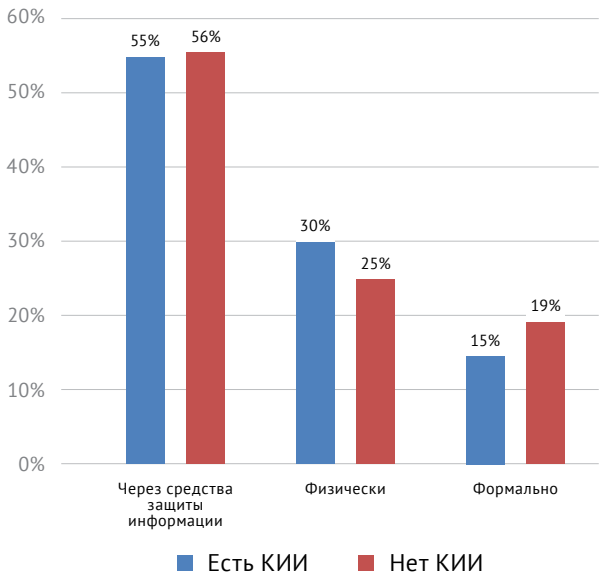


Рисунок 13. Как реализовано разделение сетей

Примечание: формально через общие коммутаторы и т. п.

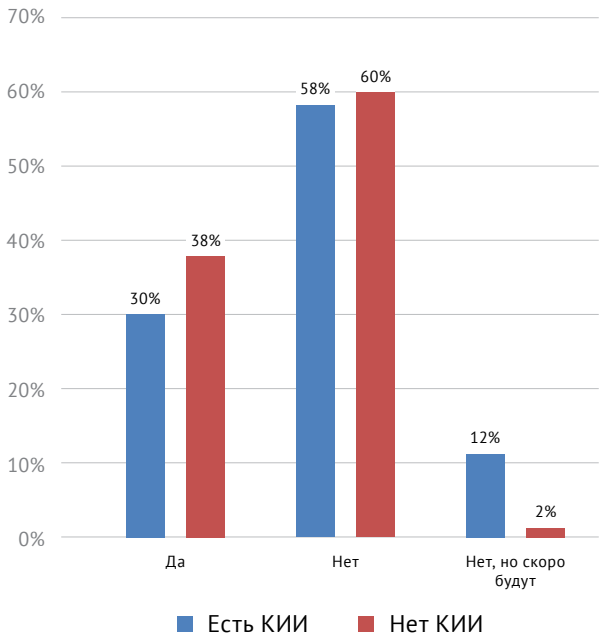


Рисунок 14. Наличие IIoT в промышленной сети организации

Владельцы объектов КИИ проявляют больший интерес к IIoT, внедрить его собираются 12%, после чего, исходя из ответов респондентов, показатели наличия КИИ как у субъектов КИИ, так и у организаций, не являющихся ими, уравняются – 42% и 40% соответственно.

Далее рассмотрены вопросы обеспечения кибербезопасности АСУ, вне зависимости от того, является система объектом КИИ или нет. Таким образом, отражена разница между ответами специалистов по ИБ и АСУ (АСУ ТП).

Ключевые меры защиты рабочих станций после ухода западных вендоров

В текущих условиях, когда западные вендоры отказались от поддержки АСУ и многих других систем, организации внедрили или собираются внедрить для защиты рабочих станций (рис. 15).

Респонденты назвали ключевыми мерами:

- антивирусная защита (18%);
- контроль подключаемых устройств (16%);
- журналирование и передача логов в отдел ИБ (13%)
- контроль целостности (13%).

Некоторые прокомментировали, что их организация собирается внедрить «много» мер по защите, а также был комментарий: *«Максимальное количество бизнес-процессов перенести на серверы, минимизировать обработку важной информации на клиентах».*

Из типов компонентов систем управления, наиболее подверженных риску компрометации, западные исследователи называют инженерные станции (рабочие места). Например, об этом говорит исследование The State of ICS/OT Cybersecurity in 2022 and Beyond компании SANS. Риск компрометации инженерной рабочей станции специалисты ставят на первое место – так ответили почти 54% опрошенных компанией. Следом идут рабочие станции операторов на различных ОС (Windows, Linux, Unix) – 43%. Среди подверженных компрометации компонентов были названы удалённый доступ (VPN), подключение к корпоративным сетям, серверы, а также системы контроля и управления доступа.

Ответы специалистов ИБ и АСУ распределились следующим образом (рис. 16, 17).

Рисунок 15. Ключевые меры защиты рабочих станций после ухода западных вендоров. Вся выборка

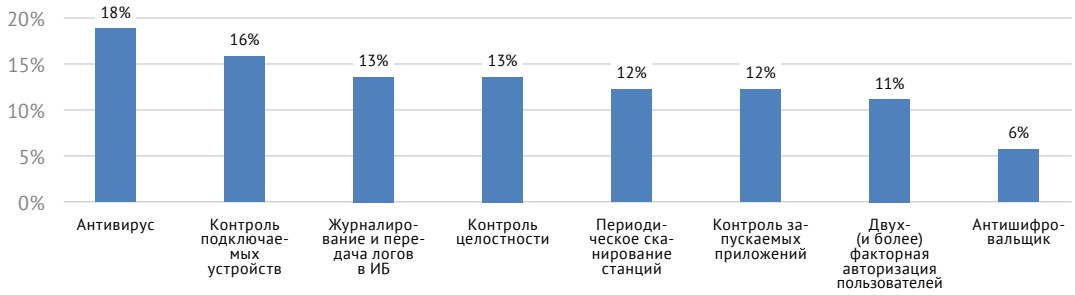


Рисунок 16. Ключевые меры защиты рабочих станций после ухода западных вендоров. Ответы специалистов ИБ

Рисунок 17. Ключевые меры защиты рабочих станций после ухода западных вендоров. Ответы специалистов АСУ

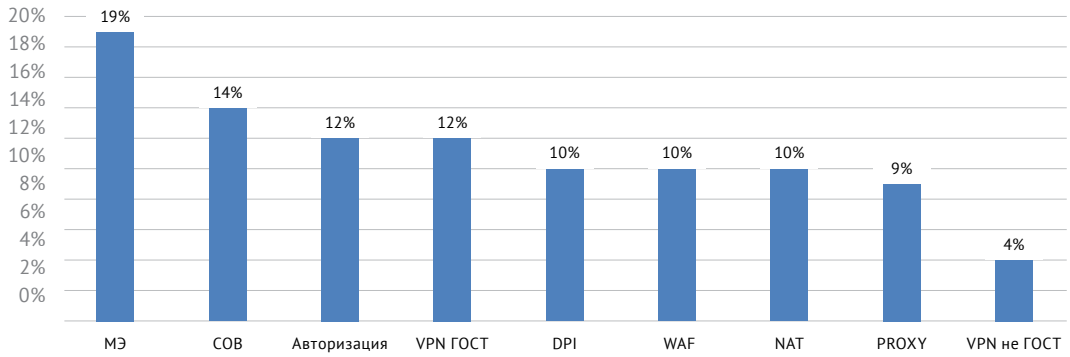


Рисунок 18. Ключевые меры защиты промышленной сети. Ответы специалистов ИБ

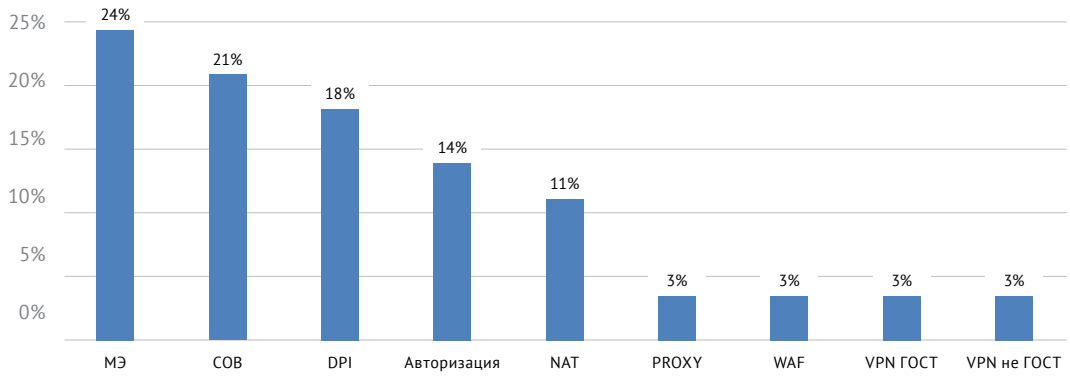


Рисунок 19. Ключевые меры защиты промышленной сети. Ответы специалистов АСУ

Приоритеты специалистов ИБ и АСУ показали некоторые различия. Для обеих групп приоритетной мерой является антивирусная защита и контроль подключаемых устройств. Однако если периодическое сканирование рабочих станций для специалистов АСУ и контроль запускаемых приложений так же важны, то для специалистов ИБ эта мера приоритетна в меньшей степени (12%).

Обе группы, как и в разрезе объектов КИИ, показали наименьший интерес к использованию антишифровальщиков и многофакторной аутентификации.

Стоит отметить, что, например, Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) в своих рекомендациях неоднократно отмечает угрозы вирусов-шифровальщиков, способных нанести организации крупный ущерб, и таким образом, именно «антишифровальщики» и настройка многофакторной аутентификации – одни из основных мер для обеспечения кибербезопасности АСУ ТП в США.

«Лаборатория Касперского» в отчёте о кибербугрозах для АСУ на 2023 отмечает рост количества хактивистов и добровольцев, в том числе внутри компаний. Таким образом, **будет высока роль как многофакторной аутентификации, так и поведенческого анализа.**

Примечание: реализуются такие меры, как правило, с применением DCAP/DLP-систем.

В зарубежных отчётах также высоко оценивают угрозы вирусов-шифровальщиков. Например, в отчёте Insights Into ICS/OT Cybersecurity 2022 компании TXOne Networks пишут о развитии атак подобного типа, поскольку шифровальщики уже предлагают в качестве услуги.

По оценке компании Dragos (в отчёте ICS/OT cybersecurity year in review 2022), по итогам 2022 года количество кибератак с помощью вирусов-вымогателей выросло на 87% по сравнению с 2021 годом, а 78% атак было направлено на производство. Металлургия, автомобильная промышленность, электроника и полупроводниковая промышленность – эти отрасли стали наиболее подверженными атакам с помощью вирусов-вымогателей.

По данным отчёта «2022 OT Cybersecurity Survey Report» компании Otorio по итогам II полугодия 2022, самые атакуемые секторы – это критический производственный сектор и электроэнергетика.

Ключевые меры защиты промышленной сети

По всем выборкам самой необходимой функцией защиты промышленной сети считают **межсетевой экран и СОВ** (система обнаружения вторжений, IDS).

Далее мнения групп разделяются. Специалисты АСУ, помимо вышеуказанных функций, отдают предпочтения DPI, авторизации и NAT и в последнюю очередь ориентируются на VPN и на PROXY с WAF. Подробнее на рисунках ниже (рис. 18, 19).

По этому вопросу один из респондентов подчеркнул, что IDS уже недостаточен, и для его организации важен функционал IPS (нефтегазовая отрасль).

Обращаясь к зарубежным исследованиям, эксперты говорят: *«Традиционные системы управления небезопасны и требуют реализации других мер, таких как брандмауэры (МЭ), воздушные зазоры и другие формы защиты. Новые решения для промышленной безопасности позволяют управлять промышленными системами управления с точки зрения кибербезопасности, как и всеми другими ИТ-устройствами в сети. Что делает эти новые системы уникальными, так это встроенные функции, такие как двойные сетевые интерфейсы для разделе-*

ния доверенных и ненадёжных сетей, полностью настраиваемый брандмауэр, встроенный VPN-клиент, параметры защищённой передачи данных, такие как MQTT, управление учётными записями пользователей и сертификаты безопасности». Как видно из рисунков выше, **наши специалисты также указывают в применяемых мерах межсетевые экраны, разделение сетей, VPN.**

Соответствие средств защиты информации официальным требованиям

Более 70% специалистов обеих категорий считают, что средства защиты информации на предприятии должны соответствовать официальным требованиям (например, ТУ от вендора, требованиям от ФСТЭК России, ФСБ России). При этом специалисты АСУ более единогласны в этом мнении – так ответили 84%.

По данному вопросу тоже был комментарий, что сертифицированные СЗИ обязательны для объектов, обрабатывающих сведения, составляющих государственную тайну, в остальных случаях всё зависит о категории объекта КИИ.

Подробнее представлено на рисунках ниже.

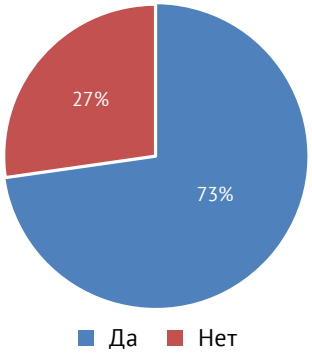


Рисунок 20. Необходимо ли, чтобы СЗИ соответствовали официальным требованиям. Ответы специалистов ИБ.

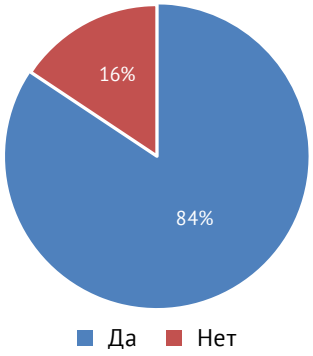


Рисунок 21. Необходимо ли, чтобы СЗИ соответствовали официальным требованиям. Ответы специалистов АСУ.

Отношение к установке только тех СЗИ, которые согласованы с производителем АСУ

Для специалистов АСУ более принципиальной, чем выбор сертифицированных средств, является установка СЗИ, рекомендованных и согласованных с производителем или поставщиком,– так считает подавляющее большинство – 91%. Что неудивительно, так как именно специалисты АСУ отвечают за непрерывность функционирования систем и критически относятся к появлению дополнительных средств, которые могут нарушить функционирование. **Решением проблемы может являться оценка соответствия СЗИ (в том числе совместимости с АСУ) в ходе пилотных проектов на этапе выбора СЗИ (на этапе проектирования).**

Среди специалистов ИБ этот показатель гораздо ниже, но всё ещё составляет более половины (62%). 38% считают, что необязательно устанавливать только СЗИ, рекомендованные разработчиками (поставщиками) систем, в том числе АСУ.

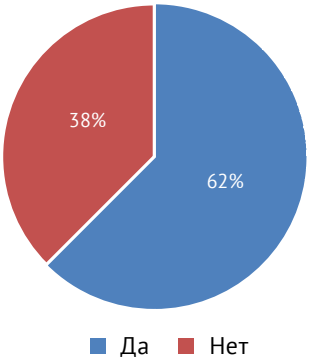


Рисунок 22. Необходима ли установка только СЗИ, рекомендованных производителем АСУ. Ответы специалистов ИБ.

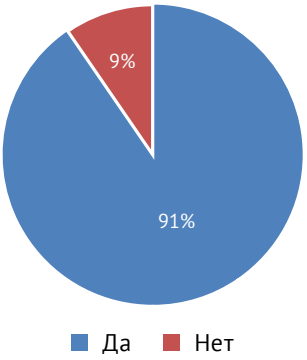


Рисунок 23. Необходима ли установка только СЗИ, рекомендованных производителем АСУ. Ответы специалистов АСУ.

Какие операционные системы преобладают сейчас и будут преобладать через 3 года

Ожидаемо, что на текущий момент большинство организаций продолжает использование ОС Windows (64%), на российских операционных системах работает только 23%, 10% используют Linux и 3% – RTOS (операционные системы реального времени) (рис. 24).

По прогнозам опрошенных специалистов, через 3 года картина поменяется на противоположную, и большинство организаций (62%) планирует продолжить или начать использовать российские ОС.

Но 19% при этом отметили, что даже в перспективе 3 года не смогут перейти с ОС Windows. Так ответили в основном представители крупных компаний из оборонного комплекса, сектора нефти и газа (по комментариям – применительно к АСУ). Аналогичный ответ встретился у представителей некоторых организаций из электроэнергетики и металлургии.

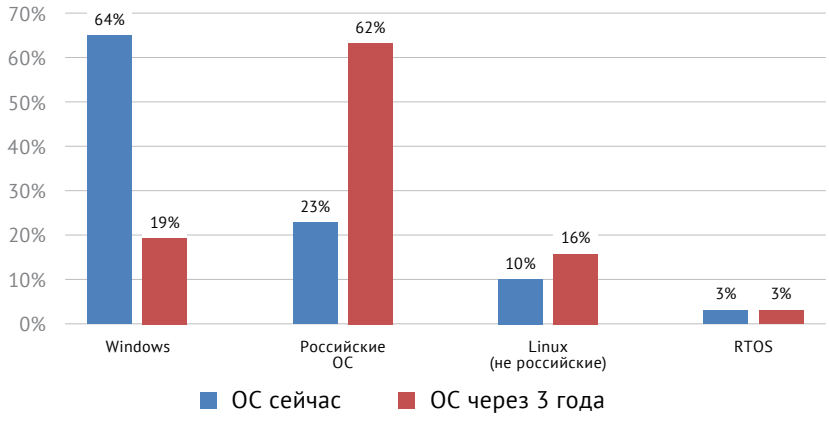


Рисунок 24. Какие ОС преобладают на рабочих станциях сейчас и какие будут преобладать через 3 года. Вся выборка.

Как видно на рисунке ниже, тенденции в ответах специалистов ИБ сохраняются (рис. 25, 26).

По группе АСУ видно: 91% специалистов ответили, что в данный момент работают на Windows, и в **перспективе на 3 года 33% прогнозируют, что на их предприятиях Windows сохранится** (против 20% по мнению специалистов ИБ).

Соответственно, и мнения по поводу перехода на российские ОС менее положительные: **только 50% специалистов АСУ считает, что через 3 года они смогут перейти на российские ОС** (против 66% у специалистов ИБ). При этом по данному вопросу были комментарии, что в организации выберут ту систему, с которой можно будет продолжать работу на уровне, аналогичном решений для Windows.

В целом можно сказать, что специалисты АСУ более скептически относятся к импортозамещению ОС в сфере АСУ (АСУ ТП): половина считает, что даже через 3 года будут преобладать иностранные ОС.

Если посмотреть на мнения зарубежных экспертов, то они отмечают, что ОС с открытым исходным кодом во многих отношениях более безопасна, чем закрытая. Эти продукты могут включать только те компоненты операционной системы, которые необходимы для их целей, что снижает количество векторов атак.

Такая же задача стоит и перед нашими специалистами – переходить на российские ОС, которые, в основном, создаются на базе Linux.

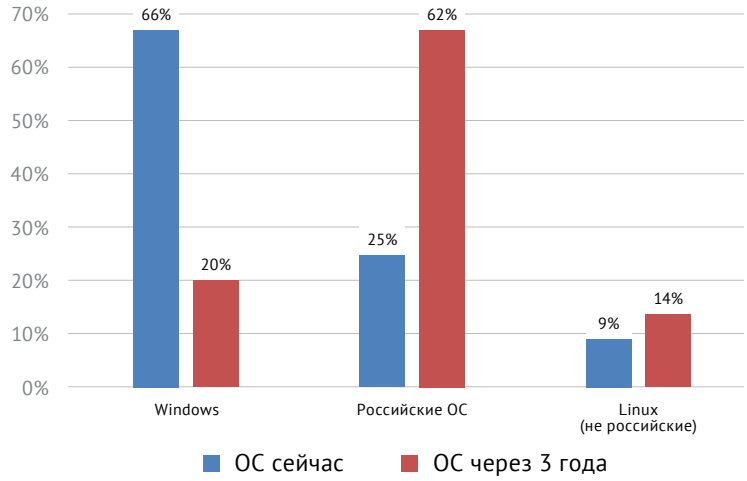


Рисунок 25. Какие ОС преобладают на рабочих станциях сейчас и какие будут преобладать через 3 года. Ответы специалистов ИБ.

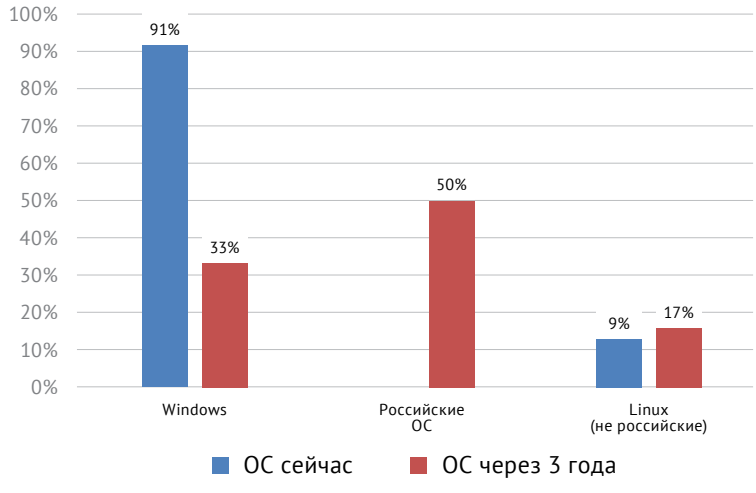


Рисунок 26. Какие ОС преобладают на рабочих станциях сейчас и какие будут преобладать через 3 года. Ответы специалистов АСУ.

Разделение корпоративной и промышленной сетей

Почти 80% специалистов отметили, что на их предприятиях промышленная и корпоративная сети разделены.

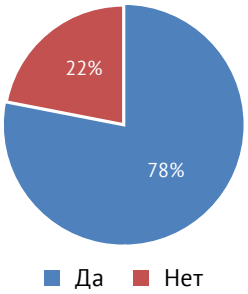


Рисунок 27. Разделены ли промышленные и корпоративные сети в организации. Вся выборка

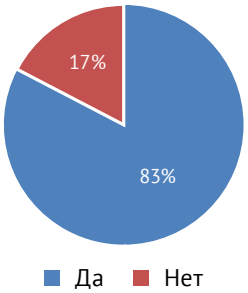


Рисунок 28. Разделены ли промышленные и корпоративные сети в организации. Ответы специалистов ИБ

При этом у специалистов АСУ данное мнение единогласное – 100%.

Корпоративные и промышленные сети не разделены в основном в малых и средних организациях.

Способы разделения промышленной и корпоративной сетей

По всем категориям ответов разделение сетей реализовано преимущественно через средства защиты информации (межсетевые экраны, инфодиоды и др.): 55% по всей выборке, у 27% разделение физическое, 18% реализовано только формально. Подробнее на рисунках ниже.

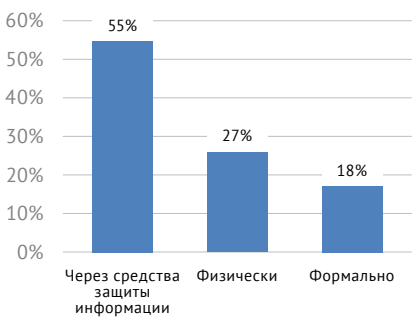


Рисунок 29. Как реализовано разделение промышленной и корпоративной сети. Вся выборка

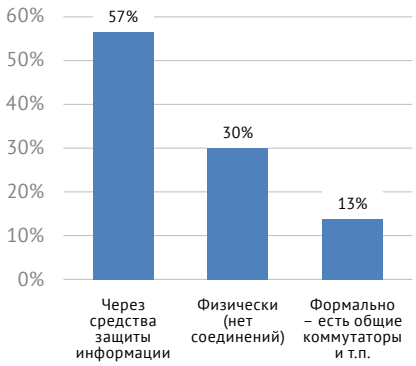


Рисунок 30. Как реализовано разделение промышленной и корпоративной сети. Ответы специалистов ИБ

Рисунок 31. Как реализовано разделение промышленной и корпоративной сети. Ответы специалистов АСУ

Ответы специалистов ИБ в целом совпадают с общей выборкой.

Исходя из ответов специалистов АСУ, на их предприятиях наибольший процент разделения сетей реализуется посредством СЗИ (73% против 57% у ИБ), в отличие от физического разделения, которое в их ответах составляет 18%, в то время как по общей выборке и ответам специалистов ИБ этот процент достигает 27–30%. Из опыта и других исследований можно отметить, что **соединение сетей через СЗИ часто встречается на тех предприятиях, где внедрено вертикальное управление производственной цепочкой в режиме реального времени и данные из АСУ ТП должны поступать непосредственно в MES-системы, из них – в ERP.**

Industrial Ethernet Book Media в отчёте «Industrial Cybersecurity 2022 Special Report» эксперты отмечают: *«Сегментация – хорошая стратегия предотвращения распространения инцидентов и снижения рисков. Однако это не решает насущных проблем».*

В том же отчёте пишут, что *«промышленная кибербезопасность в системах автоматизации концентрировалась на обмене данными между контроллерами и использовании выделенных шлюзов IT/OT, при этом системы были сегментированы на взаимосвязанные зоны. Сегодня интеграторы в первую очередь обеспечивают безопасность интерфейсов этих зон. Эти сегменты обычно включают в себя OT- сети, и их взаимодействие между устройствами, как правило, не защищено. Интеграторы устанавливают брандмауэры и строгий локальный контроль доступа для повышения безопасности в этом пространстве».*

Наличие IIoT и перспективы

У трети предприятий в периметрах промышленной сети есть устройства промышленного Интернета вещей (IIoT). У 2/3 предприятий IIoT пока отсутствуют – по всем выборкам показатель колеблется от 59 до 64%. При этом 8% рассматривают появление данной технологии в ближайшей перспективе.

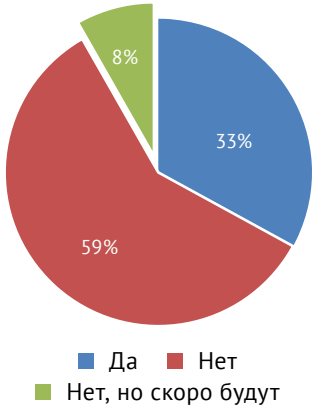


Рисунок 32. Есть ли в периметре промышленной сети IIoT. Вся выборка

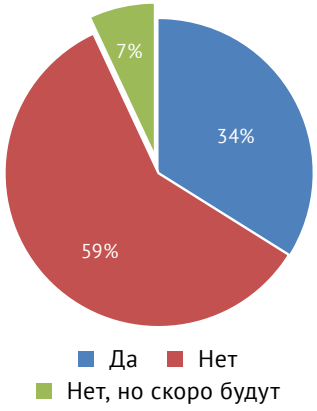


Рисунок 33. Есть ли в периметре промышленной сети IIoT. Ответы специалистов ИБ

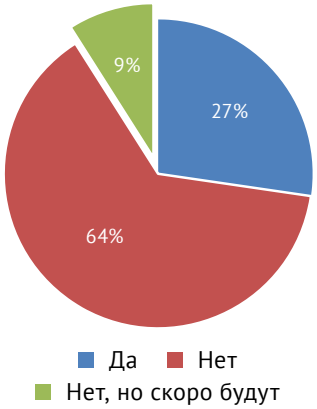


Рисунок 34. Есть ли в периметре промышленной сети IIoT. Ответы специалистов АСУ

По ответам специалистов АСУ, в их организациях наименьший процент использования IIoT в промышленных сетях (27%), но при этом в этой группе самый высокий процент, тех, кто собирается внедрять подобную систему – 9%.

В отчёте «Industrial Cybersecurity 2022 Special Report» отмечают, что *«тенденции промышленной кибербезопасности сосредоточены на потребностях, создаваемых конвергенцией ИТ и ОТ, требованиях к приложениям IoT и расширениях безопасности для полевых устройств».* **Ответы, что на российских предприятиях, в т. ч. субъектах КИИ, будут внедрять IIoT, говорит как о следовании общей тенденции на конвергенцию, так и о том, что необходимо создавать новые модели угроз, учить СЗИ работать с новыми протоколами. Объектами угроз станут все три уровня АСУ, начиная с «умных датчиков».**

«Одним из примеров является EtherNet/IP CIP Security, в котором используется проверенная технология SSL/TLS и лежащие в её основе методы для защиты связи Ethernet в режиме реального времени на основе IP. Он использует те же криптографические алгоритмы, что и Advanced Encryption Standard (AES), Rivest- Shamir-Adleman (RSA) или Diffie-Hellmann Elliptic Curve Cryptography (ECC), которые уже применяются в ИТ-системах. Это похоже на безопасность PROFINET и другие промышленные стандарты связи на базе Ethernet».

Таким образом, в случае внедрения IIoT от западных производи-

телей, которые являются лидерами как технологий, так и рынков, мы получим реализацию функций защиты информации на базе западных алгоритмов (VPN-не-ГОСТ в опросе), доверять которым не сможем как минимум при обеспечении бесперебойной работы объектов КИИ. Если на уровне умных датчиков добавлять VPN-ГОСТ, то это значительно удорожит систему, хотя первые продукты на российском рынке уже есть.

Ориентируясь на результаты опроса, специалисты АСУ, например, среди ключевых мер защиты для промышленных сетей ориентируются на VPN в последнюю очередь (независимо от того, ГОСТ он или нет). При этом для специалистов ИБ это 3-я по популярности мера (VPN ГОСТ).

Западные эксперты также говорят, что *«тенденция к промышленному Интернету вещей, цифровой трансформации и Индустрии 4.0 является ключевой движущей силой новых решений для промышленной кибербезопасности. Перспектива IIoT заключается в том, что данные являются активом предприятия»*.

Таким образом, нашим специалистам в рамках обеспечения национальной технологической безопасности необходимо уже сейчас готовиться к обеспечению безопасности IIoT, создавать собственные системы IIoT и СЗИ для них.

Отношение к решениям класса пассивного анализа зеркалированного трафика для защиты промышленной сети

Ответы как из общей выборки, так и специалистов ИБ, показали, что пассивного анализа зеркалированного трафика недостаточно для защиты технологической сети,– так считают больше половины опрошенных (65%). Мнение специалистов АСУ отличается: 55% респондентов считают, что пассивного анализа для обеспечения безопасности технологической сети достаточно. Подробнее на рисунках 35, 36.

Один из респондентов отметил, что такой меры достаточно только для объектов КИИ третьей категории значимости.

Какие пропускные способности промышленной сети минимально необходимы при всех включённых модулях?

Большая часть респондентов из всей выборки **(40%) отметили, что пропускной способности до 1 Гб/с достаточно. Для специалистов АСУ данный показатель достиг 70%** (рис. 37, 38, 39).

Один из специалистов отрасли электроэнергетики прокомменти-

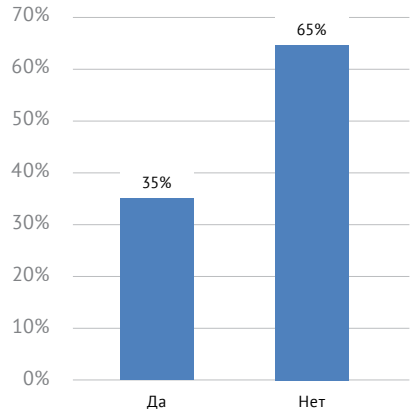


Рисунок 35. Достаточно ли пассивного анализа зеркалированного трафика для защиты сети. Ответы специалистов ИБ

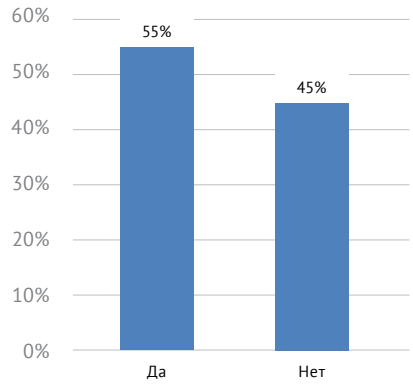


Рисунок 36. Достаточно ли пассивного анализа зеркалированного трафика для защиты сети. Ответы специалистов АСУ

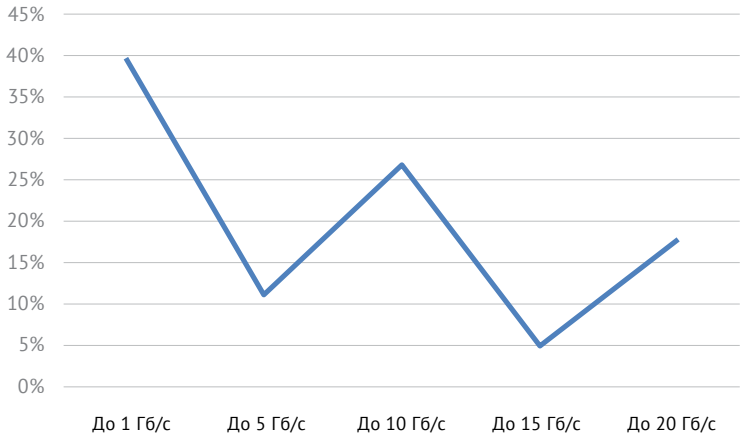


Рисунок 37. Какая пропускная способность минимально необходима для промышленной сети. Вся выборка

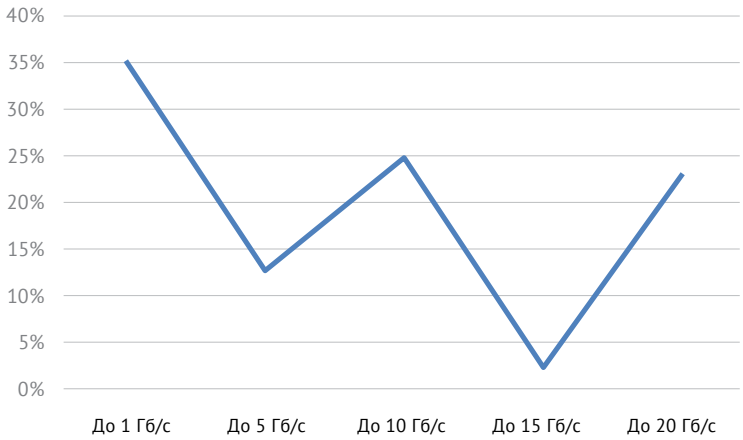


Рисунок 38. Какая пропускная способность минимально необходима для промышленной сети. Ответы специалистов ИБ

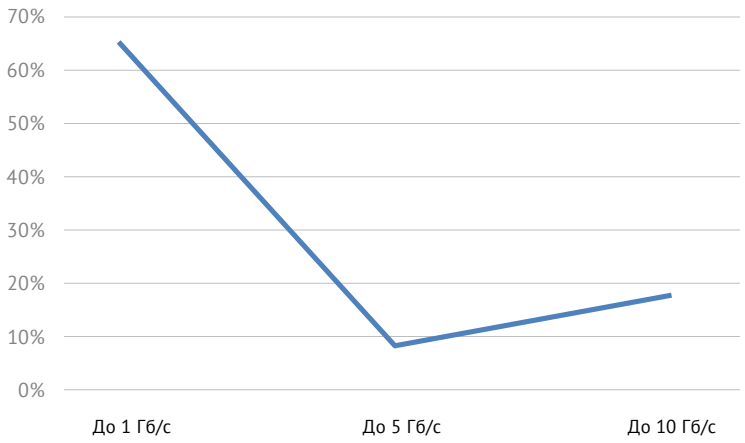


Рисунок 39. Какая пропускная способность минимально необходима для промышленной сети. Ответы специалистов АСУ

ровал свой выбор: *«100 Мбит/с для одной сети. До 4-х подсетей на объекте. До 50 объектов. Зависит от архитектуры сбора»*.

Заключение и выводы

В ходе исследования мы увидели, в чём разница и сходство в подходах к обеспечению безопасности у групп организаций в зависимости от наличия или отсутствия объектов КИИ, а также разницу и сходство между мнениями специалистов АСУ и ИБ.

Для большинства организаций-владельцев объектов КИИ характерна реализация различных комплексов мер безопасности для объектов КИИ и систем, к ним не относящимся: так считают 84% организаций. Одинаковые меры защиты всех категорий объектов применяются в основном в малых и средних компаниях.

Для владельцев объектов КИИ приоритетными мерами защиты рабочих станций являются антивирусная защита, журналирование и передача логов в отдел ИБ и многофакторная аутентификация. Для организаций, которые не владеют КИИ, также имеют значение антивирусная защита и журналирование, но на третьем месте находится сканирование рабочих станций. Для групп в разрезе специалистов ИБ и АСУ приоритетной мерой является антивирусная защита и контроль подключаемых устройств. Но если периодическое сканирование рабочих станций для специалистов АСУ и контроль запускаемых приложений одинаково важны, то для специалистов ИБ эта мера приоритетна в меньшей степени.

В отношении мер по защите промышленных сетей для владельцев КИИ приоритетно значение межсетевого экрана и системы обнаружения вторжений. Для организаций, которые не владеют КИИ, основной мерой также считают межсетевой экран. Как и владельцы КИИ, специалисты ИБ и АСУ считают межсетевой экран и СОВ самой необходимой функцией защиты промышленной сети.

Для организаций-владельцев объектов КИИ в большей степени имеет значение установка СЗИ, соответствующих официальным требованиям, что объясняется требованиями НПА и ОРД, регулирующих безопасность КИИ.

И организации-владельцы объектов КИИ, и не владельцы в большинстве случаев считают, что необходимо устанавливать СЗИ, рекомендованные производителем АСУ. Для специалистов АСУ более принципиальной, чем выбор сертифицированных средств, стала установка СЗИ, рекомендованных и согласованных с производителем или поставщиком АСУ. Это неудивительно, так как именно специалисты АСУ отвечают за непрерывность функционирования систем и критически относятся к появлению дополнительных средств, которые могут нарушить их функционирование. Решением проблемы может являться оценка соответствия СЗИ (в том числе совместимости с АСУ) в ходе пилотных проектов на этапе выбора СЗИ (на этапе проектирования).

В ходе исследования выявлены различные мнения о перспективах перехода на российские операционные системы. Специалисты АСУ более скептически относятся к импортозамещению ОС в сфере АСУ – половина считает, что даже через 3 года переход на российские ОС для них неосуществим.

Владельцы объектов КИИ проявляют больший интерес к внедрению IIoT. Ответы, что на российских предприятиях, в т. ч. субъектах КИИ, планируется внедрять IIoT, говорят как об следовании общей тенденции на конвергенцию ИТ/ОТ, так и о том, что необходимо создавать новые модели угроз, «учить» СЗИ работать с новыми протоколами, а объектами угроз станут все три уровня АСУ, начиная с «умных датчиков» («умных исполнительных устройств»). Таким образом, нашим специалистам в рамках обеспечения национальной технологической безопасности необходимо уже сейчас готовиться к обеспечению безопасности IIoT, создавать собственные системы IIoT и СЗИ для них.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчёты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

#PAYMENTSECURITY

VII международная конференция по безопасности платежей

Завершилась VII международная конференция по безопасности платежей #PAYMENTSECURITY!

13–14 июля прошла ежегодная конференция, посвящённая безопасности платежей #PAYMENTSECURITY. Конференция состояла из нескольких сессий:

- доклады экспертов информационной безопасности;
- практический воркшоп Practical Security Village от команды пентестеров Deiteriy Lab;
- авторский семинар PCI DSS Training по новой версии стандарта 4.0.

В этом году конференция прошла в традиционном очном формате, поэтому гости и участники могли лично обсудить насущные вопросы, подискутировать на важные темы информационной безопасности и пообщаться с коллегами по цеху.

Мероприятие получилось масштабным: всего конференцию посетило более 200 участников и 20 спикеров, которые были отобраны независимым программным комитетом.

- Первый день был насыщенным и состоял из докладов на темы из разных областей информационной безопасности.

Юрий Николаевич Лысенко, представитель Центрального Банка РФ, рассказал о ситуации с обеспечением информационной безопасности и киберустойчивости финансовой сферы.

Алексей Лукацкий из компании Positive Technologies объяснил, какие технологии и методики можно использовать для оценки реальной защищённости платёжной инфраструктуры.

Мона Архипова, независимый эксперт по информационной безопасности, поделилась мнением о том, кто же такой vCISO.

Виктория Гадалова, QSA-аудитор компании Deiteriy, пояснила принципиальную разницу между PCI DSS v. 4.0 и PCI DSS v. 3.2.1.

Александр Иванцов, эксперт компании Deiteriy, уделил внимание русской регуляторике, в частности ГОСТ Р 57580.

Владимир Ковалёв, QSA-аудитор компании Deiteriy, рассказал о методах хеширования с секретом.

Также было множество интереснейших докладов, записи которых мы скоро разместим на сайте: www.paymentsecurity.ru.

- В кулуарах проходили интересные дискуссии. Гости и участники конференции обсуждали прослушанные доклады, высказывали своё экспертное мнение и находили истину в жарких рассуждениях.
- После продуктивного дня гостей конференции ждала вечерняя программа, где музыканты исполнили знакомые и любимые всеми композиции. Участники могли отдохнуть и насладиться приятной компанией коллег.
- Во второй день конференции Сергей Шустиков, QSA-аудитор и генеральный директор компании Deiteriy, провёл авторский семинар PCI DSS Training, где рассказал об интересных кейсах и проблемах, с которыми сталкивались и могут столкнуться компании. Сергей объяснил и разложил по полочкам новые требования PCI DSS v. 4.0, а также ответил на вопросы заинтересованной публики.
- 13 и 14 июля параллельно с докладами и PCI DSS Training проходил воркшоп по практической информационной безопасности Practical Security Village от команды пентестеров Deiteriy Lab.

Пентестеры подготовили интересные задания, основанные на поиске и эксплуатации актуальных уязвимостей мобильных и веб-приложений, а также внутренних сервисов. Для решения некоторых заданий нужно было попрактиковаться в локпикинге и вспомнить навыки игры в Mortal Kombat.

Участники, выполнившие определённое количество заданий, получали доступ к управлению макетом маяка.

Уважаемые гости и участники конференции, мы благодарим вас за активность и заинтересованность! Будем рады видеть вас в следующем году!

---

www.paymentsecurity.ru

Positive Hack Days 12

Доверие к технологиям невозможно без гарантий защищённости, которая может быть достигнута за счёт объединения экспертного комьюнити

В Парке Горького завершился 12-й Positive Hack Days, организованный компанией Positive Technologies, лидером в области результативной кибербезопасности.

В этом году мероприятие вышло на новый уровень, превратившись в большой городской киберфестиваль. Его ключевыми идеями стали повышение доверия к технологиям и развитие осознанности их использования через киберграмотность. Интерес широкого круга пользователей, представителей бизнеса, государства и СМИ к мероприятию лишний раз подчёркивает, что информационная безопасность сегодня касается каждого.

Гости открытого пространства киберфестиваля – кибергорода узнали, как не стать жертвами мошенников на маркетплейсах, а также об особенностях ChatGPT, выборе безопасного VPN и других аспектах ИТ и ИБ. В рамках конференционной части киберфестиваля эксперты обсудили переход госорганов и частных компаний к результативной безопасности, стратегию объединения комьюнити, методы безопасной разработки, развитие рынка багбаунти. Подошла к концу **кибербитва Standoff**: за четыре дня атакующим в вымышленном Государстве F (но с настоящими системами управления и защиты) удалось реализовать недопустимые события 204 раза, а защитникам – расследовать 43 атаки. Если специалистам по кибербезопасности, участвовавшим в битве, придётся встретиться с аналогичной активностью злоумышленников в своих компаниях, они будут готовы эффективно реагировать на неё.

Гарантированная защита как результат: кто за это в ответе

Тема результативной кибербезопасности осталась ключевой и для конференционной части второго дня.

Владимир Бенгин, директор департамента кибербезопасности Минцифры России, удивился полному залу субботним утром. Он напомнил, что специалистам по ИБ в любом случае приходится отвечать непосредственно за результат. *«Мы ждали, что бизнес нас услышит,– вот он и услышал. Компаниям всё равно, какие средства защиты внедрены: им важны результат и понимание того, кто за него отвечает. К сожалению, безопасники до сих пор очень часто не могут объяснить, каким он будет. Внедрение некоей популярной системы защиты – это не результат. Нормальный результат – это когда специалист по безопасности сообщает руководству о том, что конкретно сегодня уязвимости в компании устраняются, скажем, в течение 127 дней, и это слишком рискованно: надо, чтобы в критически значимых сегментах они устранялись за 12 часов, а для этого необходимо столько-то миллионов рублей»*,– признал Владимир Бенгин.

Айдар Гузаиров, генеральный директор Innostage (компании – соорганизатора Positive Hack Days 12), заявил, что изменения за последний год в отношении целеполагания, осознанности и всего того, что творится в кибербезе, сравнимы с пятилетним периодом в более спокойные времена. *«Два года назад на PHDays мы говорили о том, что было бы здорово, если бы руководители задумались об информационной безопасности. Бойтесь своих желаний: многие менеджеры лично узнали, что такое ИБ. С другой стороны, сейчас в отрасли кибербезопасности иначе воспринимается ответственность за результат. Если два года назад я мог назвать нашу компанию только интегратором, то сейчас мы значительно больше, чем интегратор, и отвечаем за результат,*

за то, чтобы хакеры не угрожали бизнесу наших клиентов. Для нас это в первую очередь репутационные риски. Мы начинаем размышлять, как по-другому, более эффективно, можно добиться результата в области ИБ»,– подчеркнул Айдар Гузаиров.

Сергей Шерстобитов, генеральный директор Angara Security, согласился с тезисом, что российская кибербезопасность прошла пятилетку за год, отметив, что главными бенефициарами нынешнего окна возможностей становятся отечественные разработчики. *«Появляется много интересных продуктов. Клиенты пошли в сторону сервисов. Если ранее мы только рассказывали, что услуги в области ИБ могут дать большой результат в понятные сроки, то сейчас сервисы становятся востребованными практически по всем направлениям. Единственное исключение – услуги страхования, которые почему-то не взлетают»*,– сказал Сергей Шерстобитов.

«Основное изменение последнего года – новое отношение собственников к вопросам ИБ,– заметил Павел Куликов, СТО «СДЭК».– *Взломали очень много организаций, в результате чего многие перешли от парадигмы «ИБ – это постоянное совершенствование и обучение» к вопросу о конкретных результатах. Наличие на российском рынке компаний, позволяющих получить результат сразу, а не по прошествии полугода или года,– это очень хорошо. Когда перед нами встала задача по защите электронной почты, мы за три дня подключились к сервису, тогда как сами, по первоначальной оценке, готовились бы к таким работам 3,5 месяца. Но в текущих условиях этого времени нет. И от вечной непрерывности мы переходим к конкретике».*

О багбаунти как элементе результативной безопасности

Невозможно говорить о результативной кибербезопасности без осознанного использования программ багбаунти: об этом в течение прошлого года не говорили разве что из утюга (хотя разместить умный утюг на платформе багбаунти вполне реально). О том, каких конкретных результатов удаётся достичь, используя такие программы, подискутировали в рамках деловой части киберфестиваля.

Владимир Бенгин, директор департамента кибербезопасности Минцифры, отметил: *«Багбаунти – это суперкрутой стресс-тест огромного числа внутренних процессов вашей организации. Мы запустили программу сразу на двух коммерческих площадках– Standoff 365 и BI. ZONE Bug Bounty. В целом мы были уверены в защищённости Госуслуг, потому что пентест наших систем проводила практически каждая российская компания в сфере ИБ. Всего в багбаунти участвовали около 8 тысяч человек. На обеих площадках сданы сотни отчётов, результатом стало больше 30 подтверждённых уязвимостей. Найдены и критически опасные недостатки, максимальная выплата составила 350 тыс. рублей. В дальнейшем будем думать, как этот опыт масштабировать. Для компании или организации в смысле проверки защищённости нет ничего дешевле и эффективнее багбаунти».*

По словам Александра Хамитова, руководителя направления безопасности приложений Wildberries, комьюнити, участвующее в багбаунти, может не только заниматься проверкой на уязвимости, но и подкидывать интересные идеи. *«Нам встречались неожиданные предложения организовать тестирование чуть ли не из конкретного пункта выдачи заказов»*,– рассказал Александр Хамитов.

При этом многие организации пока всё же не торопятся запускать багбаунти. *«Некоторые специалисты по ИБ могут полагать, что и так знают уязвимости в системах своей компании, поэтому откладывают проверки на багбаунти-платформах. В других организациях могут думать, что если запустить программу, то придётся признать, что бреши в защите есть. Руководство может относиться к уязвимостям как к недоработке в отделе безопасности и принимать разные меры. Вероятно, существует и необоснованное опасение, что багбаунти может использоваться чёрными хакерами. На самом деле ситуация обратная: программа позволяет монетизировать уязвимости в правовом поле, чтобы люди не пытались продать информацию о них где-то в даркнете. Моё мнение таково, что в багбаунти надо обязательно участвовать»*,– отметил Дмитрий Гадарь вице-президент, директор департамента информационной безопасности АО «Тинькофф Банк».

Илья Сафронов, директор департамента защиты инфраструктуры ИБ VK, согласился с коллегой: *«Мы зрелая ИТ-компания, поэтому у нас не было страхов по поводу участия в багбаунти на платформе Standoff 365. Конечно, это не всегда приятно, когда вроде бы всё проверил в плане уязвимостей, а тебе принесли ещё в рамках программы. Но если в компании три релиза в день, то невозможно сразу же всё проверить на 100%, поэтому багбаунти очень помогает».*

Эксперты отметили, что багбаунти – это непрерывный процесс, что является основным его преимуществом, например перед пентестом. Результаты тестирования на проникновение устаревают в тот же день, когда оно заканчивается: инфраструктура меняется, появляются новые бреши в защите, есть теневые ИТ, о которых компания не знает. Багбаунти позволяет платить за результат в виде уязвимостей, а не за услугу, при этом является не серебряной пулей, а только одним из кубиков проверки защищённости. *«Неизвестно, что происходит внутри инфраструктуры, необязательно, что все уязвимости обнаружат в рамках багбаунти. Здесь нужен SOC. У нас, кстати, каждый найденный недостаток проверяется: почему WAF не отработали, почему команда AppSec на первых этапах не обнаружила эту уязвимость инструментально и т. д. Мы рассматриваем всю цепочку и стараемся исключить появление брешей в защите в дальнейшем»*,– пояснил Дмитрий Гадарь.

Комьюнити и методология результативной ИБ

Ещё одна тема, которую не обошли стороной в программе киберфестиваля,– роль сообщества в формировании подходов результативной защиты: была представлена платформа, на которой комьюнити может собирать фреймворки по построению результативной безопасности. Открытое сообщество rezbez.ru создано для экспертов в области ИБ, позволяет обмениваться знаниями и опытом и ориентировано на достижение практического результата. Чтобы обеспечить высокий уровень киберустойчивости, предлагается комплексный подход, в основе которого лежат 10 доменов по разным направлениям ИБ. Реализация шагов и практик, предложенных в каж-

дом из доменов, не только поможет соблюсти требования регуляторов, но и позволит бизнесу уверенно развиваться в цифровом пространстве. Сайт в ближайшие дни будет пополнен методиками и рекомендациями, шаблонами и примерами, чек-листами и другими полезными материалами.

Участники дискуссии согласились, что подобная платформа необходима сообществу, а вендорам следует взять на себя ответственность за создание и развитие таких площадок. При этом для привлечения экспертов важно обеспечить прозрачность их работы с точки зрения прав интеллектуальной собственности, а на первом этапе, вероятно, понадобится и финансовое поощрение.

Директор по консалтингу «Ростелеком-Солар» Роман Чаплыгин отметил, что результат необходим в разных аспектах кибербезопасности, в том числе в процессах, и нужно прививать сообществу понимание того, что целеполагание должно быть в форме результата.

Генеральный директор CyberOK Сергей Гордейчик отметил, что любая деятельность должна быть измерима: *«Вопрос измеримости безопасности, метрик безопасности стоит всегда. Соответственно, если ты затеваешь какую-то активность в области ИБ, надо понимать, к чему ты идёшь в рамках этого процесса и как будешь отслеживать прогресс».*

В России, по словам ряда участников, нет системно выстроенных, организованных площадок для сообщества по образцу западных. Тем не менее есть наработки, которые нужно развивать и которым следует придать некую системность. По мнению директора центра информационной безопасности «Инфосистемы Джет» Андрея Янкина, «между кучей замьюченных телеграм-каналов и зарегулированностью не хватает открытой площадки, на которой обычные специалисты могут свободно общаться».

Минувший год показал, что противостоять кибератакам можно только вместе, плечом к плечу. Однако, несмотря на участие представителей многих компаний в так называемых оперштабах, созданных для противодействия киберугрозам, не все игроки отечественного рынка кибербезопасности готовы делиться своими наработками. Индикаторы атак, сигнатуры, правила корреляции – это лишь малая толика того, что компании придерживают, не делясь с сообществом.

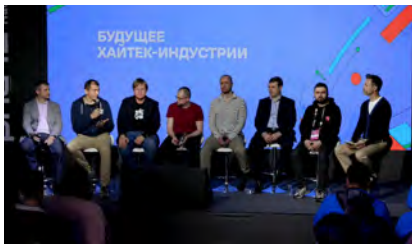
Генеральный директор и сооснователь RST Cloud («Технологии киберугроз») Николай Арефьев рассказал, почему компании не спешат делиться индикаторами компрометации: *«С одной стороны, можно отдавать индикаторы компрометации, но с контекстом будут проблемы. Как правило, организации вручную собирают всю информацию, очищают и обогащают. Получается такая парадигма: отдать сам индикатор, наверное, можно, но в это же были вложены реальные трудозатраты, потрачены человеческие ресурсы и деньги компании. Как таким делиться – вопрос открытый».*

В свою очередь, Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки в «Ростелеком-Солар», обратил внимание на морально-этический аспект публикации наработок компании: *«Сейчас всех атакуют через Exchange. Я считаю своей социальной обязанностью поделиться правилом обнаружения киберугроз, а не ждать, пока заказчика взломают».*

По мнению Теймура Хеирхабарова, директора департамента мониторинга, реагирования и исследования киберугроз BI. ZONE, нужен стандарт, который будет мотивировать российских вендоров средств защиты чаще делиться информацией с рынком кибербезопасности: *«Стандартизация протоколов, интерфейсов взаимодействия, форматов обмена данными – этого нам действительно не хватает. Каждый вендор делает API в своих решениях как хочет, форматы и правила у всех свои. Дружить при отсутствии стандартов просто невозможно».*

Андрей Янкин, директор центра информационной безопасности «Инфосистемы Джет», добавил, что для взаимодействия нужна площадка, в рамках которой компании в сфере ИБ могли бы объединиться. *«Многим игрокам, не таким крупным, это дало бы возможность влиться в реку кибербезопасности и начать быстро друг другу помогать. Эта площадка должна быть не про конкуренцию»,*– рассказал спикер. Руководитель центра мониторинга Kaspersky Сергей Солдатов высказался о возможном бюрократическом барьере на пути к созданию такой площадки и заявил, что в построении коммуникации между организациями важную роль должно играть государство.

О развитии хай-тека, DevSecOps и перспективах отечественных ОС



Будущее индустрии хай-тек обсуждали директора по разработке и совладельцы бизнеса. Из-за ухода зарубежных вендоров с российского рынка появились возможности для прорывов в различных технологических сегментах. Ушли монополисты, которые занимали свои ниши на 100%. При этом пользователи остались, и они ожидают продуктов и сервиса такого же уровня, как и раньше. *«Первый технологический рывок, который необходимо сделать отечественной индустрии, причём за короткий срок,– это наладить производство и обслуживание программного обеспечения на том же уровне, как было у зарубежных вендоров»,*– считает CTO VK Tech Алексей Тотмаков.

В свою очередь, Константин Осипов, сооснователь компании Picodata, в числе приоритетных для импортозамещения сегментов назвал SCADA- и ERP-системы, базы данных, а также системы автоматизированного проектирования (CAD).

Кроме того, возникла фундаментальная необходимость в открытых процессорных технологиях и в их реализации на базе открытых стандартов. *«Требуется инвестировать в инструменты проектирования открытого аппаратного обеспечения, так как сейчас такие средства создаются монопольно и не российскими компаниями»,*– комментирует

Игорь Лопатин, директор по исследованиям и разработкам «Yadro Центр исследований и разработки».

В качестве второго важного направления инвестиций он обозначил средства, которые позволяют разработчикам писать под эти процессоры оптимизированные библиотеки и «другие строительные кирпичики, из которых складывается софтверная экосистема для новых открытых архитектур». Игорь с умеренным оптимизмом оценил перспективы развития отечественного «железа», однако подчеркнул, что в сфере разработки центральных процессоров, которые отличаются экстремальной сложностью, быстрых результатов ждать не стоит.

«Есть области, в которые российские разработчики не шли осознанно, так как не имели «инженерки». Сейчас, с уходом иностранных игроков, нам придётся туда идти от неизбежности,– отметил Алексей Андреев, управляющий директор Positive Technologies.– *С другой стороны, освободились ниши, которые займут отечественные вендоры. В частности, речь о сегменте сетевой безопасности и нише межсетевых экранов нового поколения. В областях, в которых мы обладаем комплементарной экспертизой, у нас будут технологические прорывы».*

В 2022–2023 годах тема DevSecOps стала ещё популярнее и портрет пользователей поменялся.

Денис Кораблёв, директор по продуктам Positive Technologies, отметил, что по сравнению с прошлым годом тема DevSecOps стала гораздо популярнее. *«Из-за того, что многие западные вендоры ушли с российского рынка, различные продукты пришлось разрабатывать с чистого листа. Отрадно видеть, что большинство разработчиков при этом сразу учитывают безопасность, встраивают её в свой конвейер. Это действительно серьёзное отличие по сравнению с тем, что было раньше. В текущей ситуации все видят количество атак, которые происходят, и не могут игнорировать безопасность в своих подходах»,*– полагает эксперт.

В свою очередь, Рами Мулейс, менеджер продуктов безопасности Yandex Cloud, отметил трёхкратное увеличение числа пользователей сервиса для управления DevOps-платформой GitLab в инфраструктуре Yandex Cloud. При этом, по словам спикера, частичный уход западных вендоров затруднил разработку продуктов: *«Всё сильно осложняется тем, что готовых решений для DevSecOps всё меньше и меньше. Мы видим ставку на решения open source по безопасности».*

По словам Юрия Сергеева, основателя и управляющего партнёра Swordfish Security, важно помнить, что все разработчики, использующие решения open source, становятся ответственными за их безопасность.

С уходом зарубежных вендоров изменилась и ситуация в сфере отечественных ОС: разработчики уверены в своих перспективах и отмечают новые возможности. В частности, Владимир Тележников, начальник отдела научных исследований ГК «Астра», рассказал, что *«не всё оказалось гладко, но компания пережила стресс и сейчас находится на стадии спокойного развития продукта и движения вперёд: накоплен хороший опыт внедрения и позитивный фидбек от пользователей продукта».*

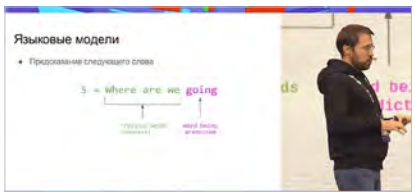
Роман Аляутдин, директор департамента разработки ОС «Аврора» («Открытая мобильная платформа»), уверен в успехе российских ОС: *«Отечественными вендорами заложен хороший базис, вокруг которого нужно строить экосистему, при этом конкурируя на рынке, в том числе с технологиями, к которым рынок приручил всех нас. Для этого у нас есть все ресурсы: люди, технологии, экспертиза».*

Кибергород – посетители парка узнали об особенностях ChatGPT и о том, как не попасть в сети мошенников

На площадке, доступной для всех посетителей Парка Горького (трек «Научпоп»), поднимали темы, близкие каждому человеку. Например, представители ритейла рассказывали о наборе признаков, указывающих на ненадёжность интернет-магазина. Павел Куликов, СТО «СДЭК», порекомендовал пользователям не переводить общение с продавцом в другие сервисы при совершении покупок на маркетплейсах: этим нередко пользуются мошенники.

«В пандемию многие ритейлеры не справлялись с большим количеством заказов, чем пользовались злоумышленники, создавая поддельные или посреднические сайты, например мимикрировали под «Азбуку вкуса». В лучшем случае покупки клиентам обходились дороже, в худшем – покупатели оставались без денег и товара. Проверяйте сайт, на котором собираетесь оплачивать покупки, хотя бы по банковским реквизитам юридического лица, которые всегда указаны на легальных сайтах»,– посоветовал Дмитрий Кузеванов, технический директор «Азбуки вкуса».

Валентин Малых, NLP-исследователь Huawei, рассказал, как функционирует система ChatGPT, под влиянием которой сотни западных экспертов, в том числе Илон Маск и Стив Возняк, призвали разработать правила для интеллектуальных помощников.



«В последние полгода о ChatGPT говорят из каждого чайника, поэтому я попробую объяснить, как работает эта технология изнутри. Сам термин NLP – про то, как мы взаимодействуем с текстами. У каждого из нас есть модель языка, которая помогает нам доносить свои мысли. Самое базовое определение языка связано с некой «затравкой», которая позволяет получить следующее слово. Если кто-то скажет «мама мыла», то все дружно ответят «раму». Подобные модели, генерирующие следующие слова, только в тысячи раз сложнее, работают в ML-помощниках»,– отметил Валентин Малых.

Егор Баяндин, CIO и сооснователь сервиса кикшеринга Whoosh, рассказал, могут ли самокаты собирать данные

об окружающей среде и пользователях и может ли хакер взломать самокат и дистанционно регулировать скорость и другие показатели. По словам Егора, самокат почти ничего не знает о своём арендаторе. Кроме того, за четыре года работы сервиса данные о пользователях ни разу не были украдены. Эксперт также предупредил о важности физической безопасности при использовании самокатов, в частности о недопустимости езды вдвоём, пояснив, что даже мотоциклисты могут попасть в аварию из-за неправильных действий пассажира.

В свою очередь, Яна Юракова (старший аналитик исследовательской группы Positive Technologies) и Сергей Полунин («Газинформсервис») объяснили, как выбрать защищённый VPN-сервис в условиях возросшей популярности этой технологии в связи с блокировками. Утечка конфиденциальных данных, по словам Яны, может возникнуть, только если владелец сервиса – недобросовестный человек, а соединение с запрашиваемым ресурсом происходит по незащищённому HTTP-протоколу (когда в браузере нет характерного замочка). Сергей отметил, что поддержка VPN-ресурсов стоит немалых денег и, если сервис бесплатен, надо понимать, какая у него модель монетизации и чем заплатит пользователь (рекламой или похищенными данными).

О кибербитве Standoff и других конкурсах

За четыре дня кибербитвы атакующим 204 раза удалось реализовать недопустимые события в воссозданных на киберполигоне секторах экономики. Из 148 предусмотренных уникальных недопустимых событий нападающие реализовали 64. Больше всего реализаций на счету команды Codeby, которая теперь является единственным четырёхкратным чемпионом кибербитвы. Ни один из сегментов не выстоял под натиском красных команд. Чаще всего были реализованы утечка конфиденциальной информации (32 раза) и распространение вируса-шифровальщика (31 раз). Максимальное количество успешных атак было реализовано в банковской системе (44) и УК City (44), на третьем месте «МеталлиКО» (37), замыкает четвёрку лидеров Atomic Energy (27).

За все время кибербитвы в Государстве F атакующие сдали 209 отчётов об уязвимостях, из них 58% – об уязвимостях критического уровня риска, 24% – высокого и 17% – среднего. Наиболее популярным типом выявленных уязвимостей стало удалённое выполнение кода (Remote Code Execution, RCE).

Команды защитников сдали жюри 667 отчётов об инцидентах в основном в сегменте Tube (37%) и расследовали 43 атаки.

Первое место среди атакующих заняла команда Codeby, набравшая в совокупности 193454 балла, второе – True0xA3 (143264 балла), третье – Bulba Hackers (58796 баллов).

На киберфестивале была обширная конкурсная программа. Участники конкурса IDS Bypass испытывали на прочность системы сетевой защиты, а в конкурсе $natch надо было взломать банкомат, мобильный банк и кассовый аппарат. Последний, кстати, участники конкурса смогли вскрыть не менее пяти раз.

Около десяти человек попробовали свои силы в непростом конкурсе ETHical hacking. Участникам предстояло пройти ряд челленджей по взлому смарт-контрактов в сети Ethereum: вывести все средства из смарт-контракта или установить флаг (значение булевой стейт-переменной контракта) в true в зависимости от описания челленджа. Шестерым специалистам удалось решить как минимум один челлендж.

О результатах всех конкурсов мы сообщим дополнительно: совсем скоро последуют новости и отчёты, посвящённые отдельным событиям киберфестиваля. Доклады, сессии, конкурсы и соревнования мероприятия транслировались онлайн на сайте PHDays. Видео большинства выступлений будут опубликованы позднее. Следите за новостями на нашем сайте.

Соорганизатором PHDays и Standoff уже третий год выступает ИТ-компания **Innostage**, разработчик и интегратор сервисов и решений в области цифровой безопасности. Бизнес-партнёрами фестиваля стали разработчик решений для информационной безопасности **Security Vision**, национальный провайдер сервисов и технологий ИБ **«Ростелеком-Солар»** и один из крупнейших универсальных банков России **Газпромбанк**. Генеральный медиапартнёр мероприятия – компания VK, а генеральный информационный партнёр – **Rambler&Co**. Информационным партнёром деловой части фестиваля стала группа компаний **«РБК»**. Технологический партнёр – **«Азбука вкуса»**. Партнёры PHDays 12 и участники выставки – компании **Axoft**, **Fortis**, **F+tech**, **«ICL Системные технологии»**, **InfoWatch**, **MONT**, **OCS Distribution**, **UserGate**, **«Инфосистемы Джет»**, **«Стахановец»**. Партнёры – **ARinteg**, **Platformix**, **Росбанк** и **«УЦСБ»**. Участник выставки и Standoff – **«Газинформсервис»**.

OS DAY 2023: десятый год объединяя разработчиков ОС

X международная научно-практическая конференция OS DAY собрала этим летом в Москве разработчиков и заказчиков отечественных операционных систем. Цель конференции – определить задачи и возможности российской ИТ-отрасли в области разработки ОС и прикладных программ, формирования единой экосистемы отечественного программного обеспечения.

Участники конференции обсуждали важнейшие вызовы современной отечественной ИТ-отрасли: необходимость единой среды разработки, создание прикладного программного обеспечения, совместимого с российскими ОС, построение единой цифровой платформы на основе отечественных операционных систем. Конференцию организовал консорциум OS DAY: ИСП РАН, Институт имени Н.Е. Жуковского, «Лаборатория Касперского», НТП «Криптософт», ГК «Астра», «Базальт СПО», «Ред Софт» и «Открытая мобильная платформа».

OS DAY собирает лидеров российского ИТ уже 10 лет подряд. Участники конференции отметили, что за это время она превратилась в одну из наиболее важных и авторитетных дискуссионных площадок отрасли. Особенно важно это сегодня, когда создание отечественного ПО приобрело для страны стратегическую значимость.

«Эта конференция позволила нам наладить взаимодействие между производителями операционных систем,– рассказал на церемонии открытия OS DAY 2023 директор Института системного программирования РАН Арутюн Аветисян.– *Мы не всегда друг с другом согласны, но всегда приходим к консенсусу. Среди нас представители компаний, которые конкурируют друг с другом, но мы вместе и делаем одно большое дело».*

«OS DAY – главное отраслевое мероприятие, посвящённое операционным системам, на котором можно пообщаться с коллегами, которые решают те же проблемы, но, возможно, другими способами, обменяться с ними опытом и даже порой изменить своё мнение»,– согласился с ним Роман Симаков, директор департамента развития системных продуктов «Ред Софт».

Обсуждение перспектив формирования российской экосистемы программного обеспечения оказалось тесно переплетено с вопросами стандартизации ПО и унификации среды его разработки, а также с вопросом обеспечения информационной безопасности. Этому был посвящён круглый стол, состоявшийся во второй день конференции. Как отметил начальник управления ФСТЭК России Дмитрий Шевцов, сегодня уже действуют требования по обеспечению информационной безопасности к операционным системам, средствам контейнеризации, виртуализации, системам управления базами данных, а созданные совместно с ИСП РАН и Минцифры России Технологический центр исследования безопасности ядра Linux и Инфраструктура для систематического исследования безопасности критичных компонентов позволяют отечественным программистам совместно работать над повышением безопасности ключевых компонентов с открытым исходным кодом, применяемых в ответственных областях. *«Сегодня те, кто планирует реализацию своего программного обеспечения*

в государственных органах, в субъектах критической информационной инфраструктуры, должны провести свои программные продукты через процедуру сертификации,– сказал Дмитрий.– Таким образом обеспечивается единство подходов в обеспечении информационной безопасности».

Разработчикам отечественного программного обеспечения предстоит вести работу в рамках задаваемых стандартов. Заместитель министра цифрового развития, связи и массовых коммуникаций РФ Александр Шойтов подчеркнул, что вопросы безопасности и доверия становятся особенно важны, когда речь заходит о технологическом суверенитете страны. *«Если мы говорим о критической инфраструктуре, для которой создаётся программное обеспечение, государство будет предъявлять повышенные требования на всех этапах, начиная с разработки, и требовать стандартизации,– подчеркнул он.– Создателям прикладного программного обеспечения предстоит встроиться в этот «конвейер».*

Первостепенной задачей участники конференции назвали поступательный переход с импортного ПО на программы отечественных вендоров. *«Сегодня очень актуально развитие продуктов, совместимых с нашими технологиями, и решений, которые мы сможем самостоятельно контролировать и развивать в нужном направлении,–* заявил заместитель руководителя департамента разработки ГК «Астра» Александр Оружейников.– *Такая задача особенно остро стоит перед компаниями, разрабатывающими операционные системы. За последний год процесс импортозамещения двигается от государственного сектора в бизнес, причём затрагиваются все его сферы. Многим стало очевидно, что сейчас минимально рискуют именно те, кто опирается на отечественные программные продукты и ноу-хау. Конференции, подобные этой, помогают нам вендорам и нашим клиентам найти собственный путь, о чём мы здесь говорили давно, задолго до событий, изменивших российский ИТ-рынок».*

«Западное ПО занимало очень большую долю российского рынка, его уход освободил много рыночных ниш,– оценил положение в отрасли Андрей Духвалов, руководитель управления перспективных технологий, стратег по развитию технологий «Лаборатории Касперского».– *Появилось много возможностей для российских компаний и компаний из дружественных стран. Сумеют ли они воспользоваться новыми возможностями, зависит от многих факторов, например от инвестиций, от поддержки государства и так далее. Я ставлю на российских производителей, у них есть возможности, достаточный уровень компетенций и другие хорошие качества. Нужно только время. Заместить отечественными продуктами западное ПО более чем реально. Назовите мне страну, в которой есть столько зрелых операционных систем. Я знаю одну, и это – Россия».*

Среди операционных систем российского производства есть как ОС широкого профиля, так и узкоспециализированные, действительно уникальные, как, например, микроядерная сертифицируемая операционная система реального времени JetOS – операционная система для бортового оборудования гражданской авиации.

«Операционные системы реального времени, программное обеспечение, необходимое для бортового оборудования сегодня – чрезвычайно важный фронт работ, потому что российское самолётостроение стало одной из краеугольных отраслей,– подчеркнула Анна Кан, начальник аналитического отдела департамента координации и сопровождения программ НИЦ «Институт имени Н.Е. Жуковского».– *Стране нужны новые самолёты, новое бортовое оборудование, новые операционные системы, потому что в настоящее время самолёт – это цифровая услуга, начиная с земли и заканчивая бортом».*

При этом все участники конференции сошлись во мнении, что, несмотря на определённые сложности, создание общей экосистемы российских ОС и прикладного программного обеспечения возможно. Валерий Егоров, заместитель директора НТП «Криптософт», отметил, что *«необходимо и дальше искать общие точки соприкосновения технологий, которые позволят провести унификацию средств разработки и программных интерфейсов, создавать общие требования, руководства и критерии разработки всех отечественных производителей ПО».*

«У нас большое число разработчиков под Windows, под Android, под IOS,– заявил Роман Аляутдин, директор департамента компании «Открытая Мобильная Платформа».– *Отечественным вендорам ОС нужно сблизиться с этими разработчиками по инструментам и языкам программирования. Однако движение должно быть встречным: сегодня разрабатываемые российские мобильные сервисы, на создание которых затрачены миллиарды рублей, несовместимы ни с одной из операционных систем, представленных на этой конференции. Необходимо сделать сервисы более кроссплатформенными, а вновь создаваемое в России прикладное ПО – совместимым с российскими операционными системами, которые становятся мейнстримом, и от этого уже никуда не деться».*

«Вопрос обеспечения совместимости отечественного ПО – ключевой для нашей ассоциации,– сообщил исполнительный директор АРПП «Отечественный софт» Ренат Лашин.– *Несколько лет назад мы создали комитет по интеграции отечественного ПО, на площадке ко-*

торого сформировано более 40 стеков российского софта под различные задачи заказчиков. Тогда же мы разработали бесплатный отраслевой каталог совместимости российского ПО, который сегодня насчитывает порядка 2000 совместимостей. Однако в процессе построения полноценных экосистем совместимых отечественных решений есть сдерживающий фактор – недостаточно чёткий сигнал регуляторов в адрес заказчиков, прежде всего коммерческих, о сжатых сроках портирования прикладного и специализированного ПО на российские операционные системы. Незавершённость построения таких экосистем, в свою очередь, ограничивает экспорт таких решений за рубеж».

Определённый итог сказанному подвёл советник генерального директора компании «Базальт СПО» Алексей Новодворский: *«Должен сказать, что за последний год в отношении импортозамещения наблюдается довольно радостная картина, потому что у нас стали намного активнее использовать отечественный софт, причём там, где этого никто делать не заставляет. И тем, кто для себя его открыл, это нравится. Это очень радует, и я всё время думаю, как бы нам не упустить этот момент».*

Тема OS DAY 2024 ещё не определена: организаторы каждый раз стремятся сделать её как можно более актуальной. Однако через год конференция состоится вновь, у создателей российского системного программного обеспечения впереди большая работа.

Конференция проводится при поддержке РАН, ФСТЭК России, АРПП «Отечественный софт», НП «РУССОФТ».

OS:DAY

Научно-практическая конференция OS DAY проводится в России ежегодно с 2014 года. Это коммуникационная площадка для теоретиков и практиков системного программирования и разработки операционных платформ, место консолидации российских разработчиков ОС и поиска точек для совместной деятельности. Задачи конференции – определить перспективные направления и технологии в сфере разработки операционных систем, обозначить главные вызовы современной ИТ-отрасли и помочь разработчикам, производителям и заказчикам обменяться опытом. Организует конференцию консорциум OS DAY, в который входят: ИСП РАН, «Лаборатория Касперского», НТП «Криптософт», ГК «Астра», «Базальт СПО», «Ред Софт», «Открытая мобильная платформа» и НИЦ «Институт имени Н.Е. Жуковского». Целью создания сообщества организаторов было определить задачи и возможности России в области разработки операционных платформ, выделить перспективные технологии, обменяться опытом, обозначить вызовы ИТ-отрасли и направления движения.

www.osday.ru

ЦИПР-2023

Подвели итоги работы индустриальных центров компетенций за год и определили главные направления импортозамещения на следующие годы

С 31 мая по 2 июня в Нижнем Новгороде прошло главное событие цифровой экономики – конференция «Цифровая индустрия промышленной России».

В конференции приняли участие Председатель Правительства РФ Михаил Мишустин, заместитель Председателя Правительства РФ Дмитрий Чернышенко, заместитель председателя правительства РФ, Министр промышленности и торговли РФ Денис Мантуров, губернатор Нижегородской области Глеб Никитин и представители крупнейших госкорпораций.

ЦИПР-2023 традиционно стал ключевой площадкой для диалога представителей бизнеса и власти по вопросам цифровой трансформации общества и ключевых отраслей экономики. В конференции приняли участие более 7 тысяч человек из 2 тысяч компаний и 77 регионов России, а также 8 иностранных делегаций (КНР, Индия, ЮАР, Беларусь, Иран, Турция, Казахстан, Бразилия). В рамках деловой программы состоялось 88 дискуссий, на которых выступили более 700 спикеров. Выставочная экспозиция составила 5500 м2 и 102 стенда с прорывными российскими решениями в области цифровых технологий. За время проведения конференции было подписано 63 соглашения, а в онлайн-музее DECIPRALAND было выставлено 120 работ от 40 художников. Центральными темами деловой программы конференции стали итоги работы за год и перспективы развития в сфере импортозамещения в России, совершенствование и популяризация российского софта, цифровые решения, влияющие на социальную экономику, культуру и тренды.

Во второй день ЦИПР-2023 прошло главное пленарное заседание «Цифровая независимость промышленной России», в котором приняли участие Председатель Правительства Российской Федерации **Михаил Мишустин**, заместитель Председателя Правительства РФ **Дмитрий Чернышенко**, генераль-

ный директор «Объединённая судостроительная корпорация» **Алексей Рахманов**, президент, председатель Правления «Норильский никель» **Владимир Потанин**, генеральный директор «Северсталь» **Алексей Мордашов**, генеральный директор «Газпром нефть» **Александр Дюков**, заместитель генерального директора «ОДК» **Александр Иноземцев**, генеральный директор «КАМАЗ» **Сергей Когогин**.

В 2022 году на пленарном заседании ЦИПР Михаилом Мишустиным было объявлено о создании индустриальных центров компетенций по ключевым отраслям экономики с целью импортозамещения ПО. На ЦИПР-2023 были подведены итоги развития ИЦК, премьер-министр дал ряд поручений, в том числе о запуске второй волны проектов разработки ИТ-решений по предложениям ИЦК.

В рамках ЦИПР ключевые игроки рынка заключили соглашения, презентовали новые решения, поделились результатами работы своих продуктов.

Помимо деловой программы в рамках ЦИПР прошли чемпионаты, фестивали и спортивные состязания.

Вице-премьер Дмитрий Чернышенко на ЦИПР-2023 открыл **презентацию международного чемпионата «Битва роботов»**. На стенде вице-премьер познакомился с командами и посмотрел выступления роботов. В специально оборудованном павильоне участники провели показательные бои, а гости стенда попробовали самостоятельно управлять роботами.

На **«Робофесте»** лучшие команды нижегородских детских технопарков «Кванториум» представили свои проекты. За три дня гости фестиваля могли познакомиться с лучшими детскими проектами в области робототехники, увидеть показательные полёты на микродронах, а также принять участие в мастер-классах.

Также на ЦИПР-2023 прошёл турнир **по фиджитал-баскетболу «Игры будущего»**. Фиджитал-баскетбол – это совмещение интерактивного баскетбола и баскетбола 3×3, где игроки сначала соревнуются в NBA2K на игровых приставках, а затем переходят на реальную игровую площадку.

VIII ежегодная конференция «Цифровая индустрия промышленной России» прошла в конгрессно-выставочном центре «Нижегородская Ярмарка». Организатором конференции стала компания «ОМГ». Стратегическим партнёром выступили Госкорпорация «Ростех», Госкорпорация «Росатом», «Ростелеком». Мероприятие прошло при поддержке Министерства цифрового развития, связи и массовых коммуникаций РФ, Правительства Москвы и Правительства Нижегородской области. Генеральный партнёр: НАЦПРОМ технологическое партнёрство. ВИП-партнёры: Институт развития ДОМ. РФ, ЛУКОЙЛ, Группа «Россети», «Национальная компьютерная корпорация». Официальные партнёры: ТРАНСНЕФТЬ, VK, МТС, МегаФон, «Ред Софт», ГК «Астра», ГК «Аметист Групп», СБЕР, «Газпромбанк», ПСБ, группа компаний «СКБ Контур», «Т Плюс», NtechLab, компания-разработчик «МойОфис», фирма «1С», ГК ICL, Группа Т1, СИБУР, Sitronics Group, F+tech, ОС Аврора (ОМП), «Ростелеком-ЦОД», «Гравитон», «Базис», «Норникель», ПК «АКВАРИУС» Страховая Группа «СОГАЗ», «Лаборатория Касперского», «Газпром нефть», ОАО «РЖД», группа компаний «Максима», «Газпром-Медиа Холдинг», Rutube, Premier, Yappy. Партнёр панельной дискуссии: Ассоциация крупнейших потребителей программного обеспечения и оборудования. Экспоненты: «Нетрика», «Осмокод», Webinar Group, Rocket Group, «Авада», «Челнок», ООО «НПО Криста», «Контроль ИТ», IT-компания STM Labs, «Хоулмонт», НИТУ МИСИС, «ИНЛАЙН ГРУП», «Мангазея Технолоджи», Гознак, TrueConf, «Код Безопасности». Бизнес-партнёры: ГТЛК, ГК «Урбантех», «РОТЕК Диджитал Солюшнс», «Финвал-Инжиниринг», «Инфосистемы Джет».

ЦИПР

Лидеры цифровой медиасферы о трендах медиапотребления и телесмотрения в России

В Москве 23 мая состоялся VII ежегодный «TeleMultiMedia Forum 2023. Лидеры цифровой медиасферы», собравший несколько сотен участников. В рамках центрального делового события отрасли первые лица медиабизнеса поделились прогнозами развития рынка на ближайшие годы, опытом создания современных форматов медиаконтента и внедрения новых сервисов и инструментов взаимодействия с аудиторией.

Мероприятие было организовано TMT Conference совместно с «Телеспутником» и ИАА TelecomDaily в гибридном формате, сочетающем очное общение и онлайн-взаимодействие. На площадке мероприятия в «Марриотт Гранд» Отеле собралось свыше 200 делегатов, онлайн-трансляция объединила более 400 зрителей. Партнёрами форума выступили: генеральный партнёр – «Триколор», золотой партнёр – компания «МТС», серебряный партнёр – Wink – цифровой видеосервис компании «Ростелеком». Партнёр сессии «Стратегии развития отечественного рынка онлайн-видеосервисов» – онлайн-кинотеатр «Иви», партнёр сессии «Оригинальные фильмы как точка роста для онлайн-кинотеатров» – онлайн-кинотеатр START, партнёр сессии «Практика продвижения медиаконтента в цифровой среде и не только» – телекомпания «Первый ТВЧ». Также партнёрами стали: компания «Медиалогистика», проект «МСК-IX», компания «Синтерра Медиа», компания GS Labs, рекламное агентство полного цикла «Агентство 2».

Голос отрасли должен быть услышан

Деловую программу «TeleMultiMedia Forum 2023» открыла пленарная дискуссия: «Российский рынок медиапотребления в новой реальности: вызовы, достижения и перспективы». Её модераторами выступили **Денис Кусков**, генеральный директор TelecomDaily, и **Евгения Стогова**, корреспондент РБК. В ходе дискуссии участники обсудили основные изменения и тренды рынка медиапотребления, рассмотрели факторы риска и показатели роста отрасли, сформировали прогноз основных векторов

развития бизнеса в области производства и распространения видеоконтента в цифровой среде.

Бэлла Черкесова, заместитель министра цифрового развития, связи и массовых коммуникаций, отметила, что россияне в среднем проводят с контентом 7–8 часов в день. «Фактически, рабочий день. Основными блоками получения контента являются ТВ и Интернет. Объём российского производства очень сильно вырос. Мы – одна из немногих стран в мире, которая производит качественный контент, это как сериалы, так и полный метр»,– указала Черкесова. Также она добавила, что в Минцифры думают о том, чтобы продвигать российский контент в Африку, Ближний Восток, Латинскую Америку. «Готовы поддерживать компании, которые занимаются его продвижением, в том числе в части перевода на разные языки»,– констатировала она.

Директор по развитию онлайн-кинотеатра «Триколора» **Алексей Липилин** заметил, что тоже видит рост интереса к российскому контенту. «Безусловно, созданы различные фонды, которые помогают развивать отрасль и производство отечественного контента. Минцифра поддерживает участников рынка. И сейчас у российских проектов есть шанс вытеснить зарубежный контент. Как и есть зарубежная альтернатива в виде киносериального рынка Турции, Бразилии и других стран Азии и Латинской Америки»,– пояснил он.

При этом Алексей Липилин отметил, что, несмотря на господдержку, в частности, возможность получения онлайн-кинотеатрами статуса аккредитованных ИТ-компаний, некоторые законы и инициативы «осложнили жизнь» отрасли. «Мы видим, что сегодня многие из законопроектов сталкиваются с крайне негативной реакцией игроков и явно не идут на пользу развитию отрасли. Хотелось бы, чтобы при разработке законопроектов анализировались последствия, которые они повлекут за собой в случае принятия. Рынку необходимо, чтобы государство взяло на себя разработку концепции развития национального цифрового телерадиовещания. Только в этом случае игроки поймут вектор развития отрасли и смогут выстраивать долгосрочные планы по созданию и усовершенствованию собственных сервисов и услуг»,– констатировал Алексей Липилин.

Александр Нечаев, заместитель генерального директора ВГТРК, в свою очередь полагает, что в ВГТРК мер господдержки хватает и отметил: «В дискуссиях всегда рождается вариант, который устроит всех». Аналогичного мнения придерживается и **Юлия Голубева**, заместитель генерального директора «Газпром-Медиа Холдинга»: «То внимание, которое госорганы уделяют медиа и креативным индустриям, беспрецедентно. И это не может не дать роста и поддержки тем, кто может и хочет что-то делать. Добавлю, что налоговые льготы на создание контента могли бы стать дополнительным драйвером роста». Так, например, по её словам, за 2020–2022 годы российский рынок рос в среднем на 15% в год, а мировой – на 13%. Одной из основных причин такой ситуации оказалось увеличение объёма государственной поддержки. «С 2018 года анимационные студии суммарно получили более 4 млрд рублей в виде субсидий Министерства культуры и Фонда кино, из которых более 3 млрд – на безвозвратной основе. Объём российского рынка анимации в 2022 году составил 18,1 млрд рублей. Частичный уход зарубежной анимации стал драйвером роста российского производства. Исследование показало, что в 2016 году мы производили около 4,4 тыс. минут, а уже в 2022 году – более 9 тыс. минут, сохранив объём рынка на уровне 2021 года. Российский рынок анимации, по прогнозам, к 2030 году может увеличиться более чем в два раза и достигнет отметку в 38,8 млрд рублей»,– подчеркнула Голубева.

Генеральный директор «МТС Медиа» **Алексей Иванов** убеждён, что отрасль «здорово и сильно развивается», однако выразил мнение, что ей нужна новая точка регулирования. «У нас есть две точки регулирования: Роскомнадзор и Минкульт. Есть разница понятийного аппарата и требований. Мы тратим на это время, которое могли бы потратить на создание контента. Нужна третья площадка, которая могла бы урегулировать требования двух регуляторов, чтобы было единообразие»,– добавил он.

Факторы роста

В сессии «Стратегии развития отечественного рынка онлайн-видеосервисов», партнёром которой выступил онлайн-кинотеатр «Иви», лидеры сегмента российских онлайн-видеосервисов дали оценку текущему состоянию отрасли, обсудили перспективные маркетинговые стратегии и эффективные инструменты увеличения выручки и расширения абонентской базы. Модераторами сессии вновь выступили Денис Кусков и Евгения Стогова.

Заместитель генерального директора по контенту «Иви» **Иван Гринин** выразил мнение, что самый главный вклад в рост рынка – экосистемность. «Развитие экосистемных подписок опережает темпы роста онлайн-кинотеатров»,– сообщил он. По мнению эксперта, экосистемы, построенные крупными холдингами, являются «локомотивом отрасли онлайн-кинотеатров». **Ксения Болецкая**, директор по взаимодействию с индустрией Яндекса, добавила, что пользователям нравится, когда они получают в пакете сразу несколько услуг, а также констатировала: «Это влияет на рост рынка и психологический фактор, потому что людям стали привычны платежи в интернете и платежи за контент. Среди других факторов – онлайн-кинотеатры хорошо поработали с originals, они научились их продвигать. Происходит перекрёстное опыление с эфиром, у которого огромные охваты».

Генеральный директор Wink **Антон Володькин** поддержал тезис о том, что все онлайн-кинотеатры научились гораздо лучше делать originals, а также отметил важность быстрого доступа к контенту через экосистемные проекты и совместные подписки. «Каналы дистрибуции так же имеют важное значение, как и требование клиентов к удобству сервиса. Из-за этого всё сложнее предсказать, какова будет дальнейшая структура рынка. Можно быть не лидером в контенте, но лидером в дистрибуции»,– считает он.

Операционный директор Start **Анастасия Мишанина** заметила, что в 2022 году онлайн-кинотеатр выпустил 20 originals, 8 из которых – фильмы. «Это абсолютный рекорд. Если говорить про 2023 год, то мы сохраняем оптимизм. Мы рассчитываем на темпы роста год к году по выручке в районе 25–30%»,– поделилась мнением эксперт. Кроме того, по её словам, Start закупает зарубежный контент так, чтобы он дополнял originals.

Ольга Титова, директор по стратегии Kion («МТС Медиа»), считает, что пенетрация OTT сейчас составляет всего 50% и полагает: «Надо объединиться, чтобы продвигать эту категорию. Очень много барьеров у населения, чтобы подключиться к OTT».

Алексей Липилин в свою очередь отдельно отметил значительный рост пользователей собственного онлайн-кинотеатра среди спутниковых клиентов. По оценке компании, их количество увеличивается двукратно из года в год, что соответствует стратегии развития онлайн-кинотеатра оператора. «По итогам 2022 года аудитория онлайн-кинотеатра «Триколор Кино и ТВ» среди наших действующих спутниковых клиентов выросла на 40%»,– привёл данные Алексей Липилин.

Макар Кожухов, заместитель генерального директора Premier, рассказал, что сервис максимально использует преимущества холдинга «Газпром-Медиа Холдинг» и показывает контент телеканалов, а также пояснил: «Но есть и планы по наращиванию собственного контента. Планы по originals не меняем – 1,5–2 наименования в месяц».

Рассуждая о замещении контента, эксперты высказали мнение, что доля интереса к турецким сериалам за последние несколько лет остаётся стабильной. «Это контент для определённой категории»,– считает Ксения Болецкая. Макар Кожухов в свою очередь уверен, что «хайп вокруг турецкого, немецкого и китайского несколько преувеличен».

Ставка на отечественное

В центре дискуссии на сессии «Оригинальные фильмы как точка роста для онлайн-кинотеатров», модераторами которой стали Денис Кусков и кинокритик **Егор Москвитин**, было производство отечественного видеоконтента. Партнёром данной сессии выступил онлайн-кинотеатр Start.

Юлия Миндубаева, исполнительный директор группы компаний Start, напомнила, что у онлайн-кинотеатра никогда не было фокуса на зарубежный контент, поскольку компания была сосредоточена на собственном производстве. «При этом стриминги и в России, и во всём мире, живут именно за счёт сериалов. Подписная модель работает лучше всего именно на них. Вместе с тем фильмы являются важным событийным элементом. Это помогает, прежде всего, оставлять подписчиков внутри за счёт ярких событий»,– отмечает она. По словам эксперта, для Start оригинальные проекты – это экономика. «Она складывается, когда есть кинотеатральный прокат. А после этого выходит онлайн-релиз. Мы не пытались экспериментировать, чтобы выпускать только в онлайн. Мы думали об этом, но никогда не решались на это. Как показывает опыт, мы поступили правильно»,– убеждена Миндубаева. Эксперт подчёркивает, что кинотеатральный прокат даёт большой охват и экономику фильму, которую невозможно получить на онлайн-релизе.

Александр Косарим, директор по контентной политике ПАО «Ростелеком»/Wink, заметил, что: «Фильм – это сложный жанр. Когда начинается кампания сериала – это протяжённое во времени событие, в течение которого происходит приток подписчиков в течение определённого времени. Когда идёт рекламная кампания для одного фильма – экономика сильнее утяжеляется». По мнению Косарима, если фильм выходит напрямую на платформе, то это поддерживает существующих зрителей, а не привлекает новых.

Мария Смирнова, директор по контенту и дистрибуции Kion («МТС Медиа»), добавила, что, поскольку почти у всех сериалов серии выходят один раз в неделю, зрителю нужно дополнительное развлечение, и именно кино играет здесь важную роль. «Фильм – это форма более короткого развлечения. Зритель всегда должен найти в определённый момент времени то, зачем он пришёл. И это выгодно отличает нас от телевидения и офлайн-кинотеатра»,– подчёркивает она.

Безопасная доставка

В ходе сессии «Доставка видеоконтента: платформы, технологии и сервисы», модератором которой выступила главный редактор «Телеспутника» **Мария Кузнецова**, речь шла о технологической составляющей рынка медиапотребления, возможностях внедрения инновационных решений, успешных кейсах, а также вызовах текущего момента.

Несмотря на то, что западные вендоры покинули российский рынок, инфраструктура и экспертиза остались в стране, считает **Денис Филипишен**, директор по вещательным и информационным технологиям «Триколора». Эксперт отмечает, что не видит сложности по поддержанию текущей инфраструктуры и реализации планов для её развития. «С другой стороны, за время совместной работы мы научились самостоятельно решать широкий круг вопросов, и с этой точки зрения «Триколор», пожалуй, лидер рынка. Говоря о поддержке инфраструктуры, сейчас мы серьёзно вкладываемся в команду и стараемся её консолидировать, чтобы сохранить компетенции внутри компании»,– отмечает он. Отвечая на вопрос, касающийся импортозамещения, **Денис Филипишен** рассказал, что на сегодняшний день «Триколор» проводит анализ рынка отечественных производителей софта и железа. «Чуда произойти пока не может, но мы видим энтузиазм, активность и полезные результаты. Как только появится возможность переходить на российские решения, мы их не упустим»,– подчёркивает эксперт.

Григорий Урьев, генеральный директор «Синтерра Медиа», директор по работе с медиарынком (B2B) ПАО «Ростелеком», добавил, что, пока маркет-мейкеры не будут вкладываться в российские решения, они никогда не станут полноценными и доработанными. «Мы идём по пути сотрудничества с производителями отечественного оборудования во всех направлениях. Мы делимся своей экспертизой и опытом с разработчиками и призываем поддерживать их форвардными контрактами или любыми другими способами»,– подчёркивает Урьев.

Григорий Кузин, директор проекта «Медиалогистика» MSK-IX, напомнил о том, что «Медиалогистика» была запущена в 2014 году, когда страна уже находилась под санкциями. «В стратегию проекта мы заложили диверсификацию: параллельно существовали системы, построенные на зарубежных и отечественных вендорах. И в текущей ситуации это сильно помогает»,– говорит он. Эксперт также поделился подробностями о расширенных возможностях по дистрибуции телеканалов в «Медиалогистике 2.0.», а также рассказал о запуске новой платформы «Медиабаза» для дистрибуции загружаемого контента. Григорий Урьев со своей стороны указал на критическую важность информационной безопасности для вещателей и медиакомпаний, предложив обойти уязвимости спутниковой доставки сигнала по земле.

Немаловажным с точки зрения снижения рисков влияния извне, по мнению участников дискуссии, является импортозамещение решений систем условного доступа (CAS) и защиты авторских (цифровых) прав (DRM). Использовать сегодня иностранные решения – это мина замедленного действия, считает **Роман Хлопов**, начальник отдела продаж GS Labs. В своей презентации он рассказал

о разработках компании и подчеркнул: «Здесь речь идёт не об импортозамещении, а скорее, о полном аналоге зарубежных решений».

Важным сегментом, которого коснулись участники сессии, стали абонентские устройства. «Одним из главных трендов ближайшего времени мы видим рост популярности телевидения в формате сверхвысокой чёткости (Ultra HD). Телезрители всё чаще выбирают более чёткую и яркую картинку. В 2022 году количество UHD-клиентов «Триколора» увеличилось на 30%, и сегодня почти 10% от нашей общей базы – это клиенты, которые имеют доступ к телевидению UHD. И число будет только увеличиваться»,– уверен Денис Филипишен. По его словам, в этом году «Триколор» готовит ещё несколько продуктов для телесмотрения и об одном из них он расскажет уже в конце июня.

Не диджиталом единым

В ходе заключительной сессии «Практика продвижения медиаконтента в цифровой среде и не только», партнёром которой выступила телекомпания «Первый ТВЧ», ведущие эксперты рынка обсудили произошедшие за последнее время изменения, а также успешные примеры продвижения медиаконтента как в онлайн-, так и в офлайн-пространстве. Модератором дискуссии вновь выступила Мария Кузнецова.

По словам **Антонины Петровой**, директора по развитию бренда «Триколора», в настоящее время люди охотно откликаются на BTL-акции – мероприятия от имени компании, конкурсы, подарочные скидки, спонсорство разнообразных программ и промоакции новых товаров. «Это работает, помогает увеличивать телесмотрение. Это прекрасный, супертаргетированный подход. Но важно выбрать формат, который подходит той или иной аудитории и соответствует контенту, который вы собираетесь продвигать»,– отметила она.

Мария Черкасская, директор по маркетингу телекомпании «Первый ТВЧ», добавила, что в прошлом году они совместно с операторами связи провели более 100 офлайн-мероприятий и онлайн-акций для привлечения аудитории. По её словам, масштабы и форматы были самые разнообразные. «Всё зависит от того, как каждый оператор работает со своими пользователями»,– подчеркнула эксперт.

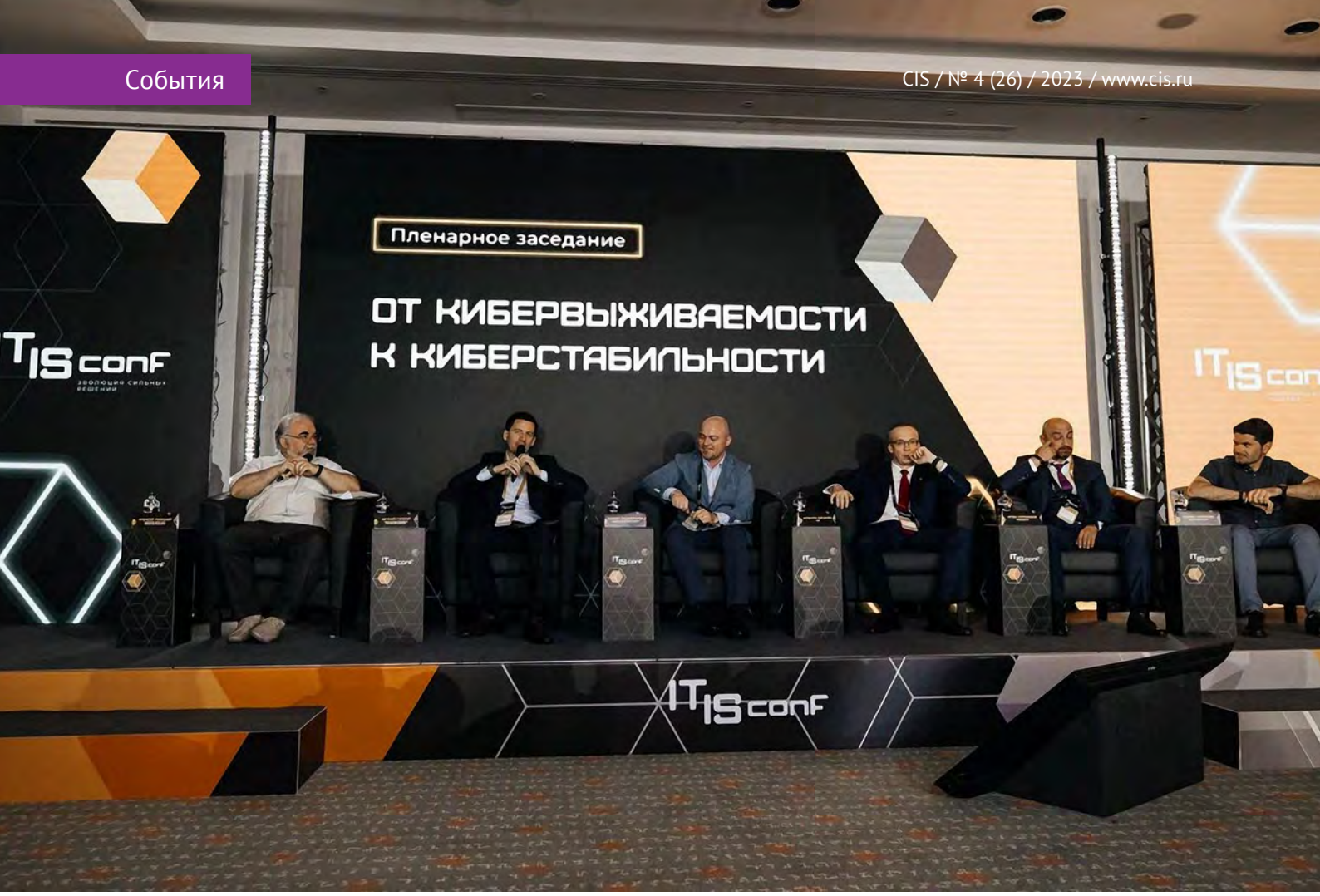
Денис Белослюдов, директор департамента специальных проектов A2, представил присутствующим разработку своей компании – проект «Медиаизмерения», который помогает представителям телеиндустрии получить объективную статистику по зрителям: их социальному портрету, возрасту, месту жительства и прочим аспектам. По его словам, выбор отечественного производителя помог избежать последствий ухода иностранных вендоров. Таким образом, A2 сыграла на импортоопережение. Белослюдов подчёркивает, что используемая аналитика больших данных помогает проводить высокотаргетированные рекламные кампании на рынке диджитал-рекламы.

В финале мероприятия организаторы вручили экспертам памятные подарки от телекомпании «Первый ТВЧ». Затем деловое общение продолжилось в зоне для нетворкинга, которая работала в течение всего форума.

Дмитрий Матвеев, Мария Кузнецова

Смотрите запись онлайн-трансляции «TeleMultiMedia Forum 2023» по ссылке: youtu.be/zoCYZ_frz68

Читайте текстовую трансляцию с форума в Телеграм-канале TMT Channel.



Главные тенденции в сфере информационных технологий и кибербезопасности

На конференции IT IS conf экспертное сообщество обсудило главные тенденции в сфере информационных технологий и кибербезопасности

14 июля в рамках крупнейшей конференции о тенденциях в ИТ и ИБ IT IS conf эксперты по кибербезопасности страны обсудили актуальные вопросы импортозамещения, кадрового голода, увеличения количества кибератак, а также стратегической важности разработки отечественных решений. В этом году мероприятие вышло на новый уровень: на конференции собрались ведущие специалисты в сфере кибербезопасности со всей страны, а также представители органов государственной власти.

Участников IT IS conf ждали пленарные заседания, презентации новых решений, практические кейсы и большая выставочная зона отечественных производителей.

Деловая часть конференции началась с планёрного заседания, в ходе которого эксперты отметили, что подход к информационной безопасности (ИБ) существенно изменился. Сегодня большинство компаний стали активно выделять ресурсы на защиту информации, обучение сотрудников, а также взяли курс на создание полноценных отделов по управлению ИБ.

Валентин Богданов, генеральный директор УЦСБ: *«Основное изменение в том, что информационная безопасность для наших заказчиков из виртуальной проблемы превратилась в реальную угрозу. Если раньше массовые атаки и проникновения для нас были чем-то далёким, то сейчас это реальность, в которой мы все живём.*

Кроме того, всё актуальнее становится услуга «безопасность как сервис». Мы понимаем, что без профессионалов, которые умеют качественно расследовать инциденты информационной безопасности и разбирать их последствия, просто невозможно развиваться».

Михаил Пономарьков, министр цифрового развития Свердловской области, подтвердил слова Валентина Богданова и отметил, что в Правительстве Свердловской области ведётся активная работа по реализации централизованной модели управления ИБ.

Также **Михаил Пономарьков** добавил, что на текущий момент в Правительстве Свердловской области функционирует полностью импортозамещённый ЦОД.

Артём Калашников, управляющий директор Центра информационной безопасности дочерних и зависимых обществ АО «Газпромбанк»: *«Почти половина из того набора средств, которые мы использовали, превратились в «кирпич». Многие продукты удалось быстро заменить, но довольно много решений, которые нам всё ещё приходится импортозамещать».*

Эльман Бейбутов, директор по развитию продуктового бизнеса Positive Technologies, отметил, что самое сложное при переходе на отечественные решения – это поменять самих себя и те процессы, которые годами запускались и налаживались.

В ходе обсуждения вопроса импортозамещения **Валентин Богданов** отметил, что самый низкий его уровень реализован в сфере радиоэлектронной и микроэлектронной продукции и составляет всего 5–10%, однако уже предпринимаются серьёзные шаги для решения этой проблемы. Так, на «ИННОПРОМ-2023» было подписано соглашение между Минпромторгом, Минобрнауки и УрФУ о создании партнёрства в сфере развития и кадрового обеспечения электронной промышленности.

Евгений Гурарий, помощник полномочного представителя Президента Российской Федерации в Уральском федеральном округе, поднял вопрос кадрового голода.

«Вопрос кадров в сфере информационной безопасности – самый проблемный во всей ИТ-отрасли. В текущих реалиях идёт колоссальная борьба за высококвалифицированных сотрудников. Кадровый вопрос стал большим вызовом и для компаний, и для университетов. Могу сказать, что в УрФО мы очень активно работаем над решением данной проблемы»,– отметил Евгений.

По итогам пленарного заседания спикеры единогласно пришли к выводу, что «безопасникам» необходимо думать на несколько шагов вперёд и выстраивать стратегию защиты, направленную на минимизацию возможных рисков.

Кроме того, были выделены главные цели киберпреступников в 2023 году ввиду высокой важности: КИИ, АСУ ТП и системы автоматизации.

IT IS conf – крупнейшая на Урале конференция в сфере информационных технологий и информационной безопасности. В этом году в конференции приняло участие более 600 человек – экспертов в сфере информационных технологий и безопасности со всей страны, руководителей ИТ-компаний, глав профильных министерств и представителей бизнес-структур. Организатором события стал Уральский центр систем безопасности. Мероприятие проводится при поддержке министерства цифрового развития и связи Свердловской области.

В числе партнёров конференции ведущие российские ИТ-компании: «Аквариус», Positive Technologies, МегаФон, Netwell, UDV Group, «Яндекс 360» и другие.

CIS / № 4 (26) / 2023 / www.cis.ru

Почему сегодня невозможно обойтись без электронного кадрового документооборота?

Пандемия ввела тренд на удалённую работу и полностью изменила привычный формат офисной работы. Бизнес и даже государственные структуры уже не могут обойтись без цифровизации документооборота.

Это позволяет сотрудникам даже из разных точек мира обмениваться корпоративными документами в электронном виде. Правда в России этот процесс находится пока на стадии внедрения. В статье мы разберём, почему стоит перейти на электронный кадровый документооборот и какие перспективы он открывает для организаций.

Что даст бизнесу кадровый ЭДО

Сейчас всё больше организаций переходят на электронный кадровый документооборот, но многие из них всё ещё не избавились от бумажной волокиты и нерационально тратят время, трудовые ресурсы и денежные средства. Приложение Nopaper сможет окончательно развеять сомнения таких компаний.

Преимущества Nopaper

1. **Меньше расходов**

ЭДО сокращает затраты на бумагу, оргтехнику, содержание архивов и доставку документов. А для защитников экологии – это ещё и плюс 100 к карме.

2. **Оптимизация времени**

Избавив своих сотрудников от бюрократии, вы сделаете для них лучший подарок. Они будут тратить меньше времени на составление, согласование и подписание документов.

3. **Порядок в документах**

Важные файлы не теряются и всегда находятся в облачном хранилище, а это ещё и сохранит нервы сотрудников при поиске нужных документов. При этом ошибки сводятся к минимуму.

4. **Маршруты подписания и согласования**

Приложение позволяет настраивать маршруты подписания и согласования, менять их в процессе работы с документом, назначать права и роли сотрудников. Вы можете отправлять ссылку на подписание документа и приглашения в любой мессенджер.

5. **Техподдержка за 2 минуты**

Служба заботы о клиентах решает задачи пользователей в среднем за 2 минуты. А ещё платформа проводит обучение сотрудников для лёгкого перехода на кадровый ЭДО.

Nopaper – кадровое ЭДО с бесплатной мобильной подписью сотрудникам за 90 секунд.

Платформа позволяет упрощать работу с ИП/ООО, самозанятыми, сотрудниками и нерезидентами. Приём на работу больше не будет долгим и изнурительным бюрократическим процессом, что облегчит жизнь как руководителю, так и потенциально новым сотрудникам. К тому же в приложении хранятся встроенные усиленные подписи: СМС-подпись, НЭП и КЭП. Сотрудникам не придётся досаждать руководителю и бегать за ним, чтобы получить подпись. Эта проблема решится нажатием одной кнопки. При этом нет риска утечки информации. В приложении создаются ключи подписи и хранятся в зашифрованном виде.

Подпись Nopaper обеспечивает:

- **Безопасность**

Алгоритмы приложения позволяют управлять авторством, обеспечивают целостность документа и контролируют устройство. Никаких форс-мажоров и непредвиденных обстоятельств.

- **Скорость**

Для получения подписи достаточно скачать приложение, пройти онлайн-верификацию и подписи в вашем смартфоне. Это займёт 5 минут, что в 3 раза быстрее большинства сервисов. А чтобы перейти на кадровый ЭДО, вам понадобится от 10 дней вместо 2–3 недель.

- **Юридическая значимость**

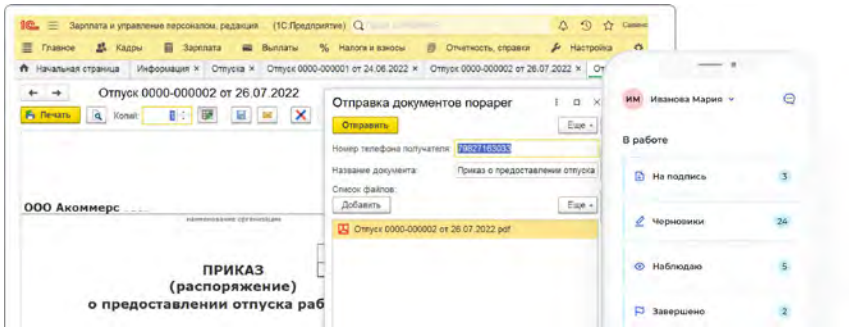
Согласно ФЗ №63 документ, подписанный электронной подписью,

Подписание 99% кадровых документов

- Оффер и изменения к нему
- Заявление на выдачу справки 2-НДФЛ
- Заявление на перечисление ЗП по реквизитам
- Заявление о подключении к ЗП проекту
- Согласие на обработку данных
- Согласие на фото и видео съемку
- Лист ознакомления с ЛНА
- Трудовой договор
- NDA
- ДС к ТД
- Приказ о переводе
- Заявления на оплачиваемый/ неоплачиваемый день
- Приказ на отпуск
- Заявление на командировку
- Отчет о командировке
- Служебные записки на премии

Оформляйте и подписывайте документы в одном окне

Отправляйте документы из 1С.
Сотрудник их получит и подпишет в Noparer.
Все подписанные документы будут доступны в Noparer и 1С.
Интеграция займёт 1 день

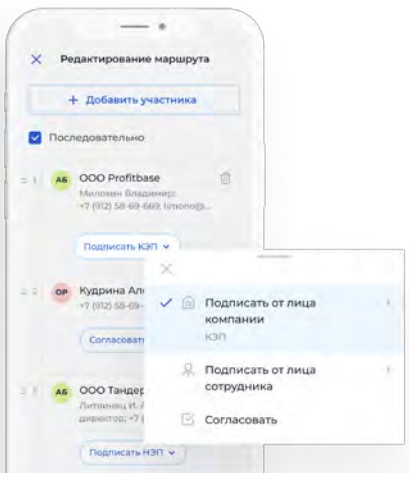


Маршруты подписания и согласования

ЮЛ, ИП, ФЛ и сотрудники

Мультипрофиль — ЭДО всех ваших юридических лиц в одном приложении.

- Добавляйте сколько угодно участников в маршрут
- Создавайте внутренние и внешние маршруты
- Подписывайте НЭП или КЭП, согласовывайте и делегируйте из маршрута
- Добавляйте, меняйте, удаляйте участников маршрута
- Напоминайте, комментируйте, отслеживайте



имеет юридическую силу. До его подписания стороны заключают соглашение об ЭДО в приложении, в котором признают ЭП аналогом собственноручной подписи.

Noparer объединяет внутренний и внешний документооборот в одном приложении

1. **Кадровый ЭДО**

Наводит порядок в кадровых внутренних документах. Если срочно нужен новый сотрудник, вы можете привлечь удалённого специалиста и оформить его через приложение Noparer всего за 1 день.

2. **ЭДО с контрагентами**

Через платформу можно легко и быстро подписать договор с партнёрами. Для этого не придётся настраивать роуминг или устанавливать ПО. Документооборот больше не будет тормозить срочные проекты.

3. **ЭДО с самозанятыми**

Вы сможете привлекать перспективные кадры из любой точки страны. Приложение позволяет оформлять фрилансеров без ограничений и бумажной волокиты.

С Noparer всё по закону и надёжно

Когда вы подписываете документы через Noparer, то наделяете их той же юридической силой, что и при подписи на бумаге, согласно п. 2 ст. 6 закона «Об электронной подписи». Такие документы примут даже в суде и в налоговой. Это подтверждает и Гражданский кодекс: письменная форма сделки считается соблюдённой при использовании сторонами аналога собственноручной подписи (ст. 160 ГК РФ). Этим аналогом и является электронная подпись, в том числе усиленная неквалифицированная подпись, сокращённо – НЭП.

Такая подпись в Noparer позволяет определить личность человека и проверить, вносили ли в документ изменения после его отправки. А криптографическое преобразование подписи обеспечивает надёжность и безопасность корпоративных данных.

Есть дополнительное требование, чтобы документы, подписанные НЭП, имели юридическую силу, способ их подписания должен быть прописан в соглашении об использовании электронной подписи. Это значит, что для использования электронной подписи вы должны зафиксировать, что

именно будет являться актом подписания, и согласовать это с контрагентом.

Nopaper учитывает данное требование:

1) при регистрации вы присоединяетесь к оферте – пользовательскому соглашению, в которой использование подписи Nopaper признаётся аналогом собственноручной подписи;
2) до обмена документами с контрагентами вы заключаете с ними Соглашение о правилах использования подписи и взаимном признании её юридической силы.

В Nopaper можно подписать 99% документов: трудовой договор, приказы, заявления. Исключения: приказ об увольнении, журналы инструктажей по охране труда и акт о несчастном случае на производстве. Их по закону нужно оформлять или дублировать на бумаге. Большинство организаций уже оценили преимущества электронного документооборота. Средняя оценка пользователями Nopaper – 4,8. Документы можно загружать как со смартфона, так и в удобном личном кабинете на ПК. Nopaper позволит оптимизировать бизнес-процессы, упростив документооборот. Платформа избавит от бумажной волокиты и ненужных затрат, что повысит эффективность работы вашей организации.

Отзывы заказчиков

На отправку документов по Москве уходило 500 рублей, а по регионам – 1000. Ждать документы приходилось неделю. Поэтому хотелось сократить время и расходы на документооборот, а также протестировать сервисы ЭДО, и в дальнейшем более уверенно перейти на кадровый электронный документооборот.

Ольга Кузьмина, директор Manpower

Благодаря сервису Nopaper процесс удалённой выдачи агентам мобильной подписи и обмена документами со смартфона стал ещё проще и эффективнее. Системой уже пользуются 1300 наших агентов и подключаются новые. С помощью Nopaper мы подписываем с ними акты, дополнительные соглашения к договорам.

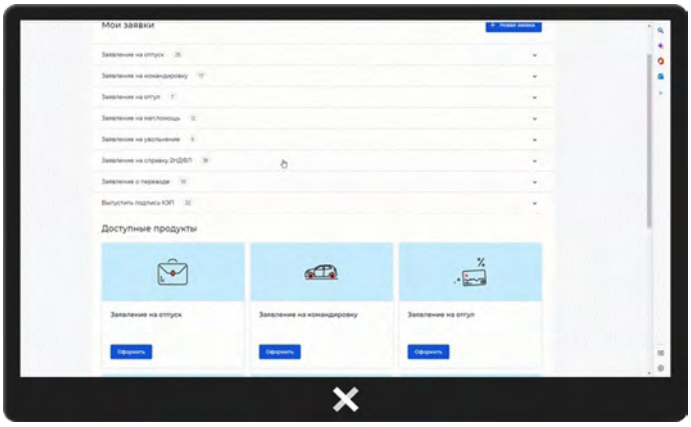
Екатерина Долгова, руководитель проекта «Цифровая агентская сеть» Департамента розничных продаж «АльфаСтрахование»

nopaper

ООО «Акоммерс»

nopaper.ru

Личный кабинет сотрудников



Для чего ещё подойдёт Nopaper

- Курьерским службам
- Промышленности
- Лизинговым компаниям
- Медицинским компаниям
- Платформы онлайн-образования
- Агентствам недвижимости
- Телекомам
- Аутстаф-компаниям
- Автохолдингам
- Страховым компаниям

Возможности клиентов с Nopaper

До 60% дешевле документооборот

Не нужно платить за:

- Электронную подпись каждый год
- Бумагу, оргтехнику
- Содержание архивов

До 50% экономия рабочего времени

Больше не нужно:

- Печатать документы
- Подписывать стопки бумаг
- Ездить в офис ради подписания бумаг

В 10 раз быстрее бизнес-процессы

- Выпуск подписи за 5 минут
- Подписать сотню документов можно в один клик
- Статус документа видно онлайн

Принципы ESG

Для 400 стандартных пачек бумаги требуется 24 дерева.

Переход на электронный документооборот это не только про экономию.

Как войти в ИТ

Сейчас это самый популярный вопрос.

Меня зовут Петелина Ангелина, мне 21 год, и я Fullstack-разработчик с опытом более 3-х лет. Чемпион России WorldSkills 2022, сертифицированный эксперт WorldSkills и соучредитель веб-студии в Москве.

Я прошла путь от фриланса и работы в компании до создания своей веб-студии, и поделюсь о сложностях, которые встречаются в начале пути.

1. Образование. Много мнений ходит по этому поводу. В 2022 году я устроилась на первую работу junior-разработчиком за 90 тыс. в месяц, имея только опыт на фрилансе и незаконченное среднее специальное образование. В большинстве компаний смотрят только на практические знания и опыт работы. После чего за год поднялась до уровня middle.
2. Знание математики и английского. В школе я была чистым гуманитарием (точнее, я так думала), и с математикой у меня всегда было плохо. В ИТ она нужна, но на простейшем уровне, если речь не идёт об области ИИ. Нужно иметь алгоритмическое мышление, остальное не так важно. Английский нужен больше, потому что большинство документации на английском языке, но высокий разговорный уровень на начальных этапах не понадобится.
3. Самое забавное, что я встречала, это удивлённые взгляды людей при виде красивой девушки айтишницы. У многих остался стереотип образа айтишника. Но сейчас всё поменялось, и в эту профессию может войти любой! Поэтому никогда не ограничивайте себя стереотипами. Нет определённого типажа людей, кому дана эта профессия или не дана.
4. Курсы. Многие думают, что, пройдя 3-х месячный курс, можно сразу устроиться на должность мидла с высокой зарплатой. Но это не так. Программирование так же, как и другие профессии, требует долгого изучения и роста. А сейчас множество сертификатов сомнительных курсов, наоборот, настораживают работодателей.

Если вы новичок в этой сфере и не знаете, как начать, то:

1. Если учитесь в школе/колледже, поступите по окончании в технический ВУЗ. Это даст хороший толчок для старта в сфере ИТ.
2. Если у вас уже есть профильное образование, изучите все сферы и профессии, которые есть в ИТ. Не всегда нужно быть именно программистом и кодить в этой сфере. Есть такие направления, как дизайн, менеджмент проектов и т. д.
3. После выбора направления найдите различные курсы в интернете. Советую рассмотреть курсы от институтов, например МГТУ им. Баумана или ВШЭ. Есть хорошие обучения от компаний-миллионников, например Яндекс или Сбер. Помните, что вам придётся много изучать самостоятельно, читать информацию в бесплатных источниках и смотреть видео на Ютубе. Любое обучение даст хорошую базу, но большая часть в ваших руках.
4. Участвуйте в различных конкурсах, хакатонах и выставках. Это поможет обрести связи и проявить навыки, что увеличит шансы дальнейшего трудоустройства.
5. По окончанию курсов, рассмотрите стажировки от крупных компаний, попробуйте выйти на фриланс и начните проходить собеседования. Проходите собеседования на уровни выше вашего, даже если не возьмут на работу, вы получите опыт и узнаете, к чему нужно быть готовыми.
6. Никогда не отчаивайтесь и не опускайте руки, если поиск первой работы/стажировки затянулся слишком надолго. Опытные программисты тоже могут искать работу месяцами.

ИТ очень интересная и перспективная, но в то же время сложная сфера, которая требует усидчивости и внимательности. Не стоит в неё идти только потому, что она популярная или из-за хорошего заработка. Эту сферу, как и любую другую, надо любить, чтобы достигнуть в ней высот.

Ангелина Петелина

Анализ проверки возраста: технологии и компромиссы

FUTURE OF PRIVACY FORUM

Подтверждение возраста – это широкий термин для методов определения возраста или возрастного диапазона человека. Не существует универсального метода определения возраста, и важно учитывать контекст, чтобы определить пропорциональный метод для каждого конкретного случая использования.

Соразмерность является ключевым фактором, поскольку в некоторых контекстах уместен более высокий уровень определённости. Это должно быть тщательно сбалансировано с рисками конфиденциальности и риском запрета доступа к законному контенту, особенно если ограничения на контент оказывают несправедливое воздействие. Возможно, будет целесообразно использовать несколько методов в рамках многоуровневого подхода.

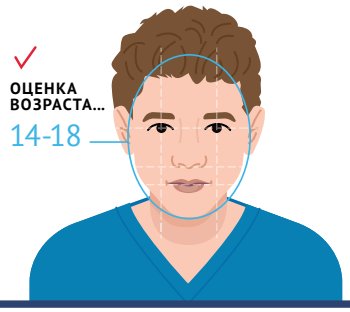
СУЩЕСТВУЮЩИЕ И НОВЫЕ МЕТОДЫ

ДОГОВОР
УКАЗАНИЕ ВОЗРАСТА

Пользователь указывает дату рождения, не предоставляя подтверждающих доказательств. Этот распространённый метод наиболее подходит в ситуациях низкого риска, поскольку дети и подростки часто обходят его стороной, указывая ложную дату рождения. Риск для конфиденциальности невелик, особенно если даты рождения не сохраняются или не сопоставляются с именем или другим косвенным идентификатором.

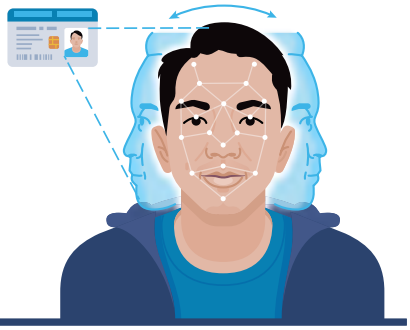
ОЦЕНКА
ОПРЕДЕЛЕНИЯ ПО ЛИЦУ

Оценивает возраст, используя изображение лица, но личность не идентифицируется. Лучше всего использовать для распределения пользователей по возрастным группам или для подтверждения, что пользователь соответствует возрастному порогу, например младше 13 или старше 21 года. Оценка менее эффективна для определения возраста в узком диапазоне, например 17 против 18.



ВЕРИФИКАЦИЯ
БИОМЕТРИЯ + УДОСТОВЕРЕНИЕ ЛИЧНОСТИ

Сопоставляет скан удостоверения личности государственного образца и фотографию или видео с использованием функции распознавания лиц. Этот метод больше подходит для услуг с более высоким уровнем риска, регулируемых или ограниченных по возрасту. Использование только удостоверения личности — один из методов, но он не обеспечивает уверенность в возрасте.



РОДИТЕЛЬСКОЕ СОГЛАСИЕ/ ПОРУЧИТЕЛЬСТВО

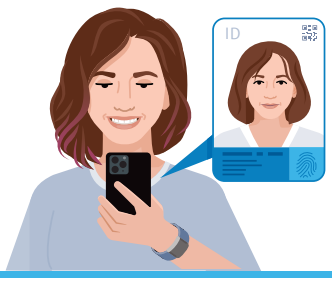
Родитель, имеющий подтверждённую учётную запись (например, с использованием удостоверения личности, кредитной карты и т. д.), указывает возраст ребёнка или подростка, предоставляя согласие или добавляя ребёнка в свою учётную запись. Это более надёжно, чем возрастные ограничения, но может повлиять на самостоятельность подростка.

ДРУГИЕ АЛГОРИТМИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ

Другие алгоритмические методы могут включать оценку возраста или возрастного диапазона на основе истории посещённых страниц, голоса или с использованием нескольких точек данных или сигналов из виртуальных игр.

ЭЛЕКТРОННОЕ УДОСТОВЕРЕНИЕ/ КОШЕЛЁК

Используя приложение wallet, пользователи добавляют один или несколько подтверждённых учётных данных для создания многоразового цифрового идентификатора, хранящегося либо на устройстве, либо в облаке. Пользователи подтверждают свой возраст с помощью сервиса, вводя код для обмена информацией, необходимой для подтверждения возраста (например, 18 лет или старше).



ВОПРОСЫ ОБ ПОДТВЕРЖДЕНИИ ВОЗРАСТА

КАКОВЫ ЦЕЛИ?

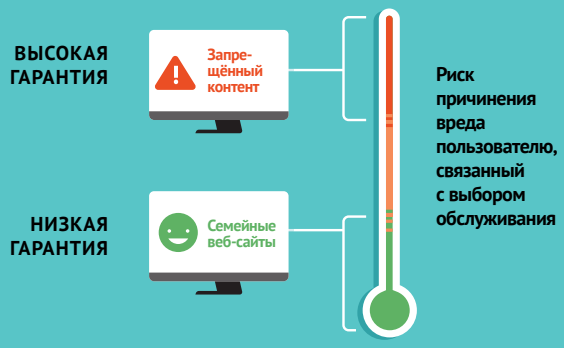
- Облегчить согласие родителей
- Ограничить доступ к услугам, предназначенным для определённого возраста, или предоставить контент, соответствующий возрасту
- Подтвердить точный возраст человека
- Разделить людей по возрастным группам (например, 13–15 лет).

КАКИЕ ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ?

Негативные последствия могут заключаться в доступе детей или подростков к услугам, контенту с ограничениями по возрасту или контактах с неизвестными лицами.

КАКОЙ МЕТОД ГАРАНТИРУЕТ НАДЛЕЖАЩУЮ ОБЕСПЕЧЕННОСТЬ?

Выберите метод или методы, которые обеспечивают уровень обеспеченности возраста (точность), пропорциональный целям и рискам услуги. Имейте в виду, что юридические обязательства могут предписывать определённый метод.



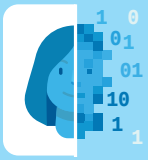
БУДЕТ ЛИ ОБЕСПЕЧЕНИЕ СБАЛАНСИРОВАНО С РИСКАМИ КОНФИДЕНЦИАЛЬНОСТИ?

После рассмотрения рисков конфиденциальности и мер по их снижению подтвердите, что цель обеспечения оправдывает уровень рисков конфиденциальности и другие последствия, связанные с выбранным методом обеспечения определения возраста.

РИСКИ ПОДТВЕРЖДЕНИЯ ВОЗРАСТА

ОГРАНИЧЕНИЕ ЗАКОННОГО ВОЗРАСТА

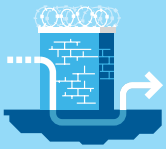
СПРАВЕДЛИВЫЙ И НЕРАВНЫЙ ДОСТУП



ПОТЕРЯ АНОНИМНОСТИ

СБОР ЛИЧНОЙ ИНФОРМАЦИИ

ОГРАНИЧЕНИЕ НЕЗАВИСИМОСТИ ПОДРОСТКОВ



ВОЗМОЖНОСТЬ ОБХОДИТЬ СИСТЕМУ

НЕОЖИДАННОЕ ИСПОЛЬЗОВАНИЕ ДАННЫХ

ИНСТРУМЕНТЫ УПРАВЛЕНИЯ РИСКАМИ

НЕМЕДЛЕННОЕ УДАЛЕНИЕ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ

РАЗДЕЛЕНИЕ ПРОЦЕССОВ ОБРАБОТКИ (3-Я СТОРОНА)

МИНИМИЗАЦИЯ ДАННЫХ

ОБРАБОТКА НА УСТРОЙСТВЕ

ПРИМЕР ИСПОЛЬЗОВАНИЯ

ПРОВЕРКА ВОЗРАСТА ДЛЯ ОНЛАЙН-ИГР

В этом сценарии 16-летний Майлз получает доступ к игровому онлайн-сервису, предназначенному для подростков и взрослых. Он имеет дополнительные функции, ограниченные по возрасту.

НАЧАЛЬНЫЙ ЭТАП

ДОГОВОР

Пользовательский интерфейс по умолчанию «ориентирован на подростков», Майлз может зарегистрироваться, указав дату своего рождения

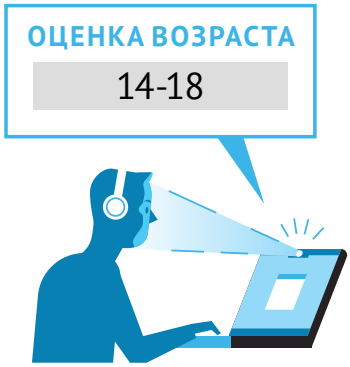
Гарантия проверки

Риск утечки персональных данных

ВТОРОСТЕПЕННЫЕ ПРИЗНАКИ

ОЦЕНКА

Позже Майлз хочет включить функцию, которую разработчик игры ограничил до 16+. Разработчик хочет получить более высокий уровень уверенности. «Живое селфи» использует характеристику лица, чтобы определить, что Майлзу от 14 до 18 лет.



Гарантия проверки

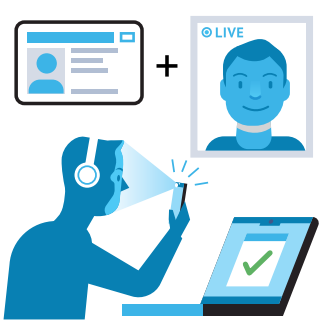
Риск утечки персональных данных

ПРИ НЕОБХОДИМОСТИ ТОЧНОЙ УВЕРЕНОСТИ

ВЕРИФИКАЦИЯ

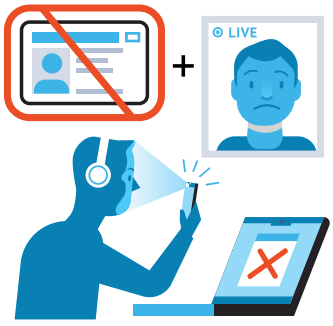
Поскольку предполагаемый возрастной диапазон включает детей, которым не разрешено использовать эту функцию (14–15 лет), необходима высокая гарантия возраста. Майлз должен отсканировать свои водительские права и сделать «живое селфи». Однако многие пользователи, в том числе 75 % 16-летних, не имеют водительских прав.

С УДОСТОВЕРЕНИЕМ ЛИЧНОСТИ



Гарантия проверки

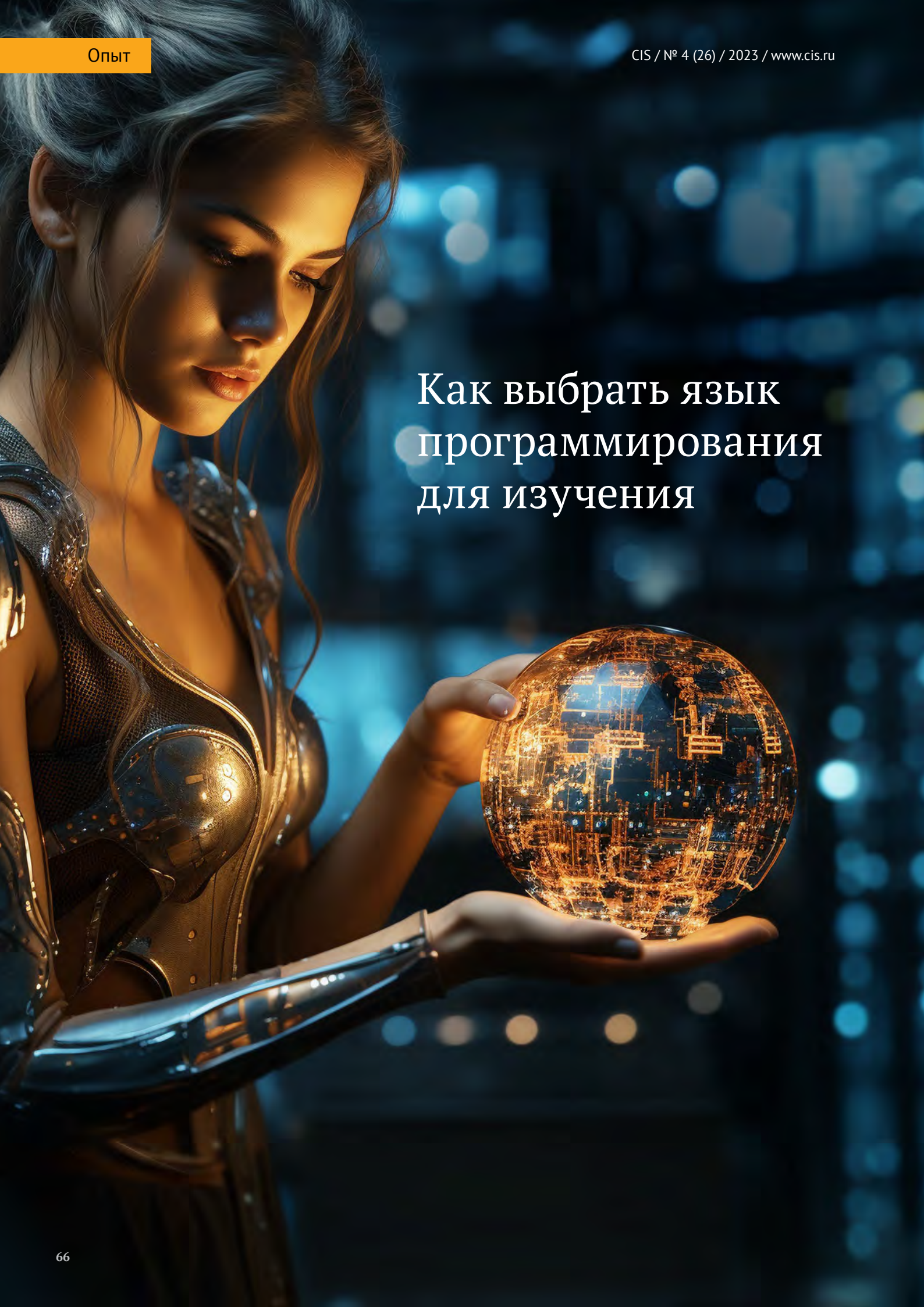
БЕЗ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ



Риск утечки персональных данных

CIS / № 4 (26) / 2023 / www.cis.ru

Как выбрать язык программирования для изучения



Данная статья будет полезна тем читателям, кто решил с нуля освоить язык программирования и на данный момент находится в активном поиске ответа на вопрос: а в какую среду программирования направить свои усилия?

Сразу ответим, что указаний на какой-то конкретный язык здесь не содержится, а все критерии выбора ориентированы на ваше субъективное мнение.

Будем рады, если несколько полезных советов помогут вам начать разбираться в данном вопросе.

Для начала обратите внимание на востребованность уже используемых программ, написанных на разных языках, ведь большинство хотят выбрать наиболее актуальный продукт. Самый простой способ сделать это – задать вопросы в поисковике: в каких кодах пишутся большинство приложений в разных областях ИТ-отрасли. Также можно попутешествовать по сайтам поиска вакансий и воочию увидеть, какие специалисты востребованы (в первую очередь в вашем регионе, далее – в стране, а если необходимо, то и в мире).

Следующий совет, если позволите, содержит предостережение: если вы решили изучать конкретный язык на волне его топового рейтинга, то имейте в виду: туда, кроме вас, на той же самой волне ринулись и другие желающие освоить написание этого кода. А потому после завершения обучения вы можете столкнуться с тем, что потенциальные работодатели в данный момент не заинтересованы в наборе начинающих программистов по этому профилю, т. к. их попросту переизбыток на рынке труда. Проекты-долгожители интернета, написанные пару-тройку десятков лет назад на таких же ранних языках программирования и сейчас бывают востребованы пользователями, просто потому, что они привычны и полностью функциональны.

Не менее важным акцентом в выборе языка программирования для начального изучения, как и в любом другом занятии, является то, что он должен быть лично для вас приятным: написание этого кода должно приносить положительные эмоции, вы должны испытывать удовлетворение от этой работы.

А когда вы определитесь с направлением будущей деятельности в ИТ-отрасли, то курсы и программы в нашем Учебном Центре CIS помогут освоить выбранную профессию.

Наши курсы предназначены как для новичков, так и для специалистов компаний и служб безопасности, работающих в сфере защиты информации.

В процессе обучения наши учащиеся получают не только теоретические знания, но и комплексные практические навыки по созданию надёжного центра информационной безопасности в своей компании.

Все курсы разрабатываются опытными тренерами в соавторстве с инженерами-практиками на основе реальных кейсов.

Учебный Центр CIS это –

- полнота учебного материала;
- содержательные лабораторные работы;
- разбор практический кейсов;
- лайфхаки от практиков.

Мы имеем лицензию Департамента образования и науки г. Москвы на право оказывать образовательные услуги. По завершению обучения учащимся выдаются именные сертификаты.

Приходите на наши курсы, и пусть на этом поприще вам сопутствует удача!

CIS Учебный Центр

cis.ru/courses

Учебный курс по продукту JMS 3.7

Цель данного курса – познакомить слушателей с системой управления жизненным циклом ключей и смарт-карт JaCarta Management System версии 3.7 от компании «Аладдин Р. Д.».

Задачами курса являются:

- сделать обзор ключевых носителей, производимых компанией «Аладдин Р.Д.»;
- познакомить слушателей с жизненным циклом ключевых носителей;
- показать процесс развёртывания JMS;
- познакомить слушателей с ключевыми настройками JMS;
- разобрать основные сценарии работы JMS;
- познакомить слушателей с процессом технического сопровождения JMS после внедрения.

Объединяя опыт

СОБИНТЕГРА

«Современная Интеграция»

- Проектирование
- Внедрение
- Разработка документаций
- Сопровождение

CIS Современные Информационные Системы

«Современные Инфосистемы»

- Разработка авторских курсов
- Проведение курсов
- Чтение авторских курсов

Курс по JaCarta Management System

- Разработан опытными тренерами
- В соавторстве с инженерами-практиками
- На основе реальных кейсов
- Полнота учебного материала
- Содержательные лабораторные работы
- Разбор практический кейсов
- Лайфхаки от практиков

Содержание курса

1. Введение в курс «Система управления жизненным циклом ключей и смарт-карт JaCarta Management System 3.7».
2. Обзор ключевых носителей.
3. Жизненный цикл ключевого носителя.
4. Архитектура и варианты развёртывания JMS.
5. Развёртывание JMS.

Лабораторная работа №1. Развёртывание сервера JMS.

6. Интерфейс сервера JMS.
7. Интерфейс консоли управления JMS.

Лабораторная работа №2. Настройка JMS для выпуска цифрового сертификата с Microsoft CA.

8. JMS клиент.
9. Типовые задачи сопровождения.

Учебный комплект

В учебный комплект входят следующие материалы:

- учебное пособие;
- ключ JaCarta PKI в формфакторе XL;
- ключ JaCarta PKI в форм-факторе Nano

Требования к слушателям курса

Слушатели курса должны обладать следующими знаниями и навыками:

- знание Windows Server 2012 или выше на уровне продвинутого пользователя, что включает понимание принципов:
  - работы домена Windows (Active Directory);
  - работы центра сертификации Microsoft (MSCA);
  - построения инфраструктуры открытого ключа (Public Key Infrastructure — PKI);
- знание Windows 10 на уровне пользователя;
- знание и понимание принципов работы MS SQL Server 2014.

Контакты и запись

По завершению обучения вам выдадут именной сертификат о прослушивании курса по JaCarta Management System.

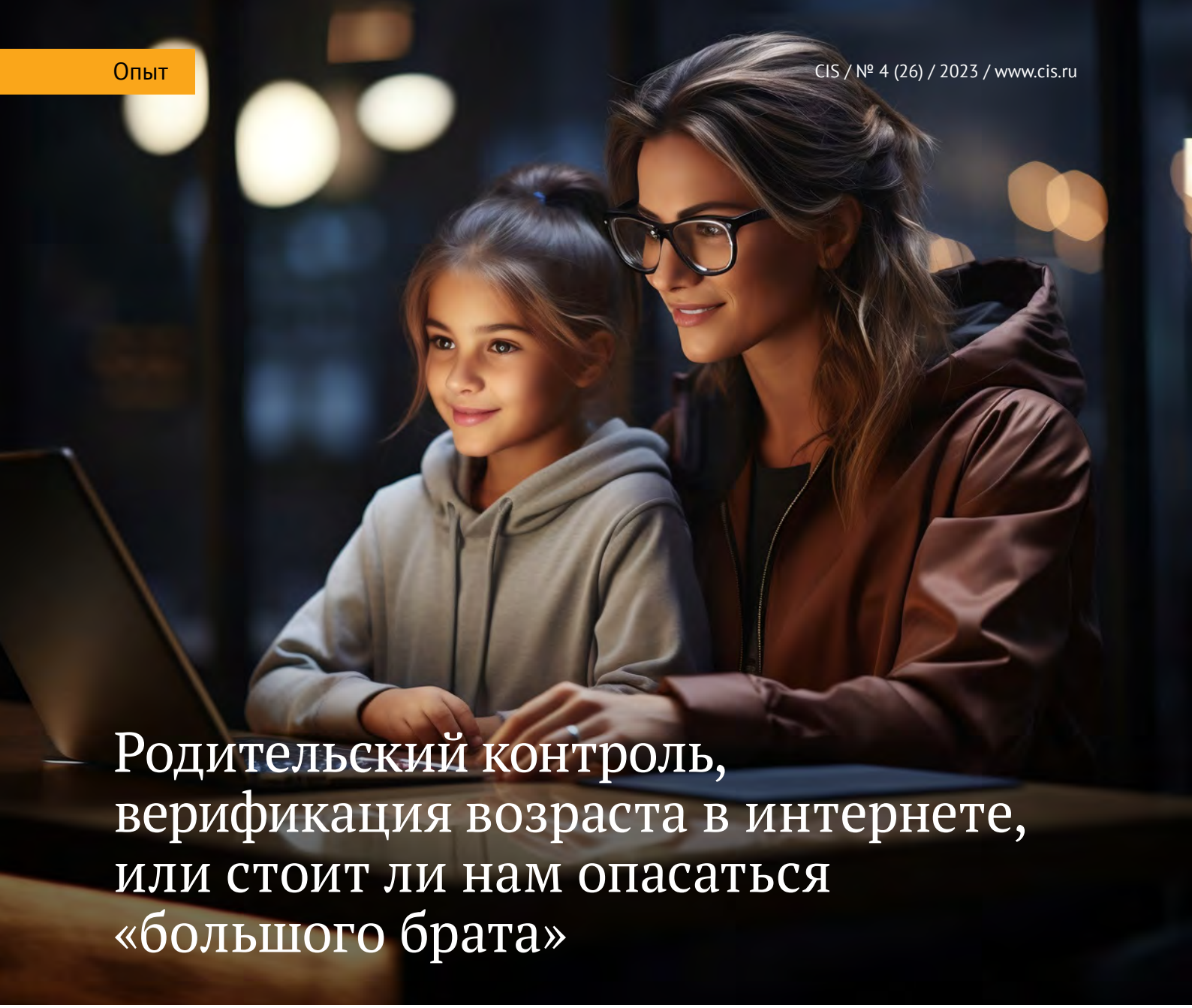
С вопросами и предложениями можно обратиться, написав на электронный адрес education@cis.ru.

Лицензия департамента образования и науки города Москвы № 041137 от 30 ноября 2020 года.

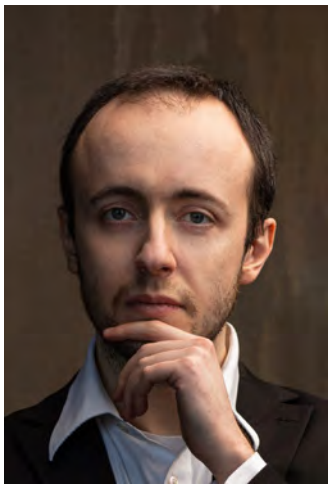
CIS Учебный Центр

education@cis.ru
cis.ru/courses

CIS / № 4 (26) / 2023 / www.cis.ru



Родительский контроль, верификация возраста в интернете, или стоит ли нам опасаться «большого брата»



Гусейнов Рустам
эксперт АИС, председатель кооператива специалистов по кибербезопасности «РАД КОП»

Рассматривая вопрос безопасности наших детей в цифровом мире, автор предлагает задуматься над более широкими вопросами приватности (privacy) и соблюдения прав человека в эпоху тотальной прозрачности, больших данных и ИИ. Стоит ли нам бояться и не доверять подобным технологиям? Или всё дело в умении правильно пользоваться соответствующим инструментарием?

Я хочу начать с простой мысли: люди не равны. Чтобы доказать это, можно обойтись без сложных теорий стратификации людей по уровням интеллекта в духе Элиота Джекса (см. концепцию Requisite Organization) и просто вспомнить, что за абстрактными «людьми» скрываются взрослые и дети, мужчины и женщины, здоровые, больные, временно недееспособные и даже преступники. И в моменте, когда мы забываем об этих различиях и из самых лучших побуждений начинаем руководствоваться максимами в духе «свободы, равенства и братства», могут происходить не самые приятные вещи, уже не раз случавшиеся под подобными прекраснодушными лозунгами. Поэтому некоторые ограничения людьми прав, свобод и зон ответственности друг друга – абсолютно нормальное явление, без которого невозможно создать ни семьи, ни организации, ни более крупного человеческого общежития.

С другой стороны, нельзя забывать о правах человека, о том, что каж-

дый из нас – субъект или может стать таковым в процессе собственного развития, что ограниченный сегодня в правах ребёнок когда-то должен стать взрослым. Нужно помнить, что развитие субъекта происходит через деятельность, через практический опыт реализации этой субъектности, а значит, если всегда и всюду контролировать ребёнка, он… не вырастет!

Не случайно лучшие представители человечества тысячи лет боролись за утверждение в качестве культурных норм концепций в духе прав человека, свободы совести, тайны частной жизни. Не случайно рабство, сословное общество или неравенство в правах воспринимались ими как глубочайшая трагедия нашего общества. Ведь за равенством базовых прав скрывается глубочайший смысл, а именно создание такой общественной конструкции, которая наилучшим из возможных способов в любой момент времени реализует интересы как целого общества, так и уникального, индивидуального микрокосма, которым является каждый человек как субъект, как личность.

И через оптику этого диалектического единства личного и общественного, свободы и ограничений вопросы родительского контроля превращаются из какой-то абстрактной борьбы чёрного и белого в понятный и конкретный процесс внедрения таких мер защиты, которые не вредя индивиду (ребёнку), ещё не обладающему всей полнотой прав в связи с его недостаточным уровнем интеллектуального, физического и духовного развития – опять таки сошлёмся на выше упомянутого Джекса – тем не менее не лишат этого индивида важнейших свобод, в том числе свободы развития и самореализации и закономерного выхода в какой-то момент из под родительской опеки. А здесь, с точки зрения автора, важны как

а) чёткие рамки и масштабы такого контроля *(например, законодательное ограничение продолжительности применения подобных мер 14 годами: достиг ребёнок подросткового возраста, значит, родительский контроль отменяется, т. к. это уже не вполне ребёнок, а уже более зрелый субъект правоотношений, с которым надо взаимодействовать как с более автономной личностью)*;
так и
б) существование независимого арбитража конфликтных ситуаций и программ повышения осведомлённости о путях их разрешения для детей и родителей *(например, суды, школьные советы, программы взаимодействия профессиональных педагогов, разбирающихся в детском развитии с семьями, т. е. такие институты, которые, с одной стороны, защищают право детей в какой-то момент превратиться в независимые личности, а с другой – проводят повышение осведомлённости родителей об оптимальных вариантах реализации этого пути)*.

И когда мы смотрим на эти вопросы таким образом, то возникает принципиальная аналогия с огнём, ножом или колесом. Да, огнём можно обжечься, ножом – зарезать, а колесом – раздавить, но должны ли мы отказываться от горячей пищи, салатов или автомобилей из-за некоторого количества неадекватных людей? Или мы должны стремиться расширить уровень подготовки всех людей, минимизировать сценарии неправильного использования инструментов, а также разработать подходы к реагированию на возникающие инциденты для их оперативного устранения?

Лично я голосую за второе, потому что, как убедительно доказывает антропология (см. в частности популярную книгу Ю. Харири Sapiens), без научно-технического прогресса и его гуманного внедрения в нашу жизнь мы как вид и цивилизация уже давно если бы не вымерли, то во всяком случае влачили бы не самое приятное полуголодное и полубольное существование. Без письменности, развитой культуры и всех тех возможностей, которые дал нам прогресс. Да, у прогресса есть свои тёмные стороны, но с ними можно работать. Как говорил кто-то из древних: «Всё есть яд, и всё есть лекарство в зависимости от дозы».

В этой парадигме все возможные частные риски, в том числе популярные в силу законодательных повесток проблемы утечек данных, подмены цифрового профиля гражданина, вопросы манипуляции сознанием с помощью профилирования интересов человека, ИИ и контекстной рекламы – все эти риски и проблемы меркнут перед главным фундаментальным вопросом: кем и в чьих интересах контролируются эти инструменты. Вряд ли кто-то будет спорить с тем, что в вопросах формирования здоровой личности сам ребёнок не компетентен и может не справиться с саморазвитием без помощи взрослых (а до некоторого возраста, в принципе, не может, как не могут дети Маугли освоить язык вне общества взрослых людей, оставаясь «волками и обезьянами»). И вряд ли кто-то будет отрицать, что интернет с огромным количеством не только полезной и высококультурной информации, но и различного насилия, порнографии и просто некачественного контента является не только «лекарством, но и ядом». Поэтому без ограничений и контроля нельзя обойтись, но эти ограничения и контроль должны служить обществу, и общество должно иметь возможность корректировать параметры этого контроля, менять его продолжительность или формат. В противном случаем мы можем оказаться в ситуации «цифрового концлагеря», прекрасно показанного в кинофильме «Особое мнение» Стивена Спилберга, где подобная система в конечном итоге из общественного достояния превратилась в инструмент манипуляций обществом в интересах узкого круга лиц.

Для меня нынешняя история с постепенным отмиранием конфиденциальности (privacy), родительским контролем и обществом всеобщей прозрачности не является проблемой само по себе: в конце концов, все наши предки жили в деревнях и общинах в небольших группах, где от внимания товарищей не ускользал ни один, даже самый интимный человеческий шаг. И, с этой точки зрения, те возможности, которые даёт нам цифровизация, и те процессы контроля, которые она пробудила к жизни, в каком-то смысле являются возвратом к этому «общинному состоянию», только теперь не в масштабах села на сто человек, а в масштабах глобального мира или по крайней мере отдельно взятой страны. Проблема возникает только там, где из-за неравенства различных групп людей в возможностях контроля и из-за отсутствия общественного надзора, такие инструменты из модерируемых обществом, служащих интересам его развития, превращаются в способ манипуляций и деструктивного ограничения свобод одними людьми других.

Барби в мире ИТ: знакомство с ИТ-конкурсом красоты «Beauty&DigITal-2023»

Мы неслучайно сравнили девушек, работающих в ИТ, с Барби. Это не просто кукла, символизирующая красоту и совершенство, как все привыкли её воспринимать. Именно эта «игрушка» заставила весь мир по-новому взглянуть на женщин.

В то время как общество «позволяло» им заниматься лишь домашними делами и зависеть от мужей, Барби активно осваивала «неженские» профессии: она была космонавтом, режиссёром, пилотом, физиком и даже кандидатом в президенты. Барби не боится стереотипов и чужих мнений, она смело идёт вперёд к своим мечтам и целям.

Именно такие женщины работают сегодня в ИТ: смелые, творческие и амбициозные. Вот уже пятый год наша редакция проводит Всероссийский ИТ-конкурс красоты «Beauty&DigITal-2023», чтобы показать всей стране, что женщины-айтишницы – это не просто «красивые куклы», а настоящие профессионалы своего дела, которые могут смело составить конкуренцию любому мужчине.

«Beauty&DigITal-2023» – это новый взгляд на женщин в мире ИТ

Чем наш конкурс отличается от сотни ему подобных? А тем, что участницы на нём проживают целую историю подготовки длиною в год. На пути к финалу их ждут различные мастер-классы от моды до журналистики. Девушки пробуют себя в разных ролях. Сегодня они раскрывают свою нежность и творчество, собирая композиции из сухоцветов, а уже завтра – стреляют из лука, чтобы снять ролик о своём хобби. Это настоящее реалити-шоу. Пройдя такой долгий путь трансформации и работы над собой, девушки выходят на сцену финальной церемонии совершенно новыми людьми.

Все участницы талантливы и уникальны по-своему, они такие разные и порой приятно непредсказуемые. Но есть кое-что, что их объединяет,– это желание прожить собственную сказку и почувствовать себя настоящей принцессой, той самой Барби. И наша редакция сделает всё, чтобы не только страна взглянула на них по-другому, но сами девушки почувствовали себя особенными. Ведь так долго участницы трудились, чтобы доказать всем, что они – профессионалы и достойны работать в этой сложной отрасли цифровых технологий. А теперь настало время напомнить им, что они ещё и прекрасные женщины.

Миссия конкурса – выявить самых достойных ИТ-девушек на звание «Мисс Beauty&DigITal» и сделать из обладательницы короны символ информационных и цифровых технологий России. И уже этой осенью состоится финальная церемония, на которой мы узнаем имя счастливой победительницы – нашей новой ИТ-королевы.

Как организаторы мы можем бесконечно говорить о своём «дитя», ведь так любим этот проект и вкладываем в него душу. Но лучше всего о самом конкурсе поведают его победительницы прошлых лет. Мы попросили участниц «Beauty&DigITal-2022» поделиться своими впечатлениями от подготовки к мероприятию.


Анна Хлюстова

Мисс Beauty&DigITal-2022 Анна Хлюстова

Как Вы смогли совмещать успешную карьеру в сфере информационных технологий с участием в конкурсах красоты во время его проведения? Какие аспекты Вашей личности и профессиональных навыков помогают достигать успеха в обеих областях?

С помощью информационных технологий мы помогаем себе сами! Ведь именно благодаря им у меня появилась возможность работать удалённо. Мне не приходится тратить время на дорогу до офиса, и появляется дополнительное время для своих проектов, в том числе конкурса «Beauty&DigITal-2022». Успехов во многих сферах жизни, не только про-

фессиональной, мне помогают достигать многозадачность и мобильность. Я легко умею переключаться из «режима профессионала» в «режим леди» и обратно, а также для меня не составляет проблем поработать или, например, выполнить задание конкурса вне дома.

В чём заключается Ваша наибольшая мотивация и страсть к информационным технологиям? Какие проекты или достижения в этой области Вас наиболее вдохновляют?

Моя главная мотивация – помощь людям в оптимизации различных процессов и реализация возможности получать услуги и информацию максимально понятно, удобно и быстро.

Больше всего меня вдохновляет стремительное развитие мобильных приложений, когда у каждого под рукой (в буквальном смысле) есть все необходимые инструменты для более комфортной жизни. Оплатить электроэнергию, не вставая с постели, не потеряться в поездке по незнакомому городу, отследить местоположение и убедиться в безопасности ребёнка, заказать еду, если нет сил готовить ужин – всё вышеперечисленное можно осуществить всего в несколько касаний! И это уже не фантастика, это – часть жизни! Благодаря информационным технологиям. Как тут не влюбиться:)

Конкурсы красоты и технологии – две совершенно разные области. Каким образом Ваш опыт участия в конкурсах красоты повлиял на профессиональную жизнь в ИТ, и наоборот, как технологии помогли Вам преуспеть в мире конкурсов красоты?

Задания конкурса «Beauty&DigITal-2022» состояли из переплетения двух областей – красоты в технологиях и технологий красоты! Во время конкурсных испытаний мне пришлось как минимум научиться монтировать видео (в ролике с образами) и разобраться с построением сайтов в конструкторе (финальное испытание). Именно это помогло получить номинацию «Мисс стиль» и главную корону конкурса. Всё оказалось взаимосвязано:)

1-я Вице-мисс Beauty&DigITal-2022 Галина Ветошкина

Как Вы смогли совмещать успешную карьеру в сфере информационных технологий с участием в конкурсах красоты во время его проведения? Какие аспекты Вашей личности и профессиональных навыков помогают достигать успеха в обеих областях?

Интересный вопрос, потому что никогда не задумывалась об этом с точки зрения моих аспектов личности и профессиональных навыков. Я всё делаю по ощущениям. Если какая-то возможность вызывает внутри приятную эмоцию, я иду в её направлении. И, пока есть интерес, я в потоке, а значит, у меня много энергии и потрясающий тайм-менеджмент. Так было и с конкурсом красоты «Beauty&DigITal-2022», он вызвал во мне бурю эмоций, я приняла в нём участие, ни разу не пожалела и получила потрясающий опыт и приятные воспоминания. Поэтому всегда прислушиваюсь к своим внутренним ощущениям, они и помогают мне достигать успеха в любых сферах жизни.


Галина Ветошкина

Как Вы подбирали образ для финальной церемонии? Расскажите более подробно, пожалуйста, почему именно этот наряд был выбран и кто Вам помогал его создавать?

У меня не было представления, каким должно быть моё платье для финальной церемонии, но, когда увидела его, сразу поняла: «Это оно!» Атласная ткань и потрясающий розовый цвет – сразу вспомнила культовый образ Мэрлин Монро в фильме «Джентльмены предпочитают блондинок». Подобрала к нему серьги, которые выигрышно сверкали при свете софитов. И чтобы сохранить акцент на платье, выбрала классические туфли-лодочки. А вообще, хочу дать такой совет всем девушкам участницам конкурса: красоту образу придаст именно ваша энергия!

Какие советы Вы можете дать девушкам, которые также хотели бы сочетать свой интерес к красоте и моде с карьерой в информационных технологиях? Какие шаги и усилия помогли Вам добиться успеха в обеих сферах?

Во-первых, каждая из нас прекрасна, и самое главное – прекрасна по-своему. И этот факт просто неоспорим. Во-вторых, вся яркость моментов и их вкус ощущается во время пути к цели, а не после её достижения. Именно осознание этих двух вещей, на мой взгляд, и есть весь секрет успеха. Поэтому я бы посоветовала девушкам отбросить все сомнения, переживания и ожидания. Получайте удовольствие от процесса, каждого конкурсного испытания, особенно от того, как вы раскрываетесь в них.

2-я Вице-мисс Beauty&DigITal-2022 Вероника Марчик

Как Вы смогли совмещать успешную карьеру в сфере информационных технологий с участием в конкурсах красоты во время его проведения? Какие аспекты Вашей личности и профессиональных навыков помогают достигать успеха в обеих областях?

На самом деле, испытания и мастер-классы были организованы таким образом, что разрываться между работой и конкурсом не пришлось. Период испытаний был долгим, но организаторы очень постарались и никаких неудобств у меня не возникло.

Так как я работаю IT-рекрутером, то многозадачность – мой основной навык. К тому же я очень активный человек и с лёгкостью могу «вписаться» в любую авантюру. Поэтому совмещение подготовки к конкурсу и работы было для меня очень интересным этапом в жизни.

В чём заключается Ваша наибольшая мотивация и страсть к информационным технологиям? Какие проекты или достижения в этой области Вас наиболее вдохновляют?

Если честно, страсть я испытываю не к самим технологиям, а к людям, которые эти технологии создают. Это ведь невероятно умные и нестандартно мыслящие люди, которые являются проводниками между настоящим и супертехнологичным будущим.

Вдохновляют меня те проекты, к результатам которых я могу прикоснуться. Чаще всего это те технологии, которые упрощают нашу повседневную жизнь: заказ такси/еды, онлайн-оплата, запись на приём и т. д.

Как Вы подбирали образ для финальной церемонии? Расскажите более подробно, пожалуйста, почему именно этот наряд был выбран и кто Вам помогал его создавать?

Скажу по секрету, что часть моего образа ждала своего звёздного часа со школьного выпускного. Я сразу решила, что возьму юбку и дополню её более современным топом. Долго решала, какой цвет лучше подойдёт к юбке цвета фуксия, и оказалось, что лучше классического белого ничего не найти.


Вероника Марчик

Причёску и макияж я доверила профессионалу-визажисту. Заручилась поддержкой и тёплыми словами родных и отправилась прямиком на финал конкурса за своим титулом «Вторая вице-мисс».

Если вы прочувствовали необыкновенную атмосферу нашего конкурса через глянцевые страницы журнала, то тоже можете стать её частью. Мы уже начали принимать заявки на «Beauty&DigITal-2024». Если вы женщина и работаете в сфере информационных технологий, то скорее отправляйте свои анкеты на почту magazine@SOVINFOSYSTEMS.RU.

Начните новую главу собственной сказки, ведь вы этого достойны! Ждём вас, наши ИТ-Барби!

CIS Современные Информационные Системы

ИТ-журнал CIS
«Современные Информационные Системы»

www.cis.ru

Гороскоп для ИТ-компаний на осень 2023 года

Зная, под каким знаком зодиака была основана ваша компания, и руководствуясь нашим гороскопом, вы будете в курсе того, что её ожидает и к чему надо готовиться для роста и развития компании.

Овен

21 марта – 20 апреля

Осенью Овнов будут ждать деловые мероприятия, возможны поездки для руководителей. Не стесняйтесь проявить инициативу, и тогда этот месяц будет особенно благоприятным для роста компании. При этом следует как можно ответственнее подходить к каждой производственной задаче. Помните, что в это время к компании могут присматриваться партнёры или более высшие инстанции.

Проявив компетентность и профессионализм, можно повысить бюджет и улучшить климат в коллективе.

Телец

21 апреля – 21 мая

Компании может поступить несколько выгодных предложений о сотрудничестве. Однако при принятии решения руководству предстоит во многом полагаться на интуицию – это поможет выбрать наиболее перспективные проекты. Кроме того, возможна смена направления деятельности, открытие нового дела или решительный переворот в области финансовых трат. В это время можно пересмотреть бюджет компании в части экономии расходов, а также принять немало решений, которые обусловят прочное финансовое положение в будущем.

Близнецы

22 мая – 21 июня

Компании предстоит найти немало оригинальных решений для самых простых задач, утверждает гороскоп для Близнецов на эту осень. Задействовав все ресурсы компании – интеллектуальные и материальные, можно выйти победителем из любой ситуации, продемонстрировав конкурентам и партнёрам профессионализм и качество услуг. Сейчас отличное время для того, чтобы выбиться из массы похожих организаций и получить более высокий статус на рынке.

Тем организациям, кто серьёзно занимается несколькими направлениями деятельности, звёзды советуют быть осмотрительнее. В конце лета может ждать несколько выгодных предложений, однако, желая сесть сразу на все стулья, можно потерять авторитет. Выберите самые надёжные и перспективные направления и постепенно двигайтесь по пути их развития.

Рак

22 июня – 22 июля

В вопросах престижа и качества компании Раки будут купаться в признании.

Если ваша организация относится к творческому направлению, то сейчас благоприятное время чтобы начать её продвижение и активное развитие. Все начинания в вопросах производства увенчаются успехом, тем более, что компания уже давно находится на стадии смены приоритетов или видов деятельности. Не стесняйтесь быть индивидуальностью на рынке и не идите на поводу у большинства.

Лев

23 июля – 22 августа

В вопросах производства нужно больше прислушиваться к внутреннему голосу – он подскажет, когда будет опасность потерять финансы в бесперспективных проектах.

Если компания ещё не достигла высокого уровня, то отношения с высшими структурами могут обостриться. Чтобы избежать этого, гороскоп подсказывает Львам, что осенью 2023 года необходимо ответственно подходить к каждому производственному процессу.

В отношениях с коллективом будьте предусмотрительнее: не раскрывайте коммерческие тайны о производственных процессах, иначе можно ожидать раскрытия конфиденциальных сведений.

Дева

23 августа – 22 сентября

Если до этого компании Девы занимались не перспективными проектами, то осенью возможны некоторые финансовые затруднения. Не стоит переживать – это временные проблемы, ведь уже спустя несколько недель всё наладится, а финансовое положение окрепнет.

Девам стоит стать особенно законопослушными компаниями: в это время даже незначительное нарушение регламента может быть чревато серьёзными последствиями. Задумайтесь об этом, прежде чем принимать любые важные решения.

Не стоит доверять коллективу сведения о производственных проблемах, иначе не очень добросовестные сотрудники могут использовать это против компании.

Весы

23 сентября – 22 октября

Для Весов сложным будет только начало месяца, так говорит гороскоп на осень 2023 года. Вероятно, будут значительные пиковые периоды в течение месяца, но они ограничатся ситуационными задачами, и компания успешно с ними справится. Готовьтесь много и усердно работать, это необходимо, чтобы быть подготовленными к нагрузке на производство. Возможны неожиданные приятные новости, поездки и переговоры. Следите за сроками выполнения производственного плана, ведь в суете можно попросту нарушить деловые договорённости.

Скорпион

23 октября – 22 ноября

Скорпионам гороскоп на осенние месяцы 2023 года говорит, что не следует искать лёгких путей в вопросах финансового благосостояния компании, начните просто усердно работать. Помните, что сейчас наступает период, когда заказчики и партнёры присматриваются к вам. Представителям знака нужно зарекомендовать себя как ответственную и перспективную компанию для сотрудничества. В таком случае вам доверят самые прибыльные и интересные проекты.

Не перерабатывайте и не забывайте о выходных. Кроме того, следует избегать больших бюджетных трат – предпочтительнее начать экономить финансы и не вкладываться в легкомысленные проекты.

Можно предусмотреть статьи затрат на открытие нового направления. Возможно, объединив все мощности компании, вы откроете прибыльный проект, который уже через некоторое время сделает её успешной среди конкурентов.

Стрелец

23 ноября – 21 декабря

В начале осени 2023 года Стрельцов ждёт безусловный успех в решении всех финансовых вопросов, утверждает гороскоп. Если вы успешная компания, то впереди новые тендеры и объёмные продажи. Если вы маленькая организация, то ждите повышения рейтинга и финансирования.

Тем компаниям, которые захотят открыть новые виды бизнеса, звёзды будут содействовать, но важно не принимать поспешных решений и не отдавать предпочтение сомнительным аферам. Помните, что финансы – хрупкая вещь, поэтому и распоряжаться ими нужно крайне разумно. Только в таком случае можно не только стабилизировать, но и приумножить бюджет компании.

Козерог

22 декабря – 20 января

Если компании Козероги достаточно активно работали, но не перетруждались, то осенью они могут добиться выполнения производственного целей. Отдельного внимания заслуживает этап планирования. Иными словами, если компания решит развиваться в новых направлениях, то сейчас самое благоприятное время. Не стоит принимать скоропалительных решений – продумывайте каждый шаг.

Присмотритесь к деловым партнёрам и коллективу: они могут навредить положению компании, если продолжите делиться с ними всеми особенностями рабочего процесса.

Если вдруг нахлынет апатия, то нужно устроить корпоратив или производственный отпуск для топ-менеджеров.

Решая деловые вопросы, прислушивайтесь к внутреннему голосу. Он поможет выигрышно истолковать каждую ситуацию, которая была полна противоречий.

Водолей

21 января – 19 февраля

Компаниям Водолеям нужно быть очень осторожными в вопросах, которые касаются капиталовложений. Если представители знака соберутся открыть дополнительное направление, то им предстоит пройти немало бюрократических процедур. Помните, что преуспеть могут только те компании, производственные процессы которых отработаны до мелочей.

Не пренебрегайте советами опытных партнёров, которые ранее проходили такой же тернистый путь. Если они что-то порекомендуют, то прислушайтесь к ним и попытайтесь учесть в своих действиях.

В вопросах финансов следует ответственнее относиться к непосредственным обязанностям перед заказчиками. В таком случае компания может достигнуть большего успеха, хорошо зарекомендовать себя на рынке и заслужить уважение партнёров и конкурентов.

Рыбы

20 февраля – 20 марта

Начало сентября ознаменуется приятными событиями и сюрпризами в развитии компаний Рыб. Если жизнь предоставляет новую возможность, то смело воплощайте её – успех гарантирован. Возможно, круг партнёров и заказчиков значительно расширится.

Гороскоп утверждает, что вторая половина сентября для Рыб сопряжена со значительным энергетическим спадом. Но многим компаниям удастся довести начатые проекты до конца с помощью внутренних резервов и волевых решений руководства.

Если перед компанией стоит конструктивная цель, которая гарантирует хорошие перспективы, то никакие препятствия не помешают.

Нужно обратить внимание на окружение, возможно в сотрудничестве с опытными партнёрами можно быстрее получить желаемое.

Календарь мероприятий

2–3 октября
Москва • Онлайн-трансляция • Конференция
FrontendConf 2023

4–5 октября
Москва • Форум
Международный форум Universe Ecom Convention 2023

5–6 октября
Санкт-Петербург • Конференция
Конференция БИТ Санкт-Петербург 2023

5–6 октября
Москва • Онлайн-трансляция • Конференция
БИТВА ЗА IT | HR IT & TEAMLEAD КОНФЕРЕНЦИЯ

5 октября
Москва • Онлайн-трансляция • Конференция
Видео+Конференция-2023

7 октября
Москва • Гала-шоу
ИТ-конкурс красоты «Beauty&DiglTal» 2023

9–14 октября
Санкт-Петербург • Онлайн-трансляция • Конференция
Joker 2023

10–16 октября
Санкт-Петербург • Онлайн-трансляция • Конференция
Heisenbug 2023 Autumn

11 октября
Онлайн-трансляция • Митап
Python meetup (Online)

14–15 октября
Тольятти • Конференция
FrontDays – поволжская конференция фронтенд-разработчиков

19 октября
Москва • Онлайн-трансляция • Конференция
Big Monitoring Meetup X

20 октября
Калуга • Онлайн-трансляция • Митап
Exoz Frontend Meetup 20.10.23

25 октября
Москва • Форум
Всероссийский бизнес-форум «Кадры для цифровой экономики России: из 2023 в 2030»

25 октября
Онлайн-трансляция • Митап
DevOps meetup (Online)

27 октября
Москва • Онлайн-трансляция • Конференция
ArchDays – конференция по архитектуре IT-решений

1–10 ноября
С.-Петербург • Онлайн-трансляция • Конференция
Mobius 2023 Autumn

2–12 ноября
С.-Петербург • Онлайн-трансляция • Конференция
HolyJS 2023 Autumn

3–4 ноября
Москва • Тренинг
«Спокойно, договоримся!». Курс по переговорам и выстраиванию долгосрочных отношений в IT

6–14 ноября
С.-Петербург • Онлайн-трансляция • Конференция
PiterPy 2023

8 ноября
Онлайн-трансляция • Митап
Frontend meetup (Online)

13–15 ноября
Онлайн-трансляция • Вебинар
Онлайн-курс «Управление проектами и активами в ИТ»

16 ноября
Москва • Онлайн-трансляция • Конференция
Особенности бухгалтерского учета в ИТ-компаниях

16–21 ноября
Москва • Онлайн-трансляция • Конференция
VideoTech 2023

17 ноября
Москва • Конференция
Enterprise Agile Russia

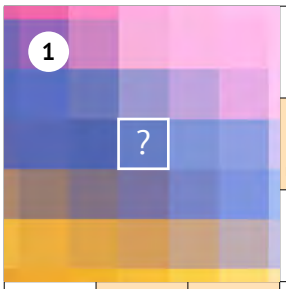
22 ноября
Онлайн-трансляция • Митап
Flutter meetup (Online)

6 декабря
Онлайн-трансляция • Митап
Ruby meetup № 23 (Online)

14–15 декабря
Ереван • Конференция
HighLoad++ Armenia 2023

Сканворд

Пришлите разгаданный сканворд и ключевое слово на почту magazine@sovinfosystems.ru до 15-го декабря и получите приз от редакции ИТ-журнала CIS.



Программа для связи компьютера и устройства

«Путь» для китайца

Вдыхая розы ...

Корабль Юрия Гагарина

Микки... из Голливуда

Сорящий деньгами

Единица силы электрического тока

Движение орудия назад

Певец... Рид

С молотом на советском гербе

Озеро на Западном Кавказе

Бывает газетный

Ансамбль из одного исполнителя

Орфографическая оплошность

Деревенский магазин (советск.)

Певица Патрисия

Настоятель-католик

Апофеоз наступления

Недостача, ущерб

Каюк, он же капут

Двуногое такси на улочке Японии

Вечно драное дерево

Средство для очищения кожи

Французский океанограф

Хранитель семейных фотографий

Двигатель на колесах

Магический символ

Бумажный штабелек

Безукоризненный вид

60-минутный осколок вечности

Утиль – вторичное ...

Ответ ударом на (разг.)

Неудачные усилия

Гороховый весельчак

Деревенские штаны

Руководитель организации

Восточная цитадель

Английская собака-охотница

Тема обсуждения в форуме

Одежда духовенства

Купеческая управа

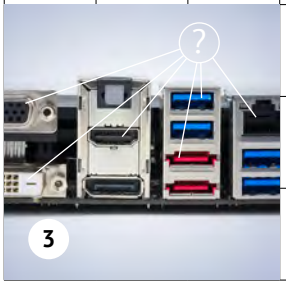
Внешнее проявление чего-либо

Спел арию мистера Икс

Наместник короля (сканд.)

Жуткий запах

Победный возглас по-старинному



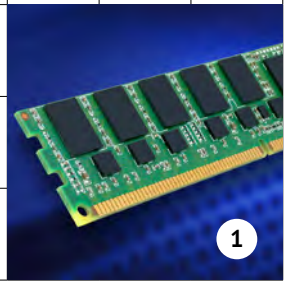
Пафос, литота

Единица колхозного пространства

Триста лет беды на Руси

Единение людей по цвету кожи

Столица Сенегала



1	2	3	4	5	6	7	8	9


CIS TV
ВСЁ ПРО ИТ
YouTube
Современные Инфосистемы
www.cis.ru