

информационные технологии



«Каждый госорган — оператор данных, требующих защиты, в том числе от человеческого фактора»

Государственные информационные системы (ГИС) обрабатывают огромное количество чувствительной информации о российских гражданах и организациях. Утечки этих данных ставят под угрозу конфиденциальную информацию субъектов персональных данных и сведения, составляющие коммерческую и другие виды тайн. Абсолютное большинство аналитиков и внутренних пользователей организаций, деятельность которых связана с использованием IT-систем, прогнозируют рост количества утечек, в том числе связанных с человеческим фактором. О том, как данные утекают из госкомпаний и чем это способно обернуться, рассказала **Галина Рябова**, директор центра развития продуктов Dozor компании «Ростелеком».

— **экспертное мнение** —

— **Количество утечек информации растет с каждым годом. В чем причина?**

— Основная причина — в росте темпов цифровой трансформации, на который серьезно повлияла пандемия. Сегодня госсектор — один из главных участников цифровизации, при этом внедрение новых технологий в госучреждениях неизбежно сопровождается усложнением IT-ландшафта. Эволюция IT-инфраструктуры, в свою очередь, требует постоянной синхронизации с процессами информационной безопасности (ИБ). Ожидаемо, что однажды что-то может выйти из-под контроля.

Сотрудники учатся выполнять свои функции в новых информационных системах, работать с новыми базами данных, взаимодействовать в цифровой среде со смежными подразделениями и т. д. Систем становится все больше, они постоянно модернизируются, и сотрудники просто не успевают адаптироваться под эти изменения. Они сосредоточены на том, чтобы оперативно и качественно справиться со своими задачами в новых реалиях, и поэтому вопросы безопасности часто отходят на второй план или вовсе остаются за бортом.

— **Это значит, что большинство утечек происходит из-за человеческого фактора?**

— Это действительно так. По нашему мнению, в госорганах и организациях есть две группы сотрудников, которые могут спровоцировать непредумышленные утечки. Первая — люди старшего возраста, которые не очень хорошо разбираются,

как устроены современные технологии. Им не понятно, почему, перенося данные на личный носитель или пересылая информацию на электронную почту, чтобы вечером поработать с домашнего ПК, они подвергают реальным рискам своего работодателя и информацию субъектов персональных данных. Человек может и не подозревать, что его учетная запись скомпрометирована или компьютер заражен трояном — программой, автоматически передающей в фоновом режиме любые данные с зараженного компьютера на сервер «хозяина».

Так или иначе, данные могут попасть к злоумышленникам, которые могут распорядиться ими самыми разными способами. Сведения могут начать в искаженном виде попадать в СМИ или распространяться в Darknet. Данные могут быть использованы для атаки на организацию, в частности, если документ содержит сведения о сотрудниках или внутренних процессах. Сценариев последствий может быть много вплоть до атаки организаций, с которыми компания-жертва взаимодействует.

Вторая группа людей, по вине которых может случиться непреднамеренная, но резонансная утечка, — молодые сотрудники. В госсекторе сейчас приходит много студентов, которые живут в информационно насыщенном мире, активно пользуются сервисами и мессенджерами, но гораздо свободнее относятся к информационному обмену. Зачастую они просто не отдадут себе отчет в том, насколько критические данные проходят через них на госслужбе и чем чревато их распространение.

Предположим, сотрудник, который готовит первую версию проекта



ПРЕДОСТАВЛЕНО «РОСТЕЛЕКОМ»

письма одного министра к другому, поделится им со своим другом, с которым любит обсудить политическую повестку. Тот начнет распространять эту информацию, опираясь на источник в министерстве. И поскольку проект письма проходит много этапов согласования, вероятно, из того, что подготовил сотрудник-нарушитель, мало дойдет до финальной версии. Однако это сложно объяснить уже взволнованной общественности.

— **Можно ли сократить вероятность информационных утечек в госорганах и организациях, если проводить обучения сотрудников цифровой грамотности?**

— Говоря медицинскими терминами, обучение — это профилактика, но едва ли кто-то видел, чтобы одним лишь витамином С можно было победить болезнь. Безусловно, обучать сотрудников нужно, чтобы они по незнанию не совершили ошибку.

По данным Минфина России, в 2019 году в России насчитывалось

около 2,4 млн работников государственных и муниципальных органов. Обучить их всему тому, что знают специалисты по ИБ, невозможно. При этом есть доля людей, которые хуже поддаются обучению, и тех, кто с обучением справится, но на практике будет ошибаться.

Повышение цифровой грамотности определенно принесет свои плоды, но оно не способно исключить вероятность утечек полностью, поэтому защита от них — задача более комплексная. Она требует также формирования подходов и политик безопасности внутри организации и обязательного использования специальных технических средств мониторинга.

— **Получается, можно решить проблему утечек информации благодаря вводу жестких ограничений, правил доступа к служебной информации и документам?**

— Теоретически это способно значительно снизить вероятность уте-

чек. Однако это слабо реализуемо на практике, потому что жесткие ограничения серьезно замедляют процессы внутри любой организации.

Запреты на перемещение информации должны быть разумно обоснованы. Например, можно создать более жесткие рамки для групп сотрудников, которые пришли в компанию недавно и еще не прошли испытательный срок. Для государственных организаций имеет смысл ограничивать действия сотрудников по отправке на внешние домены и печати документов, составляющих конфиденциальную информацию, если это не требуется для выполнения их обязанностей. Ограничения в данном случае должны касаться лишь тех групп лиц, которым обычно не требуются эти действия. Все зависит от специфики процессов и данных конкретной организации — меры контроля гибко конфигурируются.

Если в организации есть DLP-система, сотрудник ИБ-службы оперативно и в автоматическом режиме получает уведомления, когда возникает любое подозрение на некорректную работу с данными на рабочем устройстве.

— **Какие каналы следует защищать в первую очередь? Какими функциями должна обладать эффективная система для защиты от утечек?**

— По нашим данным, самые важные функции систем защиты от утечек информации, по мнению представителей государственных организаций, — контроль USB-носителей (68%), электронной почты (64%), возможность интеграции с другими системами (62%), контроль мессенджеров (58%), контроль веб-трафика (56%), профилактика инцидентов UBA (56%).

— **Кроме защиты от утечек какие задачи решают DLP-системы в государственных организациях?**

— Системы мониторинга DLP также позволяют выявлять нарушения федерального закона «О государственной гражданской службе РФ» от 27 июля 2004 года №79-ФЗ. В частности, DLP-система при соответствующей настройке политик может выявлять признаки нарушений статей 14, 15, 16 и 17 и других, которые содержат перечень обязанностей, ограничений и запретов, связанных с нахождением на гражданской службе. Нарушение некоторых из них является основанием для наложения дисциплинарного взыскания, а других — для немедленного увольнения человека с государственной службы.

Например, в соответствии со статьей 14 госслужащий обязан преду-

жеждать работодателя от любой дополнительной оплачиваемой работе, даже если это преподавание в авторитетном вузе. Другой пример — участие сотрудника в управлении коммерческой организацией, которое во многих случаях исключает возможность занятия должности в госоргане (статья 17). Благодаря автоматизированному мониторингу можно обнаружить признаки подобных нарушений.

Причем проблема скорее в том, что многие не отдают себе отчета, что их действия являются нарушениями. Молодые сотрудники в силу принятых сейчас культурных норм могут недостаточно серьезно подходить к выполнению всех существующих требований законодательства о государственной службе. В этом случае задачей DLP может быть помощь самому сотруднику или его руководителю в своевременном обнаружении и корректировании действий служащего, пока они не переросли в большую проблему.

— **Сейчас у государственных организаций есть информационные системы, администрирование которых находится в зоне ответственности привлеченных подрядчиков. Как можно проконтролировать защиту данных, доступ к которым есть у третьих лиц?**

— К тому, что доступ к чувствительной информации государственных инфосистем появляется у сторонних организаций, мы относимся с крайней тревогой. Разумеется, госконтракт на администрирование любой ГИС должен содержать пункт о конфиденциальности и неразглашении обрабатываемых сведений. Вопрос в том, как это реализуется на практике. При этом подрядчики могут меняться: сегодня одна компания администрирует ГИС, завтра — другая, исполнитель может привлекать третьих лиц для выполнения обязательств по контракту и т. д.

Решением может стать положение об обязательном применении подрядными организациями системы для предотвращения утечек конфиденциальной информации. Это поможет исключить выход данных за корпоративный периметр любой организации, администрирующей государственные инфосистемы. Аналогичные требования, по нашему мнению, должны также применяться в отношении любых исполнителей, которых подрядчик планирует привлекать для оказания соответствующих услуг.

Беседовал Анатолий Ильин

Хайтек на полях

— **IT и С/Х** —

Одна из древнейших отраслей, которая буквально кормит человечество, стоит на пороге существенных технологических изменений. Внедрение новых технологий в сельском хозяйстве обусловлено суровой необходимостью: речь даже не столько об экономической эффективности, за которой гонятся предприятия всех отраслей, сколько о борьбе с прогнозируемым продовольственным кризисом. Технологией обрабатывает весь агропромышленный комплекс: от производства сельхозтехники и разработки новых удобрений до уборки урожая и реализации готовых продуктов питания.

Голод на пороге

Аналитики говорят о необходимости технологической революции в АПК, и дело, как это ни банально, в спросе и предложении. В случае с продуктами питания спрос постоянно растет, в то время как предложение имеет объективные ограничения. По прогнозам Продовольственной и сельскохозяйственной организации ООН, количество пахотных земель на душу населения в мире сократится с 0,6 га на человека в 2000 году до 0,2 га к 2050 году, при этом спрос на еду вырастет на 70%. При сегодняшнем приросте урожайности на 1,5% в год, как оценивает ее Всемирный банк, это обернется недостатком пищи во всем мире.

Пока эксперты спорят, исчерпан ли потенциал экстенсивного развития в агросекторе, вера рынка в агротехнологии (AgTech, агротех) растет, а вместе с ней — и инвестиции в них. Согласно отчету Juniper Research, к 2025 году рынок сельскохозяйственных технологий вырастет до \$22,5 млрд с нынешних \$9 млрд. Если говорить о нашей стране, то, по оценкам Минсельхоза, российский рынок цифровых технологий в агросекторе также ждет бурный рост. Если в прошлом году оцен-

ка рынка составляла около 360 млрд руб., то к 2026 году рынок должен вырасти в пять раз.

Всходы зеленеют

Объем инвестиций в AgTech-проекты в РФ не превышает 1% от общемирового. Тем не менее на российском рынке агротех-решений заметно оживление. «Интерес к проектам этой сферы есть как со стороны инвесторов, так и со стороны промышленных партнеров, — констатирует директор департамента развития технологических конкурсов и инициатив Фонда „Сколково“ Вячеслав Гершков. — Число стартапов, которые уже вышли на коммерциализацию, приближается к 80, при этом проектов на ранней стадии и тех, у кого пока нет продаж, в нашей стране несколько сотен».

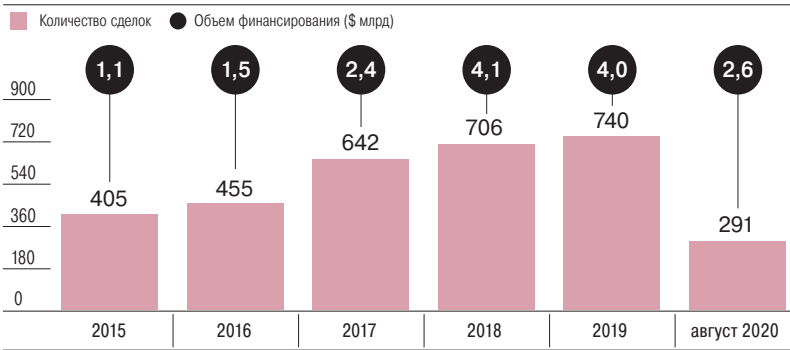
Согласно карте российского агротех-рынка, составленной Rusbase, новые решения в этой сфере условно можно поделить на два макросегмента — диджитал и биотех. Они, в свою очередь, разбиваются на несколько подсегментов: от беспилотников до генетики. Избытка венчурных инвесторов в агротехе на сегодня не наблюдается, и стартапы часто вынуждены развиваться за счет собственных ресурсов или с некоторой помощью институтов развития. Это тормозит их рост и сокращает возможности внедрения технологий. Впрочем, ежегодно появляются новые «лифты» и инструменты поддержки.

Одним из проектов для поиска и поддержки стартапов в области технологий для сельского хозяйства стал ежегодный конкурс инноваций сельхозбанка (РСХБ) AgroCode, объединяющий конференцию, хакатон, чемпионат по Data Science и конкурс идей. Кроме того, банк запускает совместные лаборатории по развитию агротехнологий с российскими вузами и создал агротех-акселератор со «Сколково», направленный на поиск инновационных агротехнологий.

«Такое обилие каналов и способов работы с агротехнологиями вызвано спецификой развития новых

ВЕНЧУРНЫЕ ИНВЕСТИЦИИ, ПРИВЛЕЧЕННЫЕ АГРОТЕХПРОЕКТАМИ (2015 ГОД — АВГУСТ 2020 ГОДА)

ИСТОЧНИК: CRUNCHBASE.



технологий — чаще всего новые подходы идут от IT в сторону агро, — объясняет директор центра развития финансовых технологий РСХБ Елена Батурова. — Сейчас молодые и амбициозные команды идентифицируют проблему и стараются ее решить при помощи доступных новых технологий. Основная сложность — не всегда четкая идентификация проблемы и часто слишком технологичное ее решение». РСХБ видит свою роль в адаптации найденных технологических решений и их встраивании в инструменты, используемые фермерами в рамках экосистемы «Свое фермерство» и других проектов.

Битва за урожай AI

По данным MarketsAndMarkets, объем мирового рынка решений на базе искусственного интеллекта (AI, artificial intelligence) в агросфере составлял \$1 млрд в 2020 году и вырастет до \$4 млрд к 2026 году при динамике роста 25,5% в год. В конце 2017 года эксперты Accenture прогнозировали, что использование ИИ-решений принесет глобальному сельскому хозяйству ежегодный рост в 3,4% вплоть до 2035 года. И это один из самых высоких показателей роста среди 16 различных отраслей.

В России на базе AI-технологий активно развивается направление беспилотной уборочной техники. Так, разработчик Cognitive Pilot, входящий в экосистему «Сбера», создал систему Cognitive Agro Pilot. Как рас-

сказали, «Б» в компании, это первая в мире универсальная система, которая «видит» и «понимает» обстановку по ходу движения и может использоваться на технике любых производителей. Эффективность работы «автопилота» в конечном итоге выражается в деньгах, говорят разработчики: использование Cognitive Agro Pilot позволяет сократить потери урожая при уборке до 13%, снизить расход топлива во время уборки до 5%, повысить производительность работы уборочной техники до 25%, сократить сроки уборочных работ и в итоге снизить себестоимость зерна на 3–5%.

По словам руководителя департамента разработки беспилотных транспортных средств Cognitive Pilot Юрия Минкина, новые технологии позволяют осваивать и труднодоступные территории, где тяжело работать человеку. «Мы рассчитываем, что с развитием роботизированных систем территорий, где возможно земледелие, станет больше. В России вообще наибольшая процент неосвоенных территорий, и у нас есть высокие шансы повысить число сельскохозяйственных земель за счет применения новых технологий, — считает он. — К тому же, как это ни удивительно, в России остро ощущается дефицит рабочей силы, особенно квалифицированной, в сельском хозяйстве. Это весомый аргумент в пользу роботизированных технологий».

В сотрудничестве с компаниями, которые разрабатывают сер-

висы аналитики, сервисы точного земледелия, например «Диджитал Агро», «Геомир» и др., Cognitive Technologies рассчитывает создавать экосистемные продукты — комплексные системы управления агрохозяйствами. Причем роль беспилотных комбайнов здесь довольно важна: чем больше техники оснащается системами автопилотирования, которые фиксируют происходящее вокруг, тем больше данных собирается.

«В будущем все эти системы: беспилотники, карты урожайности, прогнозическая аналитика и пр. — будут входить в комплексные автоматизированные системы. Здесь понятна экономическая эффективность: все это необходимо, чтобы в конечном итоге собрать больше урожая с того же поля. Да, численность населения и объемы потребления растут все больше. Но проблема голода в мире отодвигается все дальше с каждым годом, потому что растет эффективность агропроцессов», — уверен Юрий Минкин.

Против течения

С учетом изменений климата на передний план выходят разработки, позволяющие удерживать эффективность культуры при засухах или излишней влажности, подчеркивает гендиректор компании «ЭФКО Инновации» Андрей Зюзин. «Безусловно, урожайность культур остается одним из наиболее важных приоритетов, но к ней добавляются требования по составу — как, например, повысить содержание белка в культуре. Вопросы резистентности разного рода вредителям также важны», — говорит он. По его мнению, в перспективе ближайших десяти лет развитие получат такие направления агротеха, как высокоточное земледелие, новые виды биотехнологических удобрений, современная селекция с использованием технологий CRISPR, TALEN и пр.

Факторы, которые препятствуют внедрению новых подходов и технологий в российском сельском хозяйстве или тормозят их, можно ранжи-

ровать по степени их влияния, указывает Елена Батурова. «На третьем месте — огромная территориальная распределенность фермеров. В то время как в Европе расстояния измеряются километрами, в России любые вычисления идут в сотнях километров, — объясняет она. — На втором месте — проблемы низкого качества и малой доступности мобильного интернета в полях, а разветвление сложных и дорогостоящих комплексов LoRaWAN не всегда целесообразно для небольших хозяйств».

На первое место представитель РСХБ ставит сразу две проблемы: необходимость существенных инвестиций для внедрения и сложность оценки фермерами качества предлагаемых инноваций. «Новое оборудование, пусконаладка, обслуживание — все это требует больших расходов. Во втором случае каждый стартап заявляет о кардинальном изменении всего земледелия и кратном увеличении урожая. К сожалению, такие громкие заявления лишь мешают работать, создавая фон недоверия ко всем новым технологиям», — под черкнула Елена Батурова.

За последнее столетие технологии в сельском хозяйстве сильно продвинулись, существенно вырос уровень производительности труда за счет механизации, автоматизации, агротехнологий, напоминает Андрей Зюзин: «Но сельское хозяйство — это очень сложная логистическая цепочка. Недостаточно произвести урожай, необходимо его доставить, переработать, сделать продукт и т. д. На каждом из этапов есть свои нюансы, которые могут сделать всю цепочку неэффективной». Он приводит в качестве примера «очень низкое покрытие» широколопастной связью сельскохозяйственных регионов в нашей стране, где целесообразно внедрение новых информтехнологий. «Поэтому называть нас лидерами в сфере развития новых агротехнологий пока сложно», — заключает он.

Марина Эфендиева