Цифровая трансформация экономики как предвестник 4-й промышленной революции

En **The Digital Transformation of Economy as Industry 4.0 Beginning**

V. A. Artamonov,
Grand Doctor (Eng.), Full Professor, The Full Member of IAIT
artamonov@itzashita.ru

E. V. Artamonova,
PhD (Eng.), The Member of IAIT
admin@itzashita.ru

The International Public Union «The International Academy of Information Technologies» (IAIT)

In this article, we discuss the different ways of the digital transformation and industrial relations in the Industry 4.0 beginning. To forecast the technical progress in the future we set the term technological singularity. The advantages of the digital transformation are discovered in the article and we are trying to describe the key stages and implementation mechanisms of it. The digital transformation will drive to positive effects in modern society, but it may be negative effects. In our opinion, the main threats in Industry 4.0 are cyber attacks and information security incidents in critical infrastructure assets and computer networks. In the article, we are discussing how to use machine learning (ML) and artificial intelligence (AI) in the cybersecurity practice.

Keywords: digital transformation, industrial revolution, technological singularity, society, public administration, e-government, information technologies, information security, cyber attack, internet of things (IoT), cloud computing, machine learning (ML), artificial intelligence (AI)

В статье рассматриваются различные аспекты цифровой трансформации экономики и производственных отношений при осуществлении четвертой промышленной революции – так называемой Индустрии 4.0. Для предсказания технического прогресса, которое ожидает человечество в ближайшем (обозримом) будущем вводится операционное понятие технической сингулярности. Показываются преимущества цифровой трансформации, ее ключевые этапы и механизмы реализации. Наряду с позитивными моментами цифровой трансформации, влияющими на качество жизни человеческого социума, отмечены ее негативные последствия. Особую угрозу цифровой трансформации экономики представляют кибератаки и нарушение информационной безопасности критически важных объектов и сетевой инфраструктуры. Подробно рассмотрены меры противодействия угрозам и кибератакам, в том числе с применением машинного обучения и искусственного интеллекта.

Ключевые слова: цифровая трансформация, промышленная революция, технологическая сингулярность, человеческий социум, государственное управление, электронное правительство, информационно – коммуникационные технологии, информационная безопасность, кибератака, интернет вещей, облачные вычисления, машинное обучение, искусственный интеллект

Владимир Афанасьевич Артамонов,
доктор технических наук, профессор, академик МАИТ
artamonov@itzashita.ru

Елена Владимировна Артамонова,
кандидат технических наук, член МАИТ
admin@itzashita.ru

Международное научное общественное объединение «Международная академия информационных технологий» (МАИТ)

Введение

Мир стоит на пороге четвертой промышленной революции, и этот непреложный факт уже не вызывает практически никаких сомнений. Среди ученых теоретической экономики есть разные определения или признаки той или иной промышленной революции, основанные либо на наличии различных технологических укладов, либо на так называемых «*длинных волнах*» Кондратьева. Не вдаваясь в подробности, остановимся на классической и рациональной немецкой классификации.

Согласно таковой, ***Индустрия 1.0*** сформировалась при широком распространении ткацкого станка и паровой машины в конце XVIII века, ***Индустрия 2.0*** – в начале XX века при переходе к конвейеру, ***Индустрия 3.0*** – в конце 70-х прошлого века вследствие компьютеризации и распространения станков с ЧПУ.

Индустрия 4.0 или четвертая промышленная революция сегодня по-

ка только набирает обороты и заключается в развитии информационно-коммуникационных технологий (ИКТ), робототехники, искусственного интеллекта (ИИ), дальнейшей цифровизации экономики, внедрении концепции электронного правительства, электронных денег (криптовалюты), автоматизации производства и сферы услуг, расширении применения «безлюдных» технологий и транспорта, *Интернета вещей* (IoT), развитии центров обработки данных (ЦОД) и облачных вычислений.

При рассмотрении сути четвертой промышленной революции уместно будет ввести фундаментальное понятие *технологической сингулярности*. ***Технологическая сингулярность*** – это гипотетический момент в будущем, когда технологическое развитие станет настолько стремительным, что экспоненциальный график технического прогресса станет практически вертикальным. Данная концепция была предложена Верноном Винжем который предположил, что если мы сумеем избежать гибели цивилизации до этого момента, то сингулярность произойдет из-за прогресса в области искусственного интеллекта, интеграции человека с компьютером или других методов увеличения мирового разума [1]. Усиление разума, по мнению Винжа, в какой-то момент приведет к положительной обратной связи: более разумные системы смогут создать еще более разумные и делать это быстрее, чем первоначальные их конструкторы – люди. Эта положительная обратная связь, скорее всего, окажется столь сильной, что в течение очень короткого промежутка времени (месяцев, дней или даже всего лишь часов) мир преобразится значительнее, чем мы можем это представить, и внезапно окажется населенным сверхразумными созданиями.

По мнениям некоторых ученых футурологов и того же Винжа, придерживающихся концепции сингулярности, она должна наступить около 2030 года, а по самому пессимистическому сценарию – не позднее середины текущего века [2].

Если экстраполировать закон Мура (наблюдение, сделанное в 1965 году Гордоном Муром, одним из основателей корпорации Intel, которое заключается в том, что количество транзисторов на квадратный дюйм в интегральных схемах увеличивается двукратно каждый год, начиная с момента изобретения интегральных схем) на концепцию сингулярности, окажется, что примерно в то же время вычислительная мощность компьютеров сравнится с головным мозгом человека.

Сторонники теории технологической сингулярности считают, что если возникнет принципиально отличный от человеческого разум (*постчеловек*), дальнейшую судьбу цивилизации невозможно предсказать, опираясь на человеческую логику. С понятием сингулярности часто связывают идею о невозможности предсказать, что будет после нее. Вопрос этот крайне важен, поскольку, не имея возможности предсказать хотя бы некоторые последствия наших действий, нет никакого смысла в том, чтобы пытаться направить развитие в желательном направлении [3]. *Постчеловеческий мир*, который в результате появится, возможно, будет столь чуждым для нас, что сейчас мы не можем знать о нем абсолютно ничего. Единственным исключением могут стать фундаментальные законы природы, но даже тут иногда допускается существование еще не открытых законов (у нас пока нет теории квантовой гравитации) или не до конца понятых следствий из известных законов (путешествия через пространственные «дыры», рождение «вселенных-карликов», путешествия во времени и т. п.), с помощью которых *постлюди* смогут делать то, что мы привыкли считать физически невозможным.

Теперь зададимся вопросом, как же на самом деле произойдет эта самая четвертая промышленная революция, каковы ее движущие силы и механизмы реализации? Неужели, однажды проснувшись, мы в одночасье окажемся в этом самом сказочном постчеловеческом мире?

На самом деле промышленные революции, в отличие от социальных, совершаются не в короткий исторический промежуток времени, а являются результатом технологических трансформаций (развитием промышленных укладов) производственных и общественных отношений человеческого социума. И механизмом таких «тектонических» сдвигов в контексте Индустрия 4.0 является *цифровая трансформация*.

Цифровая трансформация – это процесс интеграции цифровых технологий во все аспекты бизнес-деятельности и инфраструктуру общественных отношений, требующий внесения коренных изменений в технологии, культуру, операции и принципы создания новых продуктов и услуг. Для максимально эффективного использования новых технологий и их оперативного внедрения во все сферы деятельности человека предприятия и бизнес должны отказаться от прежних устоев и полностью преобразовать процессы и модели работы. Цифровая трансформация требует смещения акцента на периферию предприятий и повышение гибкости центров обработки данных (ЦОД) и облачных вычислений, поддерживающих периферию. Этот процесс также означает постепенный отказ от устаревших технологий, обслуживание которых может дорого обходиться предприятиям, а также изменение культуры производства (переход к *Интернету вещей* – IoT), которая теперь должна поддерживать ускорение процессов, обеспечиваемое цифровой трансформацией.

Преимущества цифровой трансформации

Государственные органы управления, предприятия и бизнес быстро заменяют традиционные процессы взаимодействия цифровыми, используя самые современные технологии. Очень часто трансформация происходит не потому, что субъекты производственных отношений так решают, а потому, что это им необходимо, чтобы нормально функционировать. Сегодня на рынке вырос спрос на эффективные цифровые технологии для бизнеса, и предприятия, которые не смогли адаптироваться к новой модели цифрового потребителя, наверняка прекратят свое существование.

Предприятия, которые приветствуют перемены и готовы к ним, а также способны адаптироваться к более гибким моделям работы, имеют как никогда большой потенциал успеха. Это связано с тем, что цифровая трансформация охватывает все аспекты бизнеса и государственного регулирования и предлагает эффективные пути их совершенствования вместе с развитием цифровых технологий.

Оптимизация процессов. Новые технологии позволяют предприятиям автоматизировать более простые процессы и исключать промежуточные этапы в более сложных. Благодаря этому повышается гибкость предприятий, которые теперь могут гораздо эффективнее использовать свои кадровые ресурсы.

Поиск новых потоков доходов. С появлением новых технологий открываются новые способы получения прибыли, которые ранее могли быть недоступны.

Создание более персонализированной и привлекательной инфраструктуры обслуживания. Современные заказчики ожидают, что предприятия-производители товаров и услуг будут оперативно реагировать на их запросы и удовлетворять их специфические потребности. Современные технологии должны быть развиты настолько, что могут решить все эти задачи.

Однако для эффективного использования цифровых данных предприятия должны постоянно внедрять вновь появляющиеся технологии, тестировать их и использовать полученные результаты, чтобы лучше адаптироваться к задачам будущего. Несмотря на то, что внедрение новых технологий – это более рискованный подход, чем использование уже привычных систем и устройств, потенциальные возможности и отдача от этого шага весьма значительны.

Ключевые этапы цифровой трансформации

Несмотря на различия процессов цифровой трансформации в каждом предприятии, существует ряд ключевых, общих для всех этапов.

1. Создание плана, в котором учтены все бизнес-потребности предприятия.

В начале процесса цифровой трансформации очень важно определить направления развития, а также набор технологий, которые помогут в этом развитии. При этом предприятия должны провести инвентаризацию своих ресурсов, выделив те, которые требуют модернизации. На этом этапе может даже потребоваться пересмотр приоритетов в проектах с учетом новых бизнес-потребностей, а также выявление недостатков которые могут стать препятствием на пути цифровой трансформации.

2. Обучение персонала навыкам работы с новыми технологиями.

Этот процесс может вызвать множество трудностей, поскольку при традиционных моделях бизнеса сотрудники должны были знать только определенные системы, которые планировалось использовать еще многие годы. Для успеха цифровой трансформации сотрудники должны быть готовы к любым изменениям рабочих процессов, если эти изменения необходимы для повышения эффективности и продуктивности. Такая готовность означает и умение мыслить творчески, и знание потенциала новых технологий, и умение использовать их с максимальной эффективностью.

3. Отказ от устаревших технологий.

Очень часто предприятия тратят огромные деньги только для обслуживания своих устаревших технологий, которые уже не приносят прибыли и не способны поддержать цифровые процессы, востребованные на рынке. Это объясняется тем, что модернизация старых технологий отличается большой сложностью и обходится слишком дорого. Их сохранение препятствует также развитию предприятия в целом: на обслуживание старых технологий тратится множество ценных ресурсов, которые можно было бы вложить в технологии, более простые в использовании, повышающие качество обслуживания заказчиков и/или ускоряющие анализ данных.

Цифровая трансформация – дело непростое. Для нее необходима стратегия, пересмотр бизнес-моделей и процессов, новая инфраструктура, новое программное обеспечение, оптимизация набора услуг, эффективные механизмы внедрения, программы обучения и надежная текущая поддержка. Портфель предложений должен включать облачные решения, средства обеспечения безопасности, технологии Интернета вещей, технологии мобильного доступа и решения инфраструктуры.

Иногда трудно определить, какие ресурсы и в каких объемах потребуются для успешного внедрения цифровых технологий в будущем. Переход к модели «ИТ как услуга», а также к компонуемой инфраструктуре, уменьшает сложность операций ИТ-отделов и снижает стоимость владения активами.

4. Инфраструктура на базе интеллектуальных технологий.

Без сомнений, *искусственный интеллект* (ИИ) является неотъемлемой частью цифрового предприятия будущего, так как искусственный интеллект включается в процессы анализа данных и эксплуатационной поддержки, благодаря чему инфраструктура обслуживает сама себя.

5. Преимущества Интернета вещей.

Интеллектуальные технологии, интеллектуальные пространства и гибридные ИТ-решения в сфере IoT, которые повышают эффективность, прибыльность и конкурентоспособность предприятия и помогают ускорить и упростить преобразование протекающих бизнес-процессов настолько, насколько ранее представлялось невозможным. Будучи внедренным в Индустрию 4.0, Интернет вещей дает производству сразу несколько преимуществ:

- *гибкость* производства достигается отказом от жестких «конвейерных» решений, что в конечном счете позволяет массово принимать и выполнять индивидуальные заказы, свободней внедрять в производство новые решения, свободно использовать аутсорсинг;
- *настраиваемость* производства достигается за счет его контроля на всех уровнях и благодаря его функционированию на единой технологической платформе;

- *эффективность* производства связана со снижением издержек, проистекающих из человеческого фактора: ошибок, простоев, высокой стоимости труда.

С другой стороны, Интернет вещей может быть внедрен и в быту, например, в технологиях умного дома, освобождая человека от рутины.

Негативные последствия цифровой трансформации

Функционирование мира на базе цифровых технологий Индустрии 4.0 существенно изменит некоторые прежде фундаментальные свойства реальности, заложенные в качестве принципов в онтологию, этику, эстетику, эпистемологию и т. д. Как следствие, поменяется и значительно преобразится возможная структура личности человека.

Четвертая промышленная революция несет в себе сразу несколько предпосылок для социального расслоения. Появление роботизированных решений множества задач приведет к понижению ценности низко- и среднеквалифицированного труда. Это может подорвать материальный достаток многочисленного среднего класса, что ограничивает возможности его представителей для вложения в собственный человеческий капитал, без чего для человека создаются труднопреодолимые барьеры для вхождения на рынок высококвалифицированного труда. С другой стороны, обесценивание низкоквалифицированного человеческого труда приводит к потере развивающимися странами преимущества дешевой рабочей силы и возможностей для догоняющего развития.

В то же время четвертая промышленная революция предоставляет ряд новых возможностей для традиционно отстающих стран в связи с общим перекраиванием глобального рынка труда и понижением роли некоторых ограничивающих факторов по вливанию в него, например, географического положения, институциональной неразвитости и других подобных факторов.

Ухудшающееся положение среднего класса может привести к дисбалансу политических систем и общественных отношений, опирающихся на средний класс. Это, в свою очередь, приведет к усилению глобальной неопределенности, к значительным социальным волнениям и, как следствие, к возможным кардинальным изменениям структуры общества.

Другим не менее дестабилизирующим фактором цифровой трансформации является уязвимость цифровой природы большинства объектов Индустрии 4.0 к воздействию различного рода кибератак, и на этом аспекте мы остановимся подробнее.

Угрозы и уязвимости информационных технологий при цифровой трансформации

Киберзлоумышленники, которые действуют в государственных и международных масштабах, уже обладают значительным потенциалом, необходимым опытом и инструментами для вывода из строя *критически важной инфраструктуры* (КВИ) и систем жизнеобеспечения и тем самым нанесения ущерба целым регионам [4]. Но когда появляются новости о разрушительных, деструктивных кибератаках, как, например, недавние атаки в Венесуэле, первая мысль, которая посещает некоторых специалистов в области безопасности: «Ну, эта атака не была нацелена на рынок/регион/технологическую среду, где работает наша компания, поэтому нам, скорее всего, ничего не грозит».

Однако, не обращая внимания на такие, казалось бы, отдаленные инциденты или отдавая все силы только на решение текущих ежедневных задач по предотвращению атак, ИБ-специалисты рискуют будущим, так как от их внимания ускользает то, с какой скоростью и в каком масштабе злоумышленники наращивают и совершенствуют свой атакующий киберпотенциал.

Уже на протяжении многих лет специалисты по ИБ предупреждают общество об эскалации киберпреступной активности по всему миру. Большинство релизов посвящено следующим трем проблемам [4].

1. Злоумышленники продолжают совершенствовать вредоносное ПО и выводят его на высокие уровни сложности и силы разрушительного воздействия. Эволюция вредоносного ПО стала одним из наиболее значительных событий в ландшафте атак последних лет. С появлением вирусов-вымогателей пропала потребность в использовании человеческих ресурсов для запуска процедур с требованием выкупа. Кроме того, для некоторых злоумышленников целью является не выкуп, а уничтожение систем и данных, что доказал вирус *Nyetya* – вредоносная программа по стиранию данных, замаскированная под программу-вымогатель. По мнению исследователей угроз, самораспространяющееся вредоносное ПО очень опасно и потенциально может привести к «падению» всего Интернета и замедлению цифровой трансформации в экономике.

2. Злоумышленниками оттачиваются технологии, направленные на преодоление защиты ИТ-ресурсов, в том числе существуют намерения применять в качестве кибероружия облачные сервисы и другие технологии, используемые в легитимных целях.

Помимо создания угроз, которые могут обходить все более сложные среды типа песочниц, разработчики вредоносного ПО начинают все шире использовать шифрование, получая тем самым эффективные инструменты для сокрытия своей деятельности по контролю ИТ-ресурсов и управлению ими (*command-and-control*, C2), что дает им больше времени для достижения стоящих перед ними целей. Для осуществления своей деятельности киберпреступники также используют легитимные web-сервисы, такие как Google, Dropbox и GitHub. Такая практика делает обнаружение вредоносного трафика практически невыполнимой задачей.

Кроме того, многие злоумышленники начинают запускать множественные транзакции из одного домена, что позволяет им увеличить возврат их инвестиций. Они также повторно используют ресурсы инфраструктуры, такие как зарегистрированные адреса электронной почты, номера в автономной системе (*auto-*

nomous system numbers, ASN) и серверы имен.

3. Атаки осуществляются через бреши в обороне, которые в основном появляются в связи с расширением Интернета вещей и использованием облачных сервисов.

Сетевые интеграторы, развертывая IoT-устройства, часто не уделяют должного внимания безопасности этих систем. IoT-устройства, в которые вовремя не вносятся исправления и которые не контролируются должным образом, предоставляют злоумышленникам прекрасные возможности для проникновения в ведомственные или корпоративные сети. Что еще хуже, в ИТ-средах этих организаций, как правило, имеется достаточное количество уязвимых IoT-устройств, о которых они даже не подозревают.

Тем временем, наряду с ростом популярности Интернета вещей расширяются и IoT-ботнеты, становясь более зрелыми и автоматизированными. По мере роста этих сетей злоумышленники начинают использовать их для запуска еще более сложных распределенных атак отказа в обслуживании (*DDoS*).

Злоумышленники также успешно пользуются ситуацией, когда группам по обеспечению безопасности сложно одновременно защищать и IoT, и облачные среды. Одна из причин последнего связана с недостаточной ясностью в плане того, кто же фактически ответственен за защиту этих сред.

Необходимые меры противодействия угрозам и кибератакам на критически важную информационную инфраструктуру

Нападение злоумышленников на любую организацию или *критическую информационную инфраструктуру* (КИИ) целого региона или даже страны вполне вероятно, но будут ли готовы к этому ее защитники, и как быстро они смогут устранить последствия нападения?

Результаты сравнительного исследования возможностей в области информационной безопасности за 2018 год изложены в отчете компании Cisco [4], где подробно рассмотрены лучшие практические методики в области безопасности от 3600 респондентов из 26 стран.

Выводы из отчета свидетельствуют о том, что защитникам приходится преодолевать массу трудностей. Тем не менее, ИБ-специалисты должны понимать, что стратегическое усовершенствование систем безопасности и следование распространенным лучшим практикам позволит снизить риски, замедлить прогресс криминальной деятельности злоумышленников и обеспечить лучший мониторинг ландшафта угроз.

В итоге, рекомендуются следующие меры:

- внедрение инструментов первой линии обороны, которые можно масштабировать, как, например, облачные платформы безопасности;
- гарантия соблюдения корпоративных политик и следование лучшим практикам для своевременного внесения исправлений в приложения, системы иустройства;
- внедрение сегментации сети ИКТ для снижения рисков проникновения;
- применение инструментов мониторинга и обработки оконечных устройств нового поколения;
- своевременный доступ к точным данным и процессам анализа угроз, позволяющий встраивать эти данные в процессы мониторинга и обработки событий безопасности;
- выполнение более сложного и глубокого анализа;
- анализ и практическое использование процедур реагирования на события безопасности;
- регулярное резервное копирование данных и тестирование процедур восстановления;
- анализ эффективных практик третьих сторон и тестирование технологий безопасности для снижения риска атак на цепочки поставок;
- сканирование безопасности микросервисов, облачных сервисов и систем администрирования приложений;
- анализ систем безопасности и исследование использования SSL-аналитики и SSL-дешифрования.

ИБ-специалисты также должны рассмотреть возможность применения усовершенствованных технологий безопасности, включающих *машинное обучение и возможности искусственного интеллекта*. С учетом того, что вредоносные программы умеют скрывать свои путевые траектории внутри зашифрованного web-трафика, а внутренние нарушители могут отправлять конфиденциальные данные через корпоративные облачные системы, ИБ-подразделениям необходимы эффективные инструменты для предотвращения или обнаружения использования шифрования в целях сокрытия вредоносной деятельности.

Применение машинного обучения и искусственного интеллекта к спектру угроз ИБ

Все больше специалистов в области ИБ предприятий и государственных органов начинают изучать возможности использования машинного обучения и искусственного интеллекта, чтобы решить проблему сложного мониторинга, которую создает шифрование, и уменьшить время действия злоумышленников. Благодаря усовершенствованным возможностям машинного обучения и ИИ можно укрепить защиту информационно-коммуникационной системы организации и со временем «обучить» системы безопасности автоматически выявлять нехарактерные модели поведения web-трафика, которые могут свидетельствовать о вредоносной активности.

Машинное обучение можно использовать для автоматического обнаружения уже известных угроз (так называемые «известные-известные»), то есть типов заражения, уже замеченных ранее. Однако их истинная ценность, особенно в том, что касается мониторинга зашифрованного трафика, связана со способностью обнаруживать «известные-неизвестные» угрозы (то есть ранее не замеченные вариации известных угроз, подсемейства вредоносного ПО или связанные с ними новые угрозы) и «неизвестные-неизвестные» (абсолютно новые вредоносные) угрозы. Такая технология может обучиться

идентифицировать необычные модели поведения в больших объемах зашифрованного web-трафика и автоматически предупреждать группы по обеспечению безопасности о необходимости проведения дальнейшего расследования. Последний момент наиболее важен с учетом того, что нехватка опытных и обученных специалистов становится препятствием на пути укрепления систем «обороны» на большинстве предприятий. Автоматические и интеллектуальные средства, такие как машинное обучение и искусственный интеллект, помогут людям обойтись без получения дополнительных навыков и ресурсов, но при этом более эффективно обнаруживать известные и появляющиеся угрозы и реагировать на них.

Руководители подразделений по информационной безопасности утверждают, что они готовы добавить инструменты, использующие искусственный интеллект и машинное обучение в связи с ростом сложности и расширением аналитических возможностей инфраструктур безопасности. Однако они недовольны количеством ложных срабатываний, которыми на данный момент характеризуются такие системы, поскольку ложные тревоги повышают нагрузку на отделы безопасности. По мере развития этих технологий такие проблемы должны стать менее значимыми, и системы безопасности научатся определять «нормальную» активность в исследуемых сетевых средах. В целом 39 % специалистов по безопасности полностью полагаются на технологии автоматизации, 34 % – на машинное обучение, 32 % – на искусственный интеллект [4].

Угрозы и уязвимости электронной почты

Как бы ни менялся ландшафт угроз, якобы легитимные почтовые вложения и спам остаются важными инструментами злоумышленников для распространения вредоносного ПО, так как они могут доставить угрозу непосредственно на оконечное устройство. Составив успешную комбинацию из техник социальной инженерии, например, внедрив в письмо фишинговые и вредоносные ссылки и вложения, злоумышленникам остается только сидеть и ждать, пока ничего не подозревающие пользователи активируют эти эксплойты.

Еще в конце 2016 года исследователи в области ИБ отметили значительное увеличение активности спам-кампаний, которое, похоже, совпало с уменьшением активности наборов эксплойтов. Когда такие известные наборы эксплойтов, как *Angler*, внезапно исчезли с рынка, большинство пользователей этих наборов в стремлении сохранить свою прибыль обратилось (или вернулось) к вектору угроз по электронной почте. Однако после первоначального быстрого возврата объем глобального спама снизился и оставался примерно на одном уровне большую часть первой половины 2017 года. Затем в конце мая – начале июня 2017 года этот объем значительно снизился, прежде чем вновь взлететь вверх в середине – конце лета.

Исследователи Cisco говорят, что ботнет *Necurs*, крупнейший поставщик всего спама в мире, был активен, но с января по апрель распространял меньше спама. В мае этот ботнет посредством массовых спам-кампаний распространял программу-вымогатель *Jaff*. В этих кампаниях рассылался PDF-файл со встроенным вредоносным документом Microsoft Office и начальный загрузчик программы-вымогателя *Jaff*. Исследователи в области безопасности обнаружили уязвимость в *Jaff*, которая позволила им создать дешифратор, принуждающий операторов *Necurs* быстро вернуться к распространению обычной угрозы – программы-вымогателя *Locky*. Время, которое было необходимо злоумышленникам, стоящим за Necurs, чтобы вернуться обратно к Locky, совпало со значительным спадом в объеме глобального спама, наблюдаемого в первые две недели июня.

Фишинг, в том числе целевой, – известные и уже давно используемые тактики кражи учетных данных и другой конфиденциальной информации пользователей ввиду их очень высокой эффективности. Они стали главными причинами самых крупных и известных нарушений безопасности в последние годы. Так, 2017 год был отмечен двумя значимыми примерами: широкой атакой на пользователей Gmail и взломом энергетических систем Ирландии. Чтобы измерить превалирующую роль фишинговых URL-ссылок и доменов в современном Интернете, аналитики изучили данные из источников, которые исследуют потенциально «фишинговые» электронные письма, отправляемые пользователями, с помощью сообществ и антифишинговых средств анализа угроз.

Таким образом, и в реалиях Индустрии 4.0 не стоит забывать контролировать такую «старую» угрозу, тем более что злоумышленники постоянно совершенствуют методы социальной инженерии. В борьбе с этими угрозами наряду с применением соответствующих технологий важная роль должна отводиться обучению пользователей и повышению уровня их ответственности.

Злоумышленники научились разрабатывать угрозы, которые могут обходить даже самые технологически сложные среды *песочниц*. Когда исследователи проанализировали вредоносные вложения электронной почты, оснащенные различными техниками такого рода, они обнаружили, что отдельные образцы вредоносов, использующих конкретную технику обхода, показывали резкий взлет, а затем очень быстрое падение. Это еще один пример того, как атакующие способны быстро наращивать объемы попыток проникновения сквозь защитные барьеры, когда они находят эффективную технику взлома.

Угрозы и уязвимости технологии облачных вычислений

Облачные вычисления обеспечивают практически неограниченную мощность, устраняя проблемы масштабируемости, и открывают доступ к программным и аппаратным активам, которые большинство пользователей не могли бы себе позволить. В том числе, разработчики приложений, используя управляемые через Интернет облачные вычисле-

ния и активы, являющиеся результатом такой конфигурации, имеют доступ к ресурсам, позволяющим разрабатывать продукты ИТ, которые им были ранее не по плечу.

Однако гарантий, что все ресурсы облака идентифицируемы и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака, нет. Это высокоуровневый тип угроз, так как он связан с управляемостью облаком как единой информационной системой, и к построению защиты для него следует подходить индивидуально. Для этого необходимо использовать модель управления рисками для облачных инфраструктур, которая должна предусматривать основную парадигму безопасности облачных технологий – *безопасность самого облака и безопасность внутри облака* [5].

В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. При переходе от физической инфраструктуры к виртуальной возникает множество новых угроз. При расширении виртуализации до облака их список расширяется еще более, а возможный ущерб от их эксплуатации многократно возрастает. В отличие от физической безопасности, сетевая безопасность в первую очередь предусматривает построение надежной модели угроз, включающей в себя защиту от вторжений и *межсетевое экранирование* (МЭ). Использование МЭ подразумевает работу фильтра с целью разграничения внутренних сетей облачного *центра обработки данных* (ЦОД) на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета, или серверы из внутренних сетей. В облачных вычислениях важнейшую роль выполняет технология виртуализации. Рассмотрим основные угрозы и уязвимости, связанные с облачными вычислениями.

Проблемы при перемещении физических серверов в вычислительное облако. Требования к безопасности облачных вычислений не отличаются от требований безопасности к традиционным ЦОД. Однако виртуализация последних и переход к облачным средам приводят к появлению новых угроз. Доступ через Интернет к управлению вычислительной мощностью – одна из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ персонала к серверам контролируется на физическом уровне, в облачных же средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне является одним из главных критериев защиты.

Динамичность виртуальных машин. Виртуальные машины (ВМ) динамичны. Создать новую машину, остановить ее работу, запустить заново – все эти операции можно сделать за короткое время. ВМ клонируются и могут быть перемещены между физическими серверами. Данная изменчивость плохо влияет на сохранение целостности системы безопасности. Однако уязвимости операционной системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени (например, при восстановлении из резервной копии). Таким образом, в средах облачных вычислениях важно надежно зафиксировать целостность системы защиты, при этом она не должно зависеть от состояния и местоположения системы.

Уязвимости внутри виртуальной среды. Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным ПО высока. Риск для виртуальных систем также высок: параллельные виртуальные машины увеличивает «атакуемую поверхность». Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин вне зависимости от их расположения в облачной среде.

Защита бездействующих виртуальных машин. Когда виртуальная машина выключена, она подвергается опасности заражения. Доступа к хранилищу образов виртуальных машин через сеть достаточно. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение. В данном случае должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

Защита периметра и разграничение сети. При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что безопасность менее защищенного сегмента сети определяет общий уровень ее защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами себя защищать, перемещая сетевой периметр к самой виртуальной машине, так как корпоративный МЭ – основной компонент для реализации политики безопасности и разграничения сегментов сети – не в состоянии повлиять на серверы, размещенные в облачных средах.

Приведем основополагающие технологии для защиты от перечисленных выше угроз безопасности.

1. *Шифрование* – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в ЦОД, а также в определенных случаях (по запросу клиента), безвозвратно удалять ее.

2. *Защита данных при передаче.* Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или внести в них изменения даже в случаи доступа через ненадежные узлы. Такие технологии хорошо известны – алгоритмы и надежные протоколы *AES, TLS, IPsec* давно используются провайдерами.

3. *Аутентификация* – защита паролем. Для обеспечения более высокой надежности часто прибегают к таким средствам, как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации также рекомендуется использовать LDAP (*Lightweight Directory Access Protocol*) и SAML (*Security Assertion Markup Language*).

4. *Изоляция пользователей.* Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (*Virtual Private Network*), VLAN (*Virtual Local Area Network*) и VPLS (*Virtual Private LAN Service*).

По части предоставления услуг в «облаке» выделяют следующие основные сервисы.

- *Программное обеспечение как сервис (SaaS)* – обеспечивает аренду приложений. Потребители этих сервисов – конечные пользователи, они работают с приложениями в облаке. Модель предоставления программного обеспечения как сервиса – модель обеспечения доступа к приложениям через Интернет с оплатой по факту их использования.
- *Платформа как сервис (PaaS)* – предоставляет возможность аренды платформы. Потребители – сами компании, разработавшие приложения. Платформа обеспечивает среду для выполнения приложений, сервисы по хранению данных и ряд дополнительных сервисов, например, интеграционные или коммуникационные.
- *Инфраструктура как сервис (IaaS)* – предусматривает возможность аренды серверов, устройств хранения данных и сетевого оборудования. Потребители – владельцы приложений, ИТ-специалисты, подготавливающие образы ОС для их запуска в сервисной инфраструктуре. В этой модели могут быть запущены практически любые приложения, установленные на стандартные образы.

Применение алгоритмов машинного обучения позволяет получить более подробное представление об облачной активности пользователей, а не только число скачиваний. Алгоритмы машинного обучения действительно способны обеспечить лучший мониторинг облака и поведения пользователя в нем. Если ИБ-специалисты смогут прогнозировать поведение пользователей в плане скачивания документов последними, они сэкономят время, которое можно будет потратить на изучение легитимного поведения. Они также смогут предотвратить потенциальную атаку или инцидент с утечкой данных до того, как они произойдут.

Из организаций, использующих облака, примерно одна треть размещает в них 25–49 % своей инфраструктуры, а еще одна треть – 50–74 %.

Специалисты по ИБ чаще всего (57 %) считают именно безопасность ключевым преимуществом размещения сетей в облаке, 48 % делают это из-за масштабируемости, а 46 % – из-за удобства использования.

Проблемы цифровой трансформации органов государственного управления

Результатом цифровой трансформации органов государственного управления является *электронное правительство.*

Электронное правительство (англ. *e-Government*) – способ предоставления информации и оказания уже сформировавшегося набора государственных услуг гражданам, бизнесу, другим ветвям государственной власти и государственным чиновникам, при котором личное взаимодействие между государством и заявителем минимизировано.

С точки зрения ИКТ, *электронное правительство* (ЭП) – это система электронного документооборота государственного управления, основанная на автоматизации всей совокупности управленческих процессов в масштабах страны и служащая цели существенного повышения эффективности государственного управления и снижения издержек социальных коммуникаций для каждого члена общества. Создание электронного правительства предполагает построение общегосударственной распределенной системы управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки. ЭП является частью электронной (цифровой) экономики [6].

Задачи электронного правительства:

- оптимизация предоставления правительственных услуг населению и бизнесу;
- поддержка и расширение возможностей самообслуживания граждан;
- рост технологической осведомленности и квалификации граждан;
- повышение степени участия всех избирателей в процессах руководства и управления страной;
- снижение воздействия фактора географического местоположения.

Электронное правительство обеспечивает:

- эффективное и менее затратное администрирование;
- кардинальное изменение взаимоотношений между обществом и правительством;
- совершенствование демократии и повышение ответственности власти перед народом.

В условиях развития информационно-коммуникационных технологий все сферы деятельности государственных органов в электронном виде являются востребованными гражданами и организациями различных форм собственности. Актуальность данного направления подчеркивается динамичностью развития таких сфер как, социальная (ФСС, Пенсионный Фонд, ФМС), юридическая (адвокатура, нотариат, судопроизводство), экономическая (бюджет, финансы, налоги), культурная (наука, образование), медицинская, муниципальная сфера (ЖКХ) и т. д.

Таким образом, учитывая столь важную экономическую и социальную значимость, ЭП представляет заветную мишень не только для всякого рода экономических злоумышленников, но и для недружественных государств и международных террористических группировок.

Поскольку в основном субъектами права ЭП являются граждане и хозяйствующие субъекты производственных и финансовых отношений, то главным фактором обеспечения ИБ является *защита персональных данных* (ПДн) [6].

Проблема защиты персональных данных – это, наверное, самая злободневная, противоречивая, юридически значимая и востребованная в современном обществе сфера обеспечения безопасности информации на сегодня. С одной стороны, это еще достаточно молодая область дея-

тельности: вряд ли лет пятнадцать тому назад об этом кто-либо всерьез задумывался, а сегодня – это тренд современного постиндустриального общества. В этой предметной области можно выделить две субстанции: персональные данные и их защита.

Персональные данные могут быть представлены в любой форме – текстовой, цифровой, графической, видео или акустической (информация, зафиксированная на бумаге, информация, хранимая в памяти компьютера как в двоичном коде, так и в виде, например, звука и изображения).

Каноническую триаду безопасности ПДн составляют: *конфиденциальность, целостность и доступность* [6]. Защита ПДн как раз и нацелена на сохранение этих трех канонических свойств информации, в значительной степени влияющих на ее ценность.

Заключение

Четвертая промышленная революция сегодня набирает обороты и заключается в развитии информационно-коммуникационных технологий, робототехники, искусственного интеллекта, дальнейшей цифровизации экономики, внедрении концепции «электронного правительства», электронных денег (криптовалюты), автоматизации производства и сферы услуг, расширении применения «безлюдных» технологий и транспорта, Интернета вещей, развитии центров обработки данных и облачных вычислений. Точка «технологической сингулярности» Индустрии 4.0 будет достигнута не позднее середины текущего века. Драйвером Индустрии 4.0 является цифровая трансформация экономики.

Цифровая трансформация – это не продукт информационно-коммуникационных технологий и не услуга консалтинговых компаний и вендоров. Это неизбежный и непрерывный процесс, который проходит человеческий социум и мировое бизнес-сообщество, чтобы адаптироваться к новым реалиям цифровой экономики.

Несмотря на высокую значимость влияния цифровой трансформации на бизнес, серьезным препятствием для ее развития являются организационные трудности и ограничения, связанные с унаследованными технологиями, а для подавляющего большинства из них главные проблемы связаны с обеспечением ИБ.

Организация ИБ на большинстве предприятий уже сегодня предполагает существование нескольких технологических локаций, развернутых в облаках с различными ИБ-инструментами, со своими внутренними сервисами. Стратегия цифровой трансформации может привести к дополнительному усложнению ИТ-среды, увеличению количества задействованных облаков, использованию IoT-устройств, многие из которых разработаны без учета требований безопасности. По этой причине большой проблемой является отсутствие у «безопасников» полной видимости событий в вычислительной инфраструктуре. Как следствие, необходима смена парадигмы ИБ – *от защиты периметра объекта цифровой трансформации к защите его инфраструктуры и данных.* ■

ЛИТЕРАТУРА

1. Vinge V. The Coming Technological Singularity [Электронный ресурс]. – Режим доступа: http://wwwrohan.sdsu.edu/faculty/vinge/misc/singularity.html.

2. Новоселов А. Технологическая сингулярность как ближайшее будущее человечества. http://andrzej.virtualave.net/Articles/singularity.html

3. Hanson R. A Critical Discussion of Vinge's Singularity Concept [Электронный ресурс]. – Режим доступа: http://www.extropy.com/eo/articles/vi.html.

4. Отчет Cisco по информационной безопасности за 2018 год [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/.../cisco_2018_acr_ru.pdf.

5. Артамонов В. А. Парадигма безопасности технологии облачных вычислений // Комплексная защита информации. Материалы XXII научно– практической конференции. Полоцк, 16–19 мая 2017 г. – Новополоцк: УО «Полоцкий государственный университет». – 2017. – С. 200–203.

6. Маньшин Г. Г., Артамонов В. А., Артамонова Е. В. Защита персональных данных и вопросы электронного правительства (ч. 1–4) // Проблемы создания информационных технологий. Сб. науч. трудов. – Минск: МНОО МАИТ. – 2014. – Выпуск 25. – С. 192–216.