Проблемы киберустойчивости ИКТ-систем в условиях цифровой трансформации

En

The Challenges of IT Systems Cyber Resilience in the Conditions of Digital Transformation

V. A. Artamonov,
PhD (Eng., Grand Doctor), 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)

Considering the issues of IT systems cyber resilience in the conditions of digital transformation the authors discuss cybersecurity threats that appear in this process.

Based on the results of Fortinet's survey, the authors have identified basic trends of digital transformation in organizations. The main cybersecurity threats were defined and their significance for digital transformation processes was shown. The authors propose practical recommendations for deploying a unified security architecture in the company.

Keywords: digital transformation, resilience, cyber resilience, threats of the digital transformation, information security management, unified security architecture

В статье рассматриваются вопросы киберустойчивости систем ИКТ по отношению к угрозам, возникающим в процессе цифровой трансформации. На основе глобальных статистических исследований компании Fortinet выявлены базовые тренды, влияющие на основные бизнес-процессы организаций, в которых происходит цифровая трансформация. Определены угрозы кибербезопасности и показана их значимость для процессов цифровой трансформации. Даны практические рекомендации по интеграции систем кибербезопасности для формирования единой архитектуры безопасности организации.

Ключевые слова: цифровая трансформация, устойчивость технических систем, киберустойчивость, угрозы цифровой трансформации, управление информационной безопасностью, единая архитектура безопасности

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» (МНОО МАИТ)

Введение

Прежде чем перейти к основной теме настоящей статьи, давайте определимся с некоторыми понятиями, которые, на наш взгляд, являются ключевыми в данной работе.

Фундаментальным понятием в теории технических систем является их *устойчивость*. Применительно к таковым определение устойчивости было дано выдающимся русским математиком, Академиком Петербургской Академии наук А. М. Ляпуновым (1857–1918): «*Устойчивость – это способность системы функционировать в состояниях, близких к равновесному, в условиях постоянных внешних и внутренних возмущающих воздействий*».

Применительно к системам информационно-коммуникационных технологий (ИКТ), *киберустойчивость* – это способность *киберсистемы*, работающей по определенному алгоритму, достигать цели функционирования в условиях информационно-технических воздействий внешних угроз при наличии внутренних уязвимостей.

В ряде научных источников (например, [1]) определено, что предвестником 4-й промышленной революции (*Индустрии 4.0*) является

цифровая трансформация (ЦТ), которой также дается определение. *Цифровая трансформация – это процесс интеграции цифровых технологий во все аспекты бизнес-деятельности и инфраструктуру общественных отношений, требующий внесения коренных изменений в технологии, культуру, финансовые операции и принципы создания новых продуктов и услуг [1].* 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 акцентов на периферию предприятий и повышение гибкости центров обработки данных (ЦОД), а также облачных вычислений, поддерживающих периферию. Этот процесс означает постепенный отказ от устаревших технологий, обслуживание которых может дорого обходиться предприятиям, несет в себе изменение культуры производства (переход к Интернету вещей, IoT), которое в результате поддерживает ускорение процессов, обеспечиваемое ЦТ.

Вместе с тем, ЦТ предъявляет совершенно особые вызовы компаниям и порождает новые киберугрозы для ИТ-систем, в результате чего, большинство организаций в этих условиях перестает соответствовать текущим требованиям по киберустойчивости. С этих позиций перейдем к основной части нашей работы, в которой попытаемся дать современную интерпретацию противостояния угрозам ИКТ со стороны ЦТ.

Киберустойчивость: основные тенденции в процессе ЦТ

Известно, что цифровая трансформация оказывает значительное влияние на технологии: от принятия решений на основе данных до внедрения облачных технологий, мобильности и взрывного развития Интернета вещей (IoT), но сам процесс ЦТ выходит за рамки простого развертывания новых решений. В ходе ЦТ организации должны пересмотреть сложившиеся бизнес-модели и процессы для стимулирования инноваций и улучшения результатов своей деятельности. Именно совместное применение цифровых технологий и информационных процессов дает поводы для переосмысления моделей бизнеса, а это – нелегкая задача.

Эффективная трансформация бизнес-процессов подразумевает совместные усилия всех подразделений с участием партнеров, клиентов и других заинтересованных сторон. Императивы цифровой трансформации требуют коренного переосмысления проблем безопасности ИКТ для достижения главной цели: обеспечения киберустойчивости этих систем как в отношении внешних, так и внутренних угроз.

Интеграция бизнес-систем, информационных и операционных технологий, позволяющих принимать решения на основе потоков данных, создает новые проблемы безопасности, поскольку эти вновь подключенные системы также могут увеличить ущерб от атак на корпоративные сети. В дальнейшем система безопасности должна стать целостной и автоматизированной с самого начала, а не собираться воедино с течением времени из отдельных программно-технических решений.

Аналитикам и специалистам по ИБ, чтобы охватить влияние такого глобального процесса, как ЦТ, на кибербезопасность систем ИКТ, необходимо собрать соответствующую статистику.

Именно с этой целью компания Fortinet выпустила отчет о последствиях цифровой трансформации для безопасности [2]. В ходе этого исследования было опрошено 300 руководителей служб безопасности компаний (CISO/CSO) с численностью сотрудников не менее 2500 человек из различных отраслей промышленности в Северной Америке, Европе, Азии и Австралии. Цель опроса – собрать данные о ходе цифровой трансформации в этих компаниях, а также выявить проблемные места ЦТ.

По результатам этих статистических исследований, прежде всего, рассмотрим главные ИТ-тренды, влияющие на основные бизнес-процессы компаний (рис. 1).

На основании этого исследования были выявлены следующие тенденции.

Тенденция 1: *Цифровая трансформация является самым влиятельным трендом для бизнеса в последние 5 лет.*

Из всех опрошенных специалистов, 92 % респондентов оценили процесс ЦТ как имеющий «довольно большой» или «чрезвычайно большой» эффект для организации.

Второе и третье место в рейтинге влияния на бизнес получили две тенденции, которые часто считаются элементами ЦТ: IoT (78 %), искусственный интеллект (AI) и машинное обучение (56 %).

Далее перейдем к оценке влияния ЦТ на значимость киберугроз. На рис. 2. приведен график значимости угроз кибербезопасности систем ИКТ.

В то время как во многих статьях в отраслевых СМИ и на ИТ-форумах организационные вопросы и ограничения, которые несут в себе устаревшие технологии, обсуждаются как самые большие проблемы для ЦТ,

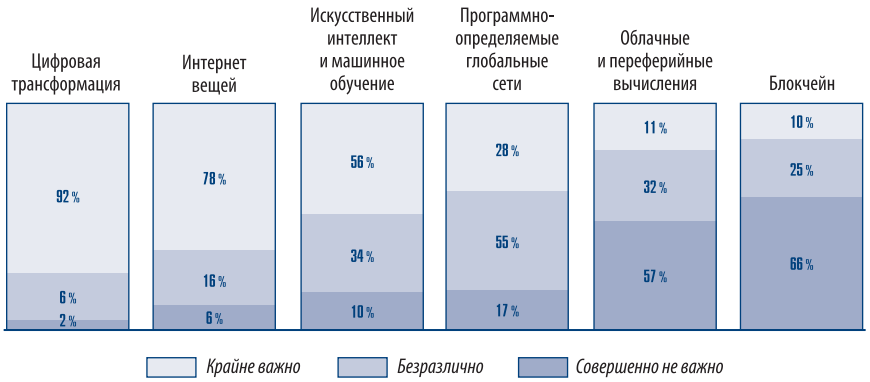

Рис. 1. ***Оценка влияния современных ИТ-трендов на основные бизнес-процессы***

Рис. 2. ***Оценка влияния ЦТ на значимость киберугроз***

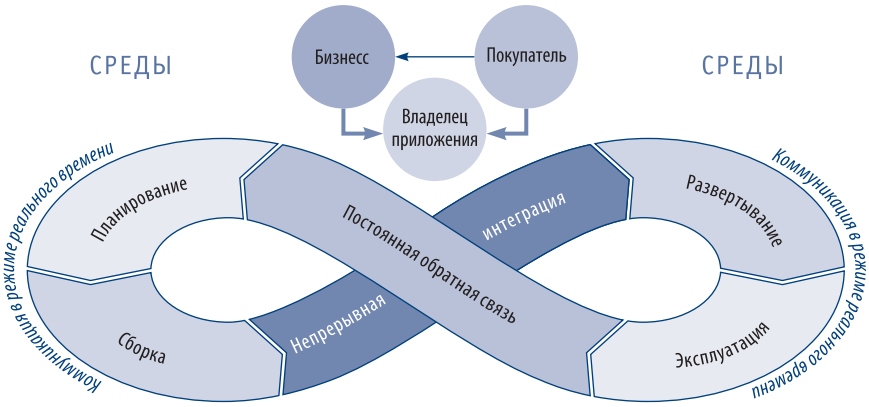

Рис. 3. ***Что такое DevOps***

что отчасти верно, специалисты по информационной безопасности в подавляющем большинстве уверены, что проблемы безопасности являются наиболее значимыми препятствиями для реализации ЦТ. А именно, 85 % опрошенных CISO/CSO (руководителей и ИБ-специалистов в компаниях) оценивают проблемы безопасности как имеющие «довольно большое» или «чрезвычайно большое» влияние на бизнес-процессы в организациях. Кроме того, второй наиболее распространенный ответ (56 %) связан с соблюдением требований отраслевых регуляторов.

Руководители ИБ-департаментов особое внимание уделяют двум источникам риска: внешнему и внутреннему. Рост полиморфных атак и угроз, которые постоянно трансформируются или изменяются, чтобы избежать обнаружения, 85 % специалистов по ИБ оценивают как «довольно большую» или «чрезвычайно большую» проблему [3]. Также следует обратить внимание (значение 81 % на рис. 2) на рост негативного влияния технологии DevOps, которая, по мнению опрошенных CISO/CSO, позволяет уязвимостям «проскальзывать» в корпоративную сеть вместе с более быстрыми темпами разработки ПО, и эта тенденция в последнее время усиливается [4]. Обе эти угрозы потенциально могут усилиться по мере того, как поверхность атаки становится более сложной в контексте проходящей в компании ЦТ. Учитывая важность упомянутых угроз для кибербезопасности, дадим расширенное толкование этим опасным технологиям.

Полиморфизм заключается в формировании кода вредоносной программы «на лету», уже во время исполнения, при этом сама процедура, формирующая код, также не должна быть постоянной и видоизменяется при каждом новом заражении. Во многих случаях изменение вредоносного кода достигается путем добавления операторов, которые не изменяют сам алгоритм работы программы (например, оператор NOP). Постоянное видоизменение программного кода вредоносной программы не позволяет создать универсальную сигнатуру для данного образца. Специалисты по кибербезопасности для противодействия этому методу успешно применяют в антивирусном программном обеспечении такие технологии, как эвристический анализ и эмуляцию.

Немного остановимся на такой популярной в последнее время в ИТ-компаниях технологии, как *DevOps*. Методология DevOps означает интеграцию деятельности разработчиков и специалистов по обслуживанию ПО, сетей и оборудования в командах и компаниях. «Модная» технология является предметом особой настороженности со стороны специалистов ИБ, так как она принципиально изменила взаимоотношения между разработчиками софта, системными администраторами, службами технической поддержки и конечными пользователями.

На рис. 3 приведена схема функционирования DevOps.

Еще одна серьезная проблема – *отсутствие полной видимости всех зон и процессов* для специалистов отделов безопасности (70 %), учитывая все более сложную вычислительную инфраструктуру, которую представляет ЦТ. Эта проблема также может являться результатом наследия неинтегрированных, многопозиционных систем и ИТ-продуктов (применявшихся в оборонной промышленности). Для обеспечения безопасности сложных, высокоразвитых распределенных сред, охватывающих удаленные филиалы, корпоративные центры обработки данных и гибридные облака, департаменты безопасности должны поддерживать наиболее полную видимость для выявления аномального поведения систем и быстрой нейтрализации угроз.

Цифровая трансформация также усилила акцент на защиту конфиденциальности и более высокие требования к ее соблюдению. По мере того, как кибератаки становятся все более изощренными и разрушительными, регулирующие органы устанавливают более строгие правила и руководящие принципы защиты

персональной идентификационной информации (англ. *Personally Identifiable Information*, PII). В результате, организации должны помнить о комплаенсе (англ. *Compliance*), то есть о следовании определенным правилам, и обращаться к лучшим в своем классе сертифицированным продуктам, процессам и специалистам, чтобы обеспечить должный уровень управления рисками. Еще до начала ЦТ системы информационной безопасности на обычном предприятии по умолчанию включали несколько разрозненных хранилищ с локальными службами и развертывались, как правило, в нескольких облачных сервисах с различными инструментами безопасности.

Стратегия ЦТ может привести к еще более сложной среде с еще большим количеством облаков и увеличением количества устройств IoT, многие из которых не были разработаны с учетом требований кибербезопасности.

Тенденция 2: *Наиболее серьезный вызов для реализации ЦТ – это безопасность и устойчивость систем к кибератакам и отсутствие прозрачности ИТ-инфраструктуры в ходе ЦТ.*

Особое внимание необходимо уделить инцидентам ИБ на объектах критической информационной инфраструктуры (КИИ); это могут быть, как таргетированные атаки (англ. *Advanced Persistent Threat*, APT), так и техногенные катастрофы, физическое похищение активов и другие угрозы. По мере усложнения атак наращиваются и «средства обороны» (то есть инфраструктура ИБ).

На этом фоне все большую популярность набирают интеллектуальные системы управления кибербезопасностью – SIEM (англ. *Security Information and Event Management*), основная задача которых – мониторинг корпоративных систем и анализ событий безопасности в режиме реального времени, в том числе с широким использованием систем искусственного интеллекта (ИИ) и глубокого машинного обучения (англ. *Deep Learning*) [5].

Тенденция 3: *Использование высокоинтеллектуальных систем для управления кибербезопасностью.*

Анализируя проблемы ЦТ для устойчивости систем ИКТ к кибератакам, приведем ранжированный в процентах сводный перечень атак, угроз и уязвимостей, а также рекомендации по предотвращению атак, ликвидации угроз и уязвимостей ЦТ (см. таблицу).

Не все организации далеко продвинулись во внедрении современных методов обеспечения безопасности, упомянутых в [2]. Также нужно учесть, что компания Fortinet проводила свои статистические исследования в основном среди так называемых высокоуровневых компаний, а потому о состоянии кибербезопасности в организациях среднего и низкого уровней можно только догадываться. Проекты по интеграции решений безопасности, обеспечению сквозной прозрачности и автоматизации контроля соответствия все еще находятся в стадии реализации в 30–40 % организаций и завершены менее чем в одной трети компаний. Такой факт, что многие из них находятся в стадии развертывания, указывает на то, что организации быстро движутся в попытках опережать развивающиеся угрозы.

Тенденция 4: *Большие объемы инфраструктуры ИКТ по-прежнему остаются уязвимыми для различного рода кибератак.*

По средним оценкам специалистов CISO/CSO, около 25 % инфраструктуры не защищены от сегодняшних угроз безопасности. По мере расширения поверхности атаки устаревшие архитектуры безопасности часто не могут масштабироваться для удовлетворения новых требований. Даже если точечные решения развернуты для обеспечения некоторой защиты, возникающее в результате этого распространение разрозненных систем означает, что общий профиль безопасности организации не может быть значительно улучшен.

Также отметим, что уязвимости, которые можно устранить с помощью обновлений программного обеспечения и исправлений, все еще остаются потенциальной проблемой для некоторых организаций.

Таким образом, можно констатировать, что далеко не все организации находятся в одинаковой степени готовности к столь сложному, а порой и длительному процессу преобразований, каковым является цифровая трансформация. Однако прорывное развитие интеллектуальных механизмов управления кибербезопасностью, в том числе на основе ИИ, вселяют в нас надежду на минимизацию этой рудиментарной тенденции в обозримой перспективе.

Таблица. ***Сводный перечень атак, угроз и уязвимостей ЦТ***

№ п/п	Атаки, угрозы и уязвимости ЦТ	Значимость угроз, %	Рекомендации по обнаружению и предотвращению атак, ликвидации угроз и уязвимостей ЦТ
1	Полиморфные атаки	85	Внедрение SIEM и систем мониторинга на базе ИИ и глубокого машинного обучения (Deep Learning)
2	Угрозы технологии DevOps	81	Переход на более безопасную технологию DevSecOps
3	Уязвимости «слепых зон» инфраструктуры ИТ-системы	70	Меры для реализации прозрачности инфраструктуры систем ИКТ, подлежащих ЦТ
4	Рост атакующего потенциала киберпреступников	68	Широкое внедрение систем автоматизации и интеграции ИБ инфраструктур систем ИТ, подлежащих ЦТ
5	Широкое использование протокола SSL	57	Для снижения доли фишинговых атак следует перейти на EV SSL сертификаты
6	Угрозы и уязвимости Интернета вещей (IoT)	47	Использование технологии блокчейн для управления аутентификацией, обеспечения неделимости информации и работоспособности ИТ-сервисов
7	Расширение пространства реализации угроз	34	Использование проактивных методов защиты информации

Заключение

Организации высокого уровня чаще интегрируют свои системы безопасности для формирования единой архитектуры безопасности. Стратегический подход означает устранение разрозненности и развертывание согласованных технологий и процессов во всех частях систем ИКТ – от конечных точек IoT до мультиоблачных инфраструктур. Такие организации придерживаются этой стратегии гораздо чаще, чем их коллеги на нижнем уровне. Высокоуровневые организации также чаще делятся информацией об угрозах в своей компании.

Одним из результатов разрозненности технологий и процессов является то, что весь объем аналитики угроз, доступный в организации, не используется во всей инфраструктуре. Только лучшие специалисты служб ИБ обращают внимание на эту проблему.

У организаций высшего уровня больше шансов убедиться, что их меры безопасности работают везде (локально, в облаке, в IoT, на мобильных устройствах и т. д.). Поскольку поверхность атаки в организации увеличивается вместе с распространением различных типов конечных точек и облачных систем, устаревшие инструменты безопасности иногда не успевают реализовать свои функции. Решение этой проблемы и обеспечение интеграции инструментов в инфраструктуру значительно улучшает состояние безопасности организации.

Топ-компании встраивают средства контроля соответствия для централизованного отслеживания и отчетности как по отраслевым стандартам, так и по стандартам безопасности.

Отрасли с жестким регулированием несколько лет назад первыми начали внедрять автоматизированный контроль соблюдения нормативных требований. В последнее время другие отрасли пытаются наверстать упущенное из-за потока новых правил и стандартов, огромных изменений в информационной инфраструктуре и меняющегося ландшафта угроз.

У организаций высшего уровня больше шансов иметь сквозную видимость во всех средах, так как сквозная видимость практически невозможна с разрозненными инструментами безопасности. Без этой прозрачности организации просто не могут идти в ногу с современным ландшафтом угроз. В то время как определение «сквозной видимости» быстро расширяется, организации, которые продвинулись дальше в этом процессе, получают наилучшие результаты. Топ-компании чаще автоматизировали более половины своих методов обеспечения безопасности.

Объем угроз, наблюдаемых сегодня в большинстве организаций, означает, что ручной мониторинг угроз и их исправление превратились из непроизводительной траты времени персонала в бессмысленную работу. Однако полная настройка автоматизации рабочих процессов требует времени и тестирования. Организации, где уровень кибербезопасности выше, продвинулись дальше по пути автоматизации, чем их менее успешные коллеги.

Основные выводы нашего исследования довольно просты:

- ЦТ – это доминирующая ныне ИТ-тенденция на рынке ИКТ-технологий, а обеспечение безопасности и нарастающие киберугрозы – самое большое препятствие на пути к полноценной цифровой трансформации.
- существуют как внутренние, так и внешние угрозы безопасности, в первую очередь, – это полиморфные угрозы и уязвимости, которые несет в себе использование DevOps.
- большинство компаний пытаются выстроить адекватную структуру безопасности, отвечающую новым реалиям, которые несет ЦТ.

Отдельные результаты исследования, безусловно, могут кого-то насторожить и заставить задуматься о целесообразности проведения ЦТ, однако надо понимать, что цифровая трансформация несет в себе и немалые плюсы. Несмотря на такие проблемы, как расширение поверхности атак, повышенная сложность управления всеми элементами ИТ-инфраструктуры и развивающийся ландшафт сложных угроз, передовым организациям все-таки удается предотвращать разрушительные атаки. Ключевым моментом на этом пути является упреждающий подход к управлению рисками, который защищает от злонамеренных атак и взломов. В частности, в организациях, придерживающихся лучших практик ИБ, уровень кибербезопасности гораздо выше, чем в тех, которые пренебрегают таковыми, и в них, как правило, не случается сбоев, потерь данных или нарушений политик ИБ.

Если говорить кратко, к лучшим практикам ИБ применительно к теме исследования можно отнести:

- проектирование такой архитектуры безопасности организации, которая обеспечивает прозрачность и видимость всей ИТ-инфраструктуры и позволяет осуществлять централизованный контроль за ней;
- выработку стратегии, использующей интеграцию для повсеместной автоматизации рабочих процессов и обмена аналитическими данными об угрозах внутри компании. ■

ЛИТЕРАТУРА

1. Артамонов В. А., Артамонова Е. В. Цифровая трансформация экономики как предвестник 4-й промышленной революции // Защита информации. Инсайд. – 2019. – № 3. – С. 25–33.

2. Fortinet 2018 Security Implications of Digital Transformation Report [Электронный ресурс]. – Режим доступа: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report.pdf (дата обращения: 14.04.2021).

3. Полиморфизм компьютерного вируса. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Полиморфизм_компьютерных_вирусов (дата обращения: 25.04.2021).

4. Что такое DevOps? Описание DevOps | Microsoft Azure/ [Электронный ресурс]. – Режим доступа: https://azure.microsoft.com/ru-ru/overview/what-is-devops/ (дата обращения: 19.04.2021).

5. Котенко И. В. Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью // Труды Института системного анализа Российской академии наук (ИСА РАН). – 2009. – Т. 41. – С. 74–103.