УДК 004.056 DOI 10.18522/2311-3103-2025-3-246-256

К.В. Якименко, В.В. Золотарев

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: МОДЕЛИРОВАНИЕ НА ОСНОВЕ ГЕТЕРОГЕННЫХ ГРАФОВ И МЕТРИК РИСКА

Данное исследование посвящено критической проблеме обеспечения информационной безопасности (ИБ) организаций в условиях активной цифровой трансформации (ЦТ), которая неизбежно влечет за собой увеличение поверхностей атаки, появление новых уязвимостей и рисков дестабилизации систем защиты. Авторы предлагают процессно-ориентированный подход, основанный на моделировании бизнес-процессов (БП) и ИТ-ландшафта с использованием гетерогенных графов. Данная модель, представляет три ключевых типа сущностей: операции, информационные системы (ИС) *и* данные *как объекты защиты, а также атрибутированные ребра, отражающие каналы передачи и их характеристики защищенности. Такой подход обеспечивает полноценную идентификацию объектов КИИ в соответствии с требованиями ФСТЭК и позволяет анализировать сложные взаимосвязи в переходных состояниях ЦТ. В рамках исследования разработан комплекс ключевых количественных метрик для управления рисками ИБ: 1. Количество Критических Путей (ККП): Отражает изменение поверхности атаки при добавлении/удалении ИС и маршрутов данных. 2. Уровень Центральности Узлов (УЦУ): Определяет наиболее критичные для связности и уязвимые ИС (точки концентрации риска). 3. Индекс Распределённости Данных (ИРД): Характеризует соотношение облачных и локальных узлов хранения/обработки данных и связанные с этим риски контроля и безопасности. 4. Время Восстановления (ВВ): Оценивает устойчивость БП к сбоям и атакам. 5. Уровень Автоматизации Защиты (УАЗ): Показывает долю автоматизированных задач ИБ для оперативного реагирования. На основе модели и метрик предложен динамический алгоритм управления ИБ процесса ЦТ. Алгоритм предусматривает: 1. Построение графовых моделей БП "как есть" и "как должно быть". 2. Непрерывное динамическое обновление модели текущего состояния в ходе ЦТ. 3. Регулярный расчет метрик для оценки рисков в* переходных состояниях. *4. Актуализация перечня рисков и защитных мер на основе анализа метрик. Результаты включают практические рекомендации по: снижению поверхности атаки; приоритезации защиты узлов с высоким уровнем критичности; оптимизации распределения данных с учетом требований безопасности и отказоустойчивости. Предложенный подход обеспечивает прозрачность и управляемость ИБ на всех этапах ЦТ, повышает устойчивость ИТ-ландшафта к угрозам и соответствие требованиям регуляторов.*

Управление информационной безопасностью; процессный подход; алгоритм управления безопасностью; угрозы информационной безопасности; цифровая трансформация.

K.V. Yakimenko, V.V. Zolotarev

INFORMATION SECURITY MANAGEMENT IN THE DIGITAL TRANSFORMATION PROCESS: MODELING BASED ON HETEROGENEOUS GRAPHS AND RISK METRICS

This study is devoted to the critical problem of ensuring information security of organizations in the context of active digital transformation, which inevitably entails an increase in attack surfaces, the emergence of new vulnerabilities and risks of destabilization of security systems. The authors propose a process-oriented approach based on modeling business processes (BP) and the IT landscape using heterogeneous graphs. This model represents three key types of entities: operations, information systems (IS), and data as objects of protection, as well as attributed edges reflecting transmission channels and their security characteristics. This approach ensures the complete identification of CII objects in accordance with the requirements of the FSTEC and allows the analysis of complex relationships in the transitional states of CT. The study developed a set of key quantitative metrics for information security risk management: 1. Number of Critical Paths (CCPs): Reflects the change in the attack surface when adding/removing ICS and data routes. 2. Node Centrality Level (UCU): Defines the most critical for connectivity and vulnerable IP (risk concentration points). 3. Data Distribution Index (DDI): Characterizes the ratio of cloud and local data storage/processing nodes and the associated control and security risks. 4. Recovery Time (BB): Evaluates the stability of the PS to failures and attacks. 5. The level of Automation of Protection (UAZ): Shows the proportion of automated information security tasks for rapid response. Based on the model and metrics, a dynamic algorithm for managing the information security of the CT process is proposed. The

algorithm provides: 1. Construction of graph models of BP "as it is" and "as it should be". 2. Continuous dynamic updating of the current state model during the CT. 3. Regular calculation of metrics for risk assessment in transition states. 4. Updating the list of risks and protective measures based on the analysis of metrics. The results include practical recommendations on: reducing the attack surface; prioritizing node protection with a high level of criticality; optimizing data distribution taking into account security and fault tolerance requirements. The proposed approach ensures transparency and manageability of information security at all stages of the IT process, increases the resilience of the IT landscape to threats and compliance with regulatory requirements.

Information security management; process approach; security management algorithm; information security threats; digital transformation.

Введение. Переход к цифровой экономике невозможен без рассмотрения вопросов создания современной информационной инфраструктуры, что регламентировано рядом нормативно правовых документов и национальных программ таких, как, например, «Цифровая экономика Российской Федерации».

Одна из основных проблем при реализации национальных программ и при обеспечении безопасности критической информационной инфраструктуры (далее – КИИ) к внешним и внутренним угрозам связана с созданием эффективной системы управления информационной безопасностью организаций в процессе цифровой трансформации (далее – ЦТ) [1].

Активный процесс цифровизации ведет к объективному увеличению количества угроз и уязвимостей в информационной инфраструктуре предприятий и государственных учреждений, а подкрепление данной тенденции курсом на импортзамещение, а также неблагоприятной внешней конъюнктурой ведет к дестабилизации систем безопасности и потере управления процессами информационной безопасности.

В предыдущей статье были рассмотрены проблемные вопросы ЦТ на примере рассмотрены угрозы и риски возникающие процессе ЦТ и предложен алгоритм информационной безопасностью процесса ЦТ.

В данной статье предполагается расширить и детализировать предложенный ранее алгоритм с учетом проведённого дополнительного исследования предложить математическую модель алгоритма на основе графа, а также сформулировать метрики которые позволят осуществлять управление информационной безопасностью ЦТ.

Основной аспект на который предполагается обратить внимание заключается в т.н. переходных состояниях.

Предполагается что цифровая трансформация представляет собой цепочку переходные состояния от изначального состояния бизнес процесса до определенного конечного которое заявлено как цель трансформации [2]. Цифровая трансформация требует интеграции технологий в существующий ИТ-ландшафт, что можно представить как цепочку взаимодействий между компонентами системы [3, 4].

При этом зачастую движение от одного состояния в другое может осуществляться не планомерно и упорядоченно, а скачкообразно, рывками. Связано это может быть с разнообразными внешними (рыночными, санкционными и иными), так и с внутренними (недостаток временны или финансовых ресурсов) факторами [5, 6].

Идея работы состоит в том, что предлагаемый алгоритм позволит не только отслеживать изменения в процессе ЦТ но осуществлять их контроль с точки зрения обеспечения информационной безопасности предприятия.

Формирование модели. Очевидным решением для формирования модели управления ИБ процесса ЦТ является использование теории графов

Граф – это математическая структура, которая состоит из множества вершин (узлов) и множества рёбер (линий), соединяющих эти вершины. Бизнес-процесс – это последовательность взаимосвязанных задач или действий, выполняемых для достижения определённой бизнес-цели. Он включает в себя ресурсы, роли и системы, необходимые для выполнения этих задач. Логично, что БП можно рассматривать как граф, для наглядной оценки взаимосвязей между различными этапами и элементами процесса. В академической литературе и практике моделирования бизнес-процессов часто используются графические представления для анализа и оптимизации процессов [7].

Одним из наиболее простых видов графов для моделирования - ориентированный граф. Ориентированные графы могут применяться для моделирования бизнес-процесса, где вершины графа описывают компоненты процесса, а дуги — направление протекания элементарных процессов [8].

Попробуем построить простейший, абстрактный БП в виде орграфа (рис. 1).

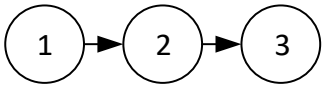

Рис. 1. Схема БП в виде орграфа

Очевидно, что простой ориентированный граф, где узлы представляют только операции, а рёбра – последовательность их выполнения, не соответствует ни задачам исследования и требованиям современных стандартов информационной безопасности по следующим причинам:

1. Отсутствие учета информационных систем (ИС). Требования правил категорирования объектов критической информационной инфраструктуры российской федерации, утвержденных постановлением Правительства Российской Федерации от 08.02.2018 № 127 и приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», требуют однозначной идентификации всех ИС и информационных активов, участвующих в критических процессах, и оценки их защищенности [9,10]. В простом графе операции не привязаны к конкретным ИС, что делает невозможным, например анализ их уязвимостей (устаревшее ПО, отсутствие шифрования в облачном сервисе и т.д.).
2. Отсутствие учета данных как объектов защиты. Согласно нормативно методических документов ФСТЭК для защиты разных видов данных могут использоваться разные ветки НМД [10]. Необходимо учитывать категории данных (персональные данные, коммерческая тайна, информация с ограничительной пометкой ДСП и т.п.). В простом графе данные не выделяются как отдельные сущности, что препятствует оценке рисков утечек или искажений.
3. Неполное отражение взаимосвязей. Требования по защите информацию подразумевают анализ всех каналов передачи данных между ИС. В простом графе рёбра отражают только логическую последовательность операций, но не физические/логические каналы связи (например, API, VPN). В свою очередь требования по защите КИИ прямо указывают на необходимость анализа и защиты от скрытых каналов передачи информации [11].

В качестве решения данной проблемы предлагается использовать гетерогенный граф, включающий узлы трёх типов – операции, ИС, данные, а также рёбра с различными атрибутами.

В первую очередь данных подход позволит обеспечить учёт ИС как узлов-исполнителей. Также каждая операция или набор операций будут связаны с определенной ИС, что позволяет с одной стороны оценивать уязвимости ИС (например, отсутствие обновлений, слабая аутентификация), а также выявлять риски, связанные с интеграцией новых ИС (например, облачных сервисов) на различных этапах и в переходных состояниях ЦТ [12].

Представление данных отдельными узлами, с опциональным указанием атрибутов их конфиденциальности позволяет обеспечить учет как самих данных с точки зрения их категорий конфиденциальности и типов (например, ПДн), а также отслеживать маршруты передачи важных данных через незащищённые каналы.

Рёбра графа, в свою очередь могут включают дополнительные атрибуты, такие как тип канала (API, HTTP, внутренняя сеть передачи данных, беспроводные каналы связи и т.п.) или уровень защищённости (шифрованный туннель, SSL-сертификат, аутентификация), что позволяет выявлять нарушения требований ФСТЭК к защите каналов передачи.

Таким образом, использование гетерогенного графа является методологически обоснованным, соответствует требованиям методических документов ФСТЭК. Данный подход позволит обеспечить идентификацию объектов защиты (ИС, данные, операции), осуществлять проектирование защитных мер на всех этапах ЦТ, а также, что является наиболее важным позволит количественно оценивать риски через метрики и осуществлять управление безопасностью процесса ЦТ в различных переходных состояниях.

Рассмотрим упрощенный бизнес процесс в виде гетерогенного графа (рис. 2). На примере упрощенного гетерогенного графа, включающего в себя ряд наборов данных, ИС и операций над данными в них, мы рассмотрим предлагаемые к использованию метрики, которые помогут осуществлять процесс управления информационной безопасностью процесса ЦТ.

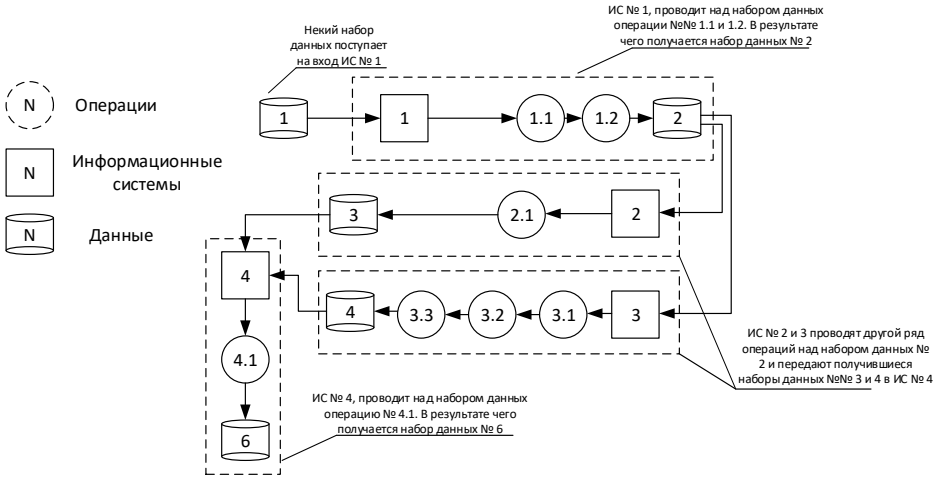

Рис. 2. БП в виде гетерогенного графа

Метрика № 1: Количество критических путей (ККП)

Термин критический путь не является стандартным для теории графов, но имеет свой контекст в теории управления проектами. Критический путь в теории управления проектами и планировании – это самая длинная последовательность задач, определяющая общую продолжительность проекта. Если в проекте есть несколько критических путей, это означает, что проект чувствителен к изменениям и требует особого внимания для своевременного завершения [13]. Количество критических путей (ККП) — это число маршрутов в графе бизнес-процесса, по которым осуществляется переход набора данных от одной ИС к другой [14]. С технической точки зрения изменение количества критических путей будет говорить нам об изменении количества информационных систем, задействованных в обеспечении функционирования БП, что в свою очередь говорит об изменении поверхности атаки доступной для злоумышленников [15].

Более приземленно критический путь можно рассмотреть, как маршрут обхода графа от точки входа (например, API, интерфейс пользователя) и до конечной ИС, обрабатывающий или хранящий выходные данные (например, база данных с ПДн, сервер отчетности). На данном пути могут находиться операции, ИС и каналы передачи данных, каждый из которых может иметь свой набор уязвимых компонентов.

В качестве примера можно рассмотреть БП формирования отчетности из предыдущей статьи. В процессе формирования отчётности критическим путём может быть цепочка состоящая из внешнего запроса → Веб-сервера обрабатывающего запрос → Сервиса агрегации данных → База данных → Генератор отчётов → Сервера публикации данных (рис. 3).

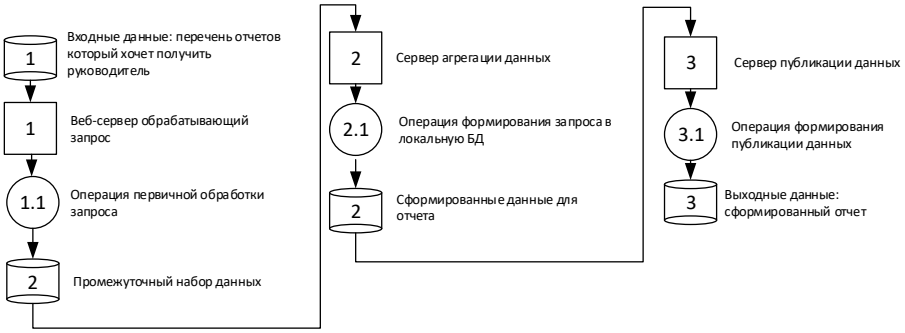

Рис. 3. Пример БП формирования отчетности

В ходе цифровой трансформации данного БП были добавлены новые источники данных предоставляющие их по запросу сервиса агрегации (рис. 4).

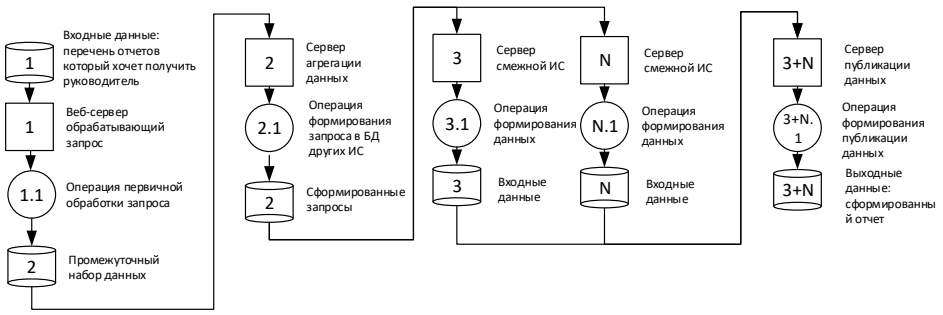

Рис. 4. Пример БП формирования отчетности после цифровой транформации

Увеличение ККП после цифровой трансформации означает, что появились новые маршруты доступа к защищаемым данным (например, интеграция облачного сервиса, добавление доступа через API). Как следствие расширяется поверхность атаки – злоумышленник имеет больше вариантов для вторжения в систему. Увеличение ККП должно быть явным сигналом к необходимости пересмотра перечня защитных мер и существующей матрицы рисков и модели угроз.

Уменьшение ККП в свою очередь будет означать упрощение архитектуры (например, удаление устаревших ИС). Сокращение уязвимых мест для совершения атак. Это хорошо, в тех случаях если не нарушается работоспособность процесса.

Таким образом в процессе управления ИБ ЦТ, мы должны стремиться к минимизации ККП без потери функциональности.

Если ККП = 0 – процесс изолирован, но, скорее всего, нефункционален (например, данные вообще никуда не передаются).

Если ККП = 1 – есть единственный путь обхода, к которому мы применяем защитные меры (например, всё шифруется и аутентифицируется). Это оптимально для высококритичных процессов. Если ККП > 1 – требуется отдельно рассматривать каждый КП и рассматривать ИС на нем, внедрять в них защитные меры.

Пример: предположим в процессе ЦТ ККП вырос с 2 до 4. Это сигнал говорящий о появлении двух маршрутов на которых могут быть новые ИС, к которым должны быть применены защитные меры.

ККП будет выступать параметром, сигнализирующим о появлении новых маршрутов на которых могут быть новые ИС, к которым в свою очередь нужно применить защитные меры. Чем меньше путей к критическим данным – тем лучше. Рост ККП также может быть сигналом к перепроектировать процесс с целью исключения избыточных взаимодействий.

Метрика № 2: Уровень центральности узлов (УЦУ)

Уровень центральности узла показывает, насколько он важен для связности всего бизнес-процесса. Чем больше маршрутов проходит через узел графа, тем выше его центральность. Например, если ИС «Сервер авторизации» участвует в 90% операций (например, проверка доступа, шифрование данных), его центральность будет крайне высокой. Если злоумышленник взломает его, он получит контроль над большей частью процесса [16].

$$\text{Сстепень}=\frac{v}{\text{n}-1},$$

где v – количество ребер, проходящих через узел, n – общее количество узлов графа.

Узел с высокой центральностью будет потенциально критическим ресурсом для атак. Например, ИС, через которую передаются все финансовые транзакции, контроллер домена и т.п., будут представлять особый интерес для злоумышленника. Помимо этого системы с узлами имеющими высокий УЦУ могут быть менее устойчивы – при выходе из строя такого узла под угрозу ставится весь БП.

Узел с низкой центральностью выполняют второстепенную роль. Даже его компрометация не нанесёт серьёзного ущерба.

В качестве примера рассмотрим ИС № 3 на рис. 3 и ИС № 3+N на рис. 4 – серверы публикации данных. До трансформации указанный сервер имел центральность по степени 0.6 (через него проходили два ребра и всего в графе было 3 однотипных узла). Предположим, что после ЦТ и добавлении пяти новых источников данных его центральность выросла и стала составлять 0.75, так как входящие в сервер данные распределены и поступают из различных системам. Это увеличивает нагрузку на указанный сервер.

Для ИБ-специалистов определение данной метрики позволит расставить приоритеты и в первую очередь рассматривать узлы с высоким УЦУ, как потенциально более интересные для злоумышленников.

УЦУ – это «индикатор важности» узла. Снижение центральности ключевых узлов уменьшает риски катастрофических последствий при атаках. Рост центральности будет сигналом к возможно пересмотру архитектуры процесса (например, внедрение распределённых систем). Естественно и то, что нельзя полностью исключить центральные узлы, но можно сделать их защиту приемлемой.

Метрика № 3 Индекс распределённости данных (ИРД)

Индекс распределённости данных (ИРД) показывает отношение количества распределённых (облачных) узлов данных к общему количеству узлов с данными. ИРД показывает насколько данные бизнес-процесса распределены между локальными и облачными системами, серверами или платформами. Чем выше ИРД, тем больше данных хранится или обрабатывается в распределённых средах (например, облаках, географически удалённых серверах), а не в одной централизованной системе.

$$\text{ИРД}=\frac{\text{Количество распределённых узлов данных}}{\text{Общее количество узлов данных}}\times 100\%.$$

Пример: Если 80% данных компании хранятся в трёх разных облачных хранилищах (AWS, Azure, Google Cloud), а 20% – на локальном сервере, ИРД будет высоким.

Высокий ИРД как и низкий имеет свои преимущества и недостатки. Преимущества заключаются в повышенной отказоустойчивости (данные не пропадут при аварии одного узла). В свою очередь увеличивается поверхность атаки (больше точек доступа для злоумышленников) и специалистам ИБ сложнее контролировать соблюдение требований по безопасность. Также могут возникнуть проблемы с согласованностью данных (дублирование, устаревшие версии и т.п.) [17, 18].

Компания хранит данные клиентов в нескольких облачных хранилищах. Это защищает от потери данных, но требует настройки единой политики доступа.

Преимуществом низкого ИРД будет простота управления и защиты поскольку все данные хранятся в одном месте (например в локальном ЦОДе). В свою очередь локальный ЦОД будет являться единой точка отказа: если злоумышленники взломают центральный узел, все данные будут скомпрометированы. Также недостатком низкого ИРД будет слабая масштабируемость – при росте нагрузки система может не справиться.

ИРД – это «индикатор гибкости и уязвимости». При слишком высоком ИРД может снижаться контроль над данными и процессами, при слишком низком снижаться устойчивость системы к атакам. Оптимальное значение зависит от типа данных, бизнес-задач и зрелости системы защиты.

Метрика № 4: Время восстановления (ВВ)

Время восстановления применительно к БП это период времени за который БП возвращаются в рабочее состояние после сбоя, атаки или иного инцидента. Например, после взлома базы данных восстановление может включать устранение уязвимости, восстановление данных из резервной копии, проверку целостности. После отказа сервера – запуск резервного оборудования или переключение на облачный ресурс [19].

Низкое ВВ (часы/минуты) говорит о том, что БП оперативно реагирует на инциденты, есть автоматизированные решения (например, резервные серверы, скрипты восстановления).

Высокое ВВ ведет к долгому простою БП, может привести к финансовым потерям, репутационным рискам, нарушению законодательства и т.п. идеальной ситуацией будет минимизация ВВ для критических систем (платежи, медобслуживание).

Метрика № 5 уровень автоматизации защиты (УАЗ)

Уровень автоматизации защиты (УАЗ) – это показатель, отражающий долю процессов информационной безопасности (ИБ), которые выполняются автоматически, без ручного вмешательства. Чем выше УАЗ, тем больше задач (мониторинг, обнаружение угроз, реагирование) решается с помощью алгоритмов, скриптов и специализированных систем (например, SIEM, SOAR) [20].

Примерами автоматизированных процессов могут быть автоматическое блокирование подозрительных IP-адресов, сканирование уязвимостей, генерация и применение правил межсетевого экрана, отправка оповещений о нарушениях в режиме реального времени.

$$\text{УАЗ}=\frac{\text{Количество автоматизированных задач ИБ}}{\text{Общее количество задач ИБ}}\times 100\%.$$

Высокий УАЗ говорит о возможности оперативного реагирования на угрозы, снижении нагрузки на сотрудников (рутину выполняют системы), минимизации человеческих ошибок (например, пропущенных уязвимостей) [21].

Алгоритм управления информационной безопасностью процесса цифровой трансформации. Исходя из проведённого исследования, сформированной модели и обозначенных проблемных вопросов ЦТ алгоритм действий, применение которого позволит учесть максимально возможное количество аспектов переходных состояний цифровой трансформации, учесть их влияние на защищенность информационных систем и сформулировать при необходимости, дополнительные защитные меры.

Алгоритм выглядит следующим образом:

1. Формирование перечня автоматизируемых бизнес-процессов, их границ и текущих показателей.
2. Определение перечня информационных систем, обрабатывающих информацию, необходимую для функционирования бизнес-процесса на текущем этапе, их взаимосвязи, перечень входных и выходных данных, текущий уровень защищенности и иные показатели информационной системы, отслеживаемые в нормальном режиме её функционирования.

3. Формирование графа бизнес-процессов «как есть» до начала ЦТ с учетом рассмотренных выше требований.
4. Формирование графа бизнес-процессов «как должно быть» после окончания процесса ЦТ, как некого целевого значения к котором мы должны прийти по завершению ЦТ.
5. Динамическое обновление графа БП «как есть» в текущий момент времени.
6. Анализ предложенных метрик.
7. Формирование\актуализация перечня рисков и защитных мер, которые необходимо предпринять в текущем переходном состоянии ЦТ.

Схема алгоритма в нотации EPC представлена на рис. 5.

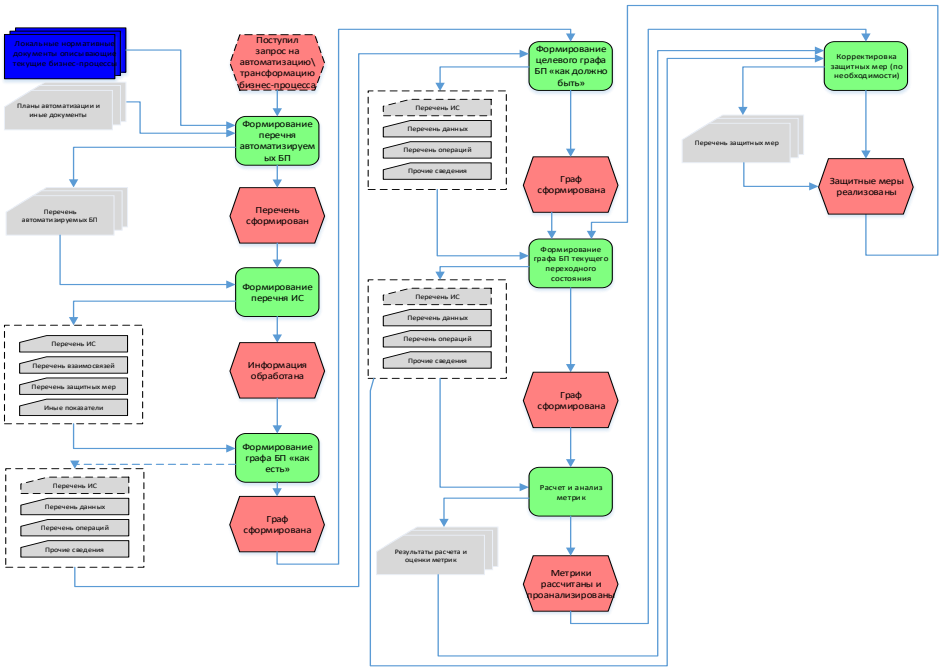

Рис. 5. Алгоритм управления

Описание алгоритма и его графическое представление наглядно демонстрирует, насколько обогащается имеющий набор данных об информационных система, инфраструктурных взаимодействия и потенциальных угрозах информационной безопасности исследуемых систем, а также какие элементы уровня организации процессов могут быть затронуты при внедрении указанного процесса.

Заключение. Исследование сосредоточено на формировании пригодных в практике рекомендаций и алгоритмов управления информационной безопасностью в процессе цифровой трансформации, с точки зрения, как традиционных подходов к управлению рисками и изменениями, так и с точки зрения комплексного подхода, учитывающего взаимосвязи бизнес-процессов и информационных систем, а также влияние изменений на смежные процессы и системы, а также организацию в целом.

Результатом исследования является формирование алгоритма управления информационной безопасностью переходных состояний цифровой трансформации, привязка данного алгоритма к переходным состояниям, измеримым метрикам информационных систем и их параметрам. Подобная привязка позволит учитывать исходное состояние информационной системы до начала процесса цифровой трансформации, а также задавать целевые значения, что в свою очередь позволит сделать процесс цифровой трансформации более прозрачным с точки зрения информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Stefan Rass.* Cyber-Security in Critical Infrastructures. Advanced Sciences and Technologies for Security Applications. – Springer, 2020.
2. *Ana-Marija Stjepić*. Mastering digital transformation through business process management: Investigating alignments, goals, orchestration, and roles. – URL: https://jemi.edu.pl/vol-16-issue-1-2020/mastering-digital-transformation-through-business-process-management-investigating-alignments-goals-orchestration-and-roles.
3. *Баланов А.Н.* Цифровая трансформация бизнеса: учебное пособие для ВУЗов. – СПб.: Лань, 2024.
4. Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16).
5. *Грибанов Ю.И.* Факторы и условия цифровой трансформации социально-экономических систем // Вестник Алтайской академии экономики и права. – 2019. – № 2-2. – С. 253-259. – URL: https://vaael.ru/ru/article/view?id=320 (дата обращения: 24.03.2025).
6. *Ревякин П.И., Зинич А.В., Помогаев В.М.* Цифровая трансформация университетов: угрозы информационной безопасности и направления снижения рисков // Экономическая безопасность. – 2024. – Т. 7, № 11. – С. 2753-2770. – DOI: 10.18334/ecsec.7.11.122061.
7. Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием. – URL: https://digital.gov.ru/uploaded/files/7metodicheskierekomendatsii06092022125913_TZmtVQB.pdf (дата обращения: 21.03.2025).
8. *Дождиков К.В.* Моделирование бизнес-процессов с помощью метаграфов // Проблемы современной экономики (Новосибирск). – 2014. – № 22-2. – URL: https://cyberleninka.ru/article/n/modelirovanie-biznes-protsessov-s-pomoschyu-metagrafov (дата обращения: 23.03.2025).
9. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных постановлением Правительства от 8 февраля 2018 г. № 127.
10. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России от 25 декабря 2017 г. № 239 (в ред. Приказов ФСТЭК России от 9 августа 2018 г. N 138, от 26 марта 2019 г. N 60, от 20 февраля 2020 г. N 35).
11. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ (последняя редакция).
12. Концепция цифровая трансформация 2030. – URL: https://www.rossetivolga.ru/i/files/2019/2/7/kontseptsiya_tsifrovaya_transformatsiya_2030.pdf (дата обращения: 21.03.2025).
13. Метод критического пути в управлении проектами. – URL: https://skillbox.ru/media/management/kak-zavershit-proekt-v-srok-s-pomoshchyu-metoda-kriticheskogo-puti-rasskazyvaem-na-primere/ (дата обращения: 24.03.2025).
14. Подробное руководство по методу критического пути. – URL: https://ru.smartsheet.com/critical-path-method (дата обращения: 24.03.2025).
15. *Пальчевский Е.В.* Прогнозирование угроз в сложных распределенных системах на основе интеллектуального анализа больших данных автоматизированных средств мониторинга // Программные продукты и системы. – 2021. – № 2. – С. 230-236. – URL: https://swsys.ru/index.php?page=article&id=4811&ysclid=m8k65v2fsd994246327.
16. Информационная безопасность и цифровая трансформация. Безопасность функционирования информационных ресурсов. Отчет ПАО «РусГидро». – URL: https://ar2023.rushydro.ru/strategic-review/information-security.html (дата обращения: 24.03.2025).
17. Роль безопасности в цифровой трансформации бизнеса. – URL: https://infars.ru/blog/rol-bezopasnosti-v-tsifrovoy-transformatsii-biznesa/ (дата обращения: 24.03.2025).
18. Технологии информационной безопасности, важные для цифровой трансформации крупного бизнеса. – URL: https://www.nic.ru/help/tehnologii-informacionnoj-bezopasnosti-vazhnye-dlya-cifrovoj-transformacii-krupnogo-biznesa_14011.html.
19. *Лобкова Е.В., Ки-Юан А.А.* Цифровая трансформация систем обеспечения безопасности // Государственное и муниципальное управление. Ученые записки. – 2023. – № 2. – С. 115-127. – URL: https://doi.org/10.22394/2079-1690-2023-1-2-115-127.
20. Цифровая трансформация, стратегия и процессы ИТ. – URL: https://kept.ru/services/tsifrovaya-transformatsiya-strategiya-i-protsessy-it (дата обращения: 24.03.2025).
21. Кибербезопасность и цифровая трансформация: 3 главных тенденции защиты данных. – URL: https://cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (дата обращения: 24.03.2025).

REFERENCES

1. *Stefan Rass.* Cyber-Security in Critical Infrastructures. Advanced Sciences and Technologies for Security Applications. Springer, 2020.
2. *Ana-Marija Stjepić*. Mastering digital transformation through business process management: Investigating alignments, goals, orchestration, and roles. Available at: https://jemi.edu.pl/vol-16-issue-1-2020/mastering-digital-transformation-through-business-process-management-investigating-alignments-goals-orchestration-and-roles.
3. *Balanov A.N.* Tsifrovaya transformatsiya biznesa: uchebnoe posobie dlya VUZov [Digital transformation of business: a textbook for universities]. Sait Petersburg: Lan', 2024.
4. Pasport natsional'noy programmy «Tsifrovaya ekonomika Rossiyskoy Federatsii», utverzhden prezidiumom Soveta pri Prezidente Rossiyskoy Federatsii po strategicheskomu razvitiyu i natsional'nym proektam (protokol ot 24 dekabrya 2018 g. № 16) [Passport of the national program "Digital Economy of the Russian Federation", approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects (minutes of December 24, 2018, No. 16)].
5. *Gribanov Yu.I.* Faktory i usloviya tsifrovoy transformatsii sotsial'no-ekonomicheskikh sistem [Factors and conditions of digital transformation of socio-economic systems], *Vestnik Altayskoy akademii ekonomiki i prava* [Bulletin of the Altai Academy of Economics and Law], 2019, No. 2-2, pp. 253-259. Available at: https://vaael.ru/ru/article/view?id=320 (accessed 24 March 2025).
6. *Revyakin P.I., Zinich A.V., Pomogaev V.M.* Tsifrovaya transformatsiya universitetov: ugrozy informatsionnoy bezopasnosti i napravleniya snizheniya riskov [Digital transformation of universities: threats to information security and directions for risk reduction], *Ekonomicheskaya bezopasnost'* [Economic Security], 2024, Vol. 7, No. 11, pp. 2753-2770. DOI: 10.18334/ecsec.7.11.122061.
7. Metodicheskie rekomendatsii po tsifrovoy transformatsii gosudarstvennykh korporatsiy i kompaniy s gosudarstvennym uchastiem [Methodological recommendations for the digital transformation of state corporations and companies with state participation]. Available at: https://digital.gov.ru/uploaded/files/7metodicheskierekomendatsii06092022125913_TZmtVQB.pdf (accessed 21 March 2025).
8. *Dozhdikov K.V.* Modelirovanie biznes-protsessov s pomoshch'yu metagrafov [Modeling business processes using metagraphs], *Problemy sovremennoy ekonomiki (Novosibirsk)* [Problems of Modern Economy (Novosibirsk)], 2014, No. 22-2. Available at: https://cyberleninka.ru/article/n/modelirovanie-biznes-protsessov-s-pomoschyu-metagrafov (accessed 23 March 2025).
9. Pravila kategorirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriev znachimosti ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy, utverzhdennykh postanovleniem Pravitel'stva ot 8 fevralya 2018 g. № 127 [Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values, approved by Government Resolution No. 127 of February 8, 2018].
10. Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Prikaz FSTEK Rossii ot 25 dekabrya 2017 g. № 239 (v red. Prikazov FSTEK Rossii ot 9 avgusta 2018 g. N 138, ot 26 marta 2019 g. N 60, ot 20 fevralya 2020 g. N 35) [On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation: Order of the FSTEC of Russia dated December 25, 2017 No. 239 (as amended by Orders of the FSTEC of Russia dated August 9, 2018 No. 138, dated March 26, 2019 No. 60, dated February 20, 2020 No. 35)].
11. Federal'nyy zakon «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» ot 26 iyulya 2017 g. № 187-FZ (poslednyaya redaktsiya) [Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 No. 187-FZ (latest revision)].
12. Kontseptsiya tsifrovaya transformatsiya 2030 [Concept of Digital Transformation 2030]. Available at: https://www.rossetivolga.ru/i/files/2019/2/7/kontseptsiya_tsifrovaya_transformatsiya_2030.pdf (accessed 21 March 2025).
13. Metod kriticheskogo puti v upravlenii proektami [The critical path method in project managemen]. Available at:https://skillbox.ru/media/management/kak-zavershit-proekt-v-srok-s-pomoshchyu-metoda-kriticheskogo-puti-rasskazyvaem-na-primere/ (accessed 24 March 2025).
14. Podrobnoe rukovodstvo po metodu kriticheskogo puti [A detailed guide to the critical path method]. Available at:https://ru.smartsheet.com/critical-path-method (accessed 24 March 2025).

15. *Pal'chevskiy E.V.* Prognozirovanie ugroz v slozhnykh raspredelennykh sistemakh na osnove intellektual'nogo analiza bol'shikh dannykh avtomatizirovannykh sredstv monitoringa [Forecasting threats in complex distributed systems based on intelligent analysis of big data of automated monitoring tools], *Programmnye produkty i sistemy* [Software Products and Systems], 2021, No. 2, pp. 230-236. Available at: https://swsys.ru/index.php?page=article&id=4811&ysclid=m8k65v2fsd994246327.
16. Informatsionnaya bezopasnost' i tsifrovaya transformatsiya. Bezopasnost' funktsionirovaniya informatsionnykh resursov. Otchet PAO «RusGidro» [Information security and digital transformation. Security of functioning of information resources. Report of PJSC RusHydro]. Available at:https://ar2023.rushydro.ru/strategic-review/information-security.html (accessed 24 March 2025).
17. Rol' bezopasnosti v tsifrovoy transformatsii biznesa [The role of security in digital business transformation]. Available at: https://infars.ru/blog/rol-bezopasnosti-v-tsifrovoy-transformatsii-biznesa/ (accessed 24 March 2025).
18. Tekhnologii informatsionnoy bezopasnosti, vazhnye dlya tsifrovoy transformatsii krupnogo biznesa [Information security technologies important for the digital transformation of large businesses]. Available at: https://www.nic.ru/help/tehnologii-informacionnoj-bezopasnosti-vazhnye-dlya-cifrovoj-transformacii-krupnogo-biznesa_14011.html.
19. *Lobkova E.V., Ki-Yuan A.A.* Tsifrovaya transformatsiya sistem obespecheniya bezopasnosti [Digital transformation of security systems], *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski* [State and Municipal Administration. Scientific Notes], 2023, No. 2, pp. 115-127. Available at: https://doi.org/10.22394/2079-1690-2023-1-2-115-127.
20. Tsifrovaya transformatsiya, strategiya i protsessy IT [.Available at: https://kept.ru/services/tsifrovaya-transformatsiya-strategiya-i-protsessy-it [Digital transformation, strategy and IT processes] (accessed 24 March 2025).
21. Kiberbezopasnost' i tsifrovaya transformatsiya: 3 glavnykh tendentsii zashchity dannykh [Cybersecurity and digital transformation: 3 main trends in data protection]. Available at: https://cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (accessed 24 March 2025).

Якименко Кирилл Викторович – Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева; e-mail: Yakimenko.KV@yandex.ru; г. Красноярск, Россия; аспирант; ORCID: 0009-0003-3374-1569.

Золотарев Вячеслав Владимирович – Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева; e-mail: zolotorev@mail.sibsau.ru; г. Красноярск, Россия; к.т.н.; зав. кафедрой безопасности информационных технологий; ORCID: 0000-0002-8054-8564.

Yakimenko Kirill Viktorovich – Reshetnev Siberian State University of Science and Technology; e-mail: Yakimenko.KV@yandex.ru; Krasnoyarsk, Russia; graduate student; ORCID: 0009-0003-3374-1569.

Zolotarev Vyacheslav Vladimirovich – Reshetnev Siberian State University of Science and Technology; e-mail: zolotorev@mail.sibsau.ru; Krasnoyarsk, Russia; cand. of eng. sc.; head of Information Technologies Security Department; ORCID: 0000-0002-8054-8564.

УДК 621.396.624 DOI 10.18522/2311-3103-2025-3-256-264

А.П. Плёнкин

ЭНЕРГЕТИЧЕСКАЯ МОДЕЛЬ МАГИСТРАЛЬНОЙ КВАНТОВОЙ СЕТИ

Уже сегодня в России и во всём мире активно разворачиваются и создаются сети квантовых коммуникаций, разрабатываются стандарты в области квантовых технологий. В рамках дорожной карты по развитию квантовых коммуникаций в России реализуется протяженность квантовых сетей более 7 тыс. км, а к 2030 году планируется более 15 тыс. км. Квантовые коммуникации сегодня – это, по сути, технология квантового распределения ключей, которая находятся на стадии интенсивного научного исследования и развития. Применительно к магистральным квантовым сетям технология распределения секретных ключей нуждается в новых подходах реализации, так как использование аппаратуры различных вендоров и протяженность волоконно-оптических линий связи накладывают преодолимые ограничения на топологии магистральных сетей. Немаловажным аспектом при проектировании квантовых сетей является расчет потерь в