УДК 330.356 **EDN EJCIOC**

Д.В. Белова

КЛАССИФИКАЦИЯ УГРОЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ, ВЫЯВЛЯЕМЫХ НА ОСНОВЕ ТЕХНОЛОГИЙ ЦИФРОВЫХ ДВОЙНИКОВ

МИРЭА – Российский технологический университет
Москва, Россия

Рассмотрена новая парадигма обеспечения экономической безопасности, в которой внимание акцентировано на переходе от пассивных методов реакции на угрозы к активным превентивным действиям для прогнозирования негативных сценариев развития событий. Предложена концепция использования цифровых двойников (ЦД) как центрального элемента системы мониторинга и прогнозирования рисков. Под цифровыми двойниками понимается виртуальная копия физических объектов и процессов, обеспечивающая постоянный мониторинг состояния организации и моделирование последствий возможных угроз. Рассмотрены основные компоненты экономического риска, охватываемые технологиями ЦД. Операционная безопасность обеспечивается путем детекции отклонений в производственном процессе, что способствует сокращению вероятности выхода оборудования из строя и улучшает качество выпускаемой продукции. Риски финансовой устойчивости уменьшаются благодаря постоянному контролю ликвидности, своевременному предупреждению случаев просрочки платежей и проведению стрессового тестирования инвестиционного портфеля. Информационная и кибербезопасность обеспечиваются благодаря применению инструментов, позволяющих анализировать поведение пользователей сети и выявлять возможные атаки на систему. Стратегия и репутация компании защищены возможностями ЦД, позволяющими оценивать риски стратегических решений и заблаговременно реагировать на потенциальные угрозы репутации. Составлена классификация угроз по ключевым компонентам производственной инфраструктуры.

Ключевые слова: цифровой двойник, экономическая безопасность, предиктивная аналитика, сценарное моделирование, машинное обучение, классификация угроз.

Введение. В современных условиях не вызывает сомнения актуальность проблемы обеспечения экономической безопасности предприятия. Усложнение бизнес-процессов, высокая изменчивость рынков и рост киберрисков говорят о необходимости перехода от ответных мер к предиктивным. Традиционные системы выявления угроз, основанные на анализе исторических данных, как правило, не успевают адаптироваться к изменениям и не способны моделировать комплексные сценарии негативного воздействия.

В этом контексте технология цифровых двойников (ЦД) дает новые возможности управления рисками. Будучи виртуальной динамической копией физического актива или процесса, ЦД позволяет не только отслеживать состояние предприятия в реальном времени, но и проводить имитационное моделирование для прогнозирования последствий прецедентов.

Цифровой двойник (ЦД) – инструмент, эффективность которого зависит от системности подхода к идентификации и категоризации угроз, которые он призван обнаруживать. В рамках статьи рассмотрим его как центральный элемент новой системы мониторинга экономической безопасности и предложим детализированную классификацию угроз экономической безопасности предприятия.

Обзор литературы. Рассмотрим подходы к классификации угроз, которые применяются в отечественных и зарубежных исследованиях. Одним из основных критериев классификации является источник происхождения угроз. По этому признаку выделяют внутренние угрозы, возникающие внутри системы вследствие управленческих ошибок, мошенничества, неэффективных процессов или неправомерных действий сотрудников [1-4], и внешние, источники которых находятся за пределами структуры предприятия (волатильность рынка, изменения в законодательстве, международную конкуренцию, геополитическую нестабильность и кибератаки) [4-6]. Другой возможный критерий – воздействие [3, 7]. Здесь выделяют угрозы: стратегические – влияют на достижение долгосрочных целей; операционные – влияют на повседневную деятельность; текущие – представляют непосредственную опасность.

В источниках [1, 3, 5, 8], помимо прочего, угрозы классифицируются по механизму действия: экономические, финансовые, правовые, технологические, социальные и экологические. Уровень и масштаб воздействия как источник классификации встречается в работах [2, 5, 9], где выделяют: микроуровень – воздействие на отдельные предприятия или кластеры; мезоуровень – воздействие на секторы или отрасли; макроуровень – воздействие на национальную или мировую экономику. Умышленность как ключевой критерий представлена в работе [3]. По этому признаку угрозы делятся на преднамеренные (мошенничество, саботаж) и непреднамеренные (ошибки, несчастные случаи).

Реже встречается классификация по признаку предсказуемости. Прогнозируемы и непредвиденные угрозы различают в работах [3, 10]. Помимо признака предсказуемости, в источнике [10] угрозы экономической безопасности классифицируются по признаку происхождения: природные, техногенные или форс-мажорные события.

Многообразие подходов к классификации позволяет сформировать комплексное и многомерное представление об угрозах экономической безопасности (рис. 1).

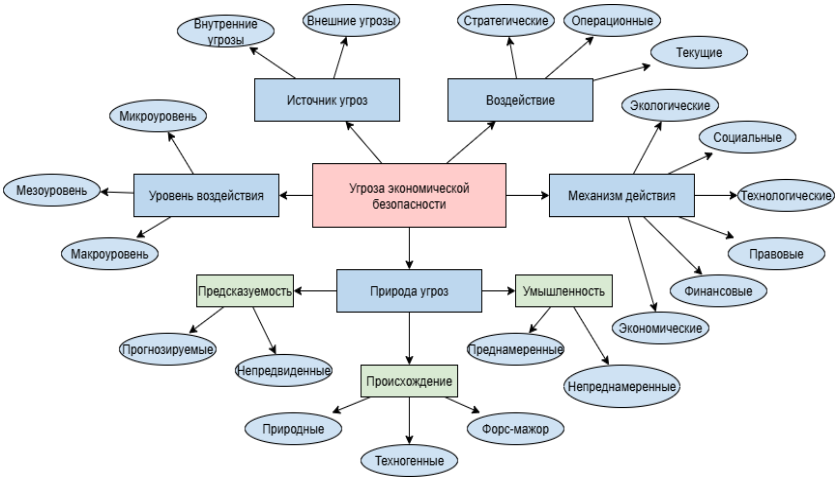

Рис. 1. Классические категории угроз экономической безопасности
Источник: составлено автором

В работе [11] описана универсальная модель управления инцидентами информационной безопасности на предприятии. Для построения синонимичной модели для инцидентов экономической безопасности и корректного выделения функций-компонентов модели необходимо классифицировать угрозы по принципу локализации объекта экономической системы в модели цифрового двойника. Подобная классификация позволит не только констатировать факт угрозы, но и точно определить, какой элемент бизнес-системы уязвим, смоделировав последствия и контрмеры.

В статье [12] представлена концептуальная схема цифрового двойника производства, направленного на прогнозирование рисков возникновения угроз и моделирование последствий реализации возможных инцидентов экономической безопасности (рис. 2).

Методика обработки данных в цифровом двойнике обусловлена их форматом, который определяется спецификой компонента бизнес-системы и способом получения информации [12]. В данном контексте рассмотрим структуру цифрового двойника, детализированную по ключевым элементам производственной инфраструктуры, а именно: производственному процессу (операций), финансам, ИТ-инфраструктуре и системе принятия решений.

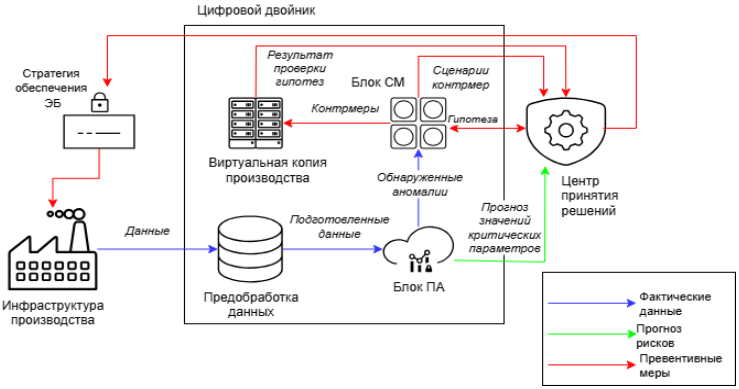

Рис. 2. Концептуальная модель цифрового двойника
Источник: [12]

Угрозы операционной и производственной безопасности. Цифровой двойник производственной линии (или цифровой двойник операций) представляет собой динамическую, виртуальную копию реальной линии, которая в режиме реального времени отражает все ее процессы. Его ядро – комплекс математических моделей, симуляций и алгоритмов машинного обучения. Данные получают от IoT-датчиков, систем управления (SCADA, MES) и бизнес-систем (ERP). За счет этого цифровой двойник производственной линии позволяет предсказывать и предотвращать угрозы операционной и производственной безопасности.

Первая группа угроз, которую выделим в этой категории – угрозы физическим активам и непрерывности производства. Используя методы прогнозного обслуживания (Predictive Maintenance), основанные на анализе временных рядов данных с вибродатчиков, термопар и акустических сенсоров, ЦД способен предсказать угрозу внезапного отказа оборудования. Собранные с реальных датчиков данные позволяют ЦД построить функциональную зависимость параметра от времени. Это позволяет получать конкретные прогнозы, что помогает избежать затрат на простой линии и срыва сроков поставки. Помимо предсказания отказов, цифровой двойник непрерывно отслеживает общую эффективность оборудования. OEE (Overall Equipment Effectiveness) – интегральный показатель эффективности производственного оборудования. Ключевые метрики:

$$Доступность = \frac{Фактическое\ \ рабочее\ \ время}{Плановое\ \ рабочее\ \ время} \times 100\%$$

$$Производительность = \frac{Количество\ \ фактически\ \ произведенных\ \ единиц}{Номинальная\ \ мощность\ \ оборудования} \times 100\%,$$

$$Качество = \frac{Количество\ \ качественных\ \ изделий}{Общее\ \ количество\ \ произведенной\ \ продукции} \times 100\%.$$

Система автоматически фиксирует и классифицирует простои, будь то переналадка, ожидание сырья или остановки и проводит корреляционный анализ, выявляя взаимосвязи между критическими показателями: скорость линии, процент брака, что позволяет предотвратить недополучение продукции, перерасход энергии и сырья, а также производство скрытого брака. Таким образом, ЦД операций оценивает риск угрозы снижения эффективности оборудования, а также интегрирует данные о качестве с визуальных систем инспекции и датчиков размеров с параметрами технологического процесса, за счет чего возможно выявление угроз качеству продукции и репутации.

С помощью статистического анализа (включая регрессионные модели) ЦД устанавливает причинно-следственные связи, определяя корреляцию основных физических показателей оборудования, показателей эффективности и процента брака. Это позволяет поддерживать режимы в «зоне качества», избегая затрат на переработку, утилизацию, потерю материалов и имиджевые потери. Кроме того, ведение цифрового следа (digital thread) для каждой единицы продукции, с полной историей параметров изготовления и используемого сырья, позволяет в случае рекламаций мгновенно проводить анализ, точно устанавливать партию и причину, минимизируя зону отзыва и защищая репутацию. Перечисленные меры, реализуемые с использованием технологий ЦД, позволяют проактивно работать с угрозами производства бракованной продукции и угрозами несоблюдения стандартов и контрактных обязательств.

Далее выделим группу угроз операционной эффективности и цепочке поставок. Цифровой двойник использует дискретно-событийное имитационное моделирование (DES) [3] для выявления «узких мест» («бутылочные горлышки» в процессах). Менеджер может в интерфейсе виртуально «запустить» увеличение такта работы одного станка и увидеть, где возникнет очередность и простой, что позволяет оптимизировать загрузку до внесения реальных изменений и избежать недогрузки мощностей и повышенных операционных расходов. Интеграция с системами складского учета и логистики позволяет моделировать сценарии методом «Что, если», например, просчитывая каскадный эффект от двухдневной задержки поставки компонента – через сколько часов линия встанет, какие заказы будут сорваны, каковы будут финансовые штрафы. Это дает возможность заранее найти альтернативных поставщиков и снизить риски срыва плана.

Угрозы ресурсной безопасности и затратам также эффективно выявляются через построение цифровым двойником моделей оптимального потребления на основе данных со счетчиков и с датчиков. Выявление неочевидных зависимостей позволяет предотвратить рост себестоимости продукции и снижение маржинальности. Более того, цифровой двойник обладает собственной объективной моделью «идеального» расхода материалов, и сравнение фактического расхода с плановым из ERP и теоретическим из ЦД позволяет находить аномалии. Несоответствие данных по

расходу сырья из ERP и данных, смоделированных ЦД, служит сигналом к проверке на брак, неучтенные потери или хищение, обеспечивая контроль над ресурсами.

В заключение стоит отметить, что ЦД производственного процесса также может найти применение в минимизации угроз человеческому фактору и компетенциям. В обозначенной ситуации он выступает как тренажер и система поддержки решений. Новый оператор может отрабатывать навыки на виртуальной копии, не рискуя остановить реальное производство, а в рабочем режиме система может давать подсказки о выходе параметров за границы безопасной работы для инструмента, снижая риск ошибок и повышая операционную надежность.

Систематизируем перечисленные виды угроз на рис. 3.

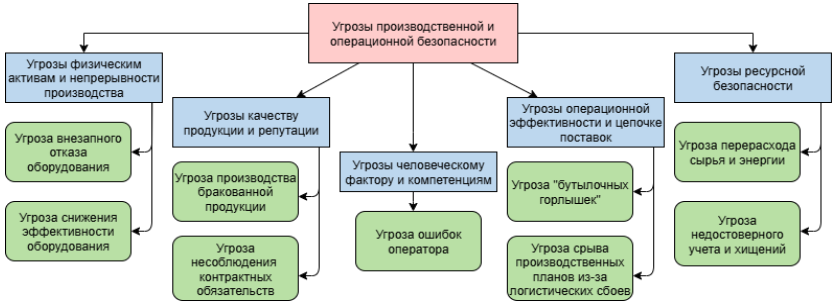

Рис. 3. Угрозы производственной и операционной безопасности
Источник: составлено автором

Угрозы финансовой устойчивости. Рассмотрим цифровой двойник, отражающий финансовую инфраструктуру предприятия, как инструмент для выявления многоуровневых угроз экономической безопасности предприятия, который позволит обеспечить переход от контроля к прогнозированию. Первая группа угроз, выделенная в этой категории, – угрозы ликвидности и платежеспособности. ЦД финансов строит динамическую модель движения денежных средств, которая интегрирует данные из ERP-систем о графиках платежей поставщикам, CRM – о поступлениях от клиентов и операционные данные о продажах. Механизм обнаружения угроз основан на постоянном перерасчете прогнозов в реальном времени на основании изменяющихся данных. С использованием механизмов ЦД финансов возможно выявить угрозы дебиторской задолженности. ФЦД применяет ML-модели для оценки рисков просрочки, анализируя историю платежей, новостной фон с использованием NLP и кредитные рейтинги контрагентов.

Для построения подобной модели необходимо сформировать признаковое пространство. В данном случае модель оперирует не «сырыми»

данными, а специально форматированными признаками. Возможный перечень признаков приведен в табл. 1.

Таблица 1.

Признаки для прогнозирования вероятности дебиторской задолженности

Категория признаков	Обозначение	Название
Историко-платежные признаки	x_1	Средний период просрочки
	x_2	Максимальная просрочка
	x_3	Доля просроченных платежей
	x_4	Коэффициент выполнения обязательств
	x_5	Время реакции на напоминание
Финансовые и поведенческие признаки	x_6	Объем закупок и их динамика
	x_7	Средний размер чека
	x_8	Частота заказов
Внешние признаки (извлекаются с помощью NLP и анализа внешних данных)	x_9	Кредитный рейтинг
	x_{10}	Тональность новостей
	x_{11}	Наличие судебных исков
	x_{12}	Возраст бизнеса клиента

Источник: составлено автором

Для каждого клиента i формируется вектор признаков $x_i = (x_1, x_2, x_3 \dots x_n)$. После формирования признакового пространства происходит расчет скоринговой оценки. Функция $S(x_i)$ преобразует вектор признаков x_i в числовую оценку (скор), где меньшее значение говорит о более высоком риске. Получение функции $S(x_i)$ возможно методами, описанными в работе [3]: регрессия или градиентный спуск. Вероятность просрочки для клиента i с характеристиками x_i рассчитывается по формуле:

$$P(delay, x_i) = \frac{1}{1+e^{-S(x_i)}}.$$

Здесь, через логическую функцию (сигмоиду) линейная функция $S(x_i)$ преобразуется в вероятность от 0 до 1.

Система присваивает каждому клиенту скор платежной дисциплины и автоматически классифицирует задолженность по категориям риска (низкий риск $P < 0{,}05$, умеренный риск $0{,}05 \le P < 0{,}2$, высокий риск $P \ge 0{,}2$).

Угрозы рентабельности и маржинальности выявляются через интеграцию ЦД финансов и ЦД операций, рассмотренном выше. Методом сценарного анализа система моделирует влияние роста цен на сырье, тарифов или логистических издержек на себестоимость продукции. В сфере валютных и рыночных угроз ЦД финансов, имеющий доступ к биржевым данным, рассчитывает валютную позицию компании в реальном времени. Механизм стресс-тестирования через моделирование Монте-Карло [3] позволяет оценить финансовые потери при различных сценариях ослабления национальной валюты.

Угрозы, связанные с инвестициями и стратегией, выявляются посредством тщательной проверки проектов в ЦД финансов до их реализации. Этот процесс включает в себя анализ множества сценариев чистой приведенной стоимости (NPV) с различными параметрами, такими как стоимость капитала, сроки и выручка. Пессимистический сценарий может выявить отрицательную NPV при увеличении затрат на 20 % и снижении выручки на 15 %, что требует пересмотра или отсрочки проекта. Угрозы поглощения исследуются через моделирование изменений в структуре капитала: например, выкуп акций может повысить капитализацию на 5 %, но также снизить финансовую устойчивость, делая компанию уязвимой для сделок выкупа долговым финансированием (LBO), что требует взвешенных решений.

Систематизируем перечисленные виды угроз на рис. 4.

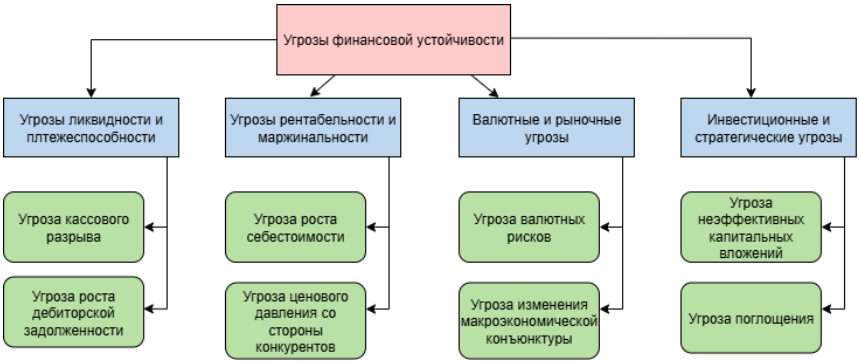

Рис. 4. Угрозы финансовой устойчивости
Источник: составлено автором

Угрозы информационной и кибербезопасности. Для выявления угроз информационной и кибербезопасности стоит анализировать IT-инфраструктуру предприятия за счет построения цифрового двойника, который представляет собой копию всей технологической среды компании, которая синхронизируется с физической инфраструктурой в реальном времени через системы мониторинга, API и средства управления.

За счет мониторинга в режиме реального времени показателей «здоровья» критического оборудования (табл. 2) средствами ЦД возможно выявление угроз операционной непрерывности. Механизм выявления угроз основан на методах прогнозного обслуживания (Predictive Maintenance) с использованием алгоритмов машинного обучения, которые анализируют временные ряды метрик и прогнозируют остаточный срок службы компонентов. Механизм аналогичен описанному в первом разделе текущей статьи.

В контексте сетевой безопасности ЦД IT-инфраструктуры моделирует потоки данных на основе стандартов NetFlow и sFlow, создавая пове-

денческий базис нормального сетевого трафика. Механизм обнаружения аномалий работает в реальном времени – резкий всплеск исходящего трафика с конкретного сервера может свидетельствовать о его участии в несанкционированной передаче данных.

Таблица 2.

Показатели «здоровья» критического оборудования

№	Показатель	Пояснение
	Показатели использования ресурсов	
1	**Загрузка центрального процессора**	Процент использования вычислительных мощностей. Устойчивая загрузка на уровне 90-100 % может указывать на необходимость масштабирования или оптимизации кода
2	**Использование оперативной памяти**	Процент занятой памяти. Высокое значение, особенно в сочетании с использованием SWAP-памяти (подкачки), ведет к резкому падению производительности
3	**Загрузка сетевых интерфейсов**	Объем передаваемых и получаемых данных. Позволяет выявить сетевые узкие места или нехарактерную активность
4	**Выполнение операций ввода-вывода**	Скорость чтения и записи данных на накопители. Высокая нагрузка может указывать на проблемы с базой данных или неоптимальные запросы
	Показатели надежности и ошибок	
5	**Температура компонентов**	Перегрев процессора, GPU, жестких дисков или компонентов материнской платы является предвестником аппаратного сбоя. Температура часто коррелирует с нагрузкой, и аномальный рост при нормальной нагрузке – тревожный сигнал
6	**Статус дисковых массивов**	Состояние аппаратных RAID-контроллеров. Предупреждения о деградации массива или о сбое диска критически важны для предотвращения потери данных
7	**Ошибки оборудования**	К этой группе отнесем ошибки памяти и ошибки дисков, которые являются индикаторами деградации модуля памяти
8	**Статус аппаратных компонентов**	Мониторинг состояния блоков питания через датчики напряжения и нагрузки, а также вентиляторов системы охлаждения
	Показатели производительности и доступности	
9	**Время отклика системы**	Задержка при ответе на запросы. Рост латентности часто является первым признаком проблем, даже если загрузка ресурсов еще не достигла пика
10	**Доступность сервиса**	Время непрерывной работы системы и отдельных служб. Внеплановые перезагрузки или падения сервисов фиксируются и анализируются
11	**Очереди запросов**	Длина очереди процессов, ожидающих обработки CPU или диском. Длинные очереди сигнализируют о том, что система не справляется с нагрузкой

Источник: составлено автором

Важной возможностью является запуск сценариев DDoS-атак на виртуальную копию для проверки устойчивости инфраструктуры и эффективности механизмов защиты, что позволяет избежать реальных простоев и связанных с ними репутационных потерь.

Для противодействия инсайдерским угрозам цифровой двойник интегрируется с SIEM-системами и применяет поведенческую аналитику. Система формирует цифровые профили пользователей, анализируя их привычные поведенческие модели: обычное рабочее время, типичные используемые ресурсы и стандартные объемы передаваемых данных. Любые отклонения от базовой нормы, например, скачивание больших объемов информации в нерабочие часы, мгновенно распознаются как аномалии, что позволяет своевременно выявлять внутренние мошеннические действия и предотвращать утечку критически важной информации.

В области оптимизации финансовых затрат цифровой двойник анализирует использование облачных ресурсов, идентифицируя недогруженные виртуальные машины и хранилища. Инструмент изменения размеров в виртуальной среде позволяет точно прогнозировать результаты модификаций конфигураций перед их интеграцией в рабочую среду.

ЦД IT-инфраструктуры включает в себя цифровую модель отраслевых стандартов и осуществляет автоматизированный аудит на соответствие этим требованиям. Система непрерывно проверяет конфигурации на предмет соответствия требованиям безопасности – отключение устаревших протоколов шифрования, настройка шифрования дисков, ведение логов безопасности. Этот механизм предотвращает риски аннулирования лицензий и исключения из реестров поставщиков, что особенно критично для компаний, работающих с государственным заказом.

Систематизируем перечисленные виды угроз на рис. 5.

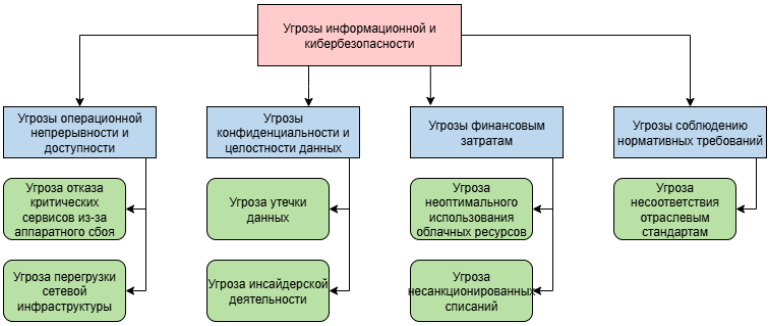

Рис. 5. Угрозы информационной и кибербезопасности
Источник: составлено автором

Несмотря на то, что ЦД является эффективным инструментом для выявления угроз информационной и кибербезопасности, он сам становится объектом для атак. Компрометация ЦД может привести к катастрофиче-

ским последствиям, поскольку он превращается из средства защиты в инструмент дезинформации и скрытого контроля.

Основные векторы атак на ЦД и их последствия приведем в табл. 3.

Таблица 3.

Показатели «здоровья» критического оборудования

Вектор атаки	Цель	Последствия
Атаки на целостность данных	Скрыть реальную атаку на физическую инфраструктуру	Принятие неверных решений на основе ложной информации, что ведет к физическому ущербу, отказам и финансовым потерям
Компрометация модели	Слепота ЦД к определенным угрозам	Система безопасности перестает видеть реальные угрозы, создавая у операторов ложное чувство безопасности
Атаки на доступ и управление	Шпионаж и диверсия	Полный контроль над управлением инфраструктурой, маскирующийся под легитимные действия системы автоматизации
Атаки на синхронизацию	Создание неопределенности и управленческого паралича	Невозможность адекватно оценить обстановку и принять правильное решение во время инцидента

Источник: составлено автором

Угрозы стратегической безопасности и репутации. Цифровой двойник принятия решений представляет собой наиболее сложную форму цифрового двойника, функционирующую как синтетическая среда для моделирования долгосрочных последствий управленческих решений в условиях неопределенности. Этот инструмент интегрирует данные из операционных и финансовых цифровых двойников, создавая уникальную «песочницу» для топ-менеджмента, позволяющую отвечать на стратегические вопросы типа «Что, если?». В такой среде возможно отслеживание комплексных (кросс-функциональных) угроз, поскольку ЦД принятия решений позволяет реализовать симуляцию взаимодействия всех органов, что позволит смоделировать каскадные сбои или последствия от неверных стратегических решений.

Ключевой угрозой, которую позволяет выявить ЦД принятия решений, является стратегическая слепота – принятие решений на основе устаревших данных или интуиции, что ведет к утрате конкурентных преимуществ. Для выявления этой угрозы ЦД использует сценарное моделирование рыночной динамики, анализируя данные о технологических трендах, поведении конкурентов и макроэкономических показателях.

Развивая тему стратегических рисков, особое внимание следует уделить угрозе некорректной M&A-стратегии (комплексный план компа-

нии по использованию сделок слияний и поглощений для достижения своих стратегических и финансовых целей). Неудачное поглощение другой компании может привести не к синергии, а к долговой нагрузке и проблемам интеграции. Механизм выявления этой угрозы заключается в виртуальном слиянии – ЦД загружает финансовые и операционные данные компании-цели, создавая ее цифровую копию и моделируя процесс интеграции. При оценке рисков необходимо учитывать вероятность возникновения сбоев, связанных с внедрением новых технологий или появлением новых участников на рынке. Продукты, которые могут кардинально изменить правила игры в отрасли, представляют серьезную угрозу для компаний. Цифровой двойник (ЦД) позволяет моделировать воздействие таких внешних условий на ключевые бизнес-показатели, что позволяет преобразовать гипотетическую угрозу в количественную оценку, требующую немедленных инвестиций в научно-исследовательские разработки.

Репутационный кризис – одна из самых опасных нематериальных угроз. Он напрямую влияет на рыночную стоимость компании и доверие клиентов. ЦД использует моделирование событий, чтобы оценить последствия скандалов или утечек данных. Система учитывает не только прямые штрафы, но и отток клиентов, падение акций и потерю партнеров. Это позволяет превратить затраты на профилактику в стратегическую инвестицию, которая окупается.

В заключение анализа необходимо отметить опасность неадекватного реагирования на изменения в макросреде. Глобальные трансформации, такие как санкции, пандемии и новые нормативные акты, требуют тщательной проверки устойчивости бизнес-модели. В ЦД принятия решений проводят тестирование виртуальной компании в экстремальных условиях, чтобы оценить надежность цепочек поставок и гибкость операционных процессов. Систематизируем перечисленные виды угроз на рис. 6.

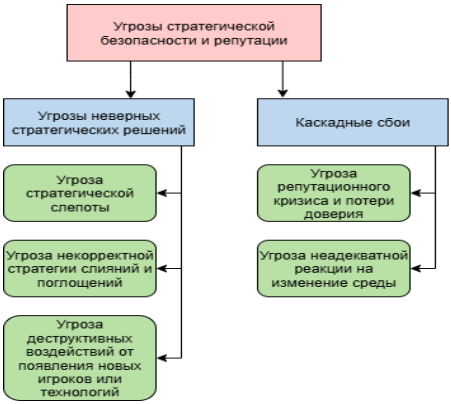

Рис. 6. Угрозы стратегической безопасности и репутации
Источник: составлено автором

Заключение. Цифровые двойники становятся новым стандартом обеспечения экономической безопасности компаний. В мире, где бизнес-процессы усложняются, рынки нестабильны, а киберугрозы растут, традиционные методы управления рисками отстают от экономической жизни. Цифровые двойники – виртуальные копии физических активов и процессов – позволяют не только отслеживать состояние предприятия в реальном времени, но и предсказывать последствия потенциальных угроз.

В статье предложена многомерная классификации угроз экономической безопасности. Она структурирована по компонентам цифрового двойника: операционная деятельность, финансы, IT-инфраструктура и стратегическое управление. Эта структура помогает выявлять угрозы, точно определять уязвимые места в бизнес-системе, моделировать каскадные эффекты и оценивать возможный ущерб.

Поступила в редакцию 11.09.2025
Принята к публикации 10.11.2025

Библиографический список

[1] Банк О.А. Использование комплексной диагностики для обеспечения экономической безопасности предприятия // Вопросы региональной экономики. 2020. № 2 (43). С. 34-40.
[2] Никулин Р.Ю. Классификация угроз экономической безопасности предприятия // Стратегии бизнеса. 2022. Т. 10. № 7. С. 167-171.
[3] Серебрякова Т.Ю., Куртаева О.Ю. Классификация угроз и ее использование в системе экономической безопасности // Инновационное развитие экономики. 2019. № 5-2. С. 259-266.
[4] Zahorodnia A., Fedorenko T. Economic security of the enterprise: modern challenges and threats // Intellectualization of Logistics and Supply Chain Management. 2024. № 26. С. 75-79.
[5] Khaustova V.Ye., Trushkina N.V. Risks and Threats to National Security: Essence and Classification // Бизнес информ. 2024. Т. 10. № 561. С. 6-22.
[6] Mykhaylychenko N., Svynarenko, T. The System of Counteracting External Threats to the Economic Security of the Enterprise // Business Inform. 2024. Т. 4. № 555. С. 95-100.
[7] Кузнецова Т.С., Свириз Е.А. Угрозы в системе экономической безопасности предприятия // Сборник XI Международной студенческой научно-практической конференции «Актуальные проблемы и перспективы развития экономики в современных условиях». Ч. I, 2019. С. 405-409.
[8] Максимова Н.А. Разработка классификации индикаторов экономической безопасности промышленных предприятий // Russian Journal of Management. 2021. Т. 9. № 4. С. 121-125.

[9] Проняева Л.И., Павлова А.В., Федотенкова О.А. Классификация угроз и оценка уровня экономической безопасности кластера // Национальные интересы: приоритеты и безопасность. 2021. Т. 17. № 2 (395). С. 225-257.
[10] Антропова Т.Г., Фленова Е.В. Классификация угроз экономической безопасности банковской системы как необходимый этап разработки инструментов управления рисками // Инновационное развитие экономики. 2020. № 2 (56). С. 245-249.
[11] Моделирование процессов управления инцидентами информационной безопасности на предприятии / Е.С. Митяков, Е.А. Максимова, С.В. Артемова, А.А. Бакаев, Ж.Г. Вегера // Russian Technological Journal. 2024. № 12 (6). С. 39-47. https://doi.org/10.32362/2500-316X-2024-12-6-39-47.
[12] Белова Д.В. Концептуальная модель цифрового двойника для прогнозирования угроз экономической безопасности предприятия // Экономическая безопасность. 2025. Т. 8. № 8. С. 2379-2402.

D.V. Belova

CLASSIFICATION OF THREATS TO THE ECONOMIC SECURITY OF AN ENTERPRISE IDENTIFIED ON THE BASIS OF DIGITAL TWIN TECHNOLOGIES

MIREA – Russian Technological University
Moscow, Russia

Abstract. A new paradigm of economic security is considered in the article, emphasizing a shift from passive threat response methods to active preventive measures aimed at predicting negative scenarios for business development. The concept of using digital twins (DTs) as a central element of risk monitoring and forecasting systems has been proposed. Digital twins are understood as virtual replicas of physical objects and processes that provide continuous monitoring of an organization's state and modeling of potential threats' consequences.The main components of economic risks covered by DT technologies have been examined. Operational safety is ensured through detection of deviations in production processes, which helps reduce equipment failure probability and improve product quality. Financial stability risks decrease due to constant liquidity control, timely prevention of payment delays, and stress testing of investment portfolios. Information and cybersecurity are maintained through tools capable of monitoring user network behavior and detecting possible system attacks. Company strategy and reputation are protected by the capabilities of DTs, enabling evaluation of strategic decision-making risks and proactive responses to potential reputational threats. A classification of threats based on key elements of production infrastructure has also been developed.

Keywords: digital twin, economic security, predictive analytics, scenario modeling, machine learning, threat classification.

References

[1] Bank O.A. (2020). The use of complex diagnostics to ensure the economic security of an enterprise. *Voprosy regional'noi ekonomiki* [Issues of Regional Economy]. No. 2 (43). pp. 34-40. (In Russ.).

[2] Nikulin R.Y. (2022). Classification of threats to the economic security of an enterprise. *Strategii biznesa* [Business Strategies]. Vol. 10. No. 7. pp. 167-171. (In Russ.).

[3] Serebryakova T.Yu., Kurtaeva O.Yu. (2019). Threat classification and its use in the economic security system. *Innovatsionnoe razvitie ekonomiki* [Innovative Economic Development]. No. 5-2. pp. 259-266. (In Russ.).

[4] Zahorodnia A., Fedorenko T. (2024). Economic security of the enterprise: modern challenges and threats. *Intellectualization of Logistics and Supply Chain Management*. No. 26. pp. 75-79.

[5] Khaustova V.Ye., Trushkina N.V. (2024) Risks and Threats to National Security: Essence and Classification. *Biznes Inform.* Vol. 10. No 561. pp. 6-22. (In Russ.).

[6] Mykhaylychenko N., Svynarenko T. (2024). The System of Counteracting External Threats to the Economic Security of the Enterprise. *Business Inform*. Vol. 4. No. 555. pp. 95-100. (In Russ.).

[7] Kuznetsova T.S., Sviriz E.A. (2019). Threats in the economic security system of an enterprise. *Sbornik XI Mezhdunarodnoi studencheskoi nauchno-prakticheskoi konferentsii "Aktual'nye problemy i perspektivy razvitiya ekonomiki v sovremennykh usloviyakh"* [Proceedings of the XI International Student Scientific and Practical Conference "Current Problems and Prospects of Economic Development in Modern Conditions"]. Part I. pp. 405-409. (In Russ.).

[8] Maksimova N.A. Development of classification of indicators of economic security of industrial enterprises. Russian Journal of Management. Vol. 9. No. 4. 2021. pp. 121-125. (In Russ.).

[9] Pronyaeva L.I., Pavlova A.V., Fedotenkova O.A. Classification of Threats and Assessment of the Level of Economic Security of a Cluster. *Natsional'nye interesy: prioritety i bezopasnost'* [National Interests: Priorities and Security]. Vol. 17. No. 2 (395). pp. 225-257. (In Russ.).

[10] Antropova T.G., Flenova E.V. Classification of threats to the economic security of the banking system as a necessary stage in the development of risk management tools. *Innovatsionnoe razvitie ekonomiki* [Innovative Economic Development]. No. 2 (56). pp. 245-249. (In Russ.).

[11] Mityakov E.S., Maksimova E.A., Artemova S.V., Bakaev A.A., Vegera Zh.G. Modeling incident management processes in information security at an enterprise. *Russian Technological Journal*. 2024. No. 12 (6). pp. 39-47. DOI: 10.32362/2500-316X-2024-12-6-39-47. (In Russ.).

[12] Belova D.V. A conceptual model of a digital twin for predicting threats to the economic security of an enterprise. *Ekonomicheskaya bezopasnost'* [Economic Security]. Vol. 8. No. 8. pp. 2379-2402. (In Russ.).