



Федеральная служба войск национальной гвардии Российской Федерации

ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ  
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ОХРАНА»  
(ФКУ «НИЦ «Охрана» Росгвардии)

Аналитический обзор программного обеспечения в области создания  
цифровых двойников и имитационного моделирования актов незаконного  
вмешательства на объекты

Москва 2025

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	5
1 Информационный поиск в области обеспечения безопасности охраняемых объектов .....	6
1.1 Анализ противоправных посягательств на объекты в том числе способов проникновения, численности, оснащенности, преследуемых целей, тактики и способов действий нарушителей .....	6
1.2 Разработка модели нарушителя .....	8
1.3 Анализ существующей системы безопасности охраняемых объектов и способов ее оценки .....	13
1.4 Анализ проблемных вопросов охраны объектов и перспективной области применения технологии цифровых двойников при охране объектов .....	21
2 Информационный поиск технических решений в области цифровых двойников .....	28
2.1 Информационный поиск и анализ нормативно-технических документов в области применения цифровых двойников .....	28
2.2 Информационный поиск и анализ научных достижений, а также существующих и перспективных технических решений в области создания цифрового двойника .....	33
2.3 Рассмотрение международного и отечественного опыта применения технологий цифрового двойника для решения задач охраны объектов и смежных задач .....	35
3 Информационный поиск технических решений в области имитационного моделирования .....	39
3.1 Информационный поиск и анализ нормативно-технических документов в области применения имитационного моделирования .....	39

4 Сравнительный анализ технологий, используемых для создания и применения цифрового двойника и ситуационного моделирования .....	55
4.1 Проведение сравнительного анализа существующих технологий и технических решений, используемых для создания и применения цифрового двойника.....	55
4.2 Проведение сравнительного анализа существующих технологий и технических решений, используемых для ситуационного моделирования.....	65
5 Анализ перспектив развития системы охраны объектов с применением цифрового двойника .....	70
5.1 Анализ возможных путей расширения функциональных возможностей системы централизованной охраны объектов и тактики локальной охраны при использовании технологии цифрового двойника .....	70
5.2 Анализ проблемных вопросов внедрения и эксплуатации существующей системы безопасности с использованием технологии цифрового двойника.....	77
ЗАКЛЮЧЕНИЕ .....	85
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ .....	87

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ**

В настоящем аналитическом обзоре применены термины по ГОСТ Р 52551–2016, а также следующие сокращения и обозначения:

АРМ - автоматизированное рабочее место

БПЛА – беспилотные летательные аппараты

ВВА – верификация, валидация и аттестация

ИИ – искусственный интеллект

ИМ – имитационное моделирование

ИТСО – инженерно-технические средства охраны

НТД – нормативно-техническая документация

СКУД – система контроля и управления доступом

ЦД – цифровой двойник

## **ВВЕДЕНИЕ**

В условиях быстро развивающихся технологий и растущих угроз безопасности актуальность создания и применения цифровых двойников объектов становится все более значимой. Цифровой двойник представляет собой виртуальную модель физического объекта, которая позволяет проводить глубокий анализ его характеристик. Этот инструмент не только облегчает процесс проектирования и эксплуатации объектов, но и повышает эффективность систем охраны, позволяя более точно оценивать риски и выбирать оптимальный состав инженерно-технических средств охраны.

В последние годы наблюдается возрастающий интерес к интеграции цифровых двойников в процессы управления безопасностью. Современные угрозы требуют комплексного подхода к защите объектов, и цифровые двойники предоставляют возможность симулировать разные сценарии, что в свою очередь способствует более обоснованному выбору средств охраны. Исследование в данной области открывает новые горизонты для оптимизации инженерных решений и повышения уровня безопасности.

Настоящая работа направлена на комплексный анализ современных угроз, существующих систем безопасности и методов их оценки, а также на исследование потенциала и проблем внедрения технологий цифровых двойников и имитационного моделирования в сфере обеспечения безопасности охраняемых объектов. Основное внимание уделяется разработке и сравнительному анализу технических решений, позволяющих создавать гибридные, многоуровневые цифровые двойники, способные интегрировать физическую модель объекта, данные в реальном времени, пространственную структуру и логику событий для достижения максимальной эффективности защиты.

## **1 Информационный поиск в области обеспечения безопасности охраняемых объектов**

### **1.1 Анализ противоправных посягательств на объекты в том числе способов проникновения, численности, оснащенности, преследуемых целей, тактики и способов действий нарушителей**

Обеспечение безопасности охраняемых объектов является одной из приоритетных задач для Федеральной службы войск национальной гвардии Российской Федерации. В условиях роста преступности, террористических угроз и технологических изменений, необходимость эффективных систем охраны становится особенно актуальной, при этом охраняемые объекты могут иметь значимые структурные и организационные отличия.

Проведенный анализ показал, что наиболее распространенными методами проникновения на охраняемую территорию являются:

- проникновение под видом персонала или посетителей;
- пересечение периметра в нерабочее время с использованием лестниц, верёвок, специального снаряжения или подкопов;
- использование уязвимостей в средствах инженерной и технической защищенности объекта.

Противоправные действия были осуществлены как отдельными лицами, так и организованными группами. В большинстве случаев проникновение осуществлялось группой от 2 до 5 человек, что свидетельствует о наличии предварительной координации, распределения ролей и четкого планирования. Действия одиночных нарушителей, чаще всего были связаны с хищениями или актами вандализма. Крупные группы, как правило, действовали при террористических актах или диверсиях.

Важно отметить разнообразие состава лиц, участвующих в правонарушениях. Среди них встречаются профессиональные преступники, террористы, бывшие сотрудники предприятий и даже недовольные работники организаций.

Технические возможности нарушителей постоянно растут и становятся все более продвинутыми. Они используют современные методы коммуникации с применением сложных алгоритмов шифрования, специализированное оборудование для сокрытия личности и минимизации обнаружения, включая камуфляжную экипировку и приспособления для уменьшения теплового излучения. Помимо этого, широко распространены инструменты для быстрого и бесшумного вскрытия замков, преодоления ограждений и нейтрализации систем охраны. В некоторых случаях было применено огнестрельное и холодное оружие, взрывчатки и беспилотные летательные аппараты.

Мотивация правонарушителей столь же разнообразна, как и сами участники. Основными целями являются материальное обогащение путем хищения активов, получение коммерческой или личной информации, умышленная порча имущества, захват заложников, дестабилизация работы объекта, сбор разведывательных данных, а также публичная демонстрация политических или идеологических установок через экстремистские акции и террористические акты. Нередко наблюдается сочетание нескольких целей, например, одновременное изъятие материальных ценностей и попытка дестабилизировать работу предприятия.

Современная тактика совершения противоправных деяний характеризуется высоким уровнем проработанности и детализации. Преступники предварительно проводят глубокую разведку территории, внимательно отслеживая графики работы персонала, маршруты патрулирования, слабые места инженерных сооружений и особенности функционирования систем охраны. Оптимальное время для нападения на объекты выбирается с расчетом на минимальное присутствие охраны, что обычно приходится на ночь, выходные и праздничные дни, а также периоды смены дежурных нарядов. Часто применяются отвлекающие маневры, такие как инсценировка возгораний, громкий шум или искусственное создание помех на отдельных участках периметра. Важнейшими принципами

остаются скорость исполнения и последующий быстрый уход с места происшествия. Насилие используется ограниченно, преимущественно в ситуациях открытого противостояния с охраной или для усиления психологического эффекта.

На основании проведенного анализа можно утверждать, что уровень профессиональной подготовки, финансовая поддержка и способность быстро адаптироваться к новым условиям у нарушителей неуклонно возрастают. Это обстоятельство требует радикального изменения традиционных подходов к обеспечению безопасности объектов.

Необходимость интеграции физических и цифровых решений, постоянного повышения квалификации сотрудников охраны, регулярного обновления технических средств охраны и внедрения передовых методик прогнозирования угроз становится очевидной. Только такой комплексный подход позволит достигнуть значительного снижения вероятности наступления негативных последствий.

## **1.2 Разработка модели нарушителя**

Типовая модель нарушителя может иметь разную степень детализации, при этом она должна максимально учитывать характеристики и особенности объекта и содержать максимально исчерпывающие сведения о возможных действиях нарушителей с учётом принятых для данного объекта угроз.

Типовая модель нарушителя представляет собой описание совокупности его качественных и количественных характеристик, к которым относятся:

- цели, которые могут преследовать нарушители каждого типа, и побуждающие мотивы;
- мотивация действий;
- типы нарушителей по внутренней организации, их количественный состав;

- уровень осведомленности о технологических особенностях объекта, его уязвимых местах, критических элементов и организации их охраны и защиты;
- уровень подготовки и квалификации нарушителей;
- оснащенность нарушителей – используемые транспортные средства, инструменты, вооружение, принадлежности и т. п.;
- тактика и способы возможных действий нарушителей;
- способы проникновения и передвижения по территории объекта;
- время и продолжительность воздействия.

Исходя из многообразия характеристик нарушителей, можно выделить следующие критерии их классификации.

1. По мотивации:

- случайный нарушитель (попал на объект неумышленно);
- преднамеренный нарушитель (действует с определённым умыслом);
- высокомотивированный нарушитель (способен на продолжение противоправных действий в случае риска собственной безопасности, при потерях в личном составе при групповом совершении противоправных действий, самопожертвенность)

2. По численности:

- одиночный;
- организованная группа.

3. По отношению к охраняемому объекту

- внешний нарушитель, не имеет разрешенного самостоятельного доступа на территорию для осуществления противоправных действий;
- внутренний нарушитель, использует служебное положение и знания для осуществления противоправных действий, либо подготовки к нему;
- группа лиц, имеющих различное отношение к охраняемому объекту, действующих по предварительному сговору.

При этом, следует разделить степень принадлежности вероятного нарушителя к персоналу охраняемого объекта:

- нарушитель – сотрудник охраны;
- нарушитель – сотрудник;
- нарушитель – посетитель;
- нарушитель – постороннее лицо.

Мотивы, которые могут побудить потенциальных нарушителей к совершению противоправных действий в отношении объекта, можно разделить:

- на политические (идеологические);
- экономические (получение материальной выгоды);
- экологические и личные.

#### 4. По преследуемым целям:

– проникновение на охраняемый объект без причинения ущерба объекту;

– причинение ущерба или нарушение функционирования объекта, в частности:

- захват заложников, стрелкового оружия и техники;
- захват критических элементов;

- диверсию в отношении критических элементов и мест их эксплуатации;

– проникновение с целью хищения или получения доступа к информации ограниченного распространения;

- случайное проникновение на охраняемый объект.

5. По степени осведомлённости о функционировании и структуре объекта, его системе охраны:

– высокая – нарушитель знает практически все об устройстве, системе охраны, составе и количестве ИТСО и уязвимых местах;

– средняя – нарушитель знает сравнительно много об объекте, но не знает уязвимых мест, имеет отрывочные знания о системе охраны,

комплексе ИТСО, значимости критических элементов системы охраны и точных местах их нахождения;

– низкая – нарушитель имеет общее представление об устройстве объекта и системе его охраны, комплексе ИТСО, но практически ничего не знает об уязвимых местах и местах нахождения критических элементов защиты.

6. По уровню физической подготовки (от этого и имеющихся инструментов зависит скорость преодоления рубежа охраны, передвижения):

– находящийся в хорошей физической форме;  
– имеющий слабую физическую подготовку или травмы (заболевания).

7. По владению техническими средствами:

– не имеющие опыт и навыки по использованию инструментов для преодоления ИТСО, не имеет специальной подготовки по преодолению систем охраны;

– имеющие опыт и навыки по разрушению ИТСО доступными инструментами в том числе прошедший специальную подготовку по преодолению систем охраны.

8. По владению огнестрельным оружием

– отсутствие навыков владения стрелковым оружием и взрывных работ;

– ограниченные навыки владения стрелковым оружием;

– уверенное владение стрелковым оружием, кроме того может обладать навыками маскировки.

9. По степени технической оснащённости:

– не оснащён;

– оснащён легкими переносными инструментами (кусачки, топор, лопата, кирка, лестница, стремянка, доска для преодоления периметра,

отвертки, молотки, монтировки, аккумуляторные шуруповёрты и т.д. для проникновения в помещения);

– оснащён специальной техникой для преодоления системы охраны или громоздким строительным оборудованием (газорежущее оборудование, пила дисковая, и др. которое может быть взято с собой или подготовлено сообщниками).

10. По вооружению:

– безоружные или вооруженные холодным оружием;

– ограниченно вооруженные огнестрельным оружием (охотничье оружие, короткоствольное оружие), возможно наличие ограниченного количества взрывчатых устройств;

– вооруженные стрелковым оружием и взрывчатыми устройствами неограниченно.

Под стрелковым оружием при моделировании могут пониматься короткоствольное полуавтоматическое и автоматическое оружие, карабины и гладкоствольные ружья, штурмовые и снайперские винтовки, автоматы, ручные и крупнокалиберные пулеметы, а также гранатометы и стрелково-гранатометные комплексы.

11. По тактике противоправного проникновения:

– открытое нападение (насильственная), осуществляемое без попытки скрытного проникновения на объект, осуществляется с изначальным применением насилия по отношению к персоналу и силам охраны или и/или с повреждением ограждения и средств ИТСО;

– скрытое проникновение на объект, когда нарушитель старается при совершении противоправных действий сохранить незаметность;

– обманное проникновение – с попыткой формирования у сил безопасности видимости санкционированных действий путём использования поддельных документов, ключей, пропусков (специальных пропусков) и т.п.;

- комбинированная – различные сочетания вышеуказанных видов тактики.

Следует ожидать, что в процессе своих действий нарушитель будет применять любую тактику, повышающую его шансы на успешное выполнение поставленной задачи.

Для конкретного объекта модель нарушителя выбирается из типовых (или создается специально) в результате анализа статистики нарушений на защищаемом и аналогичных объектах, с учетом криминогенной обстановки (в том числе угрозы совершения террористического акта) в регионе и ее прогноза, а также учета возникновения теоретически вероятных ситуаций, не имеющих прецедентов.

Наиболее распространенной моделью нарушителя является неподготовленный нарушитель, человек пытающийся проникнуть на охраняемый объект, надеясь на удачу, свою осторожность, опыт или случайно ставший обладателем конфиденциальной информации об особенностях охраны.

Неподготовленный нарушитель не располагает специальными инструментами для проникновения в закрытые помещения и тем более техническими средствами для обхода охранной сигнализации. Для защиты от неподготовленного нарушителя часто оказывается достаточным оборудование объекта ТСО и организация службы охраны.

Более сложная модель нарушителя предполагает осуществление им целенаправленных действий, например, проникновение в охраняемые помещения с целью захвата материальных ценностей или получения информации.

### **1.3 Анализ существующей системы безопасности охраняемых объектов и способов ее оценки**

Современная система безопасности охраняемых объектов представляет собой комплексную, многоуровневую структуру,

включающую в себя организационные, технические, инженерные компоненты, направленные на предотвращение, выявление и пресечение попыток проникновения на охраняемый объект. Её основными элементами являются:

- система инженерных средств охраны, включающая в себя физические заграждения и ограждения территории, контрольно-пропускные пункты и укрепленные двери, системы охранного освещения, барьеры для предотвращения несанкционированного доступа;

- система технических средств охраны, которая включает в себя подсистемы охранно-пожарной сигнализации, контроля и управления доступом, видеонаблюдения и т.д;

- система персонала охраны: посты охраны, патрульные группы, специалисты по обеспечению безопасности. Человеческий фактор остается ключевым звеном системы, так как именно он принимает решения и действия по предотвращению угроз объекту.

Подсистема организационно-управленческих мероприятий: режимы охраны, регламенты действий персонала, планы эвакуации, инструкции, основные правила доступа, документация по охране, регламенты возникновения аварий. Эта подсистема требует правильного использования технических средств и координации действий персонала.

Оценка эффективности системы безопасности объекта — это комплексный процесс, направленный на выявление уязвимостей и слабых мест, повышение уровня, снижение рисков и обеспечение безопасности объекта.

### 1.3.1 Подходы к оценке эффективности систем безопасности

Оценка существующих систем безопасности охраняемых объектов может осуществляться любыми методами, с учетом своих преимуществ и ограничений. Основными подходами являются.

Нормативно-правовой подход, основанный на проверке соответствия системы охраны объекта требованиям нормативно-правовой документации. Преимуществом такого метода является юридическая обоснованность. Однако его основным недостатком является формальный характер оценки, которая часто не учитывают реальную спецификацию конкретного объекта. В результате система может соответствовать нормам, но оставаться неэффективной в условиях угроз безопасности объекта. Такой подход подходит для базового уровня защиты, но требует применения других методов при работе с высокорисковыми объектами. Таким образом, нормативно-правовой подход — это необходимая, но недостаточная основа для построения комплексной и адаптивной системы безопасности.

Риско-ориентированный подход представляет собой современный метод оценки безопасности, который акцентирует внимание не на формальном соблюдении нормативных требований, а на анализе угроз и их последствий для данного объекта. Основная идея заключается в том, что не все риски имеют одинаковую степень опасности, поэтому следует направлять ресурсы на защиту от тех рисков, которые действительно могут привести к негативным последствиям. Такой метод позволяет перейти от шаблонных решений к индивидуализированной системе безопасности, учитывающей специфику объекта.

Ключевые этапы реализации риско-ориентированного подхода включают идентификацию угрозы, анализ уязвимостей и оценку риска. На первом этапе выявляются все виды воздействия, способные нанести вред охраняемому объекту. Например, для нефтебаз это может быть утечка нефтепродуктов или поджог, для офиса — кибератаки в системе управления или хищение данных. Угрозы классифицируются в зависимости от типа объекта: к ним относятся несанкционированное проникновение, пожары, взрывы, саботаж, природные катастрофы или кибератаки. Далее проводится анализ уязвимостей — слабых мест объекта, через которые может быть реализована угроза. Например, отсутствие замка на заднем дворе создает

риск проникновения, а слабая система авторизации делает объект уязвимым для кибератак. Этот этап включает в себя осмотр территории, проверку технических систем, опрос персонала. Оценка риска представляет собой завершающий этап риско-ориентированного метода, на котором определяется уровень опасности каждой обнаруженной угрозы именно для данного охраняемого объекта.

Для проведения анализа риска применяются специализированные методы. Наиболее распространенным является метод матрицы риска, где воздействие учитывается по шкалам вероятности и серьезности последствий, что позволяет визуализировать приоритетные зоны.

Также используется метод анализа видов и последствий отказов, изначально разработанный для промышленности, но адаптированный для обеспечения безопасности. Он помогает оценить, как выход из строя отдельных элементов системы (например, видеокамеры или резервного питания) воздействует на зону защиты.

Преимуществами риско-ориентированной метода являются обеспечение индивидуального подхода к защите объекта, позволяет эффективно распределять бюджет на организацию охраны объекта, а также обеспечивает гибкость системы безопасности при возникновении новых угроз. Однако, применение данного метода связано с рядом сложностей. Во-первых, требуется участие квалифицированных кадров, способных оценить как технические аспекты системы безопасности, так и специфику угроз (физических, информационных, террористических). Во-вторых, анализ безопасности зависит от реальных данных (статистики происшествий, региональных угроз и т.д). В-третьих, процесс требует значительных временных и ресурсных затрат, включая привлечение специалистов и проведение детальных исследований.

Таким образом, риско-ориентированный подход является наиболее разумным и современным для построения системы безопасности, поскольку он ориентирован на реальную угрозу, а не на формальное соответствие

стандартам. Однако его успешное внедрение возможно только при наличии квалифицированных специалистов и достоверной информации. Это позволяет не только минимизировать угрозы, но и снизить затраты, сконцентрировав усилия на тех рисках, которые действительно заслуживают внимания.

Подход «тестирования и моделирования» угроз системе безопасности объекта основан на практической проверке работоспособности в условиях, максимально приближенных к реальным угрозам. В отличие от теоретических расчётов или формальных проверок на соответствие нормативным требованиям, здесь система непосредственно «подвергается испытаниям» — как в лабораторной среде, так и непосредственно на охраняемом объекте. Данный подход включает в себя несколько ключевых методов. Во-первых, это имитация попытки проникновения на объект — так называемый «этичный взлом», при котором специалисты намеренно пытаются несанкционированно проникнуть на объект или в его техническую систему, используя методы, типичные для одних злоумышленников. Например, они могут обойти систему контроля и управления доступа, сделать пропуск, взломать камеру через сетевое соединение. Во-вторых, широко применяются так называемые учения, при которых имитируются действия злоумышленников — попытки проникновения на территорию, обман охраны, в то время как штатные сотрудники службы безопасности, должны отразить угрозу безопасности. Такие учения позволяют оценить не только техническое оснащение, но и человеческий фактор: реакцию персонала, отлаженность действий, качество регламентов и эффективность коммуникаций. В-третьих, используется имитационное (компьютерное) моделирование инцидентов с применением специализированного программного обеспечения. Это метод виртуального воссоздания возможных угроз и чрезвычайных ситуаций на охраняемом объекте с помощью специализированного программного обеспечения. Вместо того чтобы проводить реальные учения

— с участием людей, техники и риском нарушения работы объекта — специалисты создают цифровую копию (цифровой двойник) объекта и «запускают» в ней различные сценарии угроз. Это позволяет увидеть, как отреагируют системы безопасности и персонал — но в безопасной, контролируемой среде. Такое моделирование особенно ценно при проектировании систем безопасности, поскольку позволяет протестировать различные схемы без риска для реального объекта.

Цель всех этих методов — выявление скрытых уязвимостей, которые остаются незамеченными при формальном подходе.

Однако данный подход имеет и некоторые недостатки. Прежде всего, он отличается высокой стоимостью: требуется привлечение квалифицированных специалистов (аналитиков безопасности, инструкторов), аренда специализированного оборудования и организация учений. Кроме того, такие мероприятия невозможно провести с помощью обычного персонала — охранника или инженера по техническому обслуживанию, не отвечающего компетенциям для проведения качественного проведения учений. Также существует риск нарушения работы объекта: во время испытаний возможно временное отключение электропитания, блокировка входов и выходов, что способно вызвать панику среди персонала. Это особенно критично для объектов с непрерывным циклом работы — таких, как больницы, электростанции, аэропорты или центры обработки данных. Наконец, такие тесты характеризуются ограничением по количеству отработок испытаний: их невозможно проводить слишком часто, так как это мешает повседневной деятельности и приводит к тому, что вызывает усталость у персонала.

Таким образом, метод «тестирование и моделирование» является одним из наиболее объективных. Однако из-за высокой сложности, затратности и сопутствующих рисков он применяется только к важным объектам — таким, как ядерные установки, банковские учреждения, правительственные здания и крупные промышленные комплексы.

Интегральные методы оценки сочетают несколько подходов и используют комплексные показатели эффективности (например, время обнаружения угроз, меры защиты, уровень автоматизации). Часто применяется в рамках аудита безопасности.

Количественные показатели:

- время реакции: Время от момента срабатывания сигнализации до прибытия сил реагирования (охраны, полиция). Нормативное значение зависит от класса объекта, но обычно не должно превышать 5–15 минут;

- время задержки: Время, необходимое злоумышленнику для преодоления физического барьера или обхода ИТСО.

- вероятность обнаружения: Вероятность обнаружения проникновения системой;

- коэффициент ложных срабатываний: Отношение числа ложных срабатываний к общему числу срабатываний. Высокий коэффициент ложных срабатываний снижает уровень доверия к системе;

- среднее время наработки на отказ. Высокая наработка на отказ свидетельствует о надежности системы.

Качественные показатели:

- надежность и отказоустойчивость: способность сохранения работоспособности системы при выходе из строя одного или нескольких компонентов (наличие резервирования, автономное питание);

- удобство в эксплуатации и обслуживании: интуитивно понятный интерфейс, простота настройки, легкость замены компонентов;

- гибкость и масштабируемость: Возможность легкого подключения новых компонентов или изменения конфигурации системы;

- интегрируемость: Возможность объединения различных систем (СВН, СКУД, сигнализация) в единую платформу для централизованного управления;

– обученность и дисциплинированность персонала: Уровень подготовки сотрудников безопасности объекта, их знание регламентов, способность принимать решения в стрессовых ситуациях.

Несмотря на наличие разработанных методик, любые подходы к оценке системы безопасности объекта имеют ряд особенностей, которые ограничивают их эффективность и применимость в современных условиях.

Статичность и отсутствие адаптивности – традиционные методы основаны на фиксированном состоянии объекта и его защите на момент проведения анализа. Они не наблюдают динамику изменений: модернизацию ИТСО, изменение тактики нарушителей, сезонные факторы (например, снег, который может закрыть следы или вызвать срабатывание извещателя), изменения в режиме работы объекта. В результате оценка, проведенная несколько месяцев назад, может оказаться уже неактуальной.

Ограниченность – оценка обычно проводится на основе ограниченного набора показателей, которые могут не охватывать все возможности проникновения или действий злоумышленников. Злоумышленники постоянно совершенствуют свои методы, а статичные скрипты не позволяют предугадать их новую тактику.

Высокая стоимость – проведение всестороннего анализа уязвимостей и их рассмотрение требует значительных временных и финансовых затрат. Необходимо привлекать высококвалифицированных специалистов, проводить полевые испытания, что делает регулярную оценку безопасности нецелесообразной для многих объектов.

Отсутствие прогнозирования – существующие методы плохо позволяют прогнозировать эффективность системы при изменении условий или внедрении новых технологий без повторных дорогостоящих испытаний.

Сложность учета человеческого фактора – трудно количественно оценить влияние человеческого фактора на общую эффективность системы. Хотя персонал является ключевым фактором, его поведение сложно смоделировать и предсказать.

Эти проблемы создают серьезные риски для безопасности объектов, так как они могут привести к недооценке угрозы, неправильному выбору технических средств и, в конечном итоге, к успешному проникновению злоумышленников.

Существующие методы оценки безопасности систем, включают в себя ряд недостатков, статичности, избирательности, низкой стоимости и отсутствия возможности прогнозирования. Эти недостатки создают серьезные риски для безопасности охраняемых объектов. Технология цифровых двойников представляет собой мощный инструмент для оценки состояния безопасности объекта, позволяющий перейти от статической, экспертной оценки к динамическому, управляемому, прогнозируемому управлению системой безопасности.

#### **1.4 Анализ проблемных вопросов охраны объектов и перспективной области применения технологии цифровых двойников при охране объектов**

В последние годы технологии цифровых двойников все активнее внедряются в практику охраны объектов, предоставляя новые возможности для комплексного анализа и управления безопасностью. При создании и эксплуатации цифровых двойников возникает ряд проблемных вопросов.

##### **1.4.1 Неточность цифровой модели**

Основная цель создания цифровых двойников на производстве – сценарное моделирование.

При создании цифровых двойников крайне важно определить с каких подразделений, объектов, процессов необходимо начинать внедрение технологии, где будет достигнута наибольшая экономическая эффективность. Также необходимо решить какие данные, необходимы для создания цифровых двойников. Например, для моделирования ветровой турбины может потребоваться контроль вибраций от коробки передач,

генератора, лопастей, валов и башни, а также напряжений от системы управления, также стоит учитывать и условия внешней среды (скорость ветра, температура, влажность). Ошибочные или неучтенные в модели данные, могут исказить результаты исследований и скрыть ошибки. [1].

Также, существует риск искажения информации о физическом объекте, системе или процессе, которые необходимо воспроизвести с помощью данной технологии. При переходе на цепочку взаимодействия «человек – компьютер – цифровой двойник – компьютер – исполнительный механизм» появляется риск, связанный с верификацией цифровых моделей, на которых базируются цифровые двойники. По оценкам экспертов, к рискам снижения достоверности цифровых моделей можно отнести:

- ошибки разработчиков;
- недостоверные математические расчеты;
- недостаточность внесенных сведений или характеристик в промышленную модель;
- недостаточный учет ограничений и факторов внешней среды при разработке цифровой модели;
- отсутствие единых методов верификации цифровых моделей.

#### 1.4.2 Сложность проектирования цифровой модели

Оптимальное количество и размещение датчиков должны быть точно определены на этапе проектирования цифровых двойников. Это все выливается в сложность их разработки, которая заключается в нехватке данных и/или ИТ-ресурсов для их хранения. При недостатке ключевых параметров модели появляется погрешность прогнозирования, что снижает экономическую ценность имитационной модели. Поэтому, для того чтобы построить качественную модель, необходимо иметь все данные, влияющие на процесс, а также знать целевые показатели и косвенные признаки [2].

### 1.4.3 Срок службы цифрового двойника и его оригинала

Наиболее эффективным цифровым двойником представляется для активов компании с длительным сроком полезного использования актива. Это означает, что проектирование цифровых двойников будет производиться с учетом того, что активы должны характеризоваться длительным жизненным циклом, превышающим срок использования программного обеспечения, используемого для их проектирования, моделирования или аналитики. Для этого необходимо выбрать технологии, которые будут успешно использоваться даже в случае их устаревания.

### 1.4.4 Мониторинг работы цифрового двойника

Это есть сопровождение продукции квалифицированными специалистами, занимающимися мониторингом, контролем технического состояния и обслуживанием, что влечет за собой трудозатратность обслуживания, особенно при условии многообразия условий эксплуатации.

### 1.4.5 Оценка производственной эффективности цифрового двойника

Еще на уровне процесса создания цифрового двойника можно определить на шесть основных этапов:

- формирование ключевых показателей, необходимых для оценки эффективности проекта;
- формирование бюджета проекта с учетом срока окупаемости;
- назначение ответственных лиц за разработку и реализацию проекта, а также лиц, ответственных за дальнейшую техническую поддержку;
- создание имитационной модели с использованием цифровых технологий;
- разработка контрольных нормативов по процессам внедрения цифровых двойников в производство и внесения изменений в проект;
- контроль исполнения регламентов. При правильном подходе, обычно наблюдаются положительные результаты от внедрения цифровых

двойников. Но не всегда эффект от внедрения данной технологии на промышленном предприятии достигает прогнозных значений, а иногда внедрение цифрового двойника оказывается и вовсе нецелесообразным [3].

#### 1.4.6 Определение целей и задач цифрового двойника

Причина возникновения проблем кроется в оторванности исполнителей проекта от реальных бизнес-задач. Так, например, часть предприятий упускает моделирование процессов, для которых необходим обязательный мониторинг, в то же время в модель могут вносить процессы, которые не важны для функционирования физического объекта. Для внедрения цифровых двойников необходима ИТ инфраструктура, обеспечивающая аналитику данных. Разработка больших данных (Big data) для создания цифровых двойников требует непрерывный поток качественных данных определенного количества, которые не содержат разного рода шумов. Поэтому при создании цифровых двойников важно определить оптимальный объем и критерии оценки качества данных.

#### 1.4.7 Оценка экономической эффективности цифрового двойника

Из совокупности двух предыдущих проблем вытекает еще одна проблема: оценка экономической эффективности цифровых двойников. В нее часто включают только первоначальные инвестиционные вложения, не закладывая при этом средства на эксплуатацию цифровых двойников, включая затраты на персонал, обновление программного и аппаратного обеспечения. Оценивая эффект от внедрения, с учетом затрат на эксплуатацию и поддержку цифровой модели, можно понять, насколько детализированным должен быть цифровой двойник.

#### 1.4.8 Избыточность цифровых двойников

Еще одна проблема – излишняя сложность создаваемых цифровых двойников. Часто цифровых двойников излишне детализированы. Кроме

увеличения затрат на разработку, появляются затраты на обновление деталей, не приносящих ни экономии средств, ни экономического эффекта. К тому же слишком сложный цифровой двойник сложно анализировать, так как данные могут собираться с тысячи датчиков и их необходимо распределять среди множества пользователей и хранить в различных форматах. К сожалению, разнообразие форматов создает путаницу в массивах генерируемых данных, а в итоге может сформироваться некорректная виртуальная модель происходящего в реальном мире. Это приводит к уже ранее озвученной проблеме о некорректности цифровых двойников.

#### 1.4.9 Квалификация персонала

Нехватка квалифицированных кадров в области внедрения цифровых двойников также может повлечь за собой отсутствие окупаемости вложенных затрат. Более того, неправильный анализ специалистами результатов, полученных с помощью цифровых двойников, может привести к неверно принятым управленческим решениям. Обратная последовательность внесения изменений также является проблемой. Модернизация физического объекта или процесса должна отрабатываться на цифровых двойниках, и только за тем переноситься на физический объект, а не наоборот. В действительности часто используется обратная модель, вследствие чего эффективность цифровых двойников снижается.

#### 1.4.10 Информационная защита цифрового двойника

При внедрении цифровых двойников на предприятии появляется еще одна проблема – защита информации. Так как цифровой двойник является ключевым элементом в системе управления жизненным циклом промышленной продукции крайне важно обеспечить информационную безопасность. Цифровой двойник, который по своей природе накапливает данные, интеллектуальный капитал и, следовательно, имеет ценность для

компаний, должен быть надежно защищен, чтобы избежать любого ущерба для предприятия. Поэтому необходимо учитывать, что крайне сложно на уровне отдельных предприятий обеспечить конфиденциальность и безопасность данных, собираемых цифровых двойников по причине их огромного объема и рисков информационной безопасности.

#### 1.4.11 Недоверие к цифровым двойникам

Проблема, которая может исчезнуть с массовым распространением цифровых двойников, которая имеет распространение на сегодняшний день, это недоверие к цифровым двойникам со стороны сотрудников предприятия. Так как они отвечают за ошибки на производстве, то у них остается привычка полагаться на свой опыт, а не на прогнозы имитационной модели. Проблему можно решить переносом части ответственности с человека на систему, при этом экспертное решение останется за сотрудником предприятия.

#### 1.4.12 Качество, скорость взаимодействия цифровой модели и реального объекта

С внедрением цифровых двойников на предприятия появляется необходимость обеспечения непрерывной связи между физическим объектом и имитационной моделью. Связь должна быть быстрой и доступной, чтобы предоставить возможность взаимодействовать с цифровыми двойниками и принимать решения в режиме реального времени. К сожалению, такое состояние инфраструктуры еще не может считаться само собой разумеющимся на многих российских предприятиях. Кроме того, при внедрении цифровых двойников крайне важно учитывать специфику предприятия, его масштабы и деятельность, в противном случае модель будет неэффективна.

По данным исследований компании KMDA выделено три главные проблемы, мешающие процессам цифровой трансформации в российских компаниях, это:

- отсутствие необходимых ресурсов и бюджета (50% опрошенных);
- нехватка необходимых знаний и навыков у персонала (29%);
- незрелая цифровая культура (27%) [3].

Рассмотренные проблемы и риски, связанные с внедрением цифровых двойников, определенно могут повлиять на достижение планируемой эффективности от технологии. Данный процесс может быть работоспособен только при постоянном контроле и проведении корректировок в режиме реального времени.

## **2 Информационный поиск технических решений в области цифровых двойников**

С развитием технологий цифровизации в различных отраслях произошла смена парадигмы управления и проектирования. Одним из новых направлений является концепция цифровых двойников – виртуальных реплик физических систем, процессов или объектов. Однако успешная интеграция цифровых двойников в практику требует четкой нормативно-технической базы.

### **2.1 Информационный поиск и анализ нормативно-технических документов в области применения цифровых двойников**

Цифровые двойники представляют собой виртуальную модель, которая точно воспроизводит свойства, характеристики и поведение своего физического аналога. Способность цифровых двойников в реальном времени анализировать и визуализировать данные делает их мощным инструментом для оптимизации процессов и прогнозирования.

#### **2.1.1 Отечественные нормативно-технические документы**

Нормативно-технические документы в области цифровых двойников можно разделить на несколько категорий:

- национальные стандарты: технические условия, описывающие требования к разработке и внедрению цифровых двойников;
- международные стандарты: документы, принимаемые на уровне международных организаций (например, ISO), определяющие унифицированные методы и критерии;
- отраслевые руководства и рекомендации: Специализированные для отдельных секторов, которые регулируют применение технологий цифровых двойников, в данном случае в сфере безопасности;

– законодательные акты: положения, касающиеся интеллектуальной собственности, защиты данных и безопасности при работе с цифровыми двойниками.

На сегодняшний день существуют несколько ключевых стандартов, касающихся цифровых двойников. 16 сентября 2021 приказом № 979 был утвержден ГОСТ Р 57700.37–2021 [4] — национальный стандарт Российской Федерации «Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения». Он был разработан в рамках деятельности технического комитета 700 «Математическое моделирование и высокопроизводительные вычислительные технологии» (ТК 700) и введен в действие с 1 января 2022 года. Стандарт определяет общие положения разработки и применения цифровых двойников изделий. Он устанавливает общее понятие цифровых двойников, а также общие положения и требования по его созданию и применению.

ГОСТ Р 57700.37–2021 [4] установлены единые определения цифровой модели изделия, цифровых двойников изделия, виртуальных (цифровых) испытаний, цифровых испытательных стендов, цифровых испытательных полигонов. Распространяется на изделия машиностроения, но при необходимости на его основе в дальнейшем могут разрабатываться стандарты, устанавливающие требования к цифровым двойникам изделий различных отраслей промышленности с учётом их специфики.

Как следует из определения, в основе цифрового двойника изделия лежит цифровая модель изделия - «Система математических и компьютерных моделей, а также электронных документов изделия, описывающая структуру, функциональность и поведение вновь разрабатываемого или эксплуатируемого изделия на различных стадиях жизненного цикла, для которой на основании результатов цифровых и (или) иных испытаний по ГОСТ 16504-81 [5] — национальному стандарту Российской Федерации «Система государственных испытаний продукции».

Испытания и контроль качества продукции выполнена оценка соответствия предъявляемым к изделию требованиям».

### 2.1.2 Международные нормативно-технические документы

ISO/IEC TR 30172 [6] «Цифровые двойники. Случаи использования», стандарт, который содержит сборник примеров использования цифровых двойников в различных областях. Документ предназначен для широкого круга профессионалов и организаций, включая разработчиков IoT (сеть физических устройств со встроенными датчиками, программным обеспечением и возможностью подключения к интернету), менеджеров производства, медицинских работников, городских планировщиков и других. Некоторые примеры использования цифровых двойников, представленные в стандарте:

Производство – могут улучшить производственные процессы, обеспечивая в реальном времени информацию о работе оборудования, прогнозируя потребности в обслуживании и оптимизируя графики производства;

Здравоохранение – имеют возможность создавать в реальном времени персонализированные планы лечения, контролировать здоровье пациентов.

Умные города – позволяют городским планировщикам и администраторам управлять городской инфраструктурой с оптимизацией.

Энергетика – используются для мониторинга и оптимизации производства и распределения энергии, сокращения простоев и повышения устойчивости энергетических систем.

Стандарт выпущен в 2023 году и отражает последние достижения и тенденции в области IoT и ЦД.

ISO/IEC 30173 [7] «Цифровые двойники. Концепции и терминология». Является продолжением к стандарту ISO/IEC TR 30172 [6] (далее - TR 30172) и развивает концепции, фокусируясь на приложениях, экосистемах,

процессах жизненного цикла и классификации цифровых двойников, а также определяет круг заинтересованных сторон.

ISO 23247 [8]: Стандарт, который обеспечивает единый подход к созданию цифровых двойников в производственных процессах. TR 30172 [6] — это стандарт, который описывает создание и управление цифровых двойников продуктов, процессов и ресурсов в производственных операциях. Согласно стандарту TR 30172 [6], цифровой двойник — это цифровая модель конкретного физического элемента или процесса с подключениями к данным, которая обеспечивает конвергенцию между физическим и виртуальным состояниями с соответствующей скоростью синхронизации.

Стандарт включает четыре взаимосвязанных уровня: Уровень наблюдаемых производственных элементов — описывает физические компоненты производства, такие как машины, материалы и рабочие. Уровень связи устройств — контролирует и управляет изменениями состояния производственных элементов. Уровень цифровых двойников — обрабатывает данные и поддерживает цифровые модели. Уровень пользовательских сущностей — соединяется с бизнес-системами, такими как ERP и PLM.

TR 30172 [6] основан на технологиях интернета вещей (IoT), которые позволяют производить оптимизацию процессов, контроль качества, управление цифровыми ресурсами. Некоторые преимущества использования стандарта: оптимизация процессов, контроль качества, управление ресурсами.

### 2.1.3 Перспективы развития нормативной базы

В связи с быстрым развитием технологий необходимо постоянно обновлять и пересматривать существующие нормативно-технические документы.

Определение цифровых двойников законодательно не урегулировано. В Приказе Минпромторга России от 19 апреля 2023 г. № 1450 «Об

утверждении форм предоставления информации для включения в государственную информационную систему промышленности субъектами деятельности в сфере промышленности, органами государственной власти и органами местного самоуправления, соответствующих составу информации, предоставляемой оператору государственной информационной системы промышленности для включения в государственную информационную систему промышленности субъектами деятельности в сфере промышленности, органами государственной власти и органами местного самоуправления, утвержденному постановлением правительства Российской Федерации» [9] есть упоминание о цифровых двойниках, но в нем не указываются точные признаки или характеристики новых объектов гражданского оборота. В тоже время в отраслевых стандартах дается определение цифровых двойников с учетом сферы его применения. Так, «цифровой двойник изделия» ГОСТ Р 57700.37–2021 [4] – это система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии изделия) и (или) его составными частями, а «цифровая модель изделия» – это система математических и компьютерных моделей, а также электронных документов изделия, описывающая структуру, функциональность и поведение вновь разрабатываемого или эксплуатируемого изделия на различных стадиях жизненного цикла, для которой на основании результатов цифровых и (или) иных испытаний выполнена оценка соответствия предъявляемым к изделию требованиям.

Вот несколько направлений, которые могут быть приоритетами:

- Разработка единых стандартов: Необходима гармонизация национальных и международных стандартов для обеспечения интеграции различных систем и технологий;
- Исследования в области безопасности: Учитывая актуальность защиты данных, следует уделить внимание разработке норм и стандартов в области кибербезопасности;

– Образование и подготовка кадров: Создание образовательных программ и курсов по подготовке специалистов, умеющих работать с цифровыми двойниками.

## **2.2 Информационный поиск и анализ научных достижений, а также существующих и перспективных технических решений в области создания цифрового двойника**

Развитие технологий цифровых двойников сопровождается активными научными исследованиями и внедрением инновационных решений, направленных на повышение точности, адаптивности и функциональности виртуальных моделей. Современные подходы включают интеграцию искусственного интеллекта, машинного обучения, а также инструментов для прогнозирования и оперативного принятия решений.

Научные достижения в области цифровых двойников включают интеграцию ИИ и машинного обучения, где алгоритмы ИИ и машинного обучения анализируют данные с датчиков физических объектов, что позволяет воспроизводить текущее состояние системы, прогнозировать ее поведение, выявлять аномалии и корректировать процессы. Например, в системах безопасности ЦД обучается на исторических данных о проникновениях, чтобы предсказывать уязвимые точки и тактику злоумышленников. Разрабатываются методы верификации и валидации моделей для проверки соответствия моделей заданным спецификациям и оценки точности отражения реального объекта, что снижает риски, связанные с неточностью прогнозов, особенно в критических сферах. Современные ЦД охватывают не отдельные объекты, а их взаимодействие, например, анализируя работу подсистем безопасности (СКУД, видеонаблюдение, сигнализация) и оценивая эффективность всей системы в условиях реальных угроз. Унификация подходов к разработке и эксплуатации ЦД включает определение жизненного цикла моделей,

формирование требований к структуре данных и интерфейсам, а также обеспечение совместимости ЦД в рамках единой экосистемы.

Существующие технические решения включают специализированные платформы (Siemens Digital Twin, GE Digital Twin, PTC ThingWorx, российские аналоги), предоставляющие инструменты для проектирования и визуализации моделей, интеграции с IoT-устройствами и управления данными в реальном времени. IoT и сенсоры собирают данные о состоянии объекта и передают информацию через беспроводные сети с низким энергопотреблением. Облачные и периферийные вычисления обеспечивают хранение и обработку больших объёмов данных, а Edge-вычисления снижают задержки, что важно для систем безопасности. Технологии дополненной реальности создают интерактивные интерфейсы для работы с ЦД и полезны для обучения персонала и симуляции сценариев. Блокчейн обеспечивает защиту данных ЦД от несанкционированного доступа.

Перспективы применения ЦД в сфере безопасности включают прогнозирование угроз путём анализа данных в режиме реального времени, оптимизацию систем охраны путём определения оптимального размещения датчиков, камер и других технических средств, тренировку персонала с помощью виртуальных симуляторов на основе ЦД для отработки действий в реалистичных сценариях (пожар, взлом, ЧС) и автоматизацию решений, когда в будущем ЦД смогут самостоятельно активировать протоколы защиты при обнаружении угроз, минимизируя человеческий фактор.

Цифровые двойники становятся ключевым инструментом для повышения безопасности объектов, и их развитие требует междисциплинарного подхода, объединяющего ИИ, IoT, облачные технологии и стандартизацию процессов.

### **2.3 Рассмотрение международного и отечественного опыта применения технологий цифрового двойника для решения задач охраны объектов и смежных задач.**

Международный опыт применения цифровых двойников в сфере безопасности демонстрирует активное внедрение передовых технологий ведущими мировыми компаниями, которые интегрируют их в различные системы защиты. В США крупные финансовые учреждения, такие как Bank of America и JPMorgan Chase, успешно используют цифровые двойники для выявления кибератак и предотвращения физических вторжений. Эти системы позволяют проводить регулярные испытания устойчивости безопасности без риска для реальных объектов, что особенно важно для стратегической инфраструктуры [10]. Аналогичные подходы применяются в аэропортах, где цифровые двойники помогают оптимизировать маршруты патрулирования и распределения охранного персонала [11].

Европейский опыт представлен проектами в области «умных городов», где цифровые двойники интегрированы в системы городской безопасности. Примечательным примером служит Сингапур, где создана комплексная цифровая модель города. Эта система не только оптимизирует размещение камер видеонаблюдения и датчиков, но и позволяет прогнозировать потенциальные угрозы на основе анализа больших данных [12]. В Германии компания Siemens активно применяет свои решения Digital Twin для обеспечения безопасности промышленных объектов, что позволяет моделировать сценарии возможных вторжений и тестировать эффективность различных конфигураций систем охраны. Особое внимание уделяется обеспечению физической безопасности в условиях растущих угроз. [13].

В соответствии со стандартом ISO/IEC TR 30172[6], который содержит примеры использования цифровых двойников, в энергетическом секторе эти технологии применяются для оптимизации безопасности критических объектов. Такое применение позволяет существенно сократить

простой оборудования и повысить устойчивость систем к попыткам несанкционированного доступа. Интеграция цифровых двойников в системы безопасности становится глобальным трендом, который позволяет значительно повысить уровень защиты различных объектов и критических инфраструктур по всему миру.

Ключевые игроки, такие как «СберЛабс» и «Инфотекс», разрабатывают отечественные платформы, аналогичные зарубежным решениям Siemens Digital Twin и PTC ThingWorx, но адаптированные под российские стандарты. Их продукты ориентированы на моделирование, мониторинг и прогнозирование рисков для критической инфраструктуры. Санкт-Петербургский политехнический университет создал платформу CML-Bench — систему для разработки цифровых двойников промышленных объектов. Решение относится к классу систем управления жизненным циклом инженерных данных и уже внедрено на ряде российских предприятий[14]. «РЕД СОФТ» и «ДИПСИ НЕТВОРКС» совместно разработали проект Nadal («Цифровой двойник сети»), который автоматизирует документирование и анализ ИТ-сетей, снижая риски простоев и повышая надёжность систем[15]. Сервис SP5000 представляет собой продукт для ведения реестра цифровых двойников физических объектов, применяемый в городском хозяйстве и сфере безопасности[16]. Группа компаний «Благо» запустила цифровой двойник на базе low-code платформы SberMobile AIoT, который автоматизирует сбор данных о производстве, создаёт резервные копии процессов и обеспечивает централизованный контроль. Несмотря на прогресс, развитие цифровых двойников в России сталкивается с рядом задач, таких как необходимость масштабирования решений для массового внедрения, повышение точности моделей за счёт интеграции больших данных и искусственного интеллекта, а также адаптация международного опыта под специфику национальной безопасности. Формирующаяся экосистема цифровых двойников в РФ ориентирована на безопасность стратегических объектов и соответствует

требованиям как физической, так и кибербезопасности. Успехи компаний, вузов и исследователей создают основу для перехода от пилотных проектов к системному внедрению технологий.

Цифровые двойники находят широкое применение не только в системах охраны объектов, но и в решении ряда смежных задач, что значительно расширяет их функциональные возможности. Они позволяют создавать реалистичные симуляторы для отработки навыков реагирования на различные угрозы в безопасной среде, что особенно ценно для подготовки персонала охраны к редким, но критическим ситуациям, таким как террористические атаки, захват заложников и чрезвычайные происшествия с массовыми эвакуациями. Сотрудники могут тренироваться в виртуальных сценариях, имитирующих реальные угрозы, без риска для жизни или ущерба имуществу.

Для критически важных объектов, таких как атомные станции и военные объекты, цифровые двойники используются для прогнозирования последствий возможных аварий или атак, оптимизации мер безопасности за счёт анализа уязвимых зон и сокращения затрат на реальные учения, которые часто связаны с высокими рисками и расходами. Это позволяет не только повысить уровень безопасности, но и оптимизировать ресурсы.

В сфере управления чрезвычайными ситуациями цифровые двойники помогают анализировать потенциальные риски (пожары, наводнения, техногенные аварии) и разрабатывать оптимальные сценарии эвакуации. Например, при моделировании пожара на производственном объекте можно определить безопасные маршруты эвакуации, рассчитать время выхода персонала из опасной зоны и оценить эффективность систем оповещения.

Интеграция цифровых двойников с критической инфраструктурой позволяет не только отражать состояние системы безопасности, но и прогнозировать влияние угроз на работу объекта. Это критически важно для больниц, электростанций и центров обработки данных, где

автоматизация мониторинга в реальном времени, снижение вероятности человеческих ошибок и повышение устойчивости к технологическим сбоям имеют первостепенное значение.

В условиях использования нарушителями высокотехнологичных методов (БПЛА, шифрование) цифровые двойники становятся необходимым инструментом для прогнозирования новых способов противоправных действий и адаптации систем безопасности к меняющимся угрозам. Интеграция с IoT, облачными вычислениями и ИИ позволяет создавать самообучающиеся системы, обеспечивать предиктивную аналитику рисков и управлять ресурсами в режиме реального времени. Таким образом, цифровые двойники трансформируют подходы к безопасности, делая системы более адаптивными и устойчивыми к современным вызовам.

### **3 Информационный поиск технических решений в области имитационного моделирования**

Имитационная модель (ИМ), это модель, отвечающая требованию наличия стохастичности, определяемой исходной экспериментальной информацией и подвергающейся статистической обработке. Для реализации этой модели необходимо наличие техники с высокой вычислительной мощностью, которая может обеспечивать сам процесс моделирования. Таким образом, ИМ — это эксперимент, подверженный ошибкам измерения и реализуемый в цифровом пространстве.

#### **3.1 Информационный поиск и анализ нормативно-технических документов в области применения имитационного моделирования**

Широкое распространение ИМ порождает серьезный вызов, связанный с обеспечением доверия к результатам моделирования. Отсутствие единых требований к процессу создания, испытания и применения моделей может привести к принятию некорректных решений на основе недостоверных данных. В этой связи роль НТД – стандартов, руководств и методических рекомендаций, становится критически важной. Они призваны унифицировать терминологию, формализовать процессы ВВА и установить критерии качества имитационных исследований.

Все существующие НТД в области ИМ можно условно классифицировать по нескольким критериям: по сфере действия (международные, национальные, отраслевые), по объекту стандартизации (процессы, данные, программное обеспечение) и по этапам жизненного цикла модели.

##### **3.1.1 Международные стандарты**

IEEE 1730-2010 «Distributed Simulation Engineering and Execution Process (DSEEP)». Является развитием стандарта HLA (High Level

Architecture) и определяет процесс инженерной деятельности для создания и выполнения распределенных имитационных систем.

ISO/IEC/IEEE 15288:2015 «Systems and software engineering — System life cycle processes» [18]. Хотя стандарт не специфичен для ИМ, он предоставляет общую framework для инженерии систем, который может быть применен к управлению жизненным циклом сложных имитационных проектов.

Серия стандартов ASME V&V (American Society of Mechanical Engineers): ASME V&V 10-2006 (верификация и валидация в вычислительной гидродинамике), ASME V&V 20-2009 (верификация и валидация в имитационном моделировании). Стандарт V&V 20 предоставляет детальное руководство по планированию, исполнению и документированию процессов верификации и валидации для имитационных моделей.

### 3.1.2 Национальные и отраслевые стандарты

В Российской Федерации комплексного национального стандарта, посвященного исключительно ИМ, на данный момент не существует. Однако отдельные аспекты регулируются рядом ГОСТов:

– ГОСТ Р 51901.12-2007 «Менеджмент риска. Методы имитационного моделирования» [19]. Устанавливает требования к применению ИМ для анализа рисков;

– ГОСТ Р 57700.37-2021 «Компьютерные модели и моделирование. Процессы верификации, валидации и аттестации» [20]. Этот стандарт, базирующийся на международном опыте, является одним из наиболее прогрессивных и непосредственно касается процессов ВВА;

– отраслевые стандарты (ОСТ) и руководящие документы (РД) широко применяются в оборонной и аэрокосмической отраслях (например, РД серии «Имитационное моделирование сложных технических систем»), где требования к достоверности моделей крайне высоки.

### 3.1.3 Проблемы и вызовы современной стандартизации

Анализ существующей нормативной базы позволяет выявить ряд системных проблем. Большинство стандартов ориентировано на конкретные области (CFD, распределенные системы) и не покрывает всего многообразия методов ИМ таких, как дискретно-событийное, агентное, системно-динамическое моделирование.

Во всем многообразии ИМ наблюдается отсутствие единой терминологии. Такие термины, как «валидация», «верификация», «достоверность» могут трактоваться по-разному в различных стандартах и отраслях. Существующие документы в большинстве сфокусированы на процессы, а не на данные. Существует дефицит стандартов, регламентирующих качество исходных данных, их подготовку и управление ими в течение жизненного цикла модели.

Далее рассмотрим перспективы развития нормативно-технического обеспечения. Для преодоления рассмотренных проблем в области стандартизации ИМ необходима организация комплексного, гибкого и иерархического подхода к стандартизации:

- разработка базового рамочного стандарта;
- создание международного или национального стандарта, который бы определял общие принципы, термины и процессы жизненного цикла ИМ, универсальные для всех его видов;
- создание профилей стандартов;
- развитие специализированных дополнений (профилей) к базовому стандарту для конкретных отраслей (медицина, логистика) и методов моделирования;
- стандартизация метаданных и документирования;
- внедрение обязательных требований к документированию допущений, ограничений и проведенных процедур ВВА для обеспечения воспроизводимости результатов;
- интеграция со стандартами в области данных и ИИ;

– разработка нормативных документов на стыке дисциплин, регламентирующих использование машинного обучения для калибровки моделей и управления данными цифрового двойника.

Несмотря на наличие ряда прогрессивных международных и национальных стандартов, текущее состояние нормативной базы характеризуется фрагментированностью и отставанием от практических потребностей. Перспективным направлением является переход от набора разрозненных отраслевых документов к созданию единой, гибкой и многоуровневой системы стандартов. Такая система должна охватывать полный жизненный цикл имитационной модели — от формулировки концептуальной модели и сбора данных до верификации, валидации и анализа результатов [21].

3.2 Информационный поиск и анализ научных достижений, а также существующих и перспективных технических решений в области имитационного моделирования.

Имитационная модель, это логико-математическое описание объекта, которое может быть использовано для экспериментирования на компьютере в целях проектирования, анализа и оценки функционирования объекта. Имитационная модель отражает временной, пространственный и логический аспекты исследуемого процесса и представляет собой универсальный подход для принятия решений в условиях неопределённости.

### 3.2.1 Методики разработки имитационных моделей

Правильный выбор методологии и тщательная валидация модели позволяют получить достоверные результаты, которые могут быть использованы для принятия обоснованных решений в различных областях.

### 3.2.1.1 Общая методика разработки имитационной модели

Основной задачей имитационного моделирования является подмена изучаемой системы имитирующей. С имитирующей системой проводят эксперименты (не прибегая к экспериментам на реальном объекте) и в результате получают информацию об изучаемой системе. Метод позволяет имитировать, например, поведение преступника так, как он действовал бы в действительности, с учетом установленных систем безопасности, действия охраны итд. В результате, можно оценить эффективность всех установленных систем безопасности и работу персонала. Этапы имитационного моделирования представлены на рисунке 1.

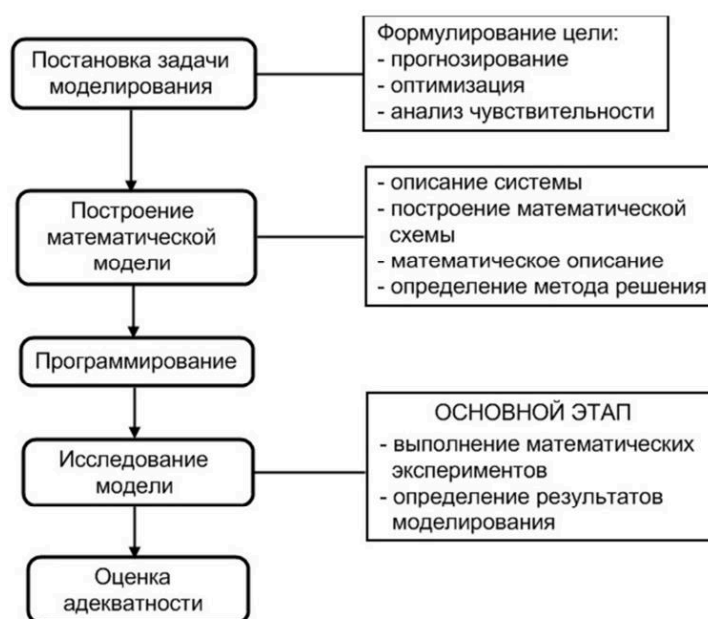


Рисунок 1 – Этапы имитационного моделирования при исследовании сложной проблемной ситуации

Структура имитационного моделирования представляется последовательно-циклической. Последовательность определяется тем, что процесс имитационного моделирования можно разбить на ряд этапов, выполнение которых осуществляется последовательно. Цикличность проявляется в необходимости возвращения к предыдущим этапам

и повторении ранее пройденного пути с измененными при необходимости данными и параметрами модели, как показано на рисунке 1.

Первый этап необходим для оценки потребности изучения объекта или проблемы, возможности и способов решения задачи, ожидаемых результатов. Этот этап очень важен для практического применения метода моделирования. Очень часто к этому этапу возвращаются после окончания исследования модели и обработки результатов для изменения постановки задачи, а иногда и самой цели моделирования.

Второй этап включает в себя формализацию описания моделируемого объекта на основе выбранной теоретической базы. На этом этапе, на естественном языке дается описание состава исследуемого объекта, взаимодействия между элементами объекта и объекта с внешней средой. На основе описания объекта выбирается концепция его формального определения. Таким образом, в конце этапа словесное описание исследуемой системы претворяется в абстрактную математическую структуру. Этот этап также включает в себя все действия по созданию имитационной модели, которые заключаются в создании компьютерной программы на основе выбранного для этой цели языка моделирования. Также, на этом этапе осуществляется и проверка полученной моделирующей программы на соответствие ее той теоретической схеме, которая была положена в основу формального описания объекта моделирования. Этот процесс часто называют верификацией модели. Второй этап заканчивается проверкой соответствия имитационной модели свойствам реальной системы. В случае отсутствия удовлетворительных результатов следует снова вернуться к моменту формализации модели, для проведения коррекции по определению теоретической базы модели.

Третий этап заключается в проведении исследования на разработанной модели путем запуска программы. Перед началом исследования полезно составить такую последовательность запусков модели, которая позволила бы получить необходимый объем информации

при заданном составе и достоверности исходных данных. Далее на основе разработанного плана эксперимента осуществляют серию запусков имитационной модели. В конце данного этапа осуществляется обработка результатов с целью представления их в виде, максимально удобном для проведения дальнейшего анализа.

Четвертый этап представляет собой анализ результатов исследования. На этом этапе определяются те свойства реальной системы, которые наиболее важны для исследователя. На основе анализа результатов подготавливаются окончательные выводы по проведенному моделированию.

Пятый этап является заключительным. На этом этапе формулируются окончательные выводы и разрабатываются рекомендации по использованию результатов моделирования для достижения поставленных целей. Часто на основе этих выводов возвращаются к началу процесса моделирования для необходимых изменений в теоретической и практической части модели и повторным исследованиям с измененной моделью. В результате нескольких подобных циклов получают имитационную модель, наилучшим образом удовлетворяющую поставленным задачам. Таким образом, метод имитационного моделирования при исследовании сложной проблемной ситуации предполагает выполнение пяти этапов. Имитационные модели позволяют оценить процессы в исследуемом объекте, и выявить в различных конкретных случаях параметры порядка. Знание последних и дает возможность строить простые модели сложных явлений [22].

### 3.2.1.2 Агентное моделирование

Агентное моделирование — направление в имитационном моделировании, которое используется для исследования децентрализованных систем, динамика функционирования которых определяется не глобальными правилами и законами (как в других

парадигмах моделирования), а наоборот, когда эти глобальные правила и законы являются результатом индивидуальной активности членов группы. Агентное моделирование позволяет рассмотреть объект исследования на более детализированном уровне и задать более сложное поведение для элементов модели.

Цель агентных моделей — получить представление об этих глобальных правилах, общем поведении системы, исходя из предположений об индивидуальном, частном поведении ее отдельных активных объектов и взаимодействии этих объектов в системе. Агент — некая сущность, обладающая активностью, автономным поведением, может принимать решения в соответствии с некоторым набором правил, взаимодействовать с окружением, а также самостоятельно изменяться.



Рисунок 2 – Виды имитационного моделирования

### 3.2.1.3 Дискретно-событийное моделирование

Дискретно-событийное моделирование (DES) — подход к моделированию, предлагающий абстрагироваться от непрерывной природы событий и рассматривать только основные события моделируемой системы, такие как: «ожидание», «обработка заказа», «движение с грузом», «разгрузка» и другие. Этот подход позволяет анализировать системы,

состоящие из последовательности событий, что особенно полезно в логистике и производстве.

Дискретно-событийное моделирование наиболее развито и имеет сферу приложений — от логистики и систем массового обслуживания до транспортных и производственных систем. Этот вид моделирования наиболее подходит для моделирования производственных процессов.

#### 3.2.1.4 Системная динамика

Системная динамика — метод моделирования в котором для исследуемой системы строятся графические диаграммы причинных связей и глобальных влияний одних параметров на другие во времени, а затем созданная на основе этих диаграмм модель имитируется на компьютере. Такой вид моделирования лучше помогает понять суть происходящего и выявлению причинно-следственных связей между объектами и явлениями. С помощью системной динамики строят модели бизнес-процессов, развития города, модели производства, динамики популяции, экологии и развития эпидемии.

#### 3.2.1.5 Статистическое имитационное моделирование

Статистическое имитационное моделирование, это вид моделирования, которое позволяет воспроизводить функционирование сложных случайных процессов. При исследовании сложных систем, подверженных случайным возмущениям, используются вероятностные аналитические модели и вероятностные имитационные модели. В вероятностном имитационном моделировании оперируют не с характеристиками случайных процессов, а с конкретными случайными числовыми значениями параметров: процесс или система. При этом результаты, полученные при воспроизведении на имитационной модели рассматриваемого процесса, являются случайными реализациями. Поэтому для нахождения объективных и устойчивых характеристик процесса требуется его многократное воспроизведение, с последующей статистической обработкой полученных данных. Такой

подход к исследованию сложных процессов и систем, подверженных случайным возмущениям, с помощью ИМ принято называть статистическим моделированием. При реализации статистического имитационного моделирования возникает задача получения случайных числовых последовательностей с заданными вероятностными характеристиками. Численный метод, решающий задачу генерирования последовательности случайных чисел с заданными законами распределения, получил название «метод статистических испытаний» или «метод Монте-Карло».

### 3.2.2 Технические достижения в области имитационного моделирования

Реализация ИМ является достаточно сложной задачей и в тоже время от качества созданной ИМ зависит работа всего цифрового двойника. ИМ можно создавать на универсальных языках программирования, используя программные пакеты или используя специальные среды разработки. Они могут быть разных видов, как общего назначения, так и специализированные, которые применяются для конкретной предметной области (моделирование транспортных потоков, производственных технологических процессов и т. п.). Наиболее распространенными инструментами для создания ИМ в мировой практике являются Anylogic, GPSS, Powersim, Arena, Aimsun, NetLogo.

В настоящее время иностранные компании-разработчики отказываются предоставлять свои программные продукты для российских пользователей, но существуют аналоги, разработанные в России и дружественных странах.

#### 3.2.2.1 Интегрированная система моделирования Actor Pilgrim.

Данное инструментальное средство разработки ИМ предназначено для выполнения и отладки ИМ развития сложных процессов с оценкой

временной, пространственной, финансовой динамики, последствий плановых или случайных структурных изменений (реинжиниринг), а также процессов массового обслуживания. Основное назначение, это анализ проектных решений. Система позволяет работать с многослойными имитационными моделями. В графе модели узлы – это процессы. Динамическая единица – Актор, выполняет функции, аналогичные транзакту в GPSS, но имеет дополнительные возможности, поскольку Актор – это программа, а не структура данных. В модели реализованы два типа направленных дуг:

- для «миграции» Акторов;
- для модельных «проводок» (операций с деньгами и финансовыми инструментами).

Пакет Pilgrim предназначен для создания дискретно-непрерывных моделей, которые имеют свойство коллективного управления процессом моделирования. В основе лежит парадигма процессно-акторного имитационного моделирования [23].

### 3.2.2.2 Система моделирования и анализа данных Imitak

Система Imitak существует в двух видах:

Visual Imitak предназначена для создания и отладки ИМ, анализа результатов моделирования и автоматизации модельных экспериментов.

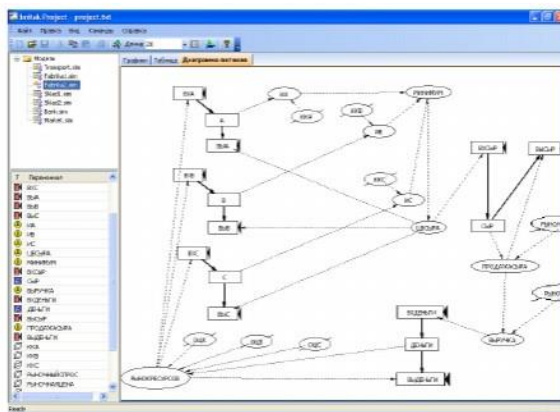


Рисунок 3 – Главное окно интегрированной системы разработки Imitak Project

В этом пакете можно строить модели системной динамики, систем массового обслуживания;

Imitak Project интегрированная система для построения комплексных имитационных моделей, состоящих из произвольного количества субмоделей. Интерфейс системы показан на рисунке 3.

### 3.2.2.3 Среда моделирования GPSS STUDIO

Данная программная система, позволяет автоматизировать разработку дискретно-событийных имитационных моделей и проводить имитационные исследования. Моделирующим ядром системы является язык имитационного моделирования GPSS World.

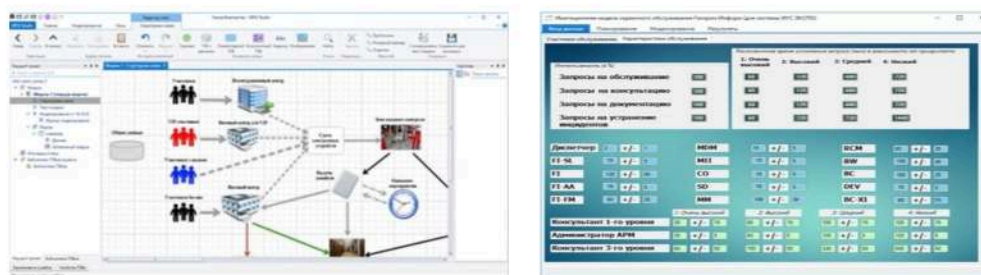


Рисунок 4 – Разработка моделей в среде GPSS STUDIO

В среде GPSS Studio реализованны:

- единое исследовательское пространство, то есть все исходные данные, модели и результаты объединяются в виде единого проекта для каждой модели, на протяжении всего процесса исследования производится автоматизация действий исследователя;
- упрощение взаимодействия с моделью, выражено тем, что для каждой модели можно создать удобный, наглядный интерфейс, что упрощает работу с моделью в процессе исследования;
- спектр инструментов для конструирования модели и проведения имитационных исследований, в том числе графических, подходящих для пользователей разного уровня подготовки;

– создание приложений, ориентированных на предметную область, дает возможность массового использования моделей.

В системе GPSS Studio есть возможность создания анимационного ролика и независимого имитационного приложения для демонстрации. Кроме того, GPSS Studio позволяет использовать дедуктивный и индуктивный подходы или их комбинацию в визуальном редакторе при создании иерархических имитационных моделей и с помощью использования блоков GPSS формировать новую логику. В процессе моделирования возможно выполнение как одиночных экспериментов, так и серии, а также детальный мониторинг переменных. Также присутствует и базовый функционал, с помощью которого можно отлаживать код, выполнять модели и анализировать результаты моделирования.

#### 3.2.2.4 Веб-приложение iWebsim

Программа iWebsim представляет собой веб-приложение, предназначенное для имитационного моделирования динамических систем, в которой реализуется комплексный подход к ИМ динамических систем, базирующийся на принципах и методологии системной динамики, дискретно-событийного моделирования и моделирования совокупностей («популяций») динамических объектов, способных к взаимодействию.

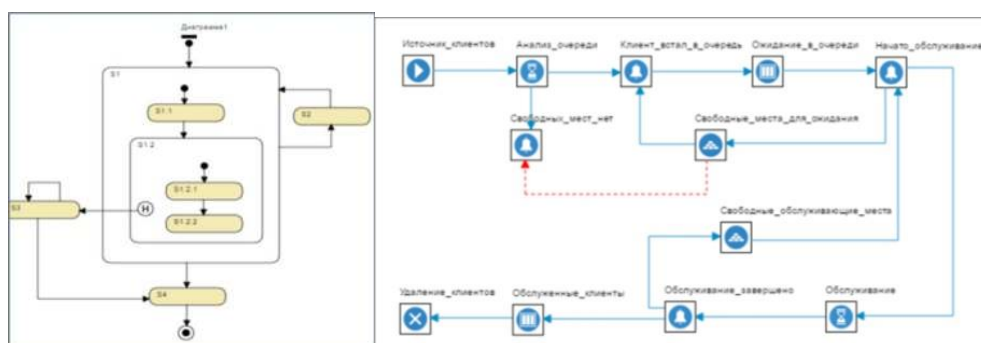


Рисунок 5 – Примеры реализации моделей в среде iWebsim

Данная программа предоставляет пользователям среду разработки моделей динамических систем и все необходимые инструменты для проведения на их основе различных имитационных экспериментов [24].

### 3.2.2.5 Среда моделирования Rand Model Designer

Предыдущее название данной системы MvStudium. Она предназначена для моделирования сложных динамических систем. Позволяет быстро создавать визуальные интерактивные модели многокомпонентных непрерывных, дискретных и гибридных (непрерывно-дискретных) систем и проводить с ними активные вычислительные эксперименты. Создание модели, визуализация результатов и управление вычислительным экспериментом не требуют написания программного кода. Модели задаются на математическом уровне абстракции. Для описания непрерывного поведения используются дифференциально-алгебраические уравнения. Для описания дискретного и гибридного поведения используются визуальные карты поведения, являющиеся расширением карт состояний UML [25].

### 3.2.2.6 Средство Anylogic

Средство Anylogic предназначено для решения широкого круга задач и поддерживающее совместную работу основных подходов к нему. Система характеризуется следующими параметрами:

- совместное применение системной динамики, агентного и дискретно-событийного моделирования;
- визуализация результатов моделирования в виде графиков, таблиц, анимации;
- имеет функцию выгрузки и загрузки данных во внешние приложения;
- имеет возможность использования разработанных самостоятельно пользовательских функций;

– возможность создания исполняемого файла для просмотра работы модели независимо от установки среды разработки [26].

### 3.2.2.7 Приложение Simul8

Интуитивно понятный инструмент SIMUL8 позволяет пользователю создавать и анализировать ИМ, учитывающую реальные ограничения, мощности, частоту отказов, графики смен и другие факторы, влияющие на общую производительность и эффективность производства. В нем можно использовать для моделирования любого процесса, где есть поток работ, однако основные области использования, это производство, здравоохранение, контакт-центры, автомобилестроение и цепочки поставок.

Построение моделей в SIMUL8 обычно основано не на программировании или статистических данных, а на отображении схем организации на экране. Однако в нем реализован двусторонний интерфейс с Visual Basic, что позволяет создавать элементы модели, которые невозможно смоделировать только с помощью графического интерфейса. Система также предоставляет собственный язык моделирования Visual Logic, который позволяющий пользователю реализовывать логику моделирования. Симуляция SIMUL8 основана на обработке рабочих элементов. Они поступают в систему через точки входа, проходят через рабочие центры, могут временно находиться в зонах хранения и покидать её через точки выхода. Помимо данного механизма, рабочим центрам могут потребоваться определённые ресурсы для обработки рабочих элементов. Симуляция состоит из ряда таких объектов и маршрутов между ними, смоделированных в виде ориентированного графического интерфейса [27].

### 3.2.2.8 Среда MATLAB/Simulink

Среда, широко используемая для математического моделирования и анализа, поддерживающая интеграцию с другими инструментами и библиотеками. Имеет среду графического программирования на основе

MATLAB, предназначенная для моделирования, симуляции и анализа многодоменных динамических систем. Разработана компанией MathWorks.

Функции Simulink:

- графическое моделирование — построение систем с помощью блок-диаграмм. Каждый блок в схеме представляет определённую математическую операцию или компонент системы, связи между блоками-линии, которые обозначают потоки данных;

- интеграция с MATLAB предоставляет возможность использовать математические функции и автоматическую генерацию кода;

- Мультидоменное моделирование — работа с механическими, электрическими, гидравлическими и другими системами;

- Поддержка аппаратных платформ — генерация кода для микроконтроллеров и ПЛИС.

## **4 Сравнительный анализ технологий, используемых для создания и применения цифрового двойника и ситуационного моделирования**

Создание цифрового двойника требует интеграции множества технологий, включая большие данные, облачные вычисления и искусственный интеллект. Эти технологии обеспечивают сбор, обработку и анализ данных, что позволяет создавать точные и актуальные модели. Также цифровые двойники позволяют не только визуализировать текущее состояние объектов, но и проводить анализ сценариев, что способствует более обоснованным решениям. Использование алгоритмов машинного обучения и аналитики данных позволяет прогнозировать потенциальные проблемы и оптимизировать процессы.

### **4.1 Проведение сравнительного анализа существующих технологий и технических решений, используемых для создания и применения цифрового двойника**

#### **4.1.1 Сравнительный анализ технических решений для создания цифровых двойников**

В современных условиях цифровизация физических объектов и пространств становится неотъемлемой частью как промышленных, так и правоохранительных, а также коммерческих процессов. В рамках данной главы проводится сравнительный анализ ряда технических решений, реализованных в Российской Федерации и за рубежом и направленных на создание цифровых двойников: программно-аппаратного комплекса «Филин», разработанного ПАО «Саратовский электроприборостроительный завод имени Серго Орджоникидзе», программной платформы Biganto Visual, а также ведущих международных решений — Siemens MindSphere, платформы совместной разработки PTC и ANSYS, и промышленной метавселенной NVIDIA Omniverse.

Комплекс «Филин» представляет собой аппаратно-программную систему, включающую 3D-камеру FilinCam со встроенным лидаром

и серверное оборудование для обработки и хранения данных. Диапазон действия лидара составляет от 0,5 до 30 метров, что позволяет эффективно сканировать как небольшие помещения, так и крупные пространства. Основное преимущество данного решения заключается в высокой скорости и точности оцифровки: для создания полной 3D-модели объекта требуется всего 10–15 минут и около пяти съёмочных точек, при этом обеспечивается полное покрытие пространства без «слепых зон». Полученная модель представляет собой полигональную сетку с наложенной фотографической текстурой, что придаёт ей высокую степень визуальной достоверности. Однако данная методология сопряжена с существенным недостатком — избыточностью данных: сканирование генерирует тяжёлые многополигональные модели, требующие значительных вычислительных ресурсов и объёмов дискового пространства для последующей обработки, и хранения.

В отличие от «Филина», платформа Biganto Visual ориентирована преимущественно на коммерческое применение в сфере недвижимости и архитектурного проектирования. Технически данное решение реализовано как программное обеспечение, не требующее специализированного оборудования на стороне пользователя: виртуальные туры доступны через веб-браузер на обычных персональных компьютерах. Biganto позволяет создавать цифровые двойники как проектируемых, так и уже существующих объектов. В последнем случае компания использует данные, полученные с помощью 3D-камеры FilinCam, что свидетельствует о синергии между двумя рассмотренными решениями. Ключевым отличием Biganto является интерактивность и гибкость визуализации: пользователь может свободно перемещаться по виртуальному пространству без дискретных «прыжков» между точками, а также взаимодействовать с объектами в реальном времени — например, использовать встроенный инструмент «рулетка» для измерения расстояний, расчёта объёмов отделочных материалов или моделирования расстановки мебели. Кроме

того, платформа поддерживает различные режимы отображения — от «бетонного» состояния до вариантов с полной отделкой и меблировкой, что расширяет её применение в маркетинге и дизайне интерьеров. Также предусмотрена функция аксонометрического вида сверху, позволяющая оценивать планировочные решения и навигацию по пространству.

На промышленном уровне широкое распространение получили интегрированные программные платформы, такие как Siemens MindSphere, а также совместные решения компаний PTC и ANSYS. В понимании Siemens цифровой двойник является неотъемлемой частью цифрового производства и предполагает создание цифровой копии всего завода, включая оборудование, производственные линии и логистические процессы.

Платформа MindSphere обеспечивает сбор, анализ и визуализацию данных в реальном времени, что позволяет осуществлять прогнозную диагностику, оптимизацию производственных процессов и управление жизненным циклом продукции. В свою очередь, PTC и ANSYS разработали совместную платформу, объединяющую возможности CAD-системы Creo и высокоточных симуляторов ANSYS, что позволяет создавать «умные» цифровые двойники, способные моделировать поведение изделия в условиях реальной эксплуатации. ANSYS Twin Builder, в частности, предоставляет инструменты для построения физически корректных моделей активов на основе данных с датчиков и уравнений, описывающих их работу.

Особое место в системе цифровых двойников занимает промышленная метавселенная NVIDIA Omniverse — платформа, специально разработанная для создания высокоточных, физически достоверных цифровых копий промышленных объектов и процессов. NVIDIA Omniverse поддерживает синхронизацию данных в реальном времени между различными CAD-, CAE- и IoT-системами, обеспечивая единое пространство для совместной работы инженеров, аналитиков и операторов. Платформа активно используется для симуляции автономных

систем, робототехники и логистических процессов с применением синтетических данных и сенсорной симуляции. Благодаря интеграции с технологиями RTX и AI, Omniverse позволяет не только визуализировать, но и «оживлять» цифровые двойники, наделяя их способностью к обучению и адаптации. В 2024 году NVIDIA расширила доступность платформы через Omniverse Cloud API, что позволяет сторонним разработчикам интегрировать её функционал в собственные промышленные приложения.

Для наглядного сопоставления ключевых характеристик рассмотренных решений представлена сравнительная таблица 1.

Таблица 1 — Сравнительный анализ технических решений для создания цифровых двойников

Наименование	«Филин»	Biganto Visual	Siemens MindSphere	PTC + ANSYS	NVIDIA Omniverse
Тип решения	Программно-аппаратный комплекс	Программная платформа (веб-ориентированная)	Облачная IoT-платформа с поддержкой ЦД	Интегрированная CAD/CAE-платформа	Промышленная метавселенная (платформа на базе USD)
Основная область применения	Следственные действия, фиксация мест происшествий	Недвижимость, архитектура, дизайн интерьеров	Управление жизненным циклом промышленных активов, прогнозная диагностика	Инженерное проектирование, физическое моделирование изделий	Симуляция сложных промышленных систем, робототехника, логистика
Источник данных	Лазерное сканирование (LiDAR)	Проектная документация / сканирование (в т.ч. FilinCam)	Данные с датчиков IoT, PLM/ERP-системы	CAD-модели, данные с датчиков, физические уравнения	Мультиформатные 3D-данные, IoT-потoki, симуляции
Тип модели	Фототекстурированная полигональная сетка	Интерактивная 3D-модель с текстурами и интерактивными инструментами	Функциональная цифровая копия с привязкой к операционным данным	Физически корректная симуляционная модель (Reduced-Order Model)	Фотореалистичная, физически достоверная сцена в реальном времени
Интерактивность	Просмотр в VR/AR, добавление аннотаций	Высокая: свободное перемещение, измерения, расстановка мебели	Аналитическая: мониторинг, управление, симуляция сценариев	Инженерная: изменение параметров, запуск симуляций	Коллаборативная: совместная работа в реальном времени, «оживление» объектов
Требования к оборудованию	Высокие (серверные мощности для обработки и хранения)	Низкие (доступ через веб-браузер)	Средние/высокие (облачная или корпоративная инфраструктура)	Высокие (мощные рабочие станции для инженеров)	Очень высокие (GPU-кластеры, DGX Cloud)
Ключевое преимущество	Скорость захвата данных	Доступность и маркетинговая привлекательность для конечного пользователя	Интеграция в сквозные цифровые процессы предприятия	Высокая точность физического моделирования поведения изделия	Масштабируемость, фотореализм и поддержка совместной работы в промышленной метавселенной

Таким образом, рассмотренные технические решения демонстрируют спектр подходов к созданию цифровых двойников — от специализированных аппаратно-программных комплексов для точечного захвата пространств («Филин») до масштабируемых облачных платформ для управления жизненным циклом промышленных активов (Siemens, PTC/ANSYS, NVIDIA). При этом наблюдается тенденция к интеграции — например, использование данных сканирования от «Филина» в платформе Biganto или совместное применение CAD и симуляционных движков в экосистемах PTC–ANSYS и NVIDIA Omniverse. Такой синтез технологий формирует основу для создания гибридных, многоуровневых цифровых двойников нового поколения, сочетающих точность, интерактивность и интеллектуальную аналитику.

#### 4.1.2 Сравнительный анализ методов создания цифровых двойников

Создание цифровых двойников — это сложный и многоаспектный процесс, в котором выбор методологического подхода определяется не только техническими возможностями, но и спецификой целевой задачи. В контексте оценки систем безопасности объектов — будь то промышленные комплексы, энергетические установки, транспортные узлы или здания общественного назначения — цифровой двойник должен обеспечивать не только точное отражение физической структуры, но и способность моделировать динамику угроз, поведение защитных механизмов, а также последствия потенциальных инцидентов. Для этого применяются различные методологические подходы, каждый из которых обладает своими особенностями, преимуществами и ограничениями. Ниже подробно рассматриваются основные методы создания цифровых двойников: физико-ориентированный, данные-ориентированный, гибридный, геометрический и событийно-ориентированный.

Физико-ориентированные методы основаны на математическом описании физических законов, управляющих поведением объекта

или системы. Такие модели строятся с использованием дифференциальных уравнений в частных производных, законов сохранения массы, энергии и импульса, а также принципов термодинамики, механики сплошных сред и электромагнетизма. Широко применяются методы конечных элементов, конечных разностей и вычислительной гидродинамики.

В контексте систем безопасности такие модели позволяют с высокой точностью воспроизводить такие процессы, как распространение огня и дыма в здании, утечка и дисперсия токсичных или взрывоопасных веществ, деформация конструкций под воздействием внешних нагрузок, тепловые режимы при авариях и др. Это особенно важно при проектировании и верификации инженерных систем: противопожарных барьеров, систем вентиляции, аварийного освещения, датчиков давления и температуры.

Однако физико-ориентированные модели обладают рядом существенных ограничений. Во-первых, они требуют глубоких знаний в предметной области и точной параметризации — даже небольшие ошибки в начальных или граничных условиях могут привести к значительным отклонениям в результатах. Во-вторых, такие модели вычислительно затратны, что затрудняет их использование в реальном времени, особенно при необходимости моделирования множества сценариев. В-третьих, они плохо адаптируются к изменениям в конфигурации объекта или к неучтённым факторам, таким как человеческий фактор или нестандартное поведение оборудования.

Данные-ориентированные методы опираются на статистический анализ и алгоритмы машинного обучения для построения моделей, способных выявлять зависимости и прогнозировать поведение системы на основе исторических или потоковых данных. К таким методам относятся регрессионные модели, нейронные сети, деревья решений, методы кластеризации и более сложные архитектуры, такие как рекуррентные нейросети и трансформеры.

В задачах оценки безопасности данные-ориентированные подходы особенно эффективны при анализе аномалий, прогнозировании отказов оборудования, распознавании подозрительного поведения с помощью видеонаблюдения. Они способны обрабатывать большие объёмы информации от распределённых сенсоров, камер, систем контроля доступа и других источников, выявляя сложные закономерности и типичные сочетания факторов, ускользающие от внимания при стандартном анализе данных. Тем не менее, такие модели страдают от ряда принципиальных недостатков. Главный из них — низкая интерпретируемость: «чёрный ящик» машинного обучения затрудняет объяснение причин срабатывания системы, что критически важно в контексте безопасности, где каждое решение должно быть обосновано и подтверждено. Кроме того, качество модели напрямую зависит от полноты и репрезентативности обучающих данных. В случае редких, но катастрофических событий (например, взрывов или терактов) собрать достаточное количество примеров для обучения практически невозможно, что делает такие модели ненадёжными в экстремальных сценариях.

Гибридные методы представляют собой синтез физико-ориентированного и данные-ориентированного подходов. Их основная идея заключается в том, чтобы использовать физические законы как каркас модели, обеспечивая её достоверность и интерпретируемость, а данные — для калибровки, уточнения параметров и адаптации к реальным условиям эксплуатации. Например, физическая модель распространения дыма может быть дополнена нейросетевым модулем, корректирующим параметры турбулентности на основе данных с датчиков температуры и давления.

В контексте систем безопасности гибридные цифровые двойники обладают уникальными преимуществами. Они позволяют моделировать как детерминированные физические процессы, так и стохастические или плохо формализуемые аспекты — например, поведение персонала при эвакуации, реакцию охранных служб или влияние погодных условий на эффективность

систем защиты. Благодаря интеграции данных в реальном времени такие модели могут динамически обновляться, обеспечивая актуальную оценку уровня угрозы и предлагая оптимальные меры реагирования.

Несмотря на высокую эффективность, разработка гибридных моделей требует мультидисциплинарной экспертизы — от физики и инженерии до информатики и теории управления. Кроме того, их вычислительная сложность может быть значительной, хотя современные подходы, такие как модельная редукция и использование edge-вычислений, позволяют частично решить эту проблему.

Геометрические методы фокусируются на создании точной трёхмерной реплики объекта с использованием технологий компьютерного зрения, лазерного сканирования, фотограмметрии и CAD/BIM-систем. Такие модели обеспечивают высокую визуальную достоверность и позволяют точно отображать пространственную структуру объекта, расположение оборудования, маршруты эвакуации, зоны доступа и другие архитектурные особенности.

Для систем безопасности геометрические модели играют важную вспомогательную роль. Они служат основой для размещения сенсоров, визуализации угроз и сценариев развития инцидентов, а также для тренировки персонала в виртуальной среде. Однако сами по себе они не способны моделировать динамику процессов и оценивать эффективность защитных мер без интеграции с другими типами моделей. Их ценность возрастает именно в составе более сложных цифровых двойников, где геометрия выступает в качестве пространственного контекста для физических, поведенческих и аналитических компонентов.

Событийно-ориентированные методы моделируют систему как последовательность дискретных событий, каждое из которых вызывает изменение её состояния. Такие подходы включают дискретно-событийное моделирование (DES), агентное моделирование и модели на основе конечных автоматов. Они особенно эффективны для описания логики

работы систем безопасности: срабатывание сигнализации, блокировка дверей, запуск протоколов реагирования, координация действий охраны и т.п.

В контексте оценки безопасности такие модели позволяют анализировать временные задержки, выявлять уязвимые места в цепочке реагирования и оптимизировать процедуры. Например, с помощью агентного моделирования можно симулировать поведение большого числа людей при эвакуации, учитывая индивидуальные особенности и взаимодействие с инфраструктурой. Однако события-ориентированные модели плохо подходят для описания непрерывных физических процессов, таких как теплопередача или распространение газа, и требуют тщательной формализации всех возможных сценариев, что может быть затруднено в условиях высокой неопределённости.

При создании цифровых двойников, ориентированных на оценку систем безопасности объектов, ни один из рассмотренных методов в чистом виде не обеспечивает полного соответствия требованиям задачи. Физико-ориентированные модели дают точность, но недостаточно гибки; данные-ориентированные — адаптивны, но непрозрачны; геометрические — визуально точны, но пассивны; событийно-ориентированные — эффективны для логики, но ограничены в физике.

Наиболее перспективным и сбалансированным подходом является гибридный метод, который интегрирует физическую достоверность, данные в реальном времени, пространственную структуру и логику событий. Именно такой подход позволяет создавать цифровые двойники, способные не только отражать текущее состояние объекта, но и прогнозировать развитие угроз, оценивать эффективность защитных мер и поддерживать принятие решений в условиях высокой неопределённости. В современных системах обеспечения безопасности критических объектов гибридные цифровые двойники становятся не просто инструментом анализа, а активным элементом интеллектуальной инфраструктуры безопасности.

## **4.2 Проведение сравнительного анализа существующих технологий и технических решений, используемых для ситуационного моделирования**

Ситуационное моделирование позволяет визуализировать и анализировать динамику систем в условиях неопределенности и изменчивости. Оно находит применение в таких областях, как управление критически важными инфраструктурами, экстренными службами и т.д. Для успешной реализации ситуационного моделирования необходимы современные технологии и инструменты, позволяющие создавать достоверные модели и проводить анализ сценариев.

Современный пространственный анализ связан с применением геоинформатики, географии, геодезии. Это с одной стороны служит развитием этих наук, с другой стороны требует внедрения новых методов анализа, обусловленных новыми задачами и требованиями. Только такой комплексный подход обеспечивает сопоставимость и анализ данных получаемых при этих исследованиях и дает возможность создания гармоничной, непротиворечивой картины мира. Ситуационные модели являются инструментом исследования окружающего мира. Как метод познания модели служат средством построения картины мира. Как информационный метод пространственное ситуационное моделирование служит инструментом извлечения информации из информационного поля. В социальном плане модели служат средством обеспечения безопасности человечества от глобальных угроз [29].

Современные подходы к моделированию угроз базируются на использовании цифровых двойников и компьютерных моделей, позволяющих воспроизводить широкий спектр сценариев — от физических вторжений до природных катастроф. Одним из передовых решений в этой области является подход, реализованный АО «Итерация», которое разрабатывает цифровые системы физической защиты, основанные на

математическом аппарате, алгоритмах и оптимизации с использованием цифровых компонентов. Такие системы позволяют не только имитировать развитие инцидентов на виртуальной копии защищаемого объекта, но и оперативно адаптироваться к новым угрозам, что особенно важно в условиях быстро меняющегося рискованного ландшафта.

Техническая реализация данного подхода включает в себя применение имитационного моделирования для симуляции сценариев на цифровой копии объекта с последующим анализом потенциальных последствий без риска для реальной инфраструктуры. Кроме того, в рамках решения АО «Итерация» активно используется статистический метод, основанный на генерации тысяч случайных сценариев с учётом вероятностных распределений. Это позволяет объективно оценивать уровень защищённости критических элементов объекта и корректировать проектные решения, например, при реконструкции комплекса инженерно-технических средств охраны (ИТСО).

Помимо специализированных решений, таких как разработка АО «Итерация», в практике имитационного моделирования широко применяются универсальные программные платформы. Например, AnyLogic сочетает в себе агентное, дискретно-событийное и системно-динамическое моделирование, что делает её гибким инструментом для анализа сложных взаимодействий между людьми, техникой и инфраструктурой в условиях чрезвычайных ситуаций. Платформа Arena, в свою очередь, ориентирована на дискретно-событийное моделирование и эффективно используется для оптимизации логистических и операционных процессов, включая маршрутизацию патрулей и распределение ресурсов охраны. Simul8 также применяется для моделирования потоков событий и оценки загрузки систем безопасности в реальном времени.

Дополнительно следует отметить использование специализированных решений на базе платформы MATLAB/Simulink,

где создаются высокоточные динамические модели физической защиты с возможностью интеграции с сенсорными и управляющими системами. Такие модели позволяют проводить детальный анализ временных характеристик срабатывания систем оповещения, задержки реакции персонала и эффективности барьеров. В последние годы также набирает популярность применение игровых движков, таких как Unity и Unreal Engine, для создания визуально насыщенных и интерактивных цифровых двойников, используемых в тренировках персонала и валидации сценариев реагирования.

В сравнении с этими универсальными и полупрофессиональными инструментами, решение АО «Итерация» отличается глубокой предметной специализацией на задачах безопасности, встроенной методологией оценки уязвимостей и возможностью прямой интеграции с существующими комплексами ИТСО. В то время как AnyLogic, Arena или MATLAB требуют значительной экспертной подготовки и адаптации под конкретную предметную область, цифровая система физической защиты от «Итерации» изначально конструируется как готовое решение для анализа угроз, проектирования и верификации мер защиты. Это обеспечивает не только более высокую скорость развёртывания, но и большую достоверность результатов за счёт использования верифицированных моделей угроз и сценариев, соответствующих нормативным требованиям в сфере антитеррористической защищённости.

Таким образом, техническое решение АО «Итерация» представляет собой целостную, ориентированную на безопасность цифровую экосистему, сочетающую в себе преимущества имитационного и статистического моделирования, а также интеграцию с реальными системами физической защиты. В совокупности с другими существующими платформами оно формирует многоуровневый инструментарий для комплексной оценки рисков и проектирования систем физической защиты нового поколения.

#### **4.2.1 Сравнительный анализ технологий ситуационного моделирования**

В современных условиях обеспечения безопасности критически важных объектов, ключевую роль играет способность прогнозировать, моделировать и оперативно реагировать на потенциальные угрозы. В этом аспекте технологии ситуационного моделирования становятся не просто инструментом поддержки принятия решений, а основой для построения адаптивных систем безопасности. Сравнительный анализ этих технологий позволяет выявить их сильные и слабые стороны, а также определить оптимальные сценарии применения в зависимости от специфики защищаемого объекта.

Одной из наиболее распространённых технологий является имитационное моделирование, основанное на создании виртуальных аналогов реальных процессов. Такие системы позволяют воспроизводить различные сценарии проникновения — от одиночных попыток до координированных атак групп террористов — и оценивать эффективность реакции охраны в условиях ограниченного времени и ресурсов. Преимущество имитационного подхода заключается в его наглядности и возможности многократного тестирования различных тактик без риска для реального персонала или инфраструктуры. Однако его недостатком является высокая зависимость от точности исходных данных: любое искажение в параметрах поведения злоумышленников или характеристик объекта может привести к некорректным выводам.

Альтернативой имитационному моделированию служит моделирование на основе агентного подхода (агентно-ориентированное моделирование), при котором каждый участник ситуации — будь то охранник, злоумышленник или техническое средство — представляется как автономный агент с собственным набором правил поведения, целей и возможностей взаимодействия. Этот метод особенно эффективен при анализе сложных, нелинейных систем, где важно

учитывать динамику взаимодействий между элементами. В контексте охраны он позволяет моделировать непредсказуемое поведение — например, адаптация группы нападающих к действиям охраны, меняя тактику в реальном времени. Тем не менее, агентное моделирование требует значительных вычислительных ресурсов и глубокого понимания психологических и тактических приемов участников, что ограничивает его применение в оперативных условиях.

Не менее перспективным направлением является моделирование на основе теории игр, которое рассматривает ситуацию как стратегическое взаимодействие между двумя или более сторонами, каждая из которых стремится максимизировать свой выигрыш. В задачах охраны это позволяет формализовать противостояние между силами охраны и нападающими, предсказывая наиболее вероятные ходы последних на основе анализа их возможных мотиваций и ресурсов. Такой подход особенно ценен при проектировании систем распределения сил и средств охраны, поскольку позволяет минимизировать уязвимости, «предугадывая» действия противника. Однако его практическая реализация сталкивается с трудностями, связанными с необходимостью точного определения функций полезности и стратегических предпочтений всех участников, что в реальных условиях часто невозможно.

Технологии машинного обучения и искусственного интеллекта всё чаще интегрируются в системы ситуационного моделирования, обеспечивая возможность самообучения моделей на основе исторических данных об инцидентах и успешных реакциях. Такие системы способны выявлять скрытые паттерны, предсказывать развитие событий и предлагать оптимальные варианты действий в режиме реального времени. Их преимущество — гибкость и способность адаптироваться к новым угрозам, но они требуют большого объёма качественных данных для обучения.

Наконец, гибридные модели, сочетающие несколько подходов — например, имитационное моделирование с элементами машинного

обучения или теории игр — демонстрируют наибольшую эффективность в комплексных задачах охраны. Они позволяют компенсировать недостатки отдельных методов, обеспечивая как детализированное воспроизведение сценариев, так и адаптивность к изменяющимся условиям. Однако разработка и эксплуатация таких систем требует высокой квалификации персонала, сложной инфраструктуры и значительных инвестиций.

Таким образом, выбор технологии ситуационного моделирования должен определяться не только техническими возможностями, но и характером защищаемого объекта, уровнем угроз, доступными ресурсами и требованиями к скорости принятия решений. Наиболее эффективным подходом представляется использование гибридных моделей, способных интегрировать достоинства разных методологий, однако их внедрение требует продуманной стратегии и поэтапного развития инфраструктуры безопасности.

## **5 Анализ перспектив развития системы охраны объектов с применением цифрового двойника**

Перспективы развития систем охраны объектов с применением цифрового двойника связаны с возможностью моделирования поведения объектов в реальном времени, прогнозирования угроз и оптимизации процессов. Это направление требует развития концепции цифрового двойника, их применения в разных областях и учёта вызовов, связанных с внедрением в современные системы безопасности.

### **5.1 Анализ возможных путей расширения функциональных возможностей системы централизованной охраны объектов и тактики локальной охраны при использовании технологии цифрового двойника**

Применение технологии цифровых двойников на охраняемых объектах можно использовать в целях подготовки паспортов безопасности, контроля устранения выявленных недостатков, моделирования угроз при

чрезвычайных обстоятельствах и иных нештатных ситуациях. Также цифрового двойника можно использовать на стадии формирования и выбора оптимального построения системы безопасности, создания информационной системы помощи в принятии решений в сложных ситуациях. Для выбора оптимального комплекса инженерно-технических средств охраны, тактики охраны, как для обобщенных примеров, так и для оценки конкретных решений по организации охраны на конкретном объекте, может применяться комплекс программного обеспечения для создания и анализа цифрового двойника комплекса ИТСО объекта и имитационного моделирования. Цифровой двойник может включать в себя информацию о структуре здания, системах безопасности, а также данные о внешней среде и потенциальных угрозах.

Работу цифрового двойника по направлению безопасности необходимо рассматривать в двух аспектах: подготовка объекта – апробация предполагаемой защиты объекта с использованием цифрового двойника и контроль безопасности объекта с применением цифрового двойника в режиме реального времени.

#### 5.1.1 Подготовка и апробация предполагаемой защиты объекта с использованием цифрового двойника

Цифровой двойник позволяют моделировать различные сценарии, включая поведение преступников, реакцию охраны и возможные последствия различных действий. Это дает возможность оценить эффективность различных стратегий охраны и выбрать наиболее оптимальные. Также технологии цифрового двойника позволяет оптимизировать существующие системы охраны, повышая их эффективность. В условиях растущих угроз, внедрение цифрового двойника в процессы охраны становится необходимым шагом к обеспечению безопасности объектов.

Этапы решения задач построения цифрового двойника, при внедрении систем безопасности:

- создание цифрового двойника объекта;
- создание цифрового двойника системы физической защиты;
- создание цифрового двойника комплекса ИТСО;
- анализ уязвимости технологических процессов;
- оценка эффективности существующей системы охраны;
- обоснование замыслов совершенствования системы охраны;
- концептуальное проектирование комплекса ИТСО;
- сравнительный анализ вариантов концептуальных проектов комплекса ИТСО по критерию эффективность/стоимость;
- подготовка и проведение компьютерных учений и тренировок.

Использование цифрового двойника позволяет осуществить неограниченное количество сеансов моделирования любой нештатной, экстремальной итд ситуации в режиме эксперимента, без нанесения ущерба реальному объекту и при этом произвести автоматическую статистическую обработку и документирование результатов. То есть создать неограниченное количество отчетов в любом удобном виде в режиме автоматического формирования, включая табличные и графические данные. Анализ результатов имитационного моделирования дает интегральную оценку эффективности системы охраны объекта от всего множества выбранных угроз, выбранными вариантами сил и средств реагирования. Кроме того, отчет о результатах моделирования включает дифференциальные оценки эффективности системы охраны как по решению отдельных задач, так и предоставляет сравнительную оценку эффективности функциональных подсистем системы охраны.

Применение цифрового двойника при проектировании ИТСО помогает найти оптимальную точку по критерию стоимость/эффективность. А использование программных средств имитационного моделирования позволяет выполнить аналогичную процедуру, но с поиском оптимальных

структур и состава систем охраны объектов. Еще на этапе концептуального проектирования проектировщик, при использовании специальных приложений, получает инструментарий быстрой генерации вариантов системы охраны буквально «набрасывая» мышкой элементы из базы

данных комплекса. Это дает возможность относительно быстрой автоматизированной сравнительной оценки эффективности созданных вариантов с помощью средств имитационного моделирования. Но конечный выбор предпочтительного варианта построения ИТСО, по результатам имитационного моделирования, принимается людьми. Структура процесса концептуального проектирования показана на рисунке 6.

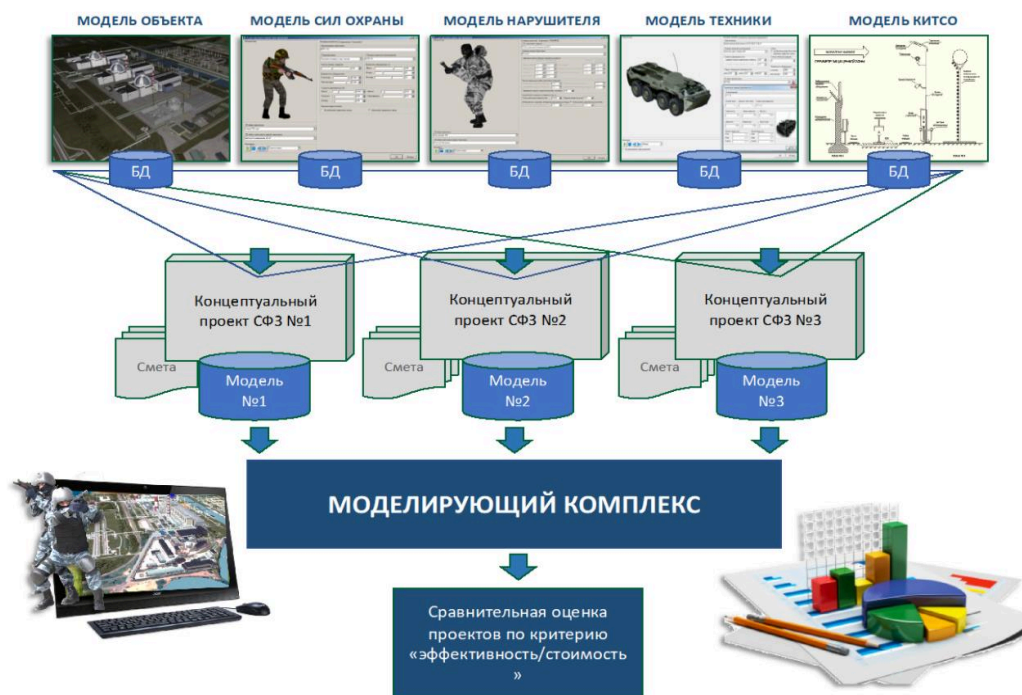


Рисунок 6 – Структура процесса концептуального проектирования

Такой подход дает обоснованную бюджетную оценку вариантов концептуального проекта. Это исключает как перерасход бюджета, так и заключение договоров с дефицитом бюджета. Вышеописанные методы обеспечения необходимой эффективности систем охраны объектов в том числе и методы имитационного моделирования требуют актуальных, достоверных, полных и непротиворечивых исходных данных. Объем этих данных поистине огромен. Эти данные образуют цифрового двойника

объекта, который включает в качестве подсистем, как самого предприятия, так и системы безопасности объекта в составе которого создается цифровой двойник системы охраны.

Цифровой двойник объекта представляет собой взаимоувязанную совокупность моделей структуры объекта и модели бизнес-процессов его функционирования. Создать базы данных цифрового двойника объекта относительно не сложно. Процесс первичного ввода данных несмотря на организационные сложности также вполне реализуемая задача. Более сложной представляется задача поддержание этих баз данных в актуальном состоянии.

С этой целью целесообразно разрабатывать и внедрять на АРМ владельцев информационных массивов приложения, предоставляющее данные в цифрового двойника в автоматизированном режиме по компьютерной сети предприятия. Для получения данных содержащихся в сторонних (относительно цифрового двойника) информационных системах предприятия. Специалисты администрирующие эти системы должны настроить соответствующие процедуры для автоматического предоставления данных.

Актуальность, достоверность и полнота данных, содержащихся в базах данных цифрового двойника, обеспечивает достоверность результатов моделирования, а, следовательно, и качество принимаемых решений [30].

#### 5.1.2 Контроль безопасности объекта с применением цифрового двойника в режиме реального времени

Цифровой двойник опирается на параметры физических объектов форма, функциональность, расположение, процесс, время, состояние, окружающая среда. Как правило, каждая характеристика формируется зарекомендовавшей себя на практике программной платформой, которая

десятилетиями отлаживалась от версии к версии, совершенствовался ее функционал и собирался в единую программную систему. Предлагались

соответствующие форматы хранения модели или ее элементов в цифровой форме. Так, например, форма объекта может создаваться с помощью программных платформ AutoCAD, SolidWorks, SolidEdge и т. д., а напряженно-деформированное состояние объекта, будь то деталь автомобиля, элемент строительной конструкции и т. п., – с помощью платформ Ansis, LCAD и т. д.

Указанные выше параметры могут создаваться на высоком уровне детализации, точности формы, которая удерживается в течение заданного времени, не допускается, например, износ или деформация при столкновении. Платформы, отвечающие за разные аспекты формирования и использования цифровых двойников, функционируют независимо одна от другой и сложны в интеграции. В работе подтверждаются указанные выше положения, дается развернутая классификация программного обеспечения цифрового двойника по реализуемому этапу его подготовки:

- создание виртуального двойника;
- сбор данных с физического объекта, мониторинга и управления физическим объектом;
- создание хранилища собираемых данных;
- создание сервисного элемента, который предоставляет услуги и интерфейс клиентам;
- создание коммуникаций между названными элементами [31].

Такой подход с применением разнообразных платформ применим для описания отдельных элементов дает возможность не ограничиваться определёнными программными продуктами. Однако в отношении цифрового двойника нужно соблюдать принцип непрерывного взаимодействия и бесшовного обмена данными между его компонентами, которые иногда необходимо обеспечивать в режиме реального времени или с заданным интервалом. В таком случае использование множества

платформ усложняет их интеграцию и получение нужного результата. Особенно это касается взаимодействия с внешней средой, моделирования физических полей. Взаимодействие и взаимовлияние элементов цифрового двойника создают проблему прогнозирования состояния физической системы с заданной точностью, погрешностью. В этом случае двунаправленные связи между цифрового двойника и управляемой системой не позволяют осуществлять эффективное управление.

Указанный недостаток может быть преодолен благодаря созданию единой платформы, позволяющей интегрировать отдельные сервисы или функции для поддержания точности цифровой модели, прогнозирования ее состояния, получения выгоды, которая может выражаться в экономическом эффекте поддержания живучести управляемой системы, либо предотвращения аварийных ситуаций или катастроф. В некоторых случаях цифровой двойник может стать альтернативой виртуальных экспериментов для прогнозирования будущего результата. Развитие вычислительной техники позволяет использовать такие технологии в промышленности, сельском хозяйстве, логистике и безопасности.

Преимущества описанного подхода — это увеличение эффективности охраны за счет оптимизации тактик реагирования, возможность тестирования новых методов охраны без риска для реальных объектов и улучшение подготовки сотрудников охраны.

Расширение функциональных возможностей ведется через интеграцию цифрового двойника с существующими системами видеонаблюдения, сигнализации и контроля доступа. Это позволит создать единую платформу для мониторинга состояния объектов и управления системами безопасности. Централизованный контроль за состоянием всех систем безопасности дает возможность анализа данных в реальном времени и принятия оперативных решений. Упрощение процесса управления и взаимодействия между различными системами. Использование цифрового двойника позволяет не только отслеживать текущее состояние

объекта, но и прогнозировать возможные угрозы на основе анализа исторических данных и текущих событий. Системы, основанные на машинном обучении, могут выявлять направления поведения, и основываясь на полученных данных прогнозировать потенциальные угрозы. Все описанные методы позволяют получить снижение вероятности возникновения инцидентов и дают возможность заранее подготовиться к возможным угрозам.

## **5.2 Анализ проблемных вопросов внедрения и эксплуатации существующей системы безопасности с использованием технологии цифрового двойника**

Цифровой двойник позволяют создавать динамичные модели, интегрированные с реальными системами, что способствует повышению эффективности, снижению затрат и улучшению качества продукции [33].

Общая ценность данной технологии в ее влиянии, на развитие протекающих процессов путем предоставления прогнозирования на основе получаемых данных в режиме реального времени. Однако внедрение цифрового двойника сталкивается с множеством трудностей, обусловленных сложностью моделей, необходимостью обработки больших объемов данных и обеспечением надежности систем, а также необходимостью вливания высоких начальных инвестиций.

### **5.2.1 Создание 3D модели объекта**

В основе любого цифрового двойника находится виртуальный прототип какого-либо физического объекта, для которого создается привязка ряда имитационных моделей с функцией сбора данных от физического оригинала, необходимых для дальнейшего анализа и отработки различных сценариев, действий в виртуальном пространстве. А виртуальная модель любого физического объекта представляет из себя сложную полигональную сетку (жарг. меш от англ. polygon mesh), являющейся

совокупностью вершин и граней, которые в итоге определяют форму многогранного объекта в трёхмерном виртуальном пространстве при объёмном моделировании. В настоящий момент существует два способа перевода реального объекта в виртуальный мир: автоматизированный и ручной.

Одной из основных проблем, при создании цифрового двойника является сам процесс разработки виртуального прототипа объекта капитального строительства.

Ручной способ построения, это способ, при котором, чертежи с бумажного или электронного носителя переводят в 3D формат непосредственно действующими сотрудниками операторами программного обеспечения при помощи предоставляемых средств. На рисунке 7 показана полигональная модель комнаты, которая была создана в ручном режиме. Необходимо отметить, что существуют ситуации, при которой чертежей вообще не существует или они частично утрачены. Подобные ситуации особенно распространены при работе со старыми объектами капитального строительства, или в случае, когда документация была утеряна. Отсюда, вытекают две основные проблемы, это скорость создания цифрового двойника и его точность.

Даже с использованием чертежей при ручном переводе в 3D формат, все равно возникают неточности, основными причинами которых могут быть как изменения, которые произошли с объектом в процессе строительства или эксплуатации и не учтенные на исходных носителях, так и человеческий фактор.

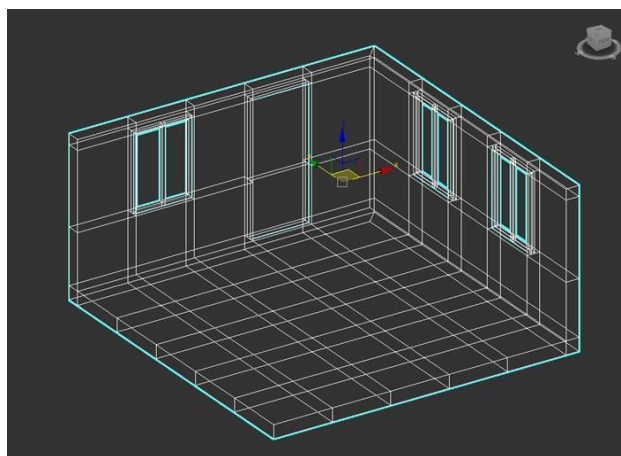


Рисунок 7 – Полигональная модель архитектурного сооружения, созданная в ручном режиме

Альтернативой ручного создания полигональной сетки является ее формирование с использованием сканирующих лазерных лидаров – оборудования способного формировать двухмерную или трёхмерную картину окружающего пространства в системах машинного зрения.

Автоматические методы построения 3D модели создаются с использованием сканирующих лазерных лидаров – оборудования способного формировать двумерную или трёхмерную картину окружающего пространства в системах машинного зрения. Такой способ, по сравнению с ручным методом, выгодно отличается прежде всего скоростью создания разработки виртуального прототипа архитектурного объекта. То есть, при использовании простого ручного лидара, работающего в комплексе со специальным программным обеспечением, позволяет сократить временные затраты в 30-60 раз, при этом избегая неточностей ручной оцифровки и любых видов чертежей, поскольку работа ведется только с реальным объектом. Дополнительным достоинством этого способа является возможность наложения фотографических текстур на полигональную сетку, что придает реалистичность отображения объекта. Это не является обязательной частью процесса создания цифрового двойника, однако улучшает презентационную часть проекта. При всех плюсах автоматического метода построения виртуальной модели,

необходимо учитывать и основной недостаток данного процесса – избыточность 3D модели. Процесс сканирования пространства априори создает тяжелую много-полигональную модель, что в свою очередь требует большие серверные мощности и объемы дискового пространства при дальнейшей обработке и хранении данных цифрового двойника. На рисунке 8 показан результат создания 3D модели жилой комнаты с использованием лидара. Даже визуально сравнив рисунков 7 и 8 можно оценить разность цифрового веса моделей, составляющую несколько порядков. Также стоит отметить, что при создании виртуальной копии объекта с использованием лидара в 3D модель могут попасть случайные предметы, которые становятся его неотъемлемой частью.

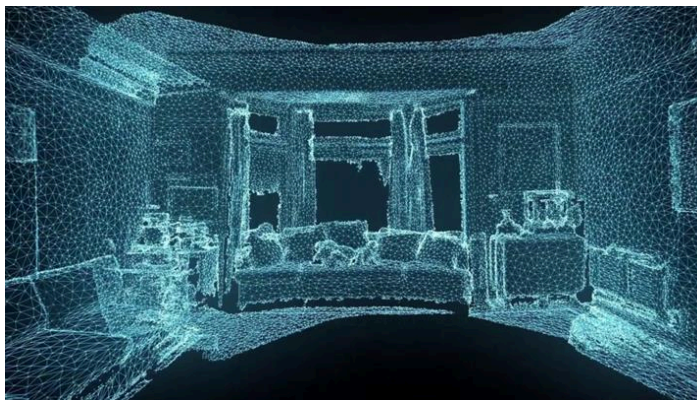


Рисунок 8 – Полигональная модель архитектурного сооружения, созданная при использовании лидара

Один из вариантов решения данной проблематики состоит в симбиозе двух методов построения 3D модели, при котором полученные данные, собранные с использованием лидара будут обрабатываться в автоматическом режиме и приводить к упрощённому виду, выявляя потенциально ошибочные или преизбыточные полигональные структуры.

В настоящий момент, подобные системы находятся в начале своего развития. При этом построение таких систем возможно с использованием технологий искусственного интеллекта, в частности нейросетевых моделей,

что в свою очередь содержит проблематику создания баз данных как для обучения системы, так и для контроля результатов обучения.

### 5.2.2. Сложность верификации и валидации цифрового двойника

Создание точной цифровой модели требует глубокого понимания физической системы и её поведения. Модели должны учитывать множество факторов, включая законы и особенности динамического взаимодействия физических и социальных объектов. Верификация и валидация моделей часто являются трудоемкими и требуют значительных ресурсов. Два этих процесса необходимы для обеспечения качества, точности и достоверности цифровых моделей. Но для начала дадим этим процессам определения.

Валидация цифрового двойника – это процесс подтверждения того, что модель в достаточной степени отражает поведение и характеристики реального объекта, равно как и всей системы, осуществляемый как правило путем сравнения результатов моделирования с эмпирическими (экспериментальными или полученными в ходе регулярной эксплуатации) статистическими данными или аналитическими решениями. Модель можно считать валидированной, при условии согласования (отклонения не более чем на заранее выбранную малую величину) результатов моделирования с данными, полученными из иных источников.

Верификация цифрового двойника – это проверка корректности реализации математических моделей и алгоритмов программного обеспечения, которые были использованы при создании цифрового двойника. Эти два процесса проходят на этапе создания, корректировки или дополнения цифрового двойника новыми элементами и от корректности их реализации зависит степень точности модели. Проблемы данного этапа выражаются в отсутствии универсальных стандартных проверенных методов, которые не реализованы по ряду причин:

– большое разнообразие моделей и систем при отсутствии универсальных подходов к процессам валидации и верификации;

– необходимость обработки больших объемов различных данных и протекающих процессов, при обработке которых необходимо учитывать их взаимосвязь и взаимодействие как внутри одной, так и при взаимодействии с другими моделями;

– хаотичность и сложность протекания некоторых процессов, которые сложно поддаются математическому моделированию (случайные и псевдослучайные процессы), но при этом могут влиять на смежные процессы цифрового двойника.

Решение данных проблем идет по двум параллельным направлениям:

– создание библиотек проверенных моделей цифрового двойника, с открытым доступом (не обязательно бесплатным). Разработка единых моделей отдельных элементов цифрового двойника (например, модель поведения нарушителя), является достаточно затратным процессом, как по временным, так и по финансовым показателям. Создание общедоступных библиотек поможет удешевить процесс создания цифрового двойника для каждого нового объекта и в тоже время вернуть часть затрат производителям моделей, при возмездной схеме распространения. А главное, в условиях быстрого технического развития, обеспечит оперативное изменение моделей по решению (в соответствии с проведенными исследованиями) уполномоченных организаций.

– стандартизация методов создания и протоколов взаимодействия моделей цифрового двойника. Для обеспечения работы цифрового двойника на реальных объектах требуется передача и обработка данных в реальном времени от множества источников, таких как системы охранного телевидения с функцией видеоаналитики, охранные системы, системы контроля и управления доступом, пожарные системы, а также различных сенсоров и иных информационных систем. Отсюда вытекает необходимость обеспечения возможности взаимодействия с разнородными протоколами и стандартами передачи данных. Особенно остро проблема совместимости

может возникать при внедрении цифрового двойника на объектах с устаревшими системами управления производственными процессами, в т.ч. безопасности. Одним из путей решения данной проблемы может быть стандартизация информационного обмена (виды и форматы данных) для многогранговой архитектуры цифрового двойника в рамках автоматизированных систем управления технологическими процессами в части безопасности, а также стандартизации протоколов связи для одноранговой архитектуры цифрового двойника.

### 5.2.3. Высокомощные вычислительные ресурсы

В процессе своей деятельности цифровые двойники работают со значительными объемами исходных данных, а также создают их значительные объёмы, которые необходимо обрабатывать и анализировать в режиме реального времени, что, в свою очередь, требует применения современных технологий и алгоритмов для анализа полученных данных, а также накладывает высокие требования на вычислительные ресурсы.

К этому можно добавить, что обработка сложных моделей в режиме реального времени требует значительных вычислительных мощностей и эффективных алгоритмов обработки данных, что приводит к необходимости установки серверов (или построения распределенной системы – единого комплекса компьютерных программ, использующих вычислительные ресурсы нескольких серверов объединенных для достижения одной общей цели) с высокой вычислительной мощностью, организаций соответствующей инфраструктуры и применения алгоритмов для анализа данных, а также учёта множества других параметров и факторов.

### 5.2.4 Обеспечение безопасности и конфиденциальности цифрового двойника

Несмотря на то, что цифровой двойник может создаваться для повышения безопасности объекта, нельзя забывать о защищенности его

самого и технических ресурсов, обеспечивающих работу. Процесс поддержки и обеспечения работоспособности цифрового двойника, тесно связан с передачей, обработкой и хранением больших объемов данных, что в свою очередь повышает риски кибератак и утечек информации. Данная проблема осложняется отсутствием возможности использования технических средств, произведенных в странах в недружественных странах, в купе с отсутствием аналогов российского производства.

## ЗАКЛЮЧЕНИЕ

Программное обеспечение по созданию и применению цифровых двойников, а также имитационного моделирования имеет значительный потенциал для улучшения устойчивости и адаптивности систем физической и информационной безопасности на объектах высоких классов важности, в том числе критически важных инфраструктурных объектов, обеспечение безопасности которых относится к основным направлениям деятельности войск национальной гвардии Российской Федерации. Причем рассматривать данные сквозные технологии имеет смысл в паре, как дополняющие и повышающие эффективность применения друг друга.

Использование этого программного обеспечения позволяет моделировать угрозы, тестировать защитные решения, оптимизировать процессы реагирования и обучать персонал в условиях, близких к реальным.

При этом практическое внедрение цифровых двойников сталкивается с рядом нерешенных проблем, включая технические ограничения, угрозы безопасности и отсутствие единых организационно-правовых подходов, а также заметную стоимость создания и поддержания цифрового двойника и имитационных моделей в актуальном состоянии.

В перспективе следует уделить особое внимание изучению вопросов, касающихся потенциального влияния на цифровые двойники как на активные элементы инфраструктуры. Цифровые двойники могут являться самостоятельными субъектами информационного взаимодействия, принимающими участие в принятии решений и формировании реакции системы на внешние воздействия. Это требует формирования новых подходов к доверию, управлению и контролю организации охраны объектов разных категорий и классов. Кроме того, требуется проведение дополнительных исследований в области теоретических и методологических основ безопасного функционирования цифровых двойников.

Однако, рассмотренные технические решения имеют большой потенциал в реализации для определения оптимального построения системы охраны объекта (собственного объекта войск национальной гвардии Российской Федерации, объекта, подлежащего охране войсками национальной гвардии Российской Федерации, или категорируемого объекта, безопасность которого контролируется войсками национальной гвардии Российской Федерации), включая комплекс ИТСО и оценки достаточности системы охраны в целом. Данные технические решения дают специалистам войск национальной гвардии Российской Федерации объективный инструмент оценки системы охраны и комплекса ИТСО объекта от угроз, в том числе угроз террористического характера.

При этом оптимизация расходов собственника на охрану объекта позволяет для дорогостоящих систем охраны (например, объектов ТЭК) компенсировать расходы на создание и поддержание в актуальном состоянии имитационной модели объекта.

Создание научно обоснованных подходов к регулированию, верификации и аттестации как программного обеспечения цифровых двойников и имитационного моделирования, так и создаваемых с помощью данного программного обеспечения моделей, станет важным условием для их безопасной и эффективной интеграции в систему охраны объекта и систему контроля антитеррористической защищенности объекта.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Сосфенов Д.А., Использование цифровых двойников в автомобильной промышленности: российский и зарубежный опыт // Экономика и управление. 2023. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/ispolzovanie-tsifrovyyh-dvoynikov-v-avtomobilnoy-promyshlennosti-rossiyskiy-i-zarubezhnyy-opyt?ysclid=memhc3l6nr722528763>
2. Балацкий Е.В., Наука и технологии: новая модель отношений // Научноисследовательские исследования. 2008. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/nauka-i-tehnologii-novaya-model-otnosheniy?ysclid=memhgb18na629314364>
3. Цёхла С.Ю., Симченко Н.А., Направления формирования экономических эффектов внедрения цифровых двойников. // Россия: тенденции и перспективы развития. 2020. [Электронный ресурс].  
Режим доступа: <https://cyberleninka.ru/article/n/napravleniya-formirovaniya-ekonomicheskikh-effektov-vnedreniya-tsifrovyyh-dvoynikov?ysclid=memi9lid6q447206514>
4. ГОСТР 57700.37—2021 Компьютерные модели и моделирование цифровые двойники изделий. Москва. Российский институт стандартизации 2021
5. ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения (с Изменением N 1) ГОСТ от 08 декабря 1981 г. № 16504-81
6. ISO/IEC TR 30172:2023 © ISO/IEC. 2023. Technical report. ISBN 978-2-8322-7604-4
7. ISO/IEC 30173:2023. Цифровой двойник. Концепции и терминология. 08 ноября 2023 г.
8. ISO 23247-1:2021(E) Automation systems and integration — Digital twin framework for manufacturing. First edition 2021-10.

9. Министерство промышленности и торговли Российской Федерации Приказ от 19 апреля 2023 г. № 1450 Об утверждении форм предоставления информации для включения в государственную информационную систему промышленности субъектами деятельности в сфере промышленности, органами государственной власти и органами местного самоуправления, соответствующих составу информации, предоставляемой оператору государственной информационной системы промышленности для включения в государственную информационную систему промышленности субъектами деятельности в сфере промышленности, органами государственной власти и органами местного самоуправления, утвержденному постановлением правительства российской федерации от 21 декабря 2017 г. № 1604.

10. Another avenue for digital twins: behavioral modeling for banks [Электронный ресурс]. – Режим доступа: <https://www.rtinsights.com/another-avenue-for-digital-twins-behavioral-modeling-for-banks/>

11. Airport terminal design & construction: ensure seamless passenger flows with digital twin simulation [Электронный ресурс]. – Режим доступа: <https://www.incontrols.com/digital-twin-simulation-for-designing-constructing-airport-terminals-ae-r3/>.

12. Virtual Singapore [Электронный ресурс]. – Режим доступа: <https://oecd-opsi.org/innovations/virtual-twin-singapore/>.

13. Industrial cybersecurity [Электронный ресурс]. – Режим доступа: <https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>.

14. CML Bench® — платформа по разработке и применению цифровых двойников изделий [Электронный ресурс]. – Режим доступа: <https://cml-software.ru/products/cml-bench>.

15. Nadal — решение для всех уровней ИТ и ИБ [Электронный ресурс]. – Режим доступа: <https://hadal.tech/>.

16. SP5000 Цифровой двойник. Сервис ведения цифровых двойников объектов [Электронный ресурс]. – Режим доступа: <https://www.iskratechno.ru/software-development/sp5000-tsifrovoy-dvoynik-servis-vedeniya-tsifrovyykh-dvoynikov-obektov/>

17. Царькова Е.Г. К вопросу правового регулирования отношений в сфере

18. ISO/IEC/IEEE 15288:2015 «Systems and software engineering — System life cycle processes» // C/S2ESC - Software & Systems Engineering Standards Committee. 2015

19. ГОСТ Р 51901.12-2007 «Менеджмент риска. Методы имитационного моделирования»

20. ГОСТ Р 57700.37-2021 «Компьютерные модели и моделирование. Процессы верификации, валидации и аттестации».

21. Иванов А.С., Петров В.К., Нормативно-технические документы в области применения имитационного моделирования: современное состояние и перспективы стандартизации. // Национальный исследовательский университет «Высшая школа экономики» Москва, Россия. УДК 681.3.06

22. Колекина А.О. Потекаева Ю.В., Имитационное моделирование: сущность, методы и особенности. // APRIORI. Серия: Естественные и технические науки. 2016. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/imitatsionnoe-modelirovanie-suschnost-metody-i-osobennosti?ysclid=memt6cnb8n730941957>

23. Емельянов А.А., Концепция и возможности акторно-ориентированной системы имитационного моделирования «Actor Pilgrim». // Прикладная информатика. (ВАК) 2012. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/kontsepsiya-i-vozmozhnosti-aktorno-orientirovannoy-sistemy-imitatsionnogo-modelirovaniya-actor-pilgrim-1?ysclid=memtd7g3xy777833450>

24. Малыгина С.Н., Неупокоева Е.О. Обзор современных средств имитационного моделирования. // Журнал Труды Кольского научного центра РАН. Серия: Технические науки. 2022. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/obzor-sovremennyh-sredstv-imitatsionnogo-modelirovaniya?ysclid=memtmcn7hx390407599>

25. Колесов Ю.Б., Сениченков Ю.Б., От научно-исследовательской до промышленной версии: на примере среды визуального моделирования rand Model Designer. // Информатика, телекоммуникации и управление. (ВАК). 2011. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/ot-nauchno-issledovatel'skoy-do-promyshlennoy-versii-na-primere-sredy-vizualnogo-modelirovaniya-rand-model-designer?ysclid=memtsijwg859444371>

26. Штыкова А.С., Обзор некоторых возможностей среды ANYLOGIC. // Форум молодых ученых. 2017. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/obzor-nekotoryh-vozmozhnostey-sredy-anylogic?ysclid=memtw8z81k691095913>

27. Якимов И.М., Кирпичников А.П., Валова К.Д., Анишкина В.Н., Имитационное моделирование в системе Simul8. // Вестник Казанского технологического университета. (ВАК) 2017. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/imitatsionnoe-modelirovanie-v-sisteme-simul8?ysclid=memu08ojsu686715981>

28. Васильев А.Н., Тархов Д.А., Малыгина Г.Ф., Методы создания цифровых двойников на основе нейросетевого моделирования. // Современные информационные технологии и ИТ-образование. (ВАК) 2018

29. Tsvetkov V.Ya. Information field // Life Science Journal. 2014. № 11 (5). P. 551-554.

30. Цветков В.Я. Триада как интерпретирующая система // Перспективы науки и образования. 2015. № 6. С. 18-23.

31. Щекочихин О.В., Современные тенденции управления киберфизическими системами на основе цифровых двойников. // УДК

004.42 Информационно-экономические аспекты стандартизации и технического регулирования. Информационные системы и процессы. 5/2021. (63) С.33-35.

32. [Электронный ресурс]. — Режим доступа: <https://ieastr.ru/gallery/33-37%20%D0%A9%D0%B5%D0%BA%D0%BE%D1%87%D0%B8%D1%85%D0%B8%D0%BD.pdf?ysclid=mehd1y4cgq876108265>

33. Измайлов М.К., Цифровые двойники как инструмент повышения эксплуатации основных средств в промышленности. // Beneficium.2025.1(54).102-111