МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Кафедра: Прикладная математика и информатика

09.04.03 Прикладная информатика
(код и наименование направления подготовки / специальности)

Прикладной анализ данных
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему: «Применение методов и моделей программной инженерии для поддержки систем безопасности организации»

Обучающийся Ю.М. Давыдов
(Инициалы Фамилия) (личная подпись)

Научный руководитель к.э.н., Т.А. Раченко
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Оглавление

Введение

В настоящее время системы безопасности сильно усложняются и обретают дополнительные технические и компьютеризированные технологии. В это же время необходимо учитывать требования к не компьютеризированным системам безопасности. Постоянное усложнение систем безопасности и сочетание в них как компьютеризированных, так и не компьютеризированных подсистем приводит к повышению трудоемкости и снижению эффективности их контроля, обслуживания и модификации.

Тема антитеррористической защищенности объектов в настоящее время исследуется как с методических [3], [5], так и с законодательных [4], [6] и технических [8], [16], [22] точек зрения.

В сфере информационных технологий также всё время усложняются информационные системы и требования к этим системам, предъявляемые законодательством и заказчиками. Вместе с этим, в IT сфере развиты методологии анализа требований, обеспечения поддержки, проектирования и моделирования IT систем, обеспечивающие минимальные затраты и высокую эффективность при соответствии всем существенным требованиям на основе прикладного анализа данных.

Изложенное обуславливает актуальность применения методов и моделей программной инженерии для поддержки систем антитеррористической безопасности организаций.

Целью работы является повышение эффективности деятельности по обеспечению антитеррористической защищенности (АТЗ) организаций путем применения методов и моделей программной инженерии.

Для достижения поставленной цели необходимо решать следующие задачи:

– провести анализ существующих моделей и методов повышения эффективности деятельности по обеспечению антитеррористической защищенности (АТЗ) организаций путем

применения методов и моделей программной инженерии;

- исследовать модели и методы программной инженерии на предмет применимости в сфере моделирования деятельности по обеспечению безопасности;
- разработать модель применения инструментов программной инженерии в управлении системами АТЗ организаций;
- выполнить практическую апробацию предложенного решения и проанализировать полученные результаты.
- оценить предложенные решения на примере системы антитеррористической защиты ТГУ

Гипотеза исследования: применение моделей и методов программной инженерии для управления системами безопасности организаций приведет к повышению качества и эффективности деятельности по обеспечению безопасности.

Научная новизна работы состоит в предложенной трехуровневой модели применения инструментов программной инженерии в управлении системами АТЗ.

Практическая значимость заключается в повышении качества и эффективности деятельности по защите предприятий и организаций за счет применения моделей и методов программной инженерии для управления системами АТЗ.

На защиту выносятся:

- трехуровневая модель применения методов программной инженерии к системам АТЗ;
- практическая реализация общесистемного уровня трехуровневой модели на примере системы АТЗ тольяттинского государственного университета;
- практическая реализация мезоуровня трехуровневой модели на примере системы АТЗ тольяттинского государственного

университета;

- практическая реализация оперативного уровня трехуровневой модели на примере системы АТЗ тольяттинского государственного университета.

Диссертация состоит из введения, трех глав, заключения и списка литературы. Во введении обоснована актуальность темы исследования, представлены объект, предмет, цели, задачи и положения, выносимые на защиту диссертации. В первой главе выполнен анализ существующих моделей и методов повышения эффективности деятельности по обеспечению антитеррористической защищенности (АТЗ) организаций, рассмотрен порядок обеспечения антитеррористической защищенности организаций, приведен пример существующего подхода к моделированию поведения системы. Во второй главе исследованы подходы и методы программной инженерии в моделировании систем, методы моделирования систем безопасности организаций в контексте свода знаний программной инженерии, рассмотрены основные нотации и методологии графического моделирования, предложена трехуровненая модель использования средств программной инженерии в системах АТЗ организаций. В третьей главе выполнена практическая апробация решения на примере системы АТЗ тольяттинского государственного университета, проведено моделирование на уровне процессов, выполнено применение графических нотаций на мезоуровне, дан пример применения анализа данных на оперативном уровне.

Глава 1 Анализ существующих моделей и методов повышения эффективности деятельности по обеспечению антитеррористической защищенности (АТЗ) организаций

1.1 Порядок обеспечения антитеррористической защищенности организаций

Для обеспечения противодействию терроризму и предотвращению пожаров на государственном уровне разработаны Федеральные Законы. Этим документам должны придерживается все руководители органов государственной и муниципальной власти, обычные граждане, индивидуальные предприниматели и юридические лица.

Учреждения подчиняющихся министерству науки и высшего образования российской федерации должны выполнять следующие законы и постановления:

- ФЗ РФ N 35 от 6 марта 2006 г. «О противодействии терроризму» [21];
- Постановление Правительства РФ от 7 ноября 2019 г. N 1421 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации» [12];
- Постановление Правительства РФ от 2 августа 2019 г. № 1006 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)» [9]
- Постановление Правительства РФ от 24 сентября 2019 г. № 1243 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по надзору в сфере образования и науки и подведомственных ей организаций, а также

формы паспорта безопасности этих объектов (территорий)» [10];

– Постановление Правительства РФ от 25 декабря 2013 г. № 1244 «Об антитеррористической защищенности объектов (территорий)» [11].

Помимо этого, деятельность в сфере обеспечения АТЗ регулируется еще целым рядом законов, указов и иных документов [13], [17], [18], [19], [20].

Для обеспечения безопасности собственных зданий и сооружений каждый объект должен быть максимально защищен от угрозы извне. Персонал должен знать свои действия на случай террористической угрозы.

Антитеррористическая защищенность объекта (далее — АТЗ) — состояние здания или территории, которое не позволит совершить террористический акт или уменьшит его предполагаемые последствия.

Чтобы обеспечить АТЗ, организация должна:

– провести оценку уязвимости;
– составить акт обследования;
– категорировать объект защиты;
– составить, согласовать паспорт безопасности;
– отслеживать, как выполняется план по повышению защищенности, проводить ежегодные проверки.

Для систематизированной работы по АТЗ разрабатывается пакет документов, центральным из которых является «План организационных и технических мероприятий по защищенности объектов с массовым пребыванием людей».

1.2 Пример существующего подхода к моделированию поведения системы

Как мы видим в ниже приведённом примере в данный момент времени все разрабатываемые модели поведения являются вербальными (текстовыми) моделями.

«Пример такого рода моделей является алгоритм разработанный Межведомственной рабочей группой с участием представителей

Минобрнауки России, Минпросвещения России, МВД России, МЧС России, Росгвардии, ФСБ России во исполнение поручений протокола совместного заседания Национального антитеррористического комитета и Федерального оперативного штаба о мерах по повышению уровня готовности образовательных организаций к действиям при возникновении угрозы совершения преступлений террористической направленности от 8 февраля 2022 г. Межведомственная рабочая группой разработала и рекомендовала к применению на объектах образования модели действий персонала образовательных организации, работников частных охранных организаций и обучающихся при совершении (угрозе совершения) преступления с применением преступниками при нападении на объект образования огнестрельного оружия и (или) самодельного взрывного устройства» [15].

В соответствии с указанием Минобрнауки России от 29.08.2022 № МН-23/783 «О проведении практических занятий по безопасности», в целях поддержания на современном уровне профессиональной и психофизической готовности персонала, студентов необходимой для осуществления успешных действий по эвакуации при угрозе или совершения террористического акта, предотвращению террористического акта, а также обучения порядка и правилам взаимодействия персонала объекта с подразделениями ФСБ, МВД, Росгвардии, МЧС. В Тольяттинском государственном университете вышел приказ № 1447 от 31.08.2022 «О проведении тренировки по эвакуации персонала, студентов при угрозе или совершении террористического акта».

«Алгоритм действий административного персонала образовательной организации» [1] и «Алгоритмы действий - персонала образовательной организации, работников охранных организаций и обучающихся при совершении (угрозе совершения) преступлений террористической направленности отрабатываемые на тренировках» [2] представляют собой текстовое описание м использованием таблиц, но при этом обладают алгоритмическим свойствами, т.к. устанавливают последовательность действий персонала, охраны и учащихся.

Также в рамках описываемой модели широко применяется обмен сообщениями, например, передача сообщений от оперативного дежурного к постам охраны.

Указанные особенности соответствуют признакам моделей, используемых при описании и проектировании информационных систем. Этим подтверждается возможность использования в моделировании систем безопасности подходов программной инженерии.

Выводы по главе:

Деятельность по обеспечению защиты организаций на примере контртеррористической защищённости представляет собой систему управления, в которой присутствуют как организационные, так и технические подсистемы.

Моделирование деятельности по антитеррористической защите ТГУ выполненное в нотации IDEF0 показывает принципиальную применимость методов программной инженерии к моделированию систем безопасности и обеспечивает лаконичность, наглядность и согласованность на любом необходимом уровне детализации.

Глава 2 Подходы и методы программной инженерии в моделировании систем

2.1 Методы моделирования систем безопасности организаций в контексте свода знаний программной инженерии

По результатам анализа, проведенного в разделе 1, установлено, что система АТЗ обладаем рядом существенных признаков, характерных для информационных систем и потенциально к системам АТЗ могут быть применены модели и методы, программной инженерии, применяемые к информационным системам.

«Свод знаний по программной инженерии SWEBOK (Software Engineering Body of Knowledge) — международный стандарт ISO/IEC TR 19759 от 2015 г. в котором описана общепринятая сумма знаний по программной инженерии. Документ был создан при сотрудничестве нескольких профессиональных организаций и предприятий и опубликован обществом IEEE Computer Society (IEEE). В конце 2013 года была одобрена и опубликована актуальная версия SWEBOK V3, которая стала стандартом ISO/IEC TR 19759:2015» [25].

«В 2016 году общество IEEE Computer Society создало комитет SWEBoK Evolution, который будет заниматься дальнейшим развитием документа.

Текущая опубликованная версия SWEBOK V3 включает 15 областей знаний (knowledge area (KA)) в сфере программной инженерии:

- KA1 software requirements — требования к ПО;
- KA2 software design — проектирование ПО;
- KA3 software construction — конструирование ПО;
- software testing — тестирование ПО;
- software maintenance — сопровождение ПО;
- software configuration management — управление конфигурацией;

- software engineering management — управление IT проектом;
- software engineering process — процесс программной инженерии;
- software engineering models and methods — модели и методы разработки;
- software quality — качество ПО;
- software engineering professional practice — описание критериев профессионализма и компетентности;
- software engineering economics — экономические аспекты разработки ПО;
- computing foundations — основы вычислительных технологий, применимых в разработке ПО;
- mathematical foundations — базовые математические концепции и понятия, применимые в разработке ПО;
- КА15 engineering foundations — основы инженерной деятельности» [25].

«В дополнение SWEBOK определяет дисциплины, имеющие отношение к программной инженерии:

- Computer engineering;
- Systems engineering;
- Project management;
- Quality management;
- General management;
- Computer science;
- Mathematics» [25].

КА1 "Требования к программному обеспечению" связана с поиском, анализом, спецификацией и валидацией требований к программному обеспечению а также управлением требованиями в течение всего жизненного цикла программного продукта.

В рамках данной области знаний в контексте применения к системам АТЗ можно выделить:

- UML (Unified Modeling Language) – унифицированный язык моделирования [23], [28], [29], [30];
- SysML (Systems Modeling Language) – язык моделирования систем [24], [26], [27].

«КА2 «Проектирование ПО» определяется как «процесс определения архитектуры, компонентов, интерфейсов и других характеристик системы или компонента другие характеристики системы или компонента» и «результат этого процесса». Рассматриваемое как процесс, проектирование программного обеспечения - это деятельность жизненного цикла программной инженерии, в ходе которой требования к программному обеспечению анализируются с целью создания описания внутренней структуры программного обеспечения, которое будет служить основой для его создания. служить основой для его создания. Программное обеспечение (результат) описывает архитектуру программного обеспечения - то есть, как программное обеспечение декомпозируется и организовано в компоненты, а также интерфейсы между этими компонентами. Он также должен описывать компоненты на таком уровне детализации, который позволяет создавать их» [25].

В рамках данной области знаний в контексте применения к системам АТЗ можно выделить такие инструмент как:

- DFD (Data Flow Diagram) – диаграмма потоков данных;
- ERD (Entity Relationship Diagram) – диаграмма сущность-связь.

КА4 «Тестирование программного обеспечения» деятельность, выполняемая для оценки и улучшения качества программного обеспечения. Эта деятельность, в общем случае, базируется на обнаружении дефектов и проблем в программных системах.

В рамках данной области знаний в контексте применения к системам АТЗ можно выделить такие инструмент как: Model-Based Testing Techniques – Технологии тестирования, основанные на моделях. В редакции SWEBOK v2

2004г данные техники не упоминаются, что свидетельствует об актуальности и современности этого инструмента.

Модель в данном контексте - это абстрактное (формальное) представление тестируемого программного обеспечения или требований к нему (раздел Моделирование в КА9 Модели и методы программной инженерии). Тестирование на основе модели используется для подтверждения требований, проверки их согласованности и создания тестовых примеров, ориентированных на поведенческие аспекты программного обеспечения. Ключевыми компонентами тестирования на основе моделей являются: нотация, используемая для представления модели программного обеспечения или его требований; модели рабочих потоков или аналогичные модели; стратегия тестирования или алгоритм, используемый для генерации тестовых примеров; вспомогательная инфраструктура для выполнения тестов; оценка результатов тестирования по сравнению с ожидаемыми результатами.

«КА6 «Конфигурационное управление» определяет систему как коллекцию компонент, организованных для выполнения заданных функций или реализации комплекса функциональности. Конфигурация системы – функциональные и/или физические характеристики аппаратного, программно-аппаратного, программного обеспечения или их комбинации, сформулированные в технической документации и реализованные в продукте. Конфигурационное управление направлено на идентификацию конфигурации системы в определенные (заданные) моменты времени, с целью систематического контроля изменений конфигурации, а также поддержки и сопровождения целостной и отслеживаемой конфигурации на протяжении всего жизненного цикла системы. Конфигурационное управление согласно глоссарию, IEEE 610 это «дисциплина приложения технических и административных указаний (инструкций) и контроля (надзора) для: идентификации и документирования функциональных и физических характеристик элементов конфигураций, контроля (управления) изменений этих характеристик, записи (сохранения) и ведения отчетности по обработке

изменений и статусу их реализации, а также проверки (верификации) соответствия заданным требованиям» [25].

КА9 «Модели и методы программной инженерии» структурируют программную инженерию с целью сделать эту деятельность систематической, повторяемой и, в конечном счете, более ориентированной на успех. Использование моделей обеспечивает подход к решению проблем, нотацию и процедуры для построения и анализа. Методы обеспечивают подход к систематической спецификации, проектированию, конструированию, тестированию и верификации конечного программного обеспечения и связанных с ним рабочих продуктов. Модели и методы программной инженерии широко варьируются по масштабу - от рассмотрения одной фазы жизненного цикла программного обеспечения до охвата полного жизненного цикла программного обеспечения.

Модели и методы программной инженерии разделены на четыре основные тематические области:

- моделирование: общая практика моделирования и принципы моделирования; свойства; синтаксис, семантика и прагматика моделирования; предусловия, постусловия и инварианты.
- типы моделей: типы и подтипы моделей, общие характеристики типов моделей, часто встречающихся в практике программной инженерии.
- анализ моделей: общие методы анализа, используемые в моделировании для проверки полноты, согласованности, корректности, прослеживаемости и взаимодействия.
- методы программной инженерии: краткий обзор широко используемых методов программной инженерии (эвристических методов, формальных методов, прототипирования и гибких методов).

Моделирование программного обеспечения становится широко распространенной техникой, помогающей инженерам-программистам понять,

разработать и донести аспекты программного обеспечения до соответствующих заинтересованных сторон. Заинтересованные стороны - это те лица или стороны, которые имеют заявленный или подразумеваемый интерес к программному обеспечению (например, пользователь, покупатель, поставщик, архитектор, сертифицирующий орган, оценщик, разработчик, инженер-программист и, возможно, другие). Хотя в литературе и на практике существует множество языков моделирования, нотаций, методов и инструментов, есть объединяющие общие концепции, которые в той или иной форме применимы ко всем ним.

Моделирование предоставляет инженеру-программисту организованный и систематический подход для представления существенных аспектов исследуемого программного обеспечения, облегчения принятия решений о программном обеспечении или его элементах, а также доведения этих важных решений до сведения других заинтересованных сторон. Существует три общих принципа, определяющих такую деятельность по моделированию:

- моделировать самое необходимое: хорошие модели обычно не представляют все аспекты или особенности программного обеспечения при всех возможных условиях. Моделирование обычно включает разработку только тех аспектов или характеристик программного обеспечения, которые требуют конкретных ответов, абстрагируясь от любой несущественной информации. Такой подход позволяет сделать модели управляемыми и полезными.
- обеспечение перспективы: моделирование обеспечивает видение исследуемого программного обеспечения с использованием определенного набора правил для выражения модели в рамках каждого вида. Этот подход, основанный на перспективах, обеспечивает размерность модели (например, структурное представление, поведенческое представление, временное представление, организационное представление и другие

представления по мере необходимости). Организация информации в представлениях фокусирует усилия по моделированию программного обеспечения на конкретных проблемах, относящихся к данному представлению, с использованием соответствующей нотации, лексики, методов и инструментов.

– обеспечение эффективных коммуникаций: моделирование использует словарь прикладной области программного обеспечения, язык моделирования и семантическое выражение (другими словами, значение в контексте). При строгом и систематическом использовании моделирование приводит к формированию отчетности, которая способствует эффективной передаче информации о программном обеспечении заинтересованным сторонам проекта.

Модель - это абстракция или упрощение компонента программного обеспечения. Следствием использования абстракции является то, что ни одна абстракция не описывает компонент программного обеспечения полностью. Скорее, модель программного обеспечения представляется как совокупность абстракций, которые, будучи взятыми вместе, описывают только избранные аспекты, перспективы или взгляды - только те, которые необходимы для принятия обоснованных решений и ответа на причины создания модели в первую очередь. Такое упрощение приводит к набору предположений о контексте, в котором находится модель, которые также должны быть отражены в модели. Затем, при повторном использовании модели, эти предположения могут быть сначала проверены, чтобы установить релевантность повторно используемой модели в ее новом использовании и контексте.

Свойства и выражение моделей.

Свойства моделей - это отличительные особенности конкретной модели, используемые для характеристики ее полноты, согласованности и

корректности в рамках выбранной нотации моделирования и используемого инструментария. Свойства моделей включают следующее:

- полнота: степень, в которой все требования были реализованы и проверены в модели.
- согласованность: степень, в которой модель не содержит противоречивых требований, утверждений, ограничений, функций или описаний компонентов.
- корректность: степень, в которой модель удовлетворяет требованиям и спецификациям проекта и не содержит дефектов.

Модели строятся для представления объектов реального мира и их поведения, чтобы ответить на конкретные вопросы о том, как должно работать программное обеспечение. Изучение моделей - либо путем исследования, либо путем имитации, либо путем обзора - может выявить области неопределенности в модели и в программном обеспечении, к которому относится модель. Эти неопределенности или вопросы без ответов относительно требований, проектирования и/или реализации могут быть обработаны соответствующим образом.

Первичным элементом выражения модели является сущность. Сущность может представлять конкретные артефакты (например, процессоры, датчики или роботы) или абстрактные артефакты (например, программные модули или протоколы связи). Сущности модели связаны с другими сущностями с помощью отношений (другими словами, строк или текстовых операторов на целевых сущностях). Выражение сущностей модели может осуществляться с помощью текстовых или графических языков моделирования; оба типа языков моделирования связывают сущности модели через определенные языковые конструкции. Значение сущности может быть представлено ее формой, текстовыми атрибутами или тем и другим. Как правило, текстовая информация придерживается синтаксической структуры, специфичной для данного языка. Точные значения, связанные с моделированием контекста, структуры или поведения с использованием этих

сущностей и отношений, зависят от используемого языка моделирования, строгости проектирования, применяемой при моделировании, конкретного представления, которое строится, и сущности, к которой может быть присоединен конкретный элемент обозначения. Для отражения необходимой семантики программного обеспечения может потребоваться несколько представлений модели.

При использовании моделей, поддерживаемых автоматизацией, модели могут проверяться на полноту и согласованность. Полезность этих проверок в значительной степени зависит от уровня семантической и синтактической строгости, применяемой при моделировании в дополнение к явной инструментальной поддержке. Корректность обычно проверяется с помощью моделирования и/или обзора.

Синтаксис, семантика и прагматика.

Модели могут быть удивительно обманчивы. Тот факт, что модель является абстракцией с недостающей информацией, может привести человека к ложному ощущению полного понимания программного обеспечения на основе одной модели. Полная модель ("полная" относится к усилиям по моделированию) может быть объединением нескольких подмоделей и любых моделей специальных функций. Изучение и принятие решений, относящихся к одной модели в этой коллекции подмоделей, может быть проблематичным.

Понимание точного значения конструкций моделирования также может быть затруднено. Языки моделирования определяются синтаксическими и семантическими правилами. Для текстовых языков синтаксис определяется с помощью нотационной грамматики, которая определяет допустимые языковые конструкции (например, форма Бэкуса-Наура (BNF)). Для графических языков синтаксис определяется с помощью графических моделей, называемых метамоделями. Как и в случае с БНФ, метамодели определяют допустимые синтаксические конструкции языка графического моделирования; метамодель определяет, как эти конструкции могут быть составлены для создания допустимых моделей.

Семантика языков моделирования определяет значение, придаваемое сущностям и отношениям, отображаемым в модели. Например, простая диаграмма из двух ящиков, соединенных линией, может быть интерпретирована по-разному. Знание того, что диаграмма, на которой размещены и соединены коробки, является диаграммой объектов или диаграммой деятельности, может помочь в интерпретации этой модели.

На практике обычно существует хорошее понимание семантики конкретной модели программного обеспечения благодаря выбранному языку моделирования, тому, как этот язык моделирования используется для выражения сущностей и отношений в этой модели, опыту разработчика (разработчиков) модели, а также контексту, в котором моделирование было предпринято и так представлено. Смысл передается через модель даже при наличии неполной информации посредством абстракции; прагматика объясняет, как смысл воплощается в модели и ее контексте и эффективно передается другим разработчикам программного обеспечения.

Однако все еще существуют случаи, когда необходимо соблюдать осторожность в отношении моделирования и семантики. Например, любые части модели, импортированные из другой модели или библиотеки, должны быть проверены на предмет семантических предположений, которые конфликтуют в новой среде моделирования; это может быть неочевидно. Модель должна быть проверена на наличие документированных предположений. Хотя синтаксис моделирования может быть идентичным, модель может означать нечто совершенно иное в новой среде, которая является другим контекстом. Также следует учитывать, что по мере созревания программного обеспечения и внесения изменений могут возникать семантические разногласия, приводящие к ошибкам. При большом количестве инженеров-программистов, работающих над частью модели с течением времени в сочетании с обновлениями инструментов и, возможно, новыми требованиями, существуют возможности для того, чтобы части модели

представляли нечто отличное от первоначального замысла автора и первоначального контекста модели.

Предварительные условия, постусловия и инварианты.

При моделировании функций или методов инженер-программист обычно начинает с набора предположений о состоянии программного обеспечения до, во время и после выполнения функции или метода. Эти предположения важны для правильной работы функции или метода и группируются для обсуждения как набор предусловий, постусловий и инвариантов.

- предварительные условия: набор условий, которые должны быть выполнены до выполнения функции или метода. Если эти предварительные условия не выполняются до выполнения функции или метода, функция или метод могут выдать ошибочные результаты;
- постусловия: набор условий, которые гарантированно будут истинными после успешного выполнения функции или метода. Как правило, постусловия представляют, как изменилось состояние программного обеспечения, как изменились параметры, переданные в функцию или метод, как изменились значения данных или как изменилось возвращаемое значение;
- инварианты: набор условий в операционной среде, которые сохраняются (другими словами, не изменяются) до и после выполнения функции или метода. Эти инварианты являются релевантными и необходимыми для программного обеспечения и правильной работы функции или метода.

Описанный подход обеспечивает эффективное моделирование систем.

2.2 Основные нотации и методологии графического моделирования

Рассмотрим систему безопасности на основании сущностей этой сферы.

Цель моделирования, как правило- многоаспектна, моделирование применяют:

- для оптимизации;
- соответствия законам, стандартам, постановлениям;
- рационализации структур;
- повышения эффективности;
- выявления дублирующего функционала;
- анализа управляющих-процессов;
- разработки инструкций.

При создании информационных систем необходимо формализовано – с помощью программных средств моделирования – представлять фактическое текущее и желаемое будущее положения дел в управлении системы безопасности.

Моделирование осуществляется в целях получения ответов на следующие вопросы:

- какие функции реализуются в управлении безопасности для получения требуемого конечного результата;
- в какой последовательности реализуются функции, то есть какие процессы реализуются в управлении безопасности;
- какие материально-информационные ресурсы перерабатываются процессами управления безопасности;
- какие материально-информационные ресурсы используются для реализации функций в качестве механизмов;
- какие информационные ресурсы используются в качестве регламента в процессе реализации функций;
- какие материально-информационные продукты порождают функции, образующие процессы в управлении безопасности;
- какие показатели используются для характеристики качества реализации функций и процессов, включая сквозные процессы.

Осуществим моделирование в целях получения ответов на следующие вопросы:

- какие функции реализуются в управлении безопасности для получения требуемого конечного результата;
- в какой последовательности реализуются функции, то есть какие процессы реализуются в управлении безопасности;
- какие материально-информационные ресурсы перерабатываются процессами в управлении безопасности;
- какие материально-информационные ресурсы используются для реализации функций в качестве механизмов;
- какие информационные ресурсы используются в качестве регламента в процессе реализации функций;
- какие материально-информационные продукты порождают функции, образующие процессы в управлении безопасности;
- какие показатели используются для характеристики качества реализации функций и процессов, включая сквозные процессы.

В объектно-ориентированном архитектурном стиле программной инженерии применяют паттерны или иначе говоря шаблоны для периодически повторяющихся действий которые позволяет решать проблему унификации алгоритма для различных типов.

В системе безопасности организации шаблонами классов могут выступать:

- инструкции;
- обследование зданий;
- поведение сотрудника охраны в определённых ситуациях;
- проведение учебных тренировок;
- техническое обслуживание, ремонт и замена оборудования;
- реагирование на ЧС.

Согласно своду знаний программной инженерии, сформированные модели необходимо подвергнуть тестированию - для этого понадобится рассмотреть и оценить альтернативные компромиссы и решения.

При тестировании сформированной модели необходимо дать ответы на вопросы, были ли использованы в процессе разработки модульное тестирование, анализ зависимостей и статический анализ.

Такой процесс создания моделей предполагает итеративный и инкрементный подход. Сначала создается возможные варианты моделей – обобщенный вид алгоритмов действий. Они могут тестироваться по основным сценариям, требованиям, известным ограничениям, параметрам качества.

В ходе доработки вариантов алгоритмов действий выявляются дополнительные детали и сведения о проекте. В результате происходит расширение основных сценариев, корректировка общего представления алгоритмов и подхода к решению проблем.

В сфере поддержки систем безопасности организации с помощью моделей программной инженерии наиболее подобной является разработка бизнес моделирования. Для бизнес моделирования наибольшее применение получили паттерны проектирования ARIS, которые характеризуют абстрактный уровень представления бизнес-процессов.

«Главным преимуществом методологии ARIS являются эргономичность и высокая степень визуализации бизнес-моделей, что делает данную методологию удобной и доступной в использовании всеми работниками организации (начиная от топ- менеджеров и заканчивая рядовыми работниками). Методология содержит более 80 моделей, и поэтому для осмысленного применения требуется время на изучение.

Методология ARIS в значительной большей степени предназначена для целей управленческого консалтинга и последующей поддержки решений, применения методологий эффективного для анализа и оптимизации бизнес-процессов (реинжиниринга), систем управления качеством, проектирования информационных систем, а также для обеспечения процесса реорганизации.

В рейтинге Gartner Group система ARIS занимает лидирующее положение на рынке средств моделирования и анализа деловых процессов» [7].

Общие принципы методологии и системы ARIS.

«ARIS – это одновременно и методология, и программный продукт, предназначенный для моделирования бизнес-процессов организаций. В дальнейшем под системой ARIS (либо инструментальной средой ARIS) будем понимать аппаратное и программное обеспечение, реализующие методологию ARIS, а под методологией ARIS – только подход к структурированному описанию деятельности организации» [7].

«Методология ARIS представляет собой современный подход к структурированному описанию деятельности организации и представлению ее в виде взаимосвязанных и взаимодополняющих графических диаграмм, удобных для понимания и анализа. Методология ARIS основывается на концепции интеграции, предлагающей целостный взгляд на процессы, и представляет собой множество различных методик, объединенных в рамках единого системного подхода.

ARIS – это сокращенное английское выражение (Architecture of Integrated Information Systems), что в переводе означает: архитектура интегрированных информационных систем. Под архитектурой подразумевается совокупность технологий, обеспечивающих проектирование, управление, применение и реализацию бизнеса в виде «деловых» процедур бизнес-процессов предприятий и организаций, а также проектирование и создание интегрированных информационных систем поддержки бизнес-процессов» [7].

«Методология ARIS реализует принципы системного структурного анализа, основным понятием которого служит структурный элемент (объект).

Структурный анализ является методологической разновидностью системного анализа. В структурном анализе предполагается использование графического представления для описания структуры и деятельности

организации. При этом реализуются основные принципы структурного анализа:

- разбиение на уровни абстракции с ограничением числа элементов на каждом уровне (обычно от 3 до 9);
- ограниченный контекст включающий только существенный на каждом уровне детали;
- использование строгих формальных правил записей; последовательное приближение к конечному результату (зависит от целей моделирования)» [7].

«Методология ARIS также использует декомпозицию и позволяет детализировать предмет моделирования с помощью альтернативных или дополняющих друг друга моделей.

Основы методологии ARIS состоят в том, что любая организация рассматривается и визуально представляется во всех аспектах, т.е. как единая система, описание которой предусматривает четыре различных «взгляда»:

- организационная структура;
- данные (потоки и структура);
- функции («деревья» функций);
- контроль и управление (деловые процессы)» [7].

«Все данные подсистемы организации в реальности и в моделях должны быть связаны между собой. Методология ARIS дает возможность описывать достаточно разнородные подсистемы в виде взаимоувязанной и взаимосогласованной совокупности различных моделей, которые хранятся в едином репозитории. Именно взаимосвязанность и взаимосогласованность моделей являются отличительными особенностями методологии ARIS» [7].

«В соответствии с правилами структурного анализа каждая из этих подсистем разбивается на элементарные блоки (модули), совокупность которых и составляет нотацию структурной модели той или иной подсистемы организации.

Естественно, что эти подсистемы не являются обособленными. Они взаимно проникают друг в друга, и поэтому одни и те же элементарные модули могут использоваться для описания различных структурных моделей. Для устранения избыточности методология ARIS ограничивает число типов моделей» [7].

«В связи с этим в методологии ARIS выделено пять типов представлений основных моделей, отражающих основные аспекты организации:

- организационные модели, описывающие иерархическую структуру системы, т.е. иерархию организационных подразделений, должностей, полномочий конкретных лиц, многообразие связей между ними, а также территориальную привязку структурных подразделений;
- функциональные модели, описывающие функции (процессы, операции), выполняемые в организации;
- информационные модели (т.е. модели данных), отражающие структуру информации, необходимой для реализации всей совокупности функций системы;
- модели процессов или управления, представляющие комплексный взгляд на реализацию деловых процессов в рамках системы и объединяющие вместе другие модели;
- модели входов и выходов, описывающие потоки материальных и нематериальных входов и выходов, включая потоки денежных средств» [7].

«Типы представления являются первой компонентой архитектуры. Они позволяют структурировать бизнес-процессы и выделять их составные части, что делает рассмотрение более простым. Применение этого принципа позволяет с различных точек зрения описывать содержание отдельных частей бизнес-процесса, используя специальные методы, наиболее полно соответствующие каждой точке зрения. Это избавляет пользователя от необходимости учитывать множество связей и соединений.

Для построения моделей и проведения структурного анализа в ARIS используют следующие методы и средства визуального описания:

- DFD (Data Flow Diagrams) – диаграммы потоков данных для анализа и функционального проектирования моделей систем. Описывают источники и адресаты данных, логические функции, потоки данных и хранилища данных к которым осуществляется доступ» [7];
- «STD (State Transition Diagrams) – диаграммы перехода состояний для проектирования систем реального времени;
- ERD (Entity-Relationship Diagrams) – диаграммы сущность-связь, описывающие объекты (сущности), свойства этих объектов (атрибуты) и их отношения объектов (связи);
- SADT (Structured Analysis and Design Technique) - технология структурного анализа, проектирования и моделирования иерархических многоуровневых модульных систем;
- IDEF0 (Integration Definitionfor Function Modeling) – подмножество SADT – стандарт описания бизнес-процессов в виде иерархически взаимосвязанных функций» [7];
- «IDEF1 – стандарт описания движения информации; используется для определения структуры информационных потоков, правил движения, принципов управления информацией, связей потоков, выявления проблем некачественного информационного менеджмента;
- IDEF1X – стандарт разработки логических схем баз данных, основанный на концепции сущность-связь;
- IDEF3 – стандарт описания процессов, основанная на сценариях. Сценарий есть описание последовательности изменения свойств объекта в рамках некоторого процесса. Стандарт позволяет описать последовательность этапов изменения свойств объекта (Process Flow Description Diagrams - PFDD) и состояния объекта на этапах (Object

State Transition Network - OSTN). Стандарт позволяет решать задачи документирования и оптимизации процессов» [7];

- «IDEF4 – стандарт описания структуры объектов и заложенных принципов их взаимодействия; позволяет анализировать и оптимизировать сложные объектно- ориентированные системы;
- IDEF5 – стандарт, позволяющий описать совокупность терминов, правил комбинирования терминов в утверждения для описания свойств и связей объектов, построить модель на основе этих утверждений. Такие модели позволяют изучать онтологию объектов. Онтология – это знания о совокупности фундаментальных свойств некоторого объекта или области, определяющих их поведение и изменение, собранные для детальной формализации;
- UML (Unified Modeling Language) – объектно-ориентированный унифицированный язык визуального моделирования. Позволяет описывать диаграммы действий, диаграммы взаимодействия, диаграммы состояний, диаграммы классов и компонент. Используется как для анализа, так и для проектирования моделей информационных систем» [7].

«Другой особенностью методологии ARIS, обеспечивающей целостность разрабатываемой системы, является использование различных уровней описания, что поддерживает теорию жизненного цикла системы, существующего в сфере информационных технологий.

Для каждого «взгляда» придерживаются три уровня анализа (требования, спецификации, внедрения), что обеспечивает целостность разрабатываемой системы» [7].

«Каждый уровень соответствует определенной фазе жизненного цикла информационной системы:

- уровень определения требований (что система должна делать);
- уровень проектной спецификации (основные пути реализации системы);

– уровень описания реализации (физическое описание конкретных программных и технических средств.

Каждый из уровней анализа состоит из своего комплекта моделей различных типов, в том числе диаграмм UML, диаграмм SAP R/3 и др. Каждый объект моделей ARIS имеет множество атрибутов, позволяющих контролировать процесс разработки моделей, определить условия для выполнения функционально-стоимостного анализа, имитационного моделирования, взаимодействия с work flow-системами и т.д.» [7].

2.3 Трехуровненая модель использования средств программной инженерии в системах АТЗ организаций

Предлагаемая модель применения методов программной инженерии к системам АТЗ (рисунок 1) предусматривает на верхнем системном или процессном уровне применение нотации IDEF0.

Рисунок 1 – Модель применения методов программной инженерии к системам АТЗ

На функциональном уровне – средства унифицированного языка моделирования. На оперативном уровне – обработка и анализ данных методами искусственного интеллекта.

Данная модель носит частный характер и является примером системы моделей и методов программной инженерии, реализованных в системе АТЗ ТГУ в рамках данной работы.

«На контекстной диаграмме верхнего уровня объект моделирования представлен единственным блоком с граничными стрелками. Стрелки на этой диаграмме отображают связи объекта моделирования с окружающей средой. Поскольку единственный блок представляет весь объект, его имя – общее для всего проекта. Это же справедливо и для всех стрелок диаграммы, поскольку они представляют полный комплект внешних интерфейсов объекта. Диаграмма А-0 устанавливает область моделирования и ее границу.

Контекстная диаграмма должна содержать краткие утверждения, определяющие точку зрения должностного лица или подразделения, с позиций которого создается модель, и цель, для достижения которой ее разрабатывают. Эти утверждения помогают руководить разработкой модели и ввести этот процесс в определенные рамки. Точка зрения определяет, что и в каком разрезе можно увидеть в пределах контекста модели.

Формулировка цели выражает причину создания модели, т.е. содержит перечень вопросов, на которые должна отвечать модель, что в значительной мере определяет ее структуру. Наиболее важные свойства объекта обычно выявляются на верхних уровнях иерархии; по мере декомпозиции функции верхнего уровня и разбиения ее на подфункции, эти свойства уточняются» [14].

«Функциональный блок, как отображающий моделируемую систему в целом (блок А0), так и блок на любом уровне декомпозиции являются преобразующими блоками. Преобразующий блок – блок IDEF0 – диаграммы, преобразующий входы в выходы под действием управлений при помощи

«механизмов». Преобразование – цель и результат работы любого блока на диаграмме любого уровня декомпозиции.

Преобразованию в блоке могут подвергаться материальные и информационные объекты, образующие соответствующие потоки.

Материальный поток – непрерывное или дискретное множество материальных объектов, распределенное во времени.

Информационный поток – множество информационных объектов, распределенное во времени.

Информация, участвующая в процессах, операциях, действиях и деятельности в целом, может быть классифицирована на три группы:

– ограничительная информация;
– описательная информация;
– предписывающая (управляющая) информация.

Ограничительная информация содержится в законах, подзаконных актах, международных, государственных и отраслевых стандартах, а также в специальных внутренних положениях и документах предприятия, в частности, в технических требованиях, условиях, регламентах и т.д.

Описательная информация – сведения об атрибутах объекта (потока) преобразуемого функциональным блоком. Содержится в чертежах, технических и иных описаниях, реквизитах и т.п. документах, являясь неотъемлемым компонентом объекта в течение всего жизненного цикла. Эта информация сама преобразуется (изменяется) в результате выполнения функции.

Предписывающая (управляющая) информация – сведения о том, как, при каких условиях и по каким правилам следует преобразовать объект (поток) на входе в объект (поток) на выходе блока. Содержится в технологических (в широком смысле) инструкциях, руководствах, документах, определяющих «настройки» и характеристики блока» [14].

Распределение описанных видов информации по сторонам блока показано на рисунке 2.

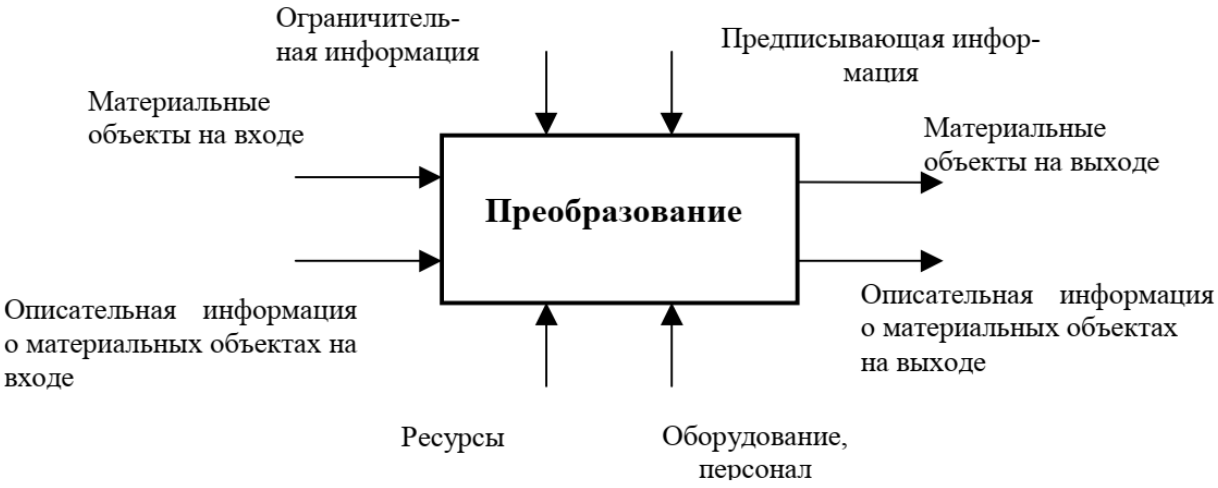


Рисунок 2 – Распределение видов информации по сторонам функционального блока IDEF0 [14]

«Деятельность (синонимы: дело, бизнес) – совокупность процессов, выполняемых (протекающих) последовательно или/и параллельно, преобразующих множество материальных или/и информационных потоков во множество материальных или/и информационных потоков с другими свойствами. Деятельность осуществляется в соответствии с заранее определенной и постоянно корректируемой целью, с потреблением финансовых, энергетических, трудовых и материальных ресурсов, при выполнении ограничений со стороны внешней среды.

В модели IDEF0 деятельность описывается блоком A0 на основной контекстной диаграмме A-0» [14].

В общем, на каждом уровне выбор моделей и методов должен соответствовать специфике организации и уровню подготовленности персонала. Например, представляет интерес использования на верхнем уровне графического языка описания систем SysML который семантически более близок к UML, что потенциально может обеспечить лучшую связь между моделями верхнего и среднего уровня.

Выводы по главе:

По результатам рассмотрения свода знаний SWEBOK определены основные составляющие программной инженерии, использование моделей и методов которых потенциально может повысить эффективность деятельности по обеспечению антитеррористической защищённости.

Установлено, что среди паттернов моделирования и проектирования, широко используемых в программной инженерии, отсутствуют (или не представлены в открытом доступе) шаблоны, ориентированные на моделирование систем безопасности.

Разработана теоретическая модель применения методов программной инженерии к системам АТЗ. Модель включает три уровня управления системой АТЗ и содержит рекомендуемые на каждом уровне модели и методы программной инженерии.

Глава 3 Практическая апробация решения

3.1 Моделирование на уровне процессов

В рамках описанных правил выполним моделирование деятельности по осуществлению антитеррористической защиты Тольяттинского государственного университета на уровне контекстной диаграммы.

Имя функционального блока, отражающее деятельность в целом «Осуществление антитеррористической защиты Тольяттинского государственного университета».

Целью моделирования является исследование возможности повышения эффективности деятельности путем применения моделей и методов программной инженерии.

К входам в рамках деятельности по АТЗ могут быть отнесены материальные и информационные объекты, например.

- сообщения о ЧС;
- запросы вышестоящих органов;
- заявления;
- служебные записки;
- работоспособность технических средств охраны.

К выходам в рамках деятельности по АТЗ могут быть отнесены материальные и информационные объекты, например.

- ежеквартальные отчёты;
- ежегодные отчёты;
- отчёты по требованию вышестоящих руководящих органов;
- проведение инструктажей, тренировок, учений при ЧС;
- эвакуация при возникновении ЧС;
- разработка ПБ;
- планирование мероприятий по обеспечению АТЗ объектов и

территорий;

- обеспечение мероприятий по АТЗ ресурсами;
- координация деятельности подразделений, должностных лиц и охранной организации по обеспечению АТЗ объектов (территорий);
- организация взаимодействия с территориальными органами безопасности, Росгвардией, МВД, МЧС, ФСБ;
- разработка и согласование проектов локальных нормативных актов в части обеспечения АТЗ объектов и территорий.

Управление в рамках деятельности по АТЗ осуществляется с использованием следующих документов.

- ФЗ РФ N 35 от 6 марта 2006 г. «О противодействии терроризму»;
- Постановление Правительства РФ от 7 ноября 2019 г. N 1421 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации»;
- Постановление Правительства РФ от 1 сентября 2021 г. N 1464 "Об утверждении требований к оснащению объектов защиты автоматическими установками пожаротушения, системой пожарной сигнализации, системой оповещения и управления эвакуацией людей при пожаре";
- Приказы и постановления Министерства науки и высшего образования Российской Федерации;
- ГОСТы по системам безопасности (система охранная телевизионная (СОТ), система контроля и управления доступом (СКУД), система охранной сигнализации (СОС));
- ГОСТы и СП по пожарной безопасности;
- ГОСТы и СП по системам оповещения и управления эвакуацией(СОУЭ);
- рекомендации Росгвардии;

– приказы и постановления Тольяттинского государственного университета;
– распоряжение ректора, проректора по безопасности;
– внутренние инструкции.

В качестве ресурсов деятельность по АТЗ использует персонал, информационные и технические системы:

Турникеты, видеокамеры, датчики движения, датчики разбития, датчики открытия, датчики задымлённости, датчики температуры, приёма-контрольные приборы, считыватели, контроллеры, сервера, металл детекторы, тревожные кнопки, системы оповещения и управлением эвакуацией, системы связи, системы подавления сотовой связи.

Для того, чтобы обеспечить наглядность на контекстном уровне необходимо ограничивать количество стрелок. На основании приведенных выше примеров можно сформировать следующие обобщающие входы:

– шаблоны и образцы отчетной документации;
– тревожные сообщения (например, телефонные звонки о минировании);
– запросы (например, письма о необходимости провести внеплановые учения, предоставить информацию с камер наблюдения и т.п.).

Обобщающие выходы:

– плановая отчётность;
– внеплановая отчетность (например, отчет о проведении внеплановых учений, информация с камер наблюдения);
– сигналы и запросы (например, вызов кинологического подразделения МВД по сообщению о минировании).

В качестве управления деятельностью по АТЗ в обобщенном виде можно отнести: законодательные и нормативные акты на государственном, отраслевом и вузовском уровне – по линии Министерства науки и высшего образования Российской Федерации. С другой стороны, управление

обеспечивается нормативными актами, приказами и письмами по линии Росгвардии, МВД, МЧС, ФСБ.

- законы;
- постановления;
- ГОСТы;
- своды правил.

В качестве обобщающих мероприятий по АТЗ можно отнести:

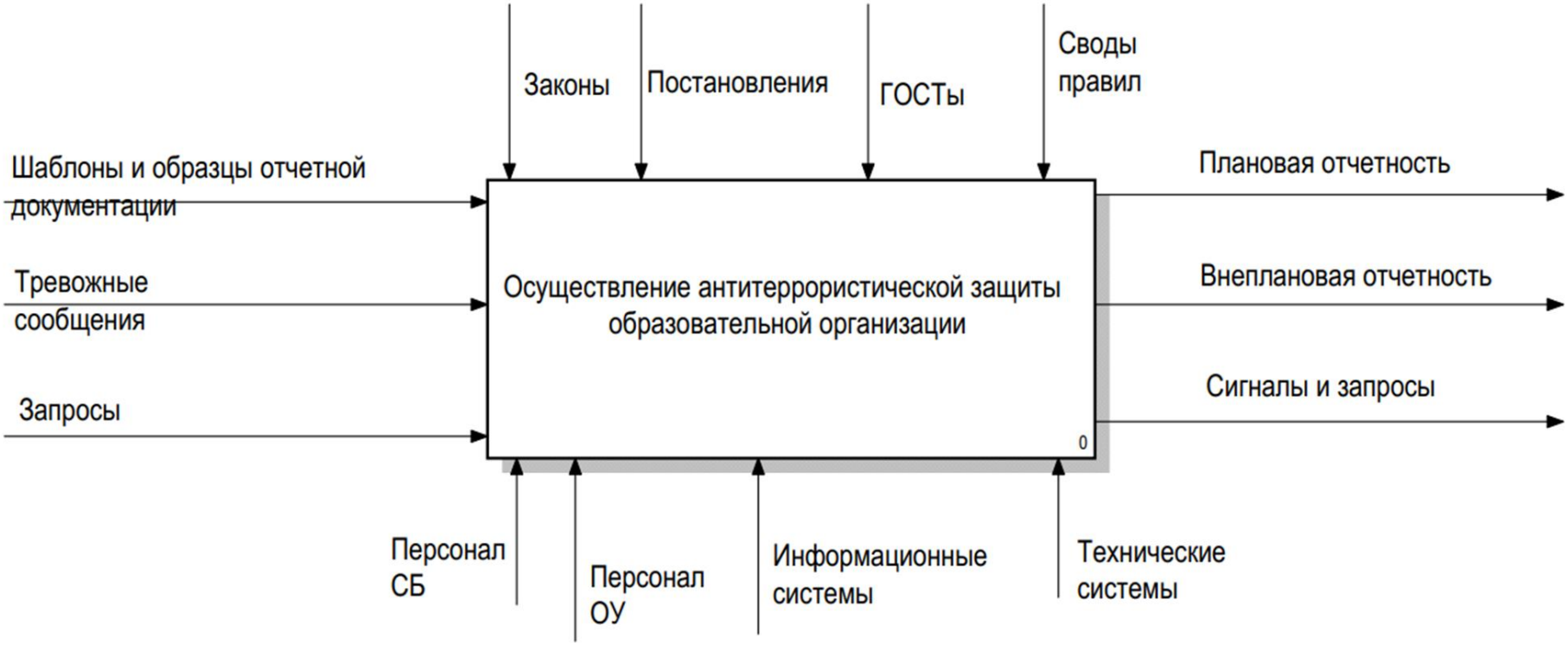
- персонал;
- информационные системы;
- технические системы.

На контекстном уровне А-0 (рисунок 3) видно, что система АТЗ является сложной - предусматривает использование человеческих, информационных и технических ресурсов.

Проблема состоит в том, что в настоящее время не реализован системный подход. В силу этого деятельность по поддержанию и обеспечению соответствия системы требованиям слабо структурирована. Это приводит к повышению трудоемкости и определяет вероятность снижения качества системы АТЗ.

Гипотеза работы состоит в том, что применение системного подхода, реализованного через модели и методы программной инженерии к системам АТЗ позволить повысить эффективность деятельности по обеспечению АТЗ.

Детализация контекстной модели (рисунок 4) выполнена с выделением основных бизнес-процессов, состоящих в управлении, реагировании, совершенствовании и мониторинге состояния системы.



Цель - исследование возможности повышения эффективности деятельности путем применения моделей и методов программной инженерии.

Точка зрения - специалист по антитеррористичекой защищенности

Рисунок 3 – Модель системы АТЗ (контекстный уровень А-0)

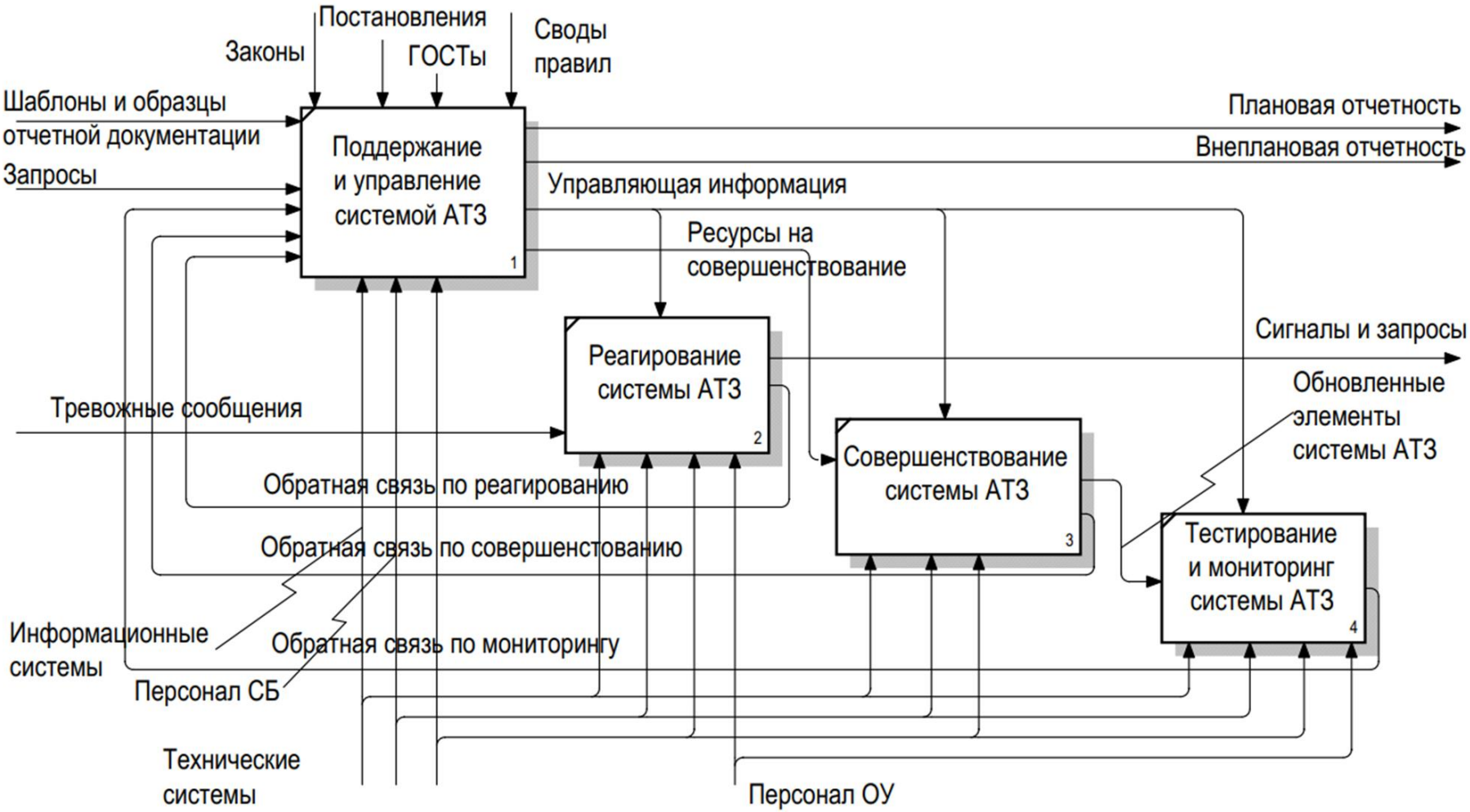


Рисунок 4 – Модель системы АТЗ (уровень А0)

В целом, по результатам анализа современного состояния проблемы построена процессная модель, обоснована необходимость системного подхода и выдвинута гипотеза о возможной эффективной реализации системного подхода моделями и методами программной инженерии.

3.2 Применение графических нотаций на мезоуровне

В целях обеспечения антитеррористической защищённости зданий, сооружений и территории университета, выполнения требований действующей инструкции по обеспечению режима секретности в РФ и требований межведомственной комиссии при обследовании и категорировании объектов (территорий) университета ТГУ разработан регламент в котором определён особый пропускной режим посетителей университета. Посетители проходят через точки доступа системы управления доступом (СКУД) расположенные во входной группе университета рядом с постом охраны.

Регламентом определён список лиц, которые проходят через пост охраны:

- работник - физическое лицо, работающее в ТГУ по трудовому договору или выполняющее работы в рамках договора гражданско-правового характера для нужд ТГУ;
- обучающиеся - студенты, аспиранты, докторанты, слушатели, зачисленные в установленном порядке в ТГУ;
- абитуриент - физическое лицо, поступающее в ТГУ;
- контрагент - физическое или юридическое лицо, предприятие, учреждение, организация, берущее на себя обязательства по осуществлению работ либо оказанию услуг в рамках договора, контракта, заключенного с ТГУ;
- посетитель - физическое лицо, посещающее сотрудников университета для решения служебных или личных вопросов, а также

мероприятия университета (конференции, форумы, концерты, выставки, спортивные мероприятия, экскурсии и т.п.).

Вербальные алгоритмы посещения университета;

- работник, приходя на работу если у него присутствует при себе пропуск прикладывает к контроллеру СКУД и проходит на своё рабочее место. Если пропуск отсутствует (потерян или оставлен дома) то работник сообщает об этом своему структурному руководителю. Структурный руководитель по телефону сообщает на пост охраны подтверждение о том, что данный работник находится в штате и данное лицо регистрируют в журнале посетителей по документу удостоверяющего личность (водительские права, паспорт) и пропускают на рабочее место. Если пропуск потерян, то работник оплачивает в кассу ТГУ штраф за потерю пропуска и с квитанцией обращается в бюро пропусков для получения дубликата электронного пропуска. При выходе с работы работник прикладывает пропуск к контроллеру СКУД и проходит через турникет или если у него нет пропуска подходит к посту охраны где сотрудник охраны делает отметку в журнале посетителей том что данный работник покинул корпус и пропускает работника через систему СКУД.
- обучающийся, приходя на учёбу если у него присутствует при себе пропуск прикладывает к контроллеру СКУД и проходит на занятия или предъявляет зачётную книжку сотруднику охранной организации, и сотрудник пропускает обучающегося через турникет. Если пропуск потерян, то обучающийся оплачивает в кассу ТГУ штраф за потерю пропуска и с квитанцией обращается в бюро пропусков для получения дубликата электронного пропуска. При выходе с учёбы обучающийся прикладывает пропуск к контроллеру СКУД и проходит через турникет или если у него нет пропуска подходит к посту охраны и предъявляет зачётную книжку

сотруднику охранной организации, и сотрудник пропускает обучающегося через турникет;

- абитуриент, приходя в университет сообщает цель своего прихода сотруднику охраны, предъявляет паспорт. Если предъявлен паспорт гражданина РФ сотрудник охраны регистрирует посетителя в журнале посетителей по документу удостоверяющего личность и пропускает абитуриента на территорию университета. Если предъявлен паспорт другого государства, то данного абитуриента отправляют в миграционную службу ТГУ за оформлением допуска. Для выхода из корпуса ТГУ абитуриенты подходят к сотруднику охраны и сообщает что собирается покинуть корпус. Сотрудник охраны делает отметку в журнале посетителей и попускает абитуриента через систему СКУД;
- контрагент, приходя в ТГУ если у него присутствует при себе пропуск прикладывает к контроллеру СКУД и проходит в университет. Если пропуск отсутствует (потерян или оставлен дома) то контрагент сообщает об этом своему заказчику работ из лиц административного персонала ТГУ. Данное лицо по телефону сообщает на пост охраны подтверждение о том, что данный контрагент пришёл по вызову и с ним заключён договор на обслуживание технических систем. Контрагента регистрируют в журнале посетителей по документу удостоверяющего личность (водительские права, паспорт) и пропускают на рабочее место. Если пропуск потерян, то работник оплачивает в кассу ТГУ штраф за потерю пропуска и с квитанцией обращается в бюро пропусков для получения дубликата электронного пропуска. При выходе из корпуса контрагент прикладывает пропуск к контроллеру СКУД и проходит через турникет или если у него нет пропуска подходит к посту охраны где сотрудник охраны делает отметку в журнале посетителей том что данный контрагент покинул корпус и пропускает

контрагента через систему СКУД;

- посетитель, приходя в университет сообщает цель своего визита сотруднику охраны, предъявляет паспорт. Сообщает о своём прибытии ожидающему его структурному подразделению. Представитель структурного подразделения спускается для встречи посетителя подтверждения его личности и дальнейшего сопровождения до конечной точки визита. Сотрудник охраны регистрирует посетителя в журнале посетителей по документу удостоверяющего личность и пропускает посетителя на территорию университета. Для выхода из корпуса ТГУ посетители подходят к сотруднику охраны вместе с сопровождающим лицом и сообщает что собирается покинуть корпус. Сотрудник охраны делает отметку в журнале посетителей и попускает посетителя через систему СКУД.

Перевод в нотацию BPMN рассмотренного выше вербального алгоритма посещения университета представлен на рисунке 5.

Рассмотрим обобщённый алгоритм обнаружения и устранения неисправности технических средств охраны. Оборудование, относящееся к техническим средствам охраны, перестало работать – охранник, обнаруживший неисправности, сообщает о происшествии ответственному дежурному и пишет рапорт который передаёт начальнику смены охраной организации. Ответственный дежурный фиксирует неисправность и сообщает в круглосуточную диспетчерскую службу технической поддержки обслуживающей организации о выявленной неисправности технических средств охраны. Прибывший инженер обслуживающей организации обнаруживает неисправность и сообщает о принятых мерах по ликвидации неисправности специалисту по АТЗ. В зависимости от того какая обнаружена неисправность специалист АТЗ принимает решение восстановить оборудование на месте или передать его в ремонт обсуживающей организации.

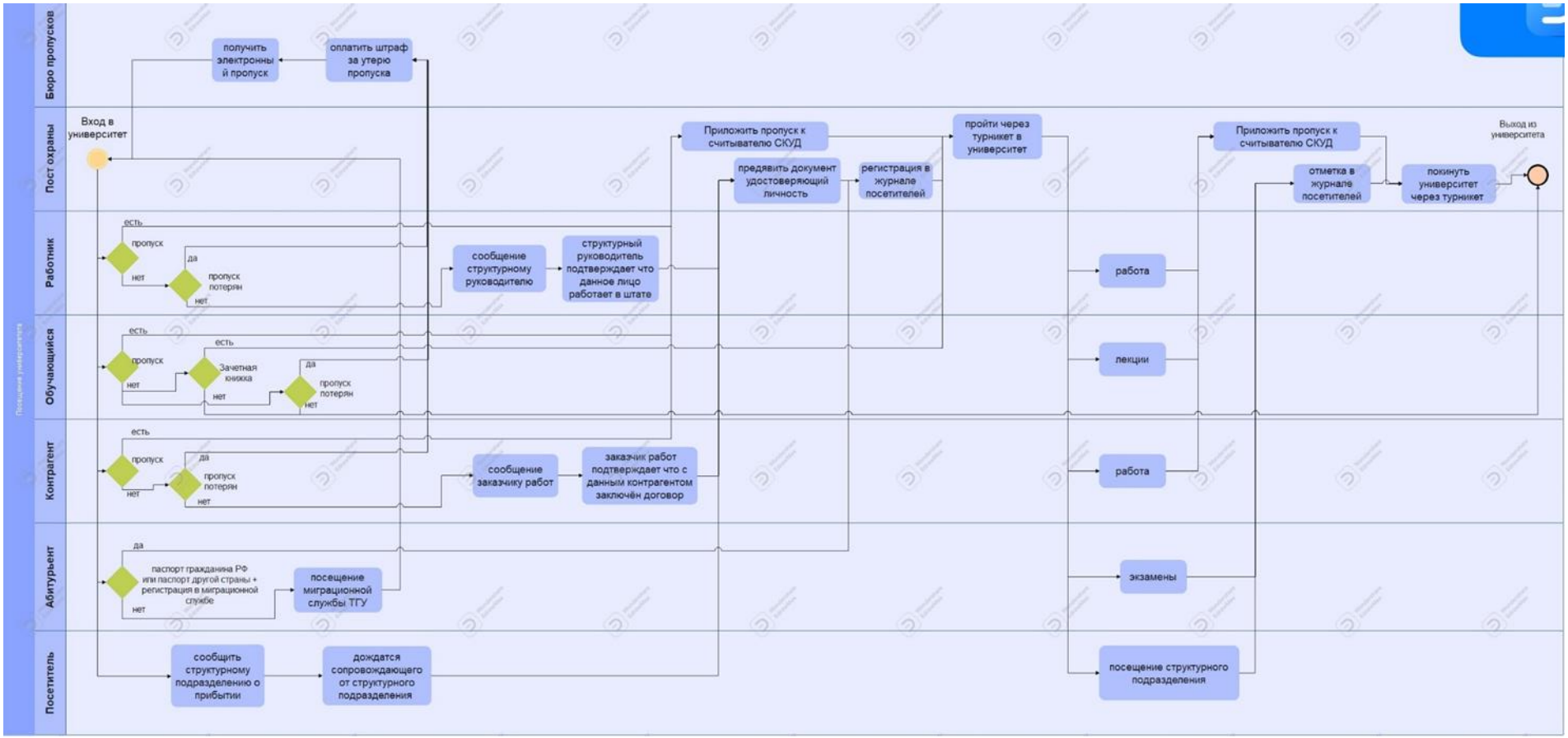


Рисунок 5 – Перевод в нотацию BPMN вербального алгоритма посещения университета

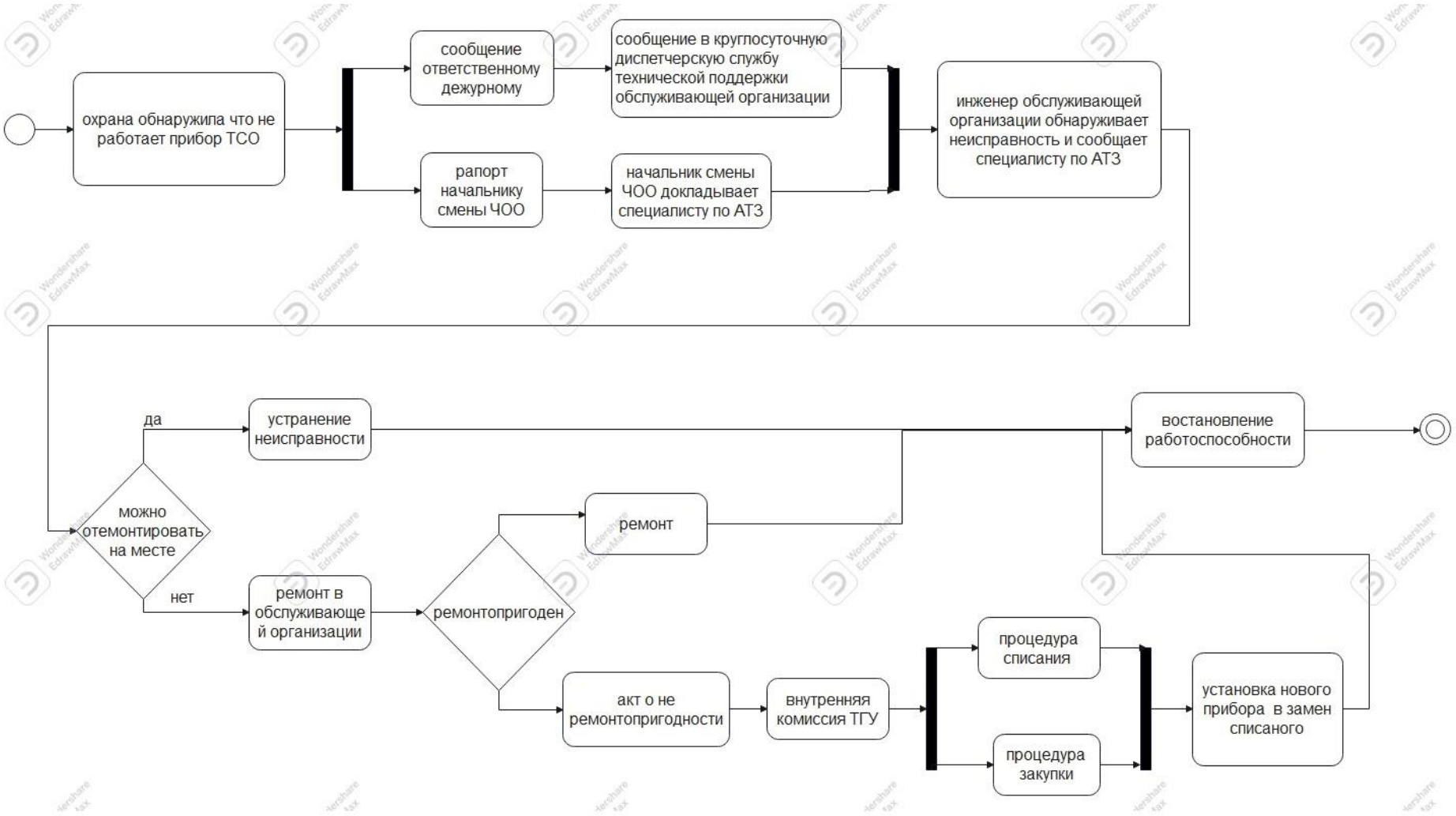


Рисунок 6 – Перевод в нотацию UML вербального алгоритма обнаружения и устранения неисправности технических средств охраны.

Если прибор вышел из строя и его не представляется возможным отремонтировать, то обслуживающая организация предоставляет АКТ неисправности и собирается комиссия, которая устанавливает факт критической неисправности прибора и начинается процедура списания прибора и закупки аналогичного прибора. Перевод в нотацию UML вербального алгоритма обнаружения и устранения неисправности технических средств охраны представлен на рисунке 6.

В качестве дальнейшего примера рассмотрен алгоритм действий при захвате заложников (рисунок 7). Разработанная диаграмма позволяет в наглядной и доходчивой форме представить информацию, которая в оригинале занимает 5 страниц текста [2].

Наряду с UML эффективно представление и в других нотациях, так в нотации BPMN разработана модель действий при обнаружении взрывного устройства (рисунок 8).

В BPMN модели действий при вооруженном нападении (рисунок 9). использовании системы плавательных дорожек обеспечивает наглядность разграничения функций и взаимодействия между руководством, охраной, ответственным дежурным, сотрудниками и обучающимися.

Также применение плавательных дорожек позволяет выделить фрагменты модели для наглядного преставления и размещения в инструкциях, на информационных стендах в ходе действий по ознакомлению.

Так разработанная модель действий, обучающихся и работников при обнаружении взрывного устройства при размещении на соответствующих стендах в большей степени обеспечит ознакомление обучающихся с необходимыми действиями, чем размещении соответствующей информации в оригинальном текстовом виде (рисунок 10).

Модель действий ответственных за АТЗ структур при обнаружении взрывного устройства (рисунок 11) обеспечивает наглядное представление взаимодействия охраны, дежурного и руководства университета.

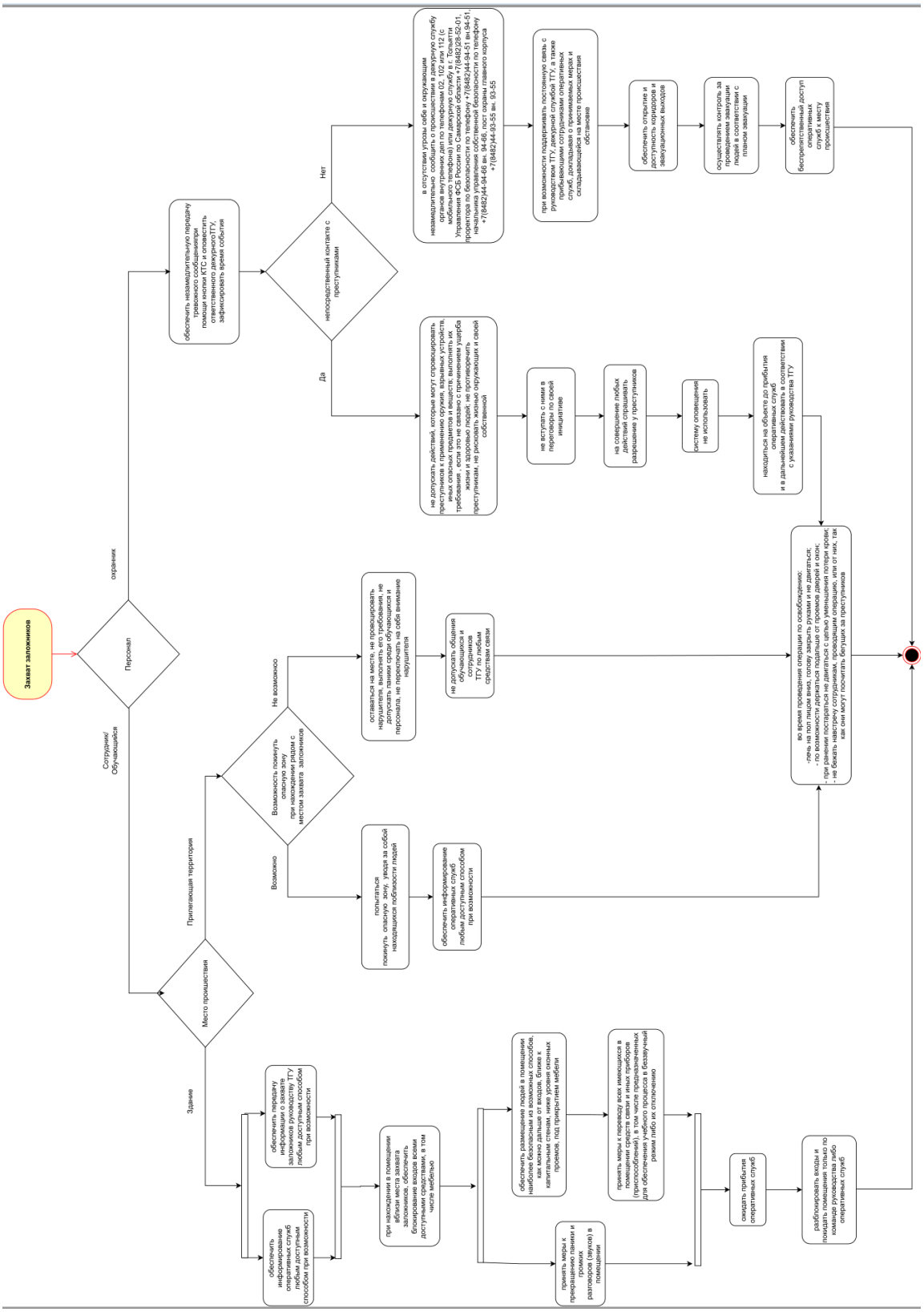


Рисунок 7 - Алгоритм действий при захвате заложников (UML)-

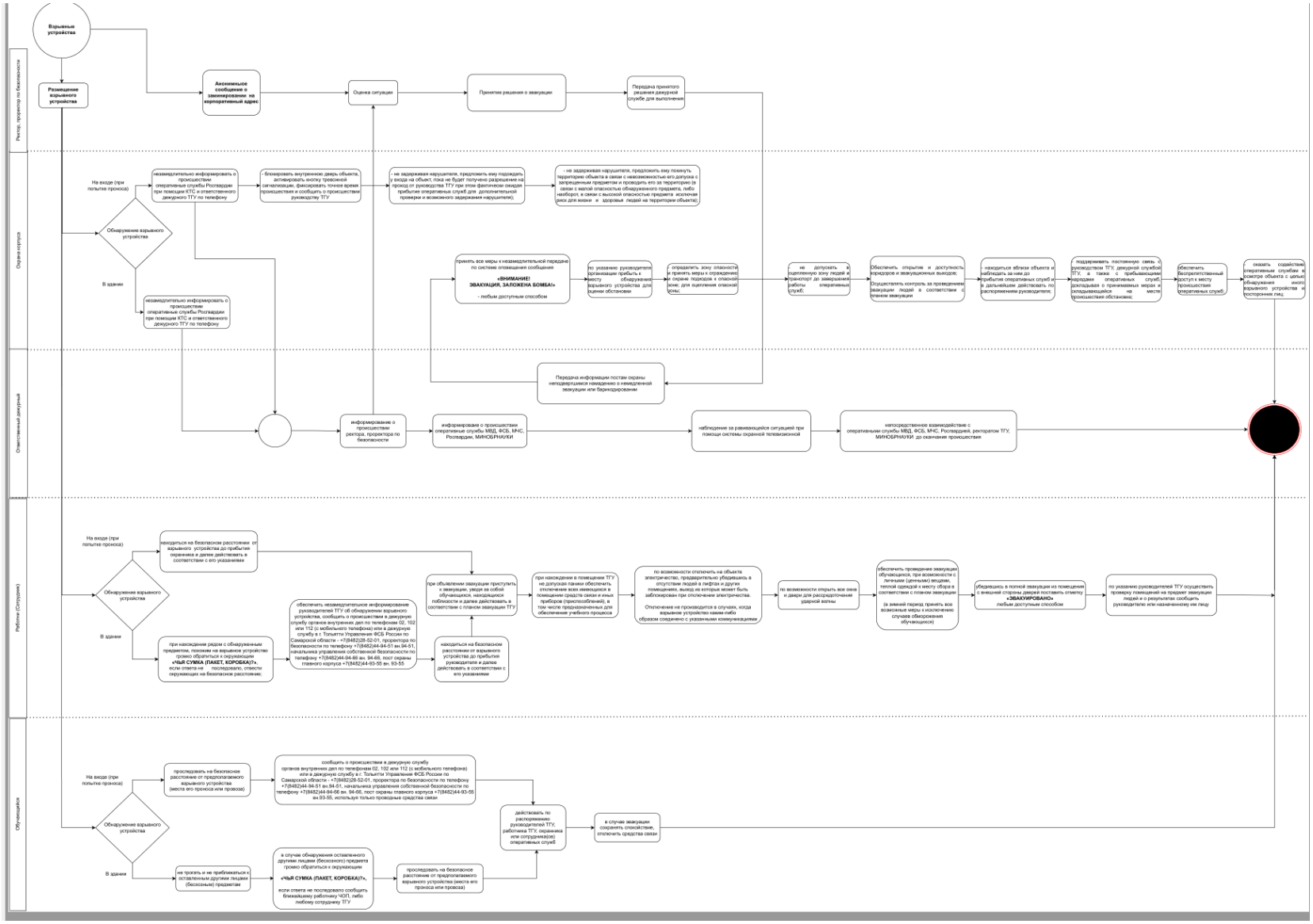


Рисунок 8 - Модель действий при обнаружении взрывного устройства (BPMN)

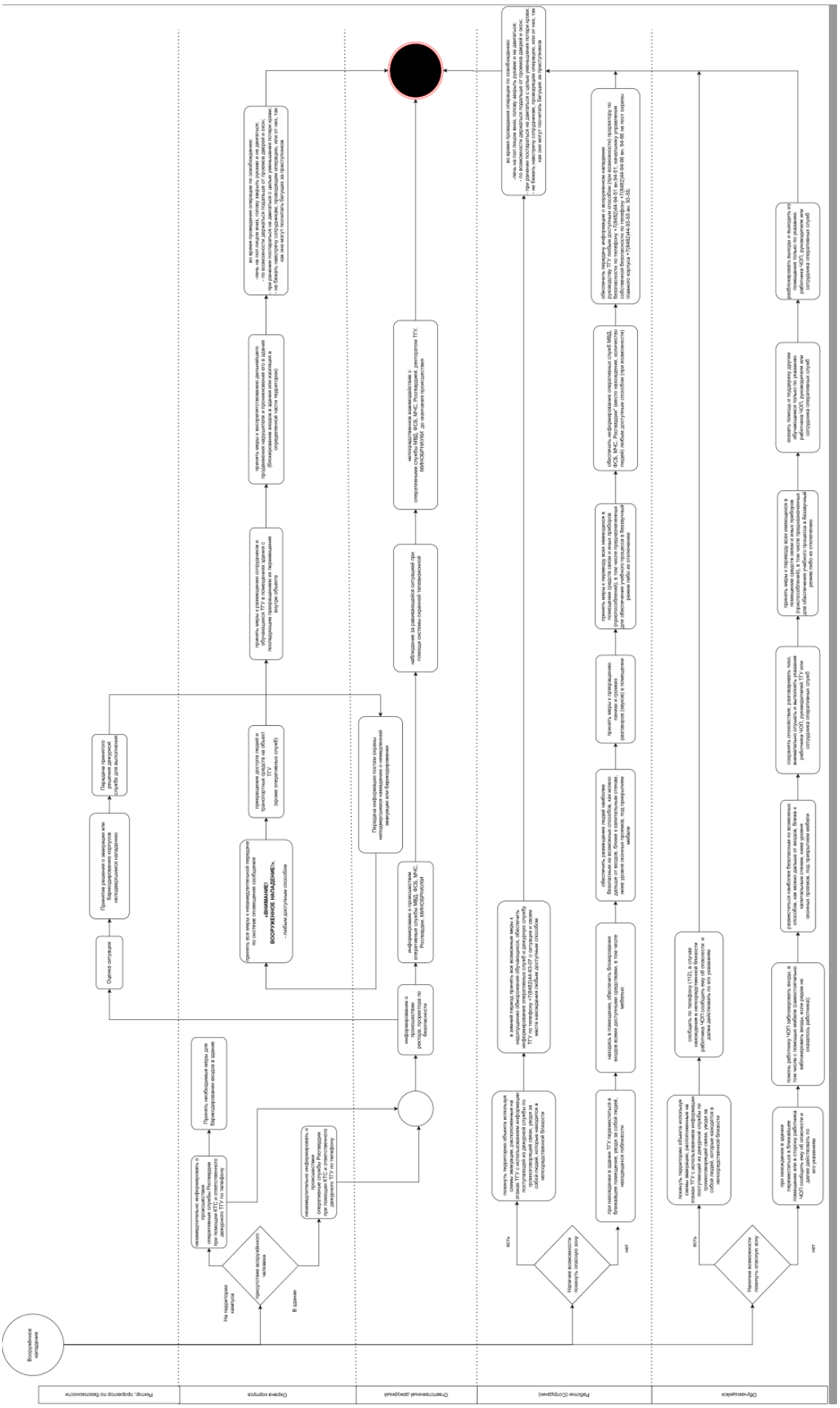


Рисунок 9 - Модель действий при вооруженном нападении (BPMN)

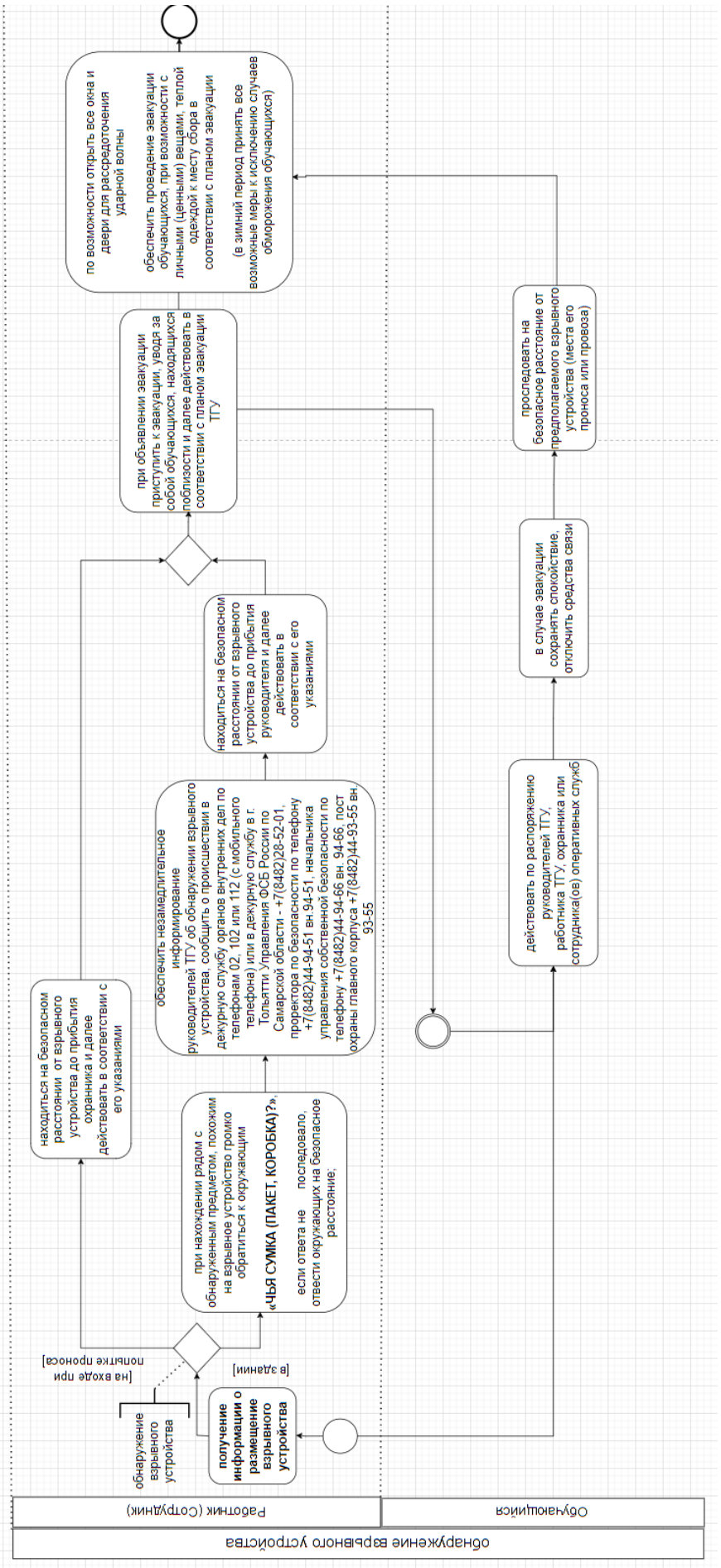


Рисунок 10 - Модель действий сотрудников и обучающихся при обнаружении взрывного устройства (BPMN)

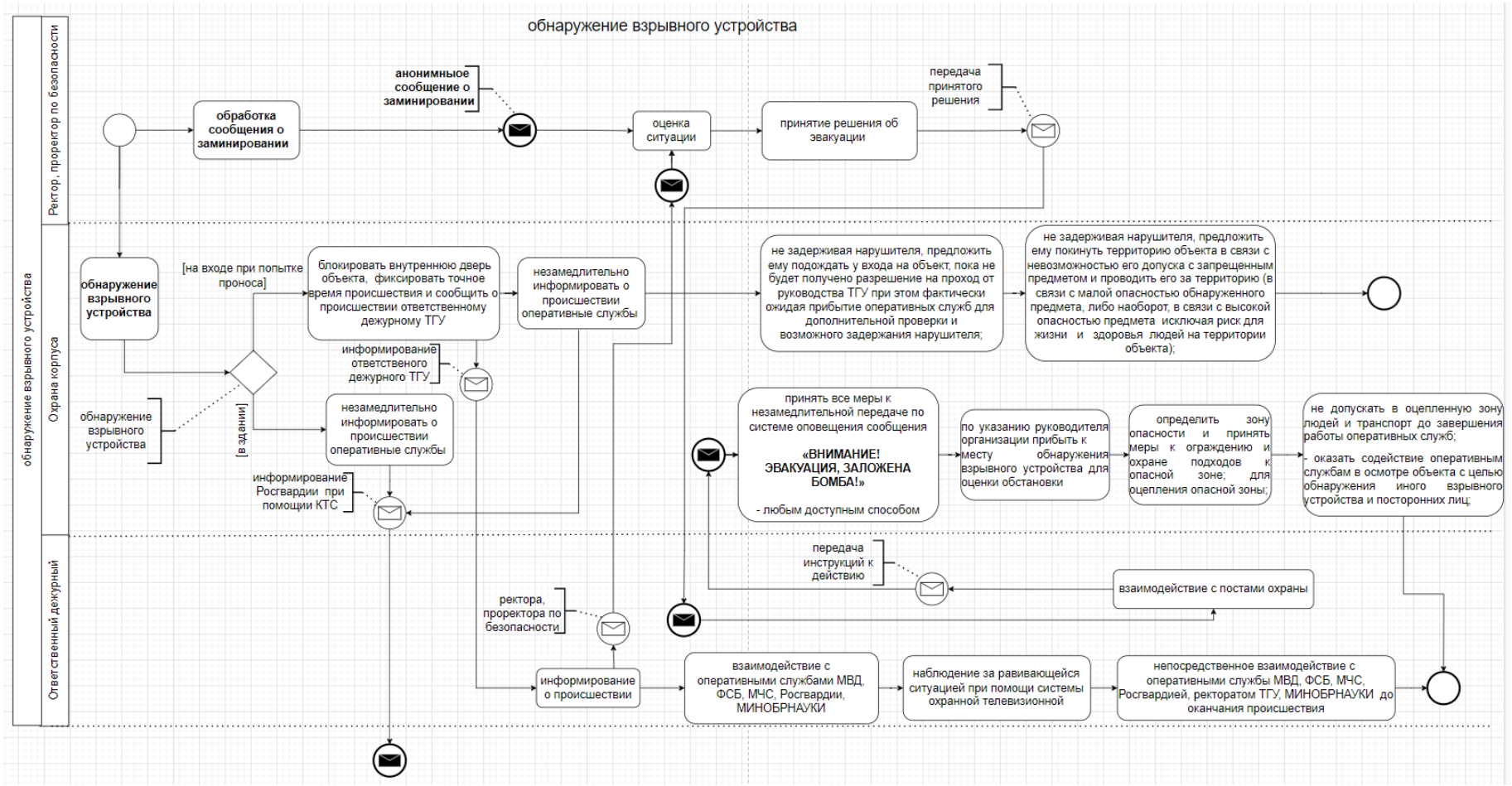


Рисунок 11 - Модель действий ответственных за АТЗ структур при обнаружении взрывного устройства (BPMN)

Такую схему целесообразно разместить на постах охраны и в комнате ответственного дежурного. Этим обеспечится быстрое и эффективное взаимодействие подразделений и служб ответственных за антитеррористическую защищенность при обнаружении взрывного устройства.

Модель действий при вооруженном нападении аналогичным образом может быть представлена для персонала и обучающихся с одной стороны и для структур, ответственных за антитеррористическую защищенность. При этом использована вертикальная компоновка плавательных дорожек.

Модель действий обучающихся и сотрудников ври вооруженном нападении показана на рисунке 12. Такие схемы целесообразно разместить на стендах по безопасности.

Модель действий ответственных за АТЗ структур при вооруженном нападении (рисунок 13) обеспечивает наглядное представление взаимодействия охраны, дежурного и руководства университета. Такую схему целесообразно разместить на постах охраны и в комнате ответственного дежурного. Этим обеспечится быстрое и эффективное взаимодействие подразделений и служб ответственных за антитеррористическую защищенность при вооруженном нападении.

Выполненные работы позволяют сформулировать следующие рекомендации по применению исследованных нотаций на мезоуровне управления АТЗ:

Нотация UML обладает сравнительно большими описательными возможностями, но менее наглядна и требует определенных знаний для прочтения диаграмм. UML моделирование эффективно при разработке, согласовании и оптимизации действий в том числе и методами имитационного моделирования. А также в качестве интерфейса для связи с моделями общесистемного и операционного уровней.

BPMN диаграммы обладают большей наглядностью и могут быть эффективно применены для доведения информации до сведения акторов.

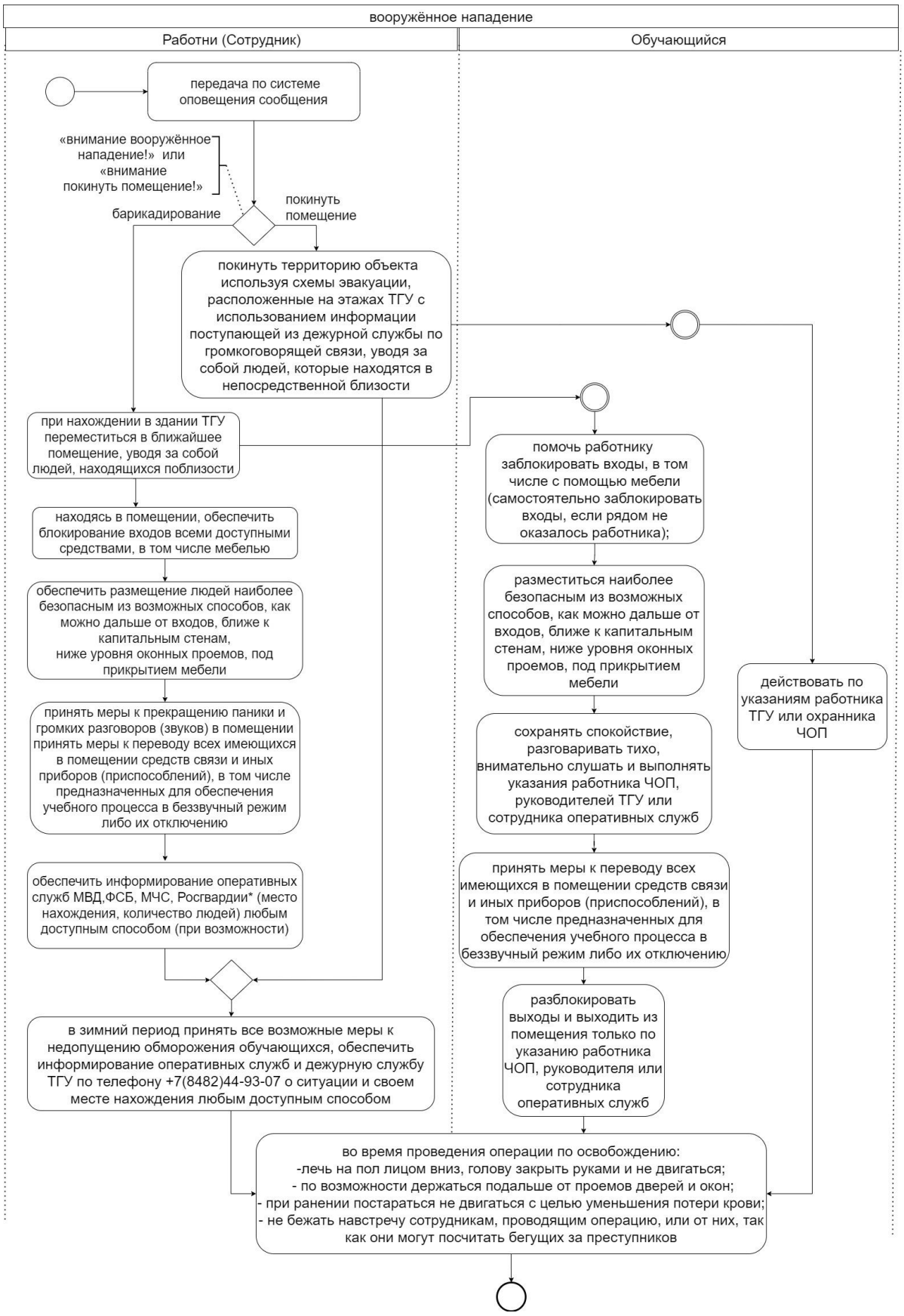


Рисунок 12 – Модель действий обучающихся и сотрудников при вооруженном нападении

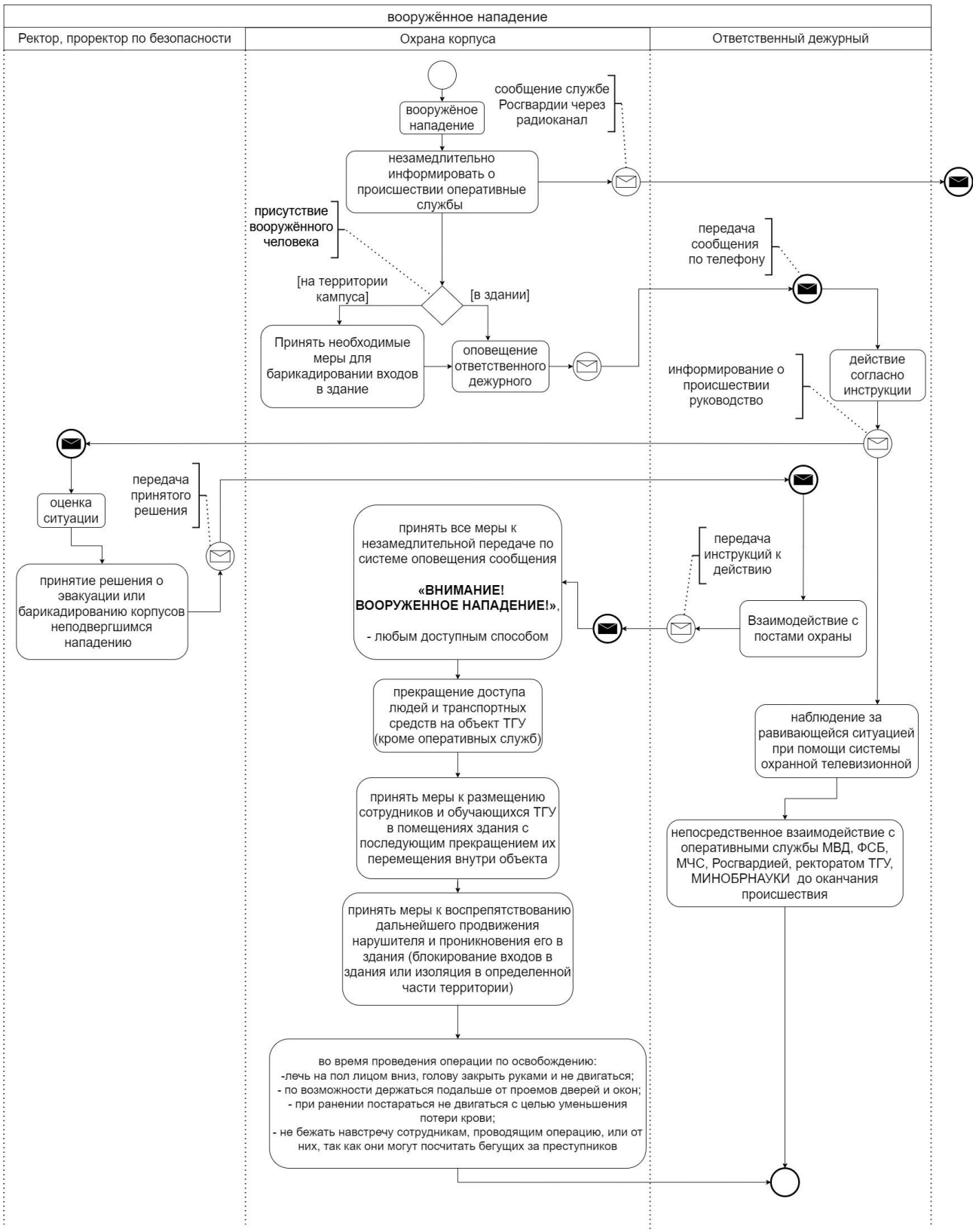


Рисунок 13 – Модель действий ответственных за АТЗ структур при вооруженном нападении

Сравнительные характеристики исследованных нотаций показаны в таблице 1.

Таблица 1 – Сравнение нотаций UML и BPMN на среднем уровне управления АТЗ

Параметр	UML	BPMN
Необходимость специальных знаний при составлении моделей	+	+
Необходимость специальных знаний при прочтении моделей	+	-
Возможность имитационного моделирования	+	-
Наглядность	-	+
Рекомендуемое применение	разработка оптимизация интеграция моделей	доведение моделей до акторов

Таким образом показано, что применения нотации UML и BPMN на мезоуровне уровне АТЗ эффективно.

3.3 Применение анализа данных на оперативном уровне

Выполнены обработка и анализ данных о результатах эвакуации обучающихся и персонала ТГУ за последние 9лет.

В исходном виде данные представлены в виде таблицы с полями

- год;
- институт;
- курс;
- корпус;
- этажность;
- количество лестничных маршей;
- количество эвакуационных выходов;
- время оценки угрозы и принятие решения мин;

– скорость передачи сообщения (мин);
– время покидания этажа (мин) ;
– время покидания этажа (мин) плюс время на передачу сообщения;
– время до полной эвакуации (мин) ;
– время до полной эвакуации (мин) плюс время на передачу сообщения.

В результате предварительного анализа данных установлено:

Время оценки угрозы и принятие решения является постоянным и составляет 20 минут.

Столбцы «время покидания этажа (мин) плюс время на передачу сообщения» и «время до полной эвакуации (мин) плюс время на передачу сообщения» являются вычисляемыми – значения в данных столбцах представляет собой сумму времен, отраженных в других столбцах и не несет никакой дополнительной информации.

График времени полной эвакуации, показанный на рисунке 14 имеет провал в годах, которые соответствуют ковидным ограничениям.

На основании изложенного проведена очистка данных: удалены строки, соответствующие ковидным ограничениям с нулевыми временами эвакуации и удалены постоянный и вычисляемые столбцы.

Порядок действий:

– лицо (охранник, секретарь и т.п.) обнаруживает опасный факт – неопознанный пакет, звонок о минировании и т.п. и сообщает об этом дежурному. Время (момент времени) сообщения дежурному - момент времени t0.
– дежурный связывается с руководством вуза и передает – время сообщения руководству - t1.
– руководство принимает решение и сообщает его дежурному – время сообщения решения дежурному - t2.
– дежурный доводит решение до поста охраны корпуса, - t3.

– охрана начинает эвакуацию. Время сигнала - t4.

– охрана докладывает дежурному, что корпус эвакуирован - t5.

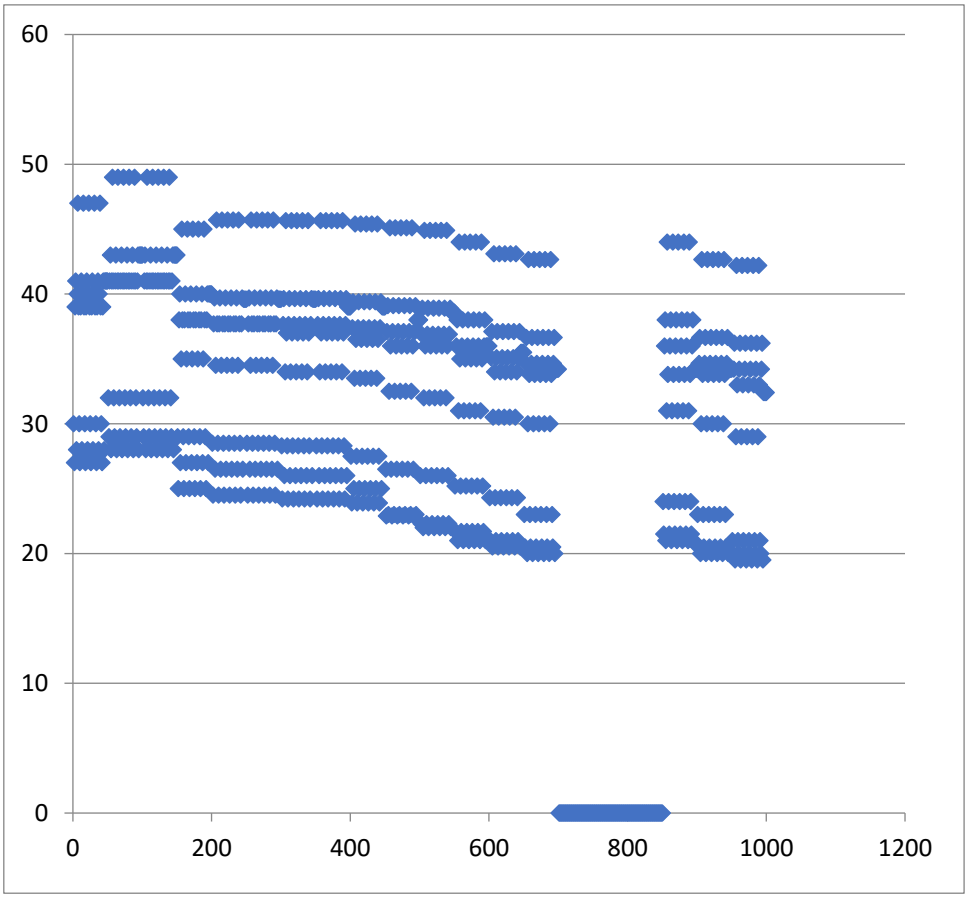


Рисунок 14 – Время полной эвакуации по неочищенным данным

На основании описанной последовательности действий выделим интервалы времени, продолжительность которых будет проанализирована:

– принятие решения дежурным T1 = t1-t0.

– принятие решения руководством T2 = t2-t1.

– доведение решения до поста охраны корпуса T3 = t3-t2.

– принятие решения охраной T4 = t4-t3.

– время эвакуации корпуса T5 = t5-t4.

Общее время эвакуации T = t5-t0 = T1+T2+T3+T4+T5 необходимо минимизировать, в случае если одновременно эвакуируются несколько

корпусов, то необходимо минимизировать общее время эвакуации самого медленного корпуса max(T5i) ->min.

Факторы, влияние которых необходимо изучить, это

- институт (Ф1);
- курс (Ф2);
- корпус (Ф3);
- этажность (Ф4);
- количество лестничных маршей (Ф5);
- количество эвакуационных выходов (Ф6).

На первом этапе исследуем зависимость интервалов времени Т1 – Т3 от факторов Ф3 – Ф6 (выбраны числовые величины).

При этом использован коэффициент парной корреляции Пирсона.

Результаты корреляционного анализа приведены в таблице 2.

Корреляция по абсолютному значению меньше 0,5 полагаем несущественной – показывающей, что рассматриваемые величины не связаны.

Таблица 2 – Результаты корреляционного анализа

Параметр	Скорость передачи сообщения (мин)	Время покидания этажа (мин)	Время до полной эвакуации (мин)
Этажность	-0.09	-0.62	0.86
Количество лестничных маршей	0.35	0.53	-0.37
Количество эвакуационных выходов	0.64	0.50	-0.53

Зависимость между количеством эвакуационных выходов и скоростью передачи сообщения (коэффициент корреляции 0,64) говорит о том, что чем меньше эвакуационных выходов тем быстрее передается сообщение. Поскольку данная зависимость никак не объяснима, полагаем ее случайной.

Обратная корреляция между этажностью и временем покидания этажа (коэффициент корреляции -0,62) означает, что в многоэтажных корпусах время покидания этажа меньше, чем в малоэтажных. Этот факт можно объяснить тем, что в многоэтажных корпусах, например, УЛК или строительном площадь этажа меньше, чем в малоэтажных, например, в главном. Данная зависимость объяснима, но практической ценности для повышения эффективности системы эвакуации не имеет.

Наиболее сильная зависимость имеет место между этажностью и полным временем эвакуации (коэффициент корреляции 0,86).

Полное время эвакуации состоит из времен:

- принятие решения дежурным T1 = t1-t0.
- принятие решения руководством T2 = t2-t1.
- доведение решения до поста охраны корпуса T3 = t3-t2.
- принятие решения охраной T4 = t4-t3.

Отбросив T1 и T2, которые очевидно никак не влияют и не могут быть изменены, рассмотрим время доведения решения до поста охраны корпуса и время принятия решения охраной в зависимости от корпуса.

Время принятия решения охраной показано в таблице 3.

Таблица 3 – Время принятия решения охраной корпуса

Корпус	минимум	максимум	среднее
Г	0.9	1.3	1.0
А	0.8	1.3	1.2
С	1.0	1.2	1.1
Э	0.8	1.1	1.0
Ф	1.0	1.4	1.3
БиД	0.8	1.4	0.9
УЛК	0.8	1.4	0.9
Е	0.9	1.2	1.0
У	0.8	1.5	1.1

Графический анализ данных таблицы 3 (рисунок 15) не позволяет выделить никаких закономерностей – для всех корпусов среднее время принятия решения охраной составляет порядка 1 минуты.

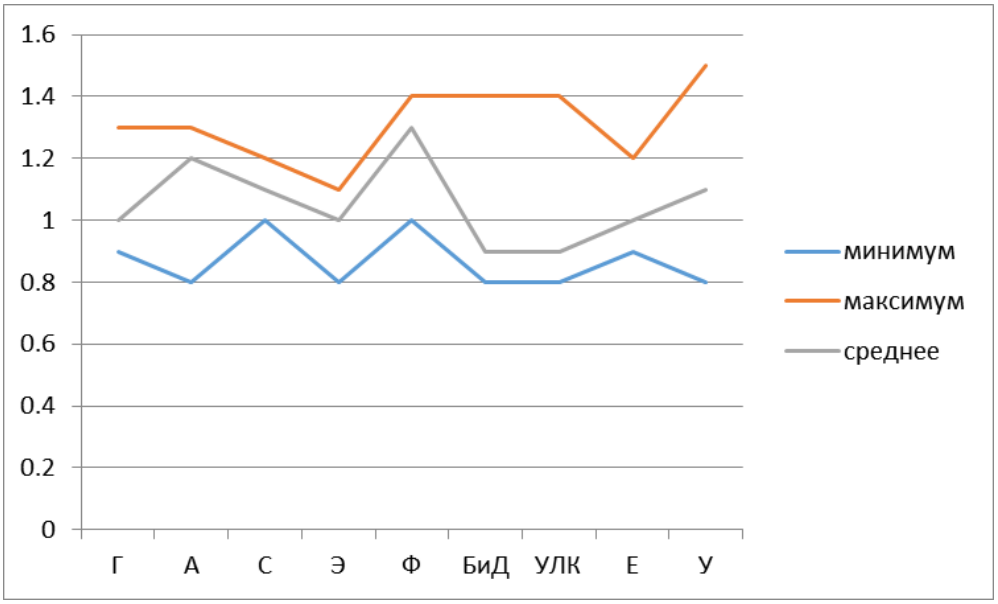


Рисунок 15 - Время принятия решения охраной корпуса

Время доведения решения до поста охраны корпуса показано в таблице 4.

Таблица 4 - Время доведения решения до поста охраны корпуса

Корпус	минимум	максимум	среднее
Г	4.7	5.4	4.9
А	6.9	7.9	7.1
С	8.2	9.8	9.2
Э	10.2	11.2	11.1
Ф	12.9	14.1	13.9
БиД	15.1	16.4	15.4
УЛК	16.2	18.0	17.1
Е	18.9	20.2	19.6
У	21.0	21.4	21.1

По таблице 4 видно, что время доведения существенно зависит от корпуса, что также подтверждается графиком, показанным на рисунке 16.

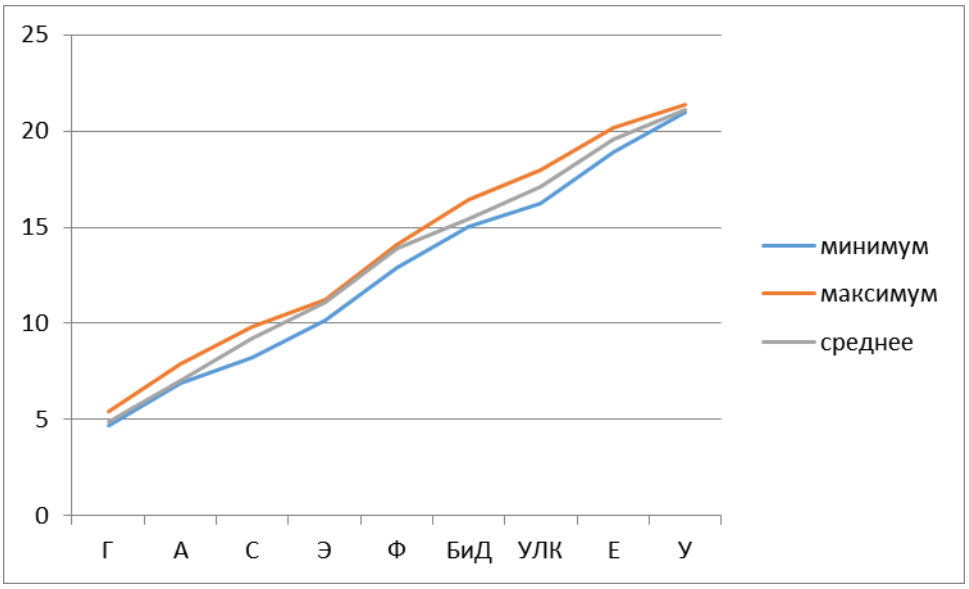


Рисунок 16 - Время доведения решения до поста охраны корпуса

Выявленная зависимость вызвана тем, что оповещение корпусов дежурным идет в определенном порядке. И одно сообщение занимает порядка 2 минут.

Среднее время полной эвакуации корпуса (минут):

Г 21,89

А 16,63

С 28,16

Э 28,11

Ф 11,0

БиД 18,74

УЛК 28,10

Е 17,49

У 17,05.

Если изменить порядок оповещения таким образом, чтобы в первую

очередь оповещать корпуса с максимальным временем эвакуации (за исключением главного корпуса, где и находится дежурный) то можно снизить общее время эвакуации по университету.

Выводы по главе:

Выполнена практическая апробация моделей и методов программной инженерии на системе АТЗ ТГУ.

Выполнено моделирование в нотации IDEF0 системы АТЗ на уровне деятельности и бизнес процессов, что обеспечивает простое и наглядное представление информации на стратегическом уровне.

На мезоуровне выполнено моделирование в нотациях UML и BPMN.

На операционном уровне выполнен анализ данных по времени эвакуации. На основании проведенного корреляционного анализа предложены мероприятия по изменению в порядке проведения эвакуации корпусов, обеспечивающие снижение общего времени эвакуации по университету.

Заключение

В ходе анализа существующих моделей и методов повышения эффективности деятельности по обеспечению антитеррористической защищенности (АТЗ) организаций рассмотрен порядок обеспечения антитеррористической защищенности организаций и пример существующего подхода к моделированию поведения системы.

В результате анализа установлено:

- деятельность по обеспечению защиты организаций на примере контртеррористической защищённости представляет собой систему управления, в которой присутствуют как организационные, так и технические подсистемы.
- моделирование деятельности по антитеррористической защите показывает принципиальную применимость методов программной инженерии к моделированию систем безопасности и обеспечивает лаконичность, наглядность и согласованность на любом необходимом уровне детализации.

В ходе исследования подходов и методов программной инженерии в моделировании систем безопасности исследованы методы моделирования систем безопасности организаций в контексте свода знаний программной инженерии, рассмотрены основные нотации и методологии графического моделирования, предложено новая трехуровненая модель использования средств программной инженерии в системах АТЗ организаций.

Результаты исследований:

- из рассмотрения свода знаний SWEBOK определены основные составляющие программной инженерии, использование моделей и методов которых потенциально может повысить эффективность деятельности по обеспечению антитеррористической защищённости.
- в результате изучения различных подходов и методов

проектирования и моделирования программного обеспечения определены основные графические нотации, потенциально применимые для достижения цели работы.

- установлено, что среди паттернов моделирования и проектирования, широко используемых в программной инженерии, отсутствуют (или не представлены в открытом доступе) шаблоны, ориентированные на моделирование систем безопасности.
- разработана теоретическая модель применения методов программной инженерии к системам АТЗ. Модель включает три уровня управления системой АТЗ и содержит рекомендуемые на каждом уровне модели и методы программной инженерии.

В ходе практической апробации предложенных решений выполнено моделирование системы АТЗ тольяттинского государственного университета на уровне процессов, на мезоуровне и на оперативном уровне.

Выполнена практическая апробация моделей и методов программной инженерии на системе АТЗ ТГУ.

Выполнено моделирование в нотации IDEF0 системы АТЗ на уровне деятельности и бизнес процессов, что обеспечивает простое и наглядное представление информации на стратегическом уровне.

На мезоуровне выполнено моделирование в нотациях UML и BPMN.

На операционном уровне выполнен анализ данных по времени эвакуации. На основании проведенного корреляционного анализа предложены мероприятия по изменению в порядке проведения эвакуации корпусов, обеспечивающие снижение общего времени эвакуации по университету.

Список используемой литературы и используемых источников

1. Алгоритмы действий административного персонала образовательной организации [Электронный ресурс]. URL: https://drive.google.com/drive/folders/13u4tojGgMiQldcvimUtBUuq3zisrIqP4?usp =sharing (дата обращения: 16.03.2024)

2. Алгоритмы действий персонала образовательной организации, работников частных охранных организаций и обучающихся при совершении (угрозе совершения) преступления в формах вооруженного нападения, размещения взрывного устройства, захвата заложников, а также информационного взаимодействия образовательных организаций с территориальными органами МВД России, Росгвардии и ФСБ России [Электронный ресурс] URL: https://sc6-surgut.gosuslugi.ru/netcat_files/30/69/Algoritm_deystviy_personala_obuchayuschihsya_i_sotrudnikov.pdf?ysclid=lvjdtg2u6e765127705 (дата обращения: 20.04.2024)

3. Бекмурзин М.С. Зарубежный опыт антитеррористической работы и перспективы его применения в российских условиях // Вестник Московского университета МВД России. 2013. №9. URL: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-antiterroristicheskoy-raboty-i-perspektivy-ego-primeneniya-v-rossiyskih-usloviyah (дата обращения: 29.04.2024).

4. Как организовать антитеррористическую защищенность объекта в 2024 году [Электронный ресурс] URL: https://www.trudohrana.ru/article/104130-22-m3-antiterroristicheskaya-zashchishchennost-organizatsii?ysclid=lvkud3sf9m691224166 (дата обращения: 20.04.2024)

5. Лошаков А.С. Анализ антитеррористической безопасности организации в современных условиях // Вестник экономической безопасности. 2008. №3. URL: https://cyberleninka.ru/article/n/analiz-antiterroristicheskoy-

bezopasnosti-organizatsii-v-sovremennyh-usloviyah (дата обращения: 29.04.2024).

6. Могинов А.Ф. Вопросы совершенствования правового регулирования применения информационных инструментов противодействия терроризму в субъектах российской федерации // Вестник магистратуры. 2019. №3-2 (90). URL: https://cyberleninka.ru/article/n/voprosy-sovershenstvovaniya-pravovogo-regulirovaniya-primeneniya-informatsionnyh-instrumentov-protivodeystviya-terrorizmu-v (дата обращения: 29.04.2024).

7. Моделирование бизнес-процессов с использованием методологии ARIS. Министерство транспорта российской федерации федеральное государственное бюджетное образовательное учреждение высшего образования «Российский университет транспорта (МИИТ)» Москва – 2017

8. Петров Александр Валерьевич Построение системы антитеррористической безопасности // ЭСГИ. 2018. №1 (17). URL: https://cyberleninka.ru/article/n/postroenie-sistemy-antiterroristicheskoy-bezopasnosti (дата обращения: 29.04.2024).

9. Постановление Правительства РФ от 2 августа 2019 г. № 1006 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)" [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102580502&intelsearch=+%CF%E%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5++%EF%F0%E0%EF%E2%E8%F2%E5%EB%FC%F1%F2%E2%E0+%F0%EE%F1%F1%E8%E9%F1%EA%EE%E9+%F4%E5%E4%E5%F0%E0%F6%E8%E8+%EE%F2+2+%E0%E2%E3%F3%F1%F2%E0+2019 (дата обращения: 20.04.2024)

10. Постановление Правительства РФ от 24 сентября 2019 г. № 1243 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по надзору в сфере образования

и науки и подведомственных ей организаций, а также формы паспорта безопасности этих объектов (территорий)" [Электронный ресурс] URL: https://www.mos.ru/atk/documents/postanovleniya-i-rasporyazheniya-pravitelstva-rossiiskoi-federacii/view/232677220/ (дата обращения: 20.04.2024)

11. Постановление Правительства РФ от 25 декабря 2013 г. № 1244 "Об антитеррористической защищенности объектов (территорий)" [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102170326&intelsearch=%EF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5+1244+%EE%E1+%E0%ED%F2%E8%F2%E5%F0%F0%EE%F0%E8%F1%F2%E8%F7%E5%F1%EA%EE%E9+%E7%E0%F9%E8%F9%E5%ED%ED%EE%F1%F2%E8 (дата обращения: 20.04.2024)

12. Постановление Правительства РФ от 7 ноября 2019 г. № 1421 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства науки и высшего образования Российской Федерации, его территориальных органов и подведомственных ему организаций, объектов (территорий), относящихся к сфере деятельности Министерства науки и высшего образования Российской Федерации, формы паспорта безопасности этих объектов (территорий) и признании утратившими силу некоторых актов Правительства Российской Федерации" [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102617462&intelsearch=%CF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5+%CF%F0%E0%E2%E8%F2%E5%EB%FC%F1%F2%E2%E0+%D0%D4+%EE%F2+7+%ED%EE%FF%E1%F0%FF++2019+%E3.+%B91421 (дата обращения: 20.04.2024).

13. Постановление Правительства РФ от 7 октября 2017 г. № 1235 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности

этих объектов (территорий)" [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102446066&intelsearch=%CF%EE%F1%F2%E0%ED%EE%E2%EB%E5%ED%E8%E5+%CF%F0%E0%E2%E8%F2%E5%EB%FC%F1%F2%E2%E0+%D0%D4+%EE%F2+7+%EE%EA%F2%FF%E1%F0%FF+2017+%E3.+%B9+1235 (дата обращения: 20.04.2024)

14. РД IDEF 0 – 2000. Методология функционального моделирования IDEF0. Руководящий документ.

15. Типовая модель действий нарушителя, совершающего на объекте образования преступление террористической направленности и алгоритмов действий персонала образовательной организации, работников частных охранных организаций и обучающихся при совершении (угрозе совершения) преступления в формах вооруженного нападения, размещения взрывного устройства, захвата заложников [электронный ресурс] URL https://www.ihim.uran.ru/netcat_files/userfiles/Tipovaia_model_narusitela_MON.pdf

16. Трофимов С. А. Структурно-функциональная характеристика антитеррористической деятельности // Проблемы законности. 2012. №120. URL: https://cyberleninka.ru/article/n/strukturno-funktsionalnaya-harakteristika-antiterroristicheskoy-deyatelnosti (дата обращения: 29.04.2024).

17. Указ Президента РФ от 15 февраля 2006 г. № 116 "О мерах по противодействию терроризму" [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102104819&intelsearch=&firstDoc=1 (дата обращения: 20.04.2024)

18. Указ Президента РФ от 26 декабря 2015 г. №664 «О мерах по совершенствованию государственного управления в области противодействия терроризму» [Электронный ресурс] URL: https://www.mos.ru/atk/documents/ukazy-prezidenta-rossiiskoi-federacii/view/228311220/ (дата обращения: 20.04.2024)

19. Федеральный закон от 25 июля 2002 г. № 114-ФЗ "О противодействии экстремистской деятельности" [Электронный ресурс] URL:

http://pravo.gov.ru/proxy/ips/?docbody=&link_id=14&nd=102079221&intelsearch= (дата обращения: 20.04.2024)

20. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ "О безопасности" [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102144301&rdk=&intelsearch= (дата обращения: 20.04.2024)

21. Федеральный закон от 6 марта 2006 г N 35 ФЗ «О противодействии терроризму» [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102170326&backlink=1&&nd=102105192 (дата обращения: 20.04.2024)

22. Шамаев Артур Мурадинович Информационное обеспечение антитеррористической деятельности // ИСОМ. 2015. №5-2. URL: https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-antiterroristicheskoy-deyatelnosti (дата обращения: 29.04.2024).

23. Язык UML. Руководство пользователя [Электронный ресурс] URL: https://e-univers.ru/upload/iblock/27c/lxgwtpt72sojroee152h2pg5ivcs8i2l.pdf?ysclid=lvkth084tx32966991 (дата обращения: 20.04.2024)

24. A Practical Guide to SysMLThe Systems Modeling Language [Электронный ресурс] URL: https://msl.overdrive.com/media/2015882 (дата обращения: 20.04.2024)

25. Guide to the Software Engineering Body of Knowledge Version 3.0 SWEBOK A Project of the IEEE Computer Society [электронный ресурс] URL https://ieeecs-media.computer.org/media/education/swebok/swebok-v3.pdf

26. SysML Diagram Tutorial [Электронный ресурс] URL: https://sysml.org/tutorials/sysml-diagram-tutorial/ (дата обращения: 20.04.2024)

27. SysML Tutorials for Model-Based Systems Engineering [Электронный ресурс] URL: https://sysml.org/tutorials/ (дата обращения: 20.04.2024)

28. UML. Основы. Краткое руководство по стандартному языку объектного моделирования [Электронный ресурс] URL: https://picloud.pw/media/resources/posts/2018/02/20/UML_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%8B.pdf (дата обращения: 20.04.2024)

29. UML. Специальный справочник [Электронный ресурс] URL: https://dl.booksee.org/genesis/716000/73d17ecb63ea90abec898449a95ba5ce/_as/[Gradi_Buch,_Dzheims_Rambo,_Ivar_YAkobson]_YAzuek_(BookSee.org).pdf (дата обращения: 20.04.2024)

30. Unified Modeling Language Specification (version 2.1) [Электронный ресурс] URL: https://www.omg.org/spec/UML/2.2/Superstructure/PDF (дата обращения: 20.04.2024)