МОДЕЛИРОВАНИЕ СИСТЕМЫ МОНИТОРИНГА И УПРАВЛЕНИЯ РИСКАМИ В СЕТЯХ МОБИЛЬНОЙ СВЯЗИ

В.Н. Максименко, *к.т.н, доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru;*
А.С. Беседина, *Московский технический университет связи и информатики, zelenovalrxa@yandex.ru;*
М.Ю. Суптеля, *Московский технический университет связи и информатики supteiya.mariya@mail.ru.*

УДК 621.391

Аннотация. В статье представлены результаты моделирования мониторинга и управления рисками системы *MVNO* (*Mobile Virtual Network Operator/в*иртуальный оператор сотовой связи) средствами объектно-ориентированного анализа и проектирования в нотации визуального языка *UML (Unified Modeling Language).*

Ключевые слова: сеть сотовой подвижной связи; уязвимость; угроза; атака; информационная безопасность; сеть виртуального оператора сотовой связи; мониторинг; управление рисками; объектно-ориентированный анализ.

MODELING OF MONITORING AND RISK MANAGEMENT SYSTEM IN MOBILE COMMUNICATIONS NETWORKS

Vladimir Maksimenko, *Ph.D., associate professor, Moscow technical university of communications and informatics;*
Alexandra Besedin, *Moscow technical university of communications and informatics;*
Maria Suptelya, *Moscow technical university of communications and informatics.*

Annotation. The article presents the simulation results of monitoring and risk management of the *MVNO* system (Mobile Virtual Network Operator / virtual mobile communications operator) by means of object-oriented analysis and design in the notation of the visual language *UML* (Unified Modeling Language).

Keywords: mobile cellular network; vulnerability; threat; attack; information security; virtual mobile operator network; monitoring; risk management; object-oriented analysis.

Введение

Время жизненного цикла информационных систем постоянно сокращается. Это ускорение обусловлено внедрением беспроводных сотовых сетей третьего и последующих поколений, новых алгоритмов обработки сигналов и высокоскоростных сетей передачи, что создало предпосылки для оказания информационных услуг в любое время и в любом месте. Одновременно с развитием информационных технологий повышается сложность решаемых задач, необходимость управления информационными процессами в реальном масштабе времени и одновременной обработки информации территориально-распределенных объектов – источников исходных данных. Использование бизнес-модели *MVNO* приводит к расширению круга участников рынка оказания информационных услуг за счет инновационных предложений, не подкрепленных практической реализацией. Все эти условия создают требования для поиска новых методов процесса проектирования, обеспечивающих сокращение времени жизни стадии проектирования и взаимопонимание между инициаторами услуги,

системными аналитиками, архитекторами системы, программистами и конечными пользователями. Сложность проектирования повышается за счет необходимости учета аспектов информационной безопасности и создания защищенной информационной системы. Многие вопросы, связанные с информационной безопасностью, с которыми сегодня сталкиваются инфокоммуникационные компании, использующие бизнес-модель *MVNO*, могут быть успешно решены, если применить объектно-ориентированный анализ и проектирование при разработке и эксплуатации системы управления качества услуг и анализа рисками информационной безопасности.

Методика объектного моделирования

Многие вопросы, связанные с информационной безопасностью, с которыми сегодня сталкиваются компании, оказывающие инфокоммуникационные услуги на основе бизнес-модели *MVNO,* могут быть решены, если применить объектно-ориентированный подход на всех этапах жизненного цикла информационной системы *MVNO*. В частности, проектирование системы мониторинга и анализа рисками жизненного цикла, с использованием визуального языка моделирования *UML* позволяет оценить качество услуг в области информационной безопасности компании на ранних стадиях жизненного цикла [1-3].

Инфраструктура традиционного мобильного оператора *MNO (Mobile Network Operator)* состоит из трех уровней:

- Сеть радиодоступа (сеть базовых станций).
- Ядро голосовой сети и ядро пакетной сети (передача данных).
- Бизнес-приложения *OSS/BSS (Operation Support System/Business Support System,* системы планирования номерной емкости, управления качеством услуг, биллинга и т.д.).

Практически во всех развитых странах уровень проникновения мобильной радиотелефонной связи вплотную приблизился к 100%, а в ряде стран превышает эту отметку, поэтому развитие классических сетей сотовой подвижной связи возможно только за счет внедрения новых информационных услуг. Классическая вертикальная модель оказания услуг мобильной связи сдерживает внедрение новых информационных услуг в связи с необходимостью больших капитальных затрат. Сеть радиодоступа является наиболее дорогостоящей частью операторской инфраструктуры – затраты на ее строительство и лицензирование не сравнимы со стоимостью создания остальных уровней. Кроме того, внедрение новых информационных услуг требует других компетенций от специалистов, работающих в области телекоммуникаций. Предложенная в последнем десятилетии прошлого века бизнес-модель *MVNO* (операторов виртуальных сетей мобильной связи) позволила привлечь новых участников на рынок мобильной связи, не требуя от них затрат на строительство сети радиодоступа, так как они арендует готовую радиосеть у действующего традиционного оператора – *MNO* (рис. 1). [4, 5].

Количество *MVNO* продолжает расти, также продолжает расти количество «потребительских» *MVNO*. Ранее виртуальные операторы были более ориентированы на ценовую конкуренцию и голосовые услуги, то по мере заполнения рынка *MVNO* становятся «нишевыми» и пытаются предложить более широкий ассортимент дополнительных услуг, чем у уже существующих мобильных операторов. Эта стратегия представляется наиболее перспективной, поскольку успешный выход на рынок с «традиционным» перечнем услуг мобильного оператора возможен лишь при использовании ценовой конкуренции,

потенциал которой в условиях современной рыночной конъюнктуры сведен к минимуму. Другая возможность для *MVNO* – использование имеющейся инфраструктуры и других ресурсов «потребительских» компаний. Это позволяет значительно сократить переменные затраты, повышая рентабельность бизнеса или балансировать на точке безубыточности, принося пользу основному продукту или услуге бренда [1, 2, 6].

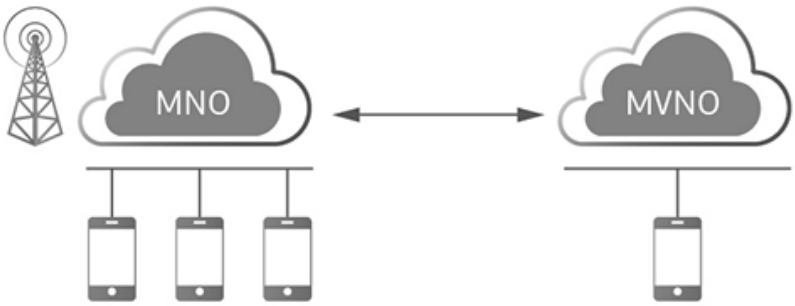

Рисунок 1

Успешность той или иной бизнес-модели зависит от того как решены вопросы информационной безопасности. Как операторы классических сетей мобильной связи, так и операторы виртуальных сетей не освобождаются от необходимости разработки системы мониторинга и оценки рисков.

Уровень информационной безопасности сети *MVNO* определяется окончательной величиной риска безопасности. Под риском безопасности, согласно терминологии *ETSI* (*European Telecommunications Standards Institute* / Европейский институт по стандартизации в области телекоммуникаций), понимается результат и степень опасности воздействия угрозы безопасности. По всем видам угроз безопасности определяется порог риска, который состоит в решении, по каким видам угроз необходимо принять процедуры оценки риска, а по каким нет. Выбор архитектуры безопасности сети *MVNO* (механизмов безопасности и средств управления безопасностью) в процессе проектирования позволяет составить окончательный остаточный риск (или уровень безопасности) для угрозы каждого вида[1] [1].

Для того чтобы проектировать информационную систему, необходимо руководствоваться стандартами[2,3,4,5]. *CASE*-средства (*Computer-Aided Software Engineering*) могут эффективно применяться на большинстве стадий процесса проектирования. Возможна реализация нескольких разновидностей *CASE*-

[1] Приказ ФСТЭК России №17. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Введ. 11.02.2013. – М: ФСТЭК России. – С. 37.

[2] Стандарты в области управления рисками информационной безопасности. [В интернете] URL: http://xn7sbab7afcqes2bn.xn--p1ai/content/standarty-v-oblastiupravleniya-riskami-informacionnoy-bezopasnosti

[3] ISO/IEC 15288:2008 «Системная инженерия – процессы жизненного цикла систем (Standard for Systems Engineering – System life cycle-processes). 2008.

[4] ГОСТ 34.601-90. Структура процесса проектирования автоматизированных систем, 1996.

[5] ГОСТ Р ИСО/МЭК 12207:2008. Процессы жизненного цикла программных средств, 2008.

методологий, зависящих от масштаба проекта и исходных условий, при которых будет вестись разработка [1, 5].

В качестве примера могут быть использованы следующие исходные условия:

- разрабатывается совершенно новая система;
- существует информационная система (ИС), которая может быть использована в качестве исходного прототипа или должна быть интегрирована с разработанной;
- разрабатывается типовая система, которая не является полным продуктом, но представляет собой комплекс компонентов, адаптированных к конкретным условиям;
- важнейшим требованием выступает быстрота разработки приложений;
- важнейшими признаются показатели проекта такие как управляемость, надежность и качество.

В зависимости от принятых требований, для разработки ИС могут быть использованы различные стандарты, учитывающие этапы и процессы жизненного цикла систем. Каждый процесс описывается набором его результатов, которые достигаются посредством различных видов деятельности и поддерживается компьютерными средствами системной инженерии.

Представленные в перечни работы будут описывать один типичный виток спиральной модели жизненного цикла информационной системы (ЖЦИС) в целом. На втором и последующих витках речь будет идти уже не о создании системы, а об очередной ее модернизации, например, в целях расширения прикладной функциональности. Результатом очередного витка спирали будет новое «поколение» системы. Визуальные модели создают четкость представления используемых архитектурных решений и позволяют понять, что система разрабатывается в полном объеме. Построение таких моделей позволяет сразу решить несколько характерных задач.

Во-первых, методика визуального моделирования допускает работу со сложными и очень сложными системами и проектами, к которым, в том числе, можно отнести сети *MVNO* [8].

Во-вторых, визуальные модели позволяют рационально осуществлять связь между операторами сетей *MVNO* и разработчиками новых сервисов.

В общем случае при реконструкции сложной ИС сети *MVNO* идет разделение на части, каждая из которых в процессе разработки рассматривается отдельно. Существует два разных способа разделения этого раздела на подсистемы: структурное (или функциональное) разделение и разбиение объектов (компонентов).

Если подход использует дизайн, в котором информационная система разделена на объекты (компоненты), то для визуального моделирования может использоваться унифицированный язык моделирования *UML* (*Unified Modeling Language*). С точки зрения визуального моделирования язык *UML* дает возможность предоставить инструменты для создания визуальных моделей, которые являются:

- одинаково понятными всем разработчикам, участвующим в создании проекта;
- средством сообщения в рамках создания проекта.

Модель *UML* – это совокупность конечного множества конструкций языка, главными из которых являются сущности и отношения между ними.

Диаграммы *UML* – это основная накладываемая на модель структура, которая облегчает создание и использование модели. Это графическое представление некоторой части графа модели.

Особенность использования *UML* заключается в том, что каждая модель (диаграмма) является самодостаточным взглядом на разрабатываемую систему и предназначена как для изложения проблем, так и для предложения решения. Самодостаточность моделей означает, что аналитик или разработчик может извлечь из конкретной модели всю необходимую ему информацию, не обращаясь к другим источникам.

Моделирование системы информационной безопасности

Модель системы ИБ (информационной безопасности) в компании-оператора сети *MVNO* представлена на рис. 2.

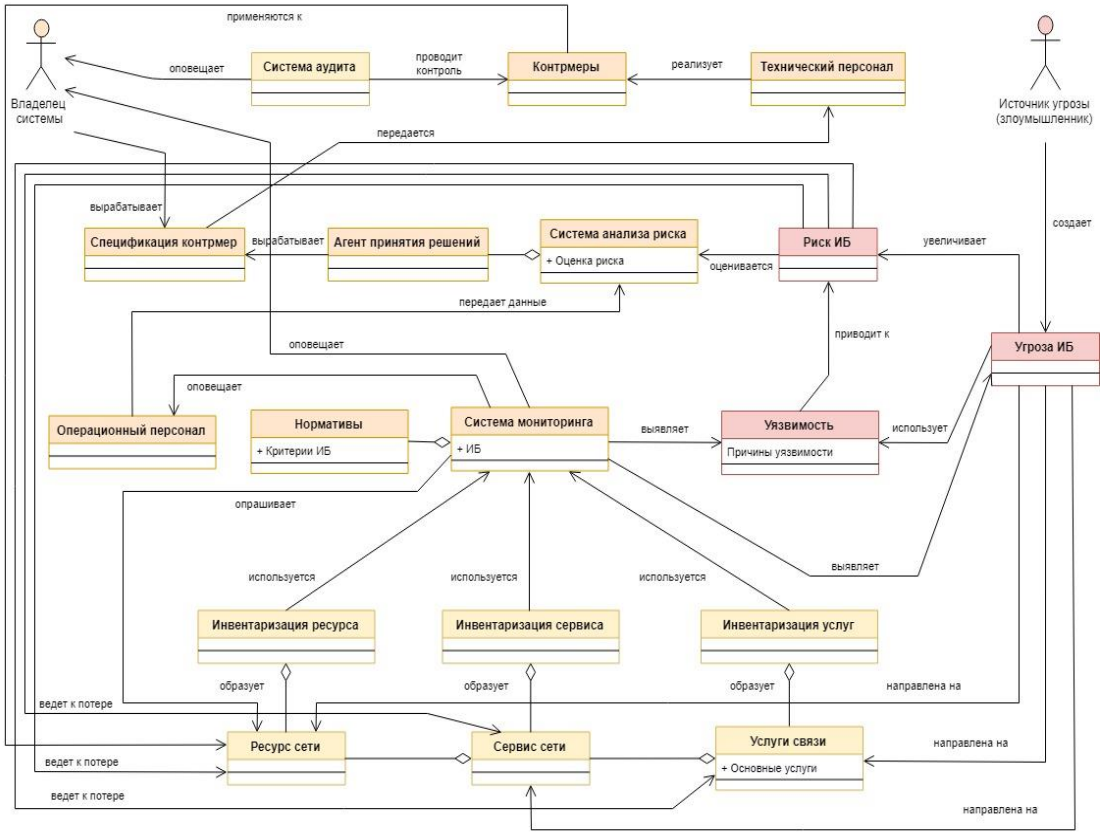

Рисунок 2

Разработанная модель системы ИБ представляет собой диаграмму классов, где основными действующими лицами являются:

- Владелец системы.
- Источник угрозы (злоумышленник).

Учитывая функциональную декомпозицию, активы системы представлены в виде следующих классов:

- Ресурс сети.
- Сервис сети.
- Услуги связи.

В целом данные активы системы образуют следующие классы:

- Инвентаризация ресурса.
- Инвентаризация сервиса.
- Инвентаризация услуг.

Источник угрозы (злоумышленник) создает угрозы, которые направлены на ресурс сети, сервис сети и услуги связи, используя для этого имеющиеся в ИС уязвимости. Каждая угроза безопасности увеличивает информационные риски, которые могут привести к потере ресурсов, сервисов и услуг сети.

Так как Владелец системы заинтересован в защите ресурсов, сервисов и услуг сети, он принимает решение о разработке контрмер по каждому типу известных уязвимостей.

Для защиты активов системы Владелец системы разрабатывает систему защиты, включающую в себя Систему мониторинга, выполняющую функции сбора информации о состоянии ресурсов, сервисов и услуг сети. При этом Система мониторинга выявляет уязвимости и предполагает причины уязвимости.

Каждая уязвимость создает риск для активов системы. Поэтому система мониторинга, обнаружив вторжение, формирует с помощью критериев безопасности сообщение и оповещает об инциденте Владельца системы, Оперативный персонал и Агента принятия решений.

Агент принятия решений, используя разработанные контрмеры, оповещает Технический персонал об их применении, который реализует данные контрмеры для управления ИБ, воздействуя на ресурсы сети.

Разработка модели системы управления рисками в сетях *MVNO*

Модель управления рисками в компании можно представить с помощью диаграммы классов (рис. 3). Она иллюстрирует сущности, задействованные в процессе управления рисками в компании, и отношения между ними [7-12].

На диаграмме видно, что Агент угроз создает угрозу ИБ, используя для этого имеющиеся в ИС уязвимости. При этом каждая угроза безопасности увеличивает риски.

В свою очередь Владелец системы, заинтересованный в защите активов компании, разрабатывает систему защиты, включающую в себя систему мониторинга.

Система мониторинга выявляет уязвимости и предполагает причины уязвимости. Каждая уязвимость создает риск для активов компании. Поэтому система мониторинга, обнаружив вторжение, формирует с помощью критериев безопасности сообщение и оповещает Оперативный персонал об инциденте.

Далее Операционный персонал передает данные в Систему анализа рисков, которая состоит из двух основных шагов:

1. Идентификация риска:

1.1 Введение в идентификацию риска.

1.2 Определение угроз.

1.3 Определение существующих или планируемых мер и средств контроля и управления.

1.4 Выявление уязвимостей.

1.5 Определение последствий при потере конфиденциальности, целостности или доступности активов.

2. Установление значения риска:

2.1 Методология установления значения риска.

2.2 Оценка последствий.

2.3 Установление значений уровня рисков.

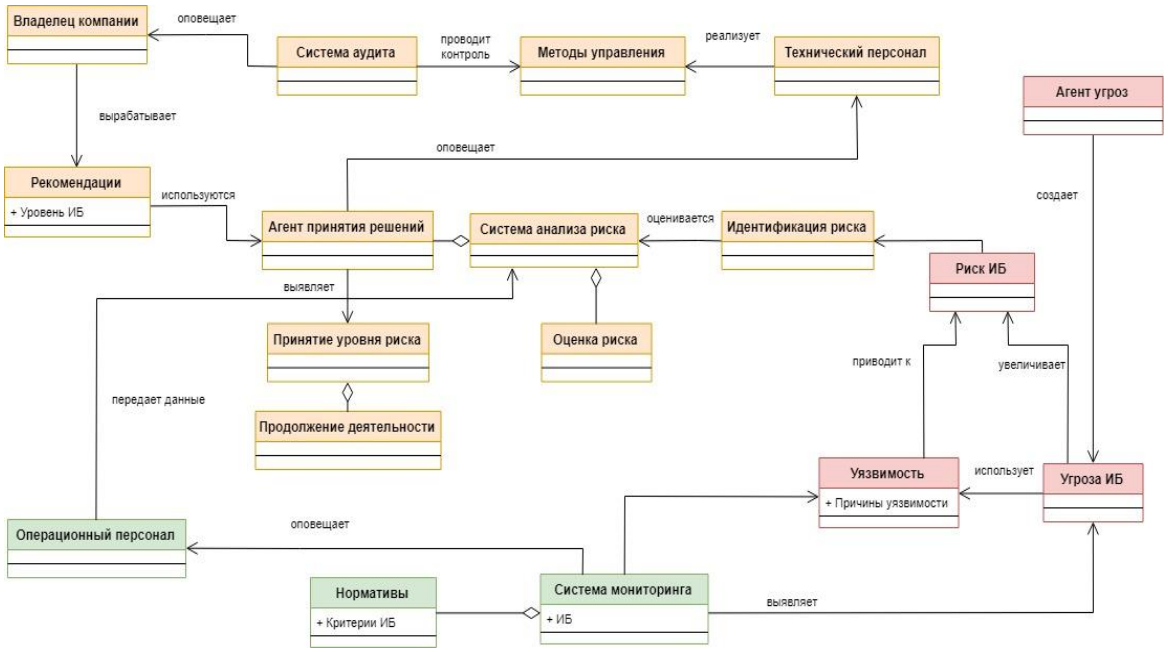

Рисунок 3

При обнаружении угрозы безопасности системе необходимо определить угрозу и оценку уровня безопасности по уровню воздействия:

- Нулевой.
- Средний.
- Высокий.

В зависимости от определенного уровня угрозы система принимает решение продолжать свою работу, либо прекратить ее.

Порядок проведения анализа рисков представлен на рис. 4.

В свою очередь, Агент принятия решений, используя разработанные методы управления, оповещает Технический персонал об их применении.

Задача Системы аудита объективно оценить – насколько текущее состояние ИБ компании соответствует предъявляемым требованиям и стандартам ИБ. Владельцу системы предоставляется аудиторский отчет, который содержит описание текущего состояния ИБ в компании, описание обнаруженных уязвимостей и рекомендации по их устранению.

Рис. 5 отражает диаграмму последовательности управления рисками в компании.

Основными элементами диаграммы последовательности являются объекты:

- Владелец компании.
- Качественный анализ рисков.
- Количественный анализ рисков.
- Проектирование сценария реагирования на риск.
- Проектирование сценария, расчет возможных сценариев по корректировке рисков.
- Управление и контроль рисками.

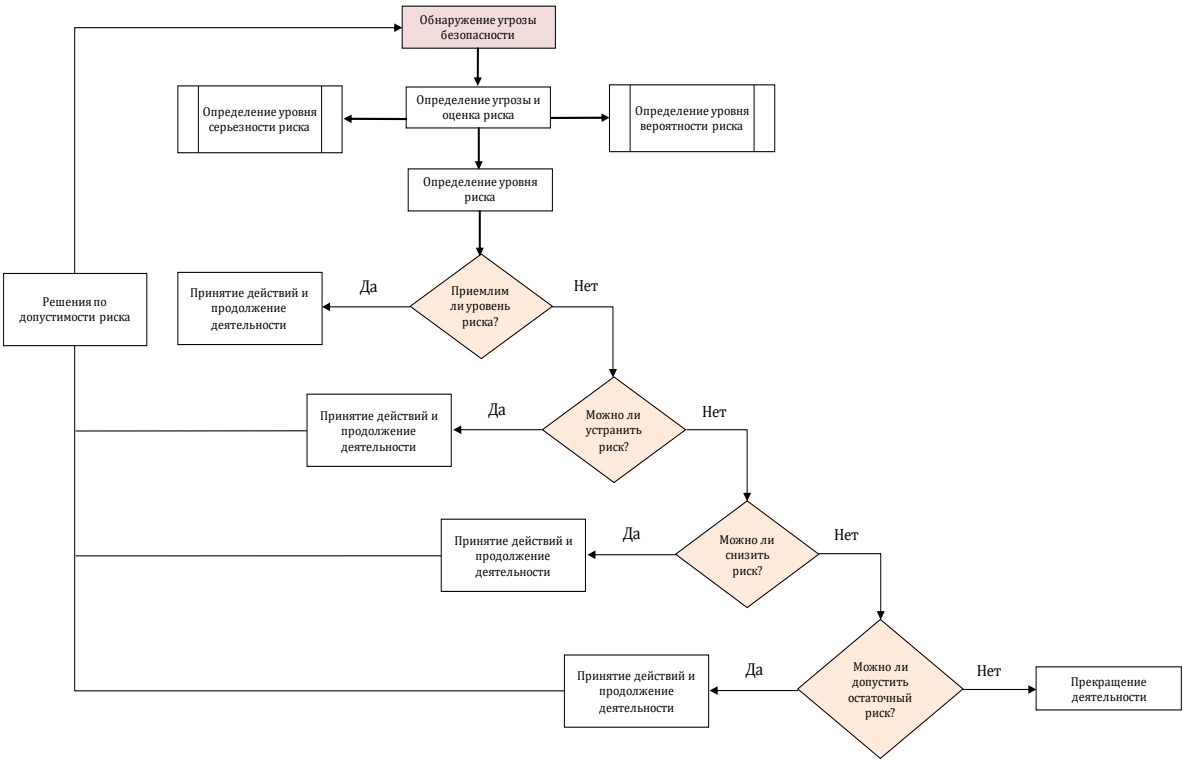

Рисунок 4

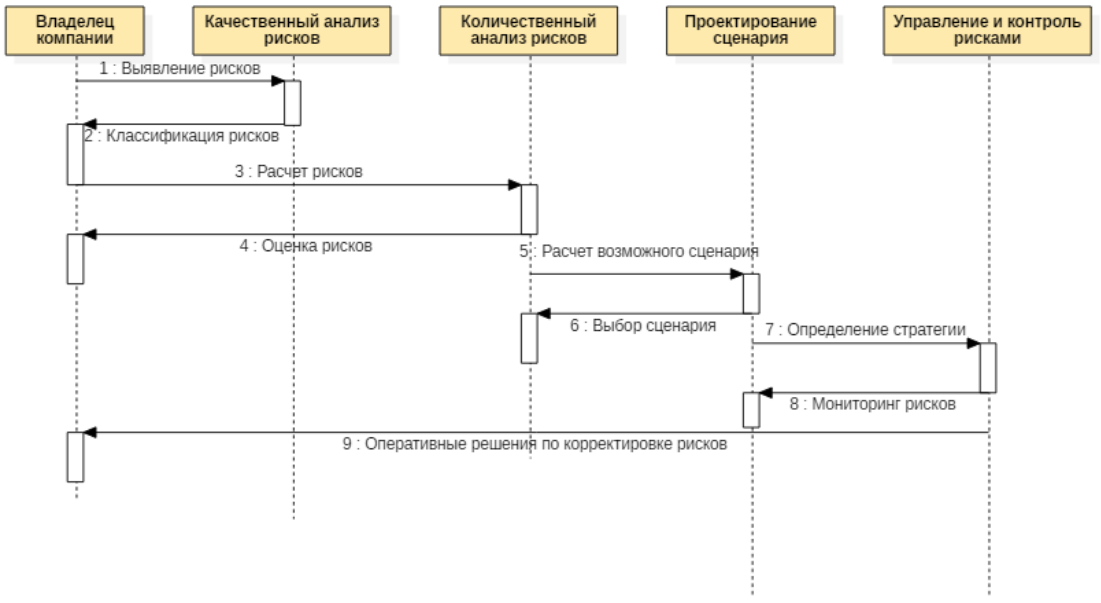

Рисунок 5

Важным аспектом в данной диаграмме является явное отображение течения времени, графические связи между элементами, взаимное расположение элементов на диаграмме и сообщения между ними.

Заключение

С помощью языка *UML,* который позволяет генерировать исходные данные в виде графического описания для моделирования объектов в программные коды, была разработана общая модель системы информационной безопасности и модель системы управления рисками в сетях *MVNO.*

Использование данной модели позволит максимизировать положительные и минимизировать отрицательные последствия наступления рисковых событий, сформировав базу данных компании в области управления рисками. Внедрение системы управления рисками способно также решить проблему появления непредвиденных рисков для компании, упростить принятие решений в области рисков и снизить затраты на управление рисками.

Данную модель можно использовать компании-оператору в качестве визуализированного представления взаимодействия отдельных компонентов системы в общей структуре системы информационной безопасности компании-оператора *MVNO.*

Литература

1. Максименко В.Н. Конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапе проектирования // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 11. – С. 57-64.
2. Максименко В.Н. Особенности оценки качества инфокоммуникационных услуг контакт-центра // T-Comm: Телекоммуникации и транспорт, 2010. – Т. 4. – № 10. – С. 39-41.
3. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сети сотовой подвижной связи // Известия ЮФУ. Технические науки, 2007. – № 4 (76). – С. 151-155.
4. Шинаков К.Е., Рытов М.Ю., Голембиовская О.М., Чиркова К.Ю. Оценка риска безопасности информационных систем, обрабатывающих конфиденциальную информацию // Вестник БГТУ, 2016. – № 2 (50). – С. 56-61.
5. Некрылова Н.В. Предпосылки реализации элементов управления рисками бизнес-процессов в стандартах на системы менеджмента промышленного предприятия // Известия высших учебных заведений. Поволжский регион. Общественные науки, 2015. – № 2 (34). – С. 204-215.
6. Беседина А.С., Панской К.М., Максименко В.Н. Анализ способов мошенничества информационной безопасности в виртуальных сетях операторов сотовой связи // Экономика и качество систем связи, 2019. – № 1(3).
7. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи, 2017. – № 2 (4). – С 42-48.
8. Максименко В.Н., Филиппов А.А. Центр обработки данных в структуре системы управления качеством оператора сотовой связи // T-Comm: Телекоммуникации и транспорт, 2008. – Т. 2. – № 6. – С. 47-51.
9. Долгова Н.Д., Максименко В.Н. Анализ алгоритмов вычисления уровня доверия к пользователю в социальной сети // в сборнике: технологии информационного общества Материалы XIII Международной отраслевой научно-технической конференции, 2019. – С. 345-348.
10. Максименко В.Н. Категорный подход к исследованию аспектов защиты информации и управления качеством сервисов и услуг в сетях сотовой подвижной связи // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 9. – С. 41-49.

11. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи, 2017. – № 2 (4). – С. 42-48.
12. Максименко В.Н., Даричева А.Н. Методические подходы к оценке качества услуг контакт-центра // Экономика и качество систем связи, 2017. – № 1 (3). – С. 79-88.