**Федеральное государственное образовательное бюджетное учреждение высшего образования**

**«Финансовый университет при Правительстве Российской Федерации» (Финансовый университет)  
Факультет «Информационных Технологий и Анализа Больших Данных»**

**Департамент «Информационная безопасность»**

**Контрольная работа:**

«Моделирование в AnyLogic»

**Выполнил:**

студент кафедры ИБ,

группа ИБ18-3,

Гильмутдинов Ринат

**Проверил работу:**

Кораблёв Юрий Александрович

Москва – 2020

Оглавление

[**Задача** 3](#_Toc58399277)

[**Описание задачи** 4](#_Toc58399278)

[**Модель** 5](#_Toc58399279)

[**Блок сообщений сотрудников** 5](#_Toc58399280)

[**Диаграмма состояний сотрудников** 6](#_Toc58399281)

[**Системно-динамическая диаграмма на основе потоков** 8](#_Toc58399282)

[**График количества сотрудников по статусу безопасности** 8](#_Toc58399283)

[**Результаты моделирования** 12](#_Toc58399284)

[**Выводы** 14](#_Toc58399285)

# **Задача**

Я выполнил моделирование в AnyLogic, выбрав тему корпоративной информационной безопасности. В своей работе я рассмотрел проблему «появления ям и просадок информационной безопасности».

Модель позволяет решить следующую задачу:

Сотрудники компании сталкиваются со сбоями в работе их персональных компьютеров. Часто подобные проблемы могут привести к утечке информации, потому что их устройства на время становятся уязвимыми. В таком случае сотрудник создаёт обращение в службу поддержки информационной безопасности, затем начинает ожидать помощь. Чтобы решить проблему, у технической поддержки время ограничено. При потере 10 единиц безопасности, сотрудник становится под угрозой. Чтобы вывести такого сотрудника снова в нормальное состояние, необходимо принять либо пассивные, либо активные методы решения проблем.

Необходимо сделать следующие выводы:

Какое оптимальное количество сотрудников технической поддержки по информационной безопасности необходимо, чтобы решить проблемы пользователей вовремя? За оптимальное количество принято такое количество, когда только часть сотрудников департамента информационной безопасности задействована в помощи. При этом общее состояние информационной безопасности в компании среди всех сотрудников должно быть на уровне 75%.

Инструменты и средства, которыми мы обладаем:

Мы не будем углубляться в разные виды средств и возьмём в качестве инструментов устранения угроз и решения проблем с ними следующее: во-первых, сотрудники могут делиться советами друг с другом и помогать, такой способ будет пассивным и малоэффективным, он будет прибавлять 1 единицу безопасности; во-вторых, мы можем внедрять различные субъекты информационной безопасности (опытные специалисты, антивирусы, сетевые фильтры, политики безопасности), которые будут улучшать состояние безопасности активно, в таком случае будет прибавляться 5 единиц безопасности.

# **Описание задачи**

Рассмотренная мною проблема основывается на нехватке ресурсов субъектов информационной безопасности, к которым могут относиться активные участники процессов в деятельности обеспечения информационной безопасности, воздействующие на объект информационной безопасности независимо от характера этого воздействия: наносящего ущерб, разрушение или противодействующего этому. В своей работе за предмет субъекта ИБ я взял сотрудников департамента информационной безопасности некой организации, где численность сотрудников составляет 200 человек.

Мы должны решить проблему «ям и просадок информационной безопасности». Что же это такое?

**Ямы и просадки информационной безопасности** - момент во времени, когда устремляется поток запросов на оказание поддержки информационной безопасности или появляются инциденты, но служба информационной безопасности не способна вовремя решить их, потому что появляется нехватка ресурсов. Нехватка ресурсов может быть вызвана как отсутствием субъектов информационной безопасности, так и занятости этих субъектов.

Основное исследование построено на расчёте оптимальности пула ресурсов для решения проблем с информационной безопасности, где пул представляет из себя службу безопасности, а изменение значения внедрённых субъектов – процент сотрудников службы безопасности, выделенных на решение инцидентов.

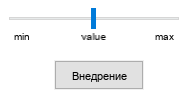
Сотрудники организации, у которых нет проблем и инцидентов, связанных с информационной безопасностью, представлены «зелёными персонами». Сотрудники организации, у которых есть проблемы и инциденты, связанные с информационной безопасностью, представлены «красными персонами».

# **Модель**

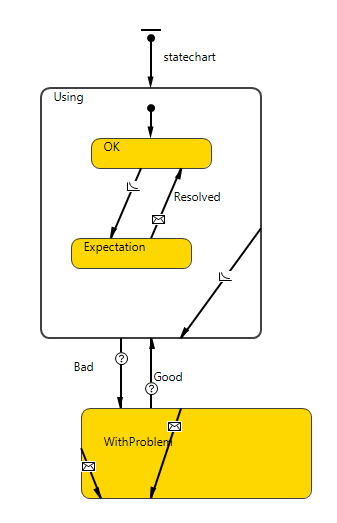
Модель состоит из четырёх частей: блока «сообщений» сотрудников, диаграммы состояний сотрудников, системно-динамической диаграммы на основе потоков, графика количества сотрудников по статусу безопасности.

**Блок сообщений сотрудников.** Он начинает работать, когда на вход (“enter”) подаётся команда из-за перехода состояния сотрудника (“OK” 🡪 “Expectation”). Далее в качестве очереди выступает блок “queue”. Затем блок задержки ‘administratorsActions’, который отвечает за вместимость обращений сотрудника: изначально его значение равняется 50. В самом конце блок “problemSolved”, который передаёт Сотрудникам (“employee”) сообщение, что обращение выполнено. Ещё есть кнопка «Внедрение», которое отвечает за активное улучшение безопасности в компании за счёт внедрения средств, её действие основано на функции deliverToAllAgentsInside(), которая доставляет сообщение ‘Внедрение субъектов безопасности’ всем агентам.



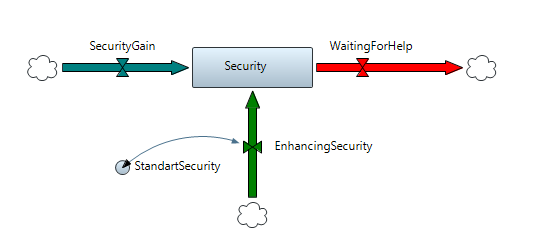


**Диаграмма состояний сотрудников.** Состоит из двух основных диаграмм – нормальное состояние (“Using”) и проблемное состояние (“WithProblem”). Внутри первого существуют ещё два состояния “OK” и “Expectation”, которые меняются из-за статуса сообщений, которые создал агент. Внутри второго существуют два перехода, которые реагируют на получаемые извне сообщения об изменении состояния безопасности. Переход между двумя внешними состояниями осуществляется по двум переходам “Bad” и “Good” в зависимости от изменений значения “Security”.



1. ‘Using’:
   1. При входе в основное состояние ‘Using’ персоны окрашиваются в зелёный цвет для индикации, что у них всё хорошо;
   2. При входе в состояние ‘OK’ осуществляется генерация нового сообщения (агента Appeal), которое подаётся на процессинговый блок ‘enter’;
   3. Затем происходит вход в состояние ‘Expectation’, из которого агент Employee может перейти, если получит сообщение ‘Внедрено’, свидетельствующее, что работа с его обращением завершена.
   4. Также в ‘Using’ есть переход ‘NewSubject’, который отправляет раз в 12 секунд сообщение ‘Улучшение состояния ИБ’ случайному агенту Employee, если единицы безопасности более 5;
   5. Если обращение сотрудника не могут долго выполнить и уровень безопасности опускается, то происходит переход ‘Bad’.
2. ‘WithProblem’:
   1. При входе в основное состояние ‘WithProblem’ персоны окрашиваются в красный цвет для индикации, что у них есть проблемы;
   2. Первый переход ‘NewSubjectEffect’ происходит в момент, когда агент получает сообщение "Улучшение состояния ИБ". Он является показателем пассивного улучшения безопасности в компании;
   3. Второй переход ‘IntroductionEffect’ происходит в момент, когда агент получает сообщение "Внедрение субъектов безопасности". Он является показателем активного улучшения безопасности в компании и происходит, когда жмут кнопку «Внедрение».
   4. В случае выхода из проблемной ситуации происходит переход ‘Good’, если значение Security хотя бы равно 0.

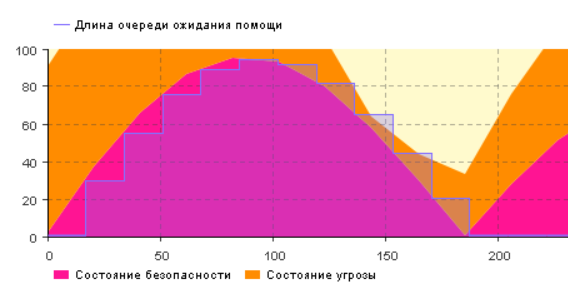
**Системно-динамическая диаграмма на основе потоков.** Данная диаграмма отвечает за изменение значения “Security” на основе положительных потоков “SecurityGain” (корпоративное состояние ИБ растёт пассивно), “EnhancingSecurity” (задействуются новые силы) и отрицательного потока “WaitingForHelp” (необходимое количество сообщений сотрудников не может быть исполнено).



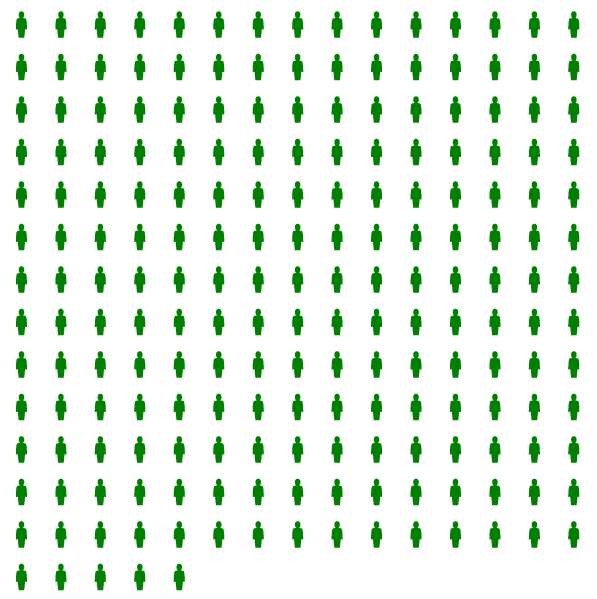
В данном случае реализация довольно простая, поскольку потоки имеют одну логику, отличаясь лишь положительным или отрицательным статусом воздействия на безопасность. В их основе лежит функция inState(), которая проверяет, является ли для агента Employee активным указанное состояние диаграммы состояний.

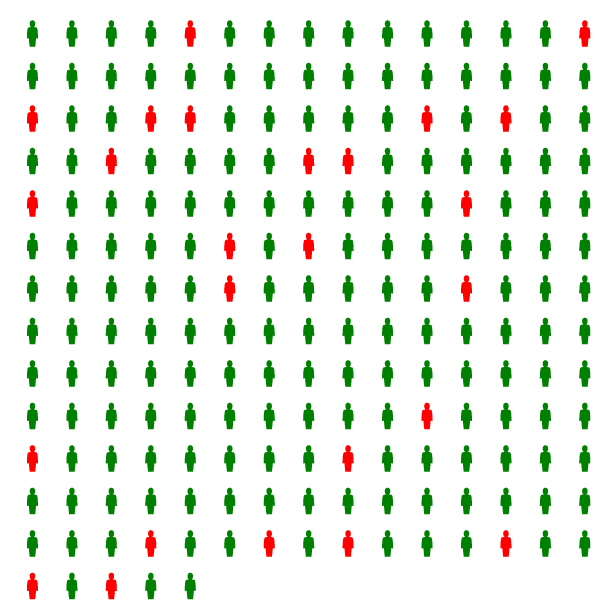
**График количества сотрудников по статусу безопасности.** Значения данного графика зависят от количества сотрудников, которые находятся в состоянии “Using”. Значения состояний безопасности и угрозы вычисляются на основе количества таких сотрудников и общего количества сотрудников. В качестве статистики используется переменная ‘numberUsing’: она вычисляет значение количества на основе функции inState(), где за нужное состояние считается ‘Using’.

Для наглядности Временная диаграмма с накоплениями, которая отображается количество сотрудников слита с Временным графиков, который отображает длину очереди. Такое слияние нужно, потому что невозможно на временной диаграмме разместить динамическое значение size(), так как оно просто не будет отображаться.



В самом начале запуска моделирования все сотрудники не имеют проблем:



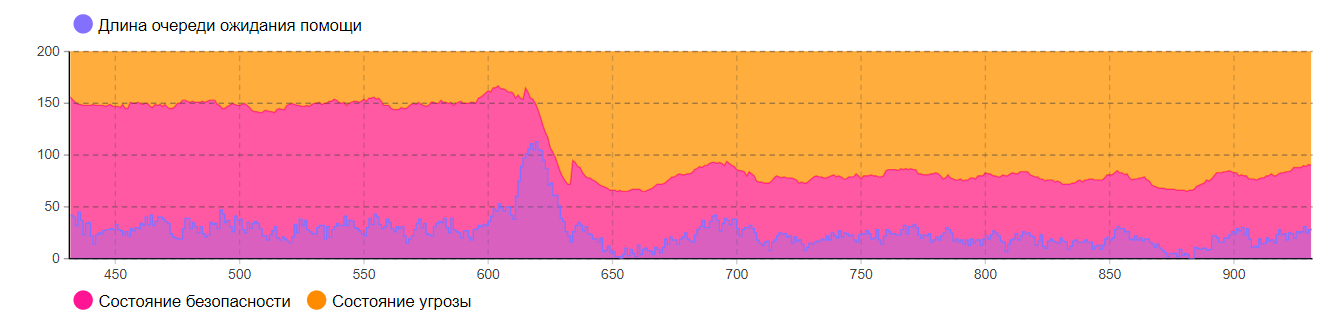
По истечению времени начинают появляться запросы на помощь, то есть у сотрудников появляются проблемы, они становятся «красными»:

Нахождение в состоянии «информационной опасности» происходит до тех пор, пока проблемы не будут устранены. Затем сотрудников переходит в рабочее состояние, то есть в состояние «информационной безопасности».

Можно увидеть, что запросы сотрудников и их состояние тоже отслеживаются. Время и задержка исполнения запросов изменяется прямо пропорционально изменению пулу субъектов, направленных на устранение инцидентов.

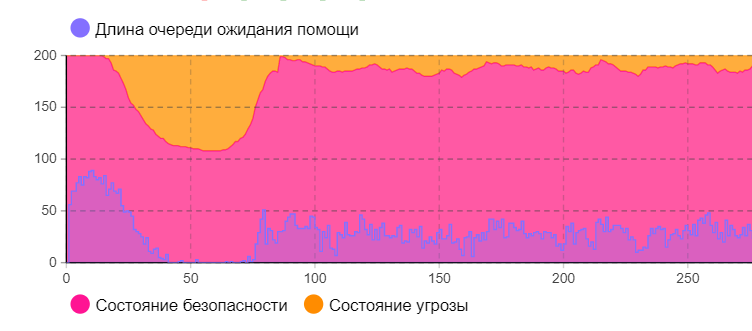
# **Результаты моделирования**

При внедрении 30 ресурсов субъектов, начинается сильная просадка, образуется яма инцидентов:



При внедрении 80 ресурсов субъектов, начинается сильная просадка, образуется яма инцидентов:

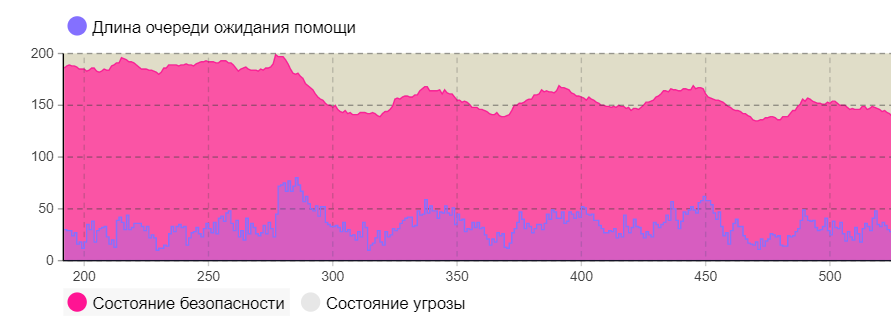




После различных вариантов найти наиболее оптимальный набор субъектов для решения инцидентов информационной безопасности, а именно движении ползунка от 0 до 100, я остановился на 60:



Видно, что просадки имеются, но они не такие большие, обращения сотрудников не находятся долго в очереди:



# **Выводы**

Моя работа посвящена рассмотрению влияния количества ресурсов на своевременное решение проблем, связанных с информационной безопасностью. За критерии решения и определения оптимального выделения ресурсов принято экспертное мнение. Экспертное мнение связано с допустимостью количества сотрудников, находящихся в состоянии информационной угрозы. Как видно по графику ниже, в состоянии безопасности постоянно находится около 75% персонала, что является вполне допустимой нормой.

Таким образом, при найденных параметрах, а именно при количестве обслуживающих единиц 60, условие решения задачи соблюдается. Так как 150 из 200 сотрудников находятся постоянно в безопасности, при этом 40 сотрудников департамента информационной безопасности свободны от технической поддержки.

