УДК 004.056.5
DOI 10.33764/2618-981X-2024-6-248-255

А. Ю. Солдатов[1], К. А. Иванов[1], В. В. Селифанов[1]*

Вопросы построения модели системы управления угрозами информационной безопасности

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: dglasmann@mail.ru

Аннотация. На сегодняшний день построение системы управления угрозами является важной задачей в области обеспечения информационной безопасности. Для полноценного обеспечения функциональности всей системы защиты необходимо обеспечить корректную работу подсистемы управления угрозами. Это необходимо для актуализации конфигурации системы в случае появления новых угроз безопасности информации для конкретной защищаемой системы после внедрения изменений в эту систему. В связи с тем, что оценка доверия и качества работы системы управления угрозами является масштабной и трудозатратной активностью, в статье показано создание модели такой системы и проведена ее оценка. В качестве метода исследования было использовано имитационное моделирование и модель типа «система массового обслуживания». Приведены результаты построения модели системы управления угрозами и варианты ее применения. Для построения модели используется прикладное программное обеспечение AnyLogic. Построенная имитационная модель позволяет наглядно рассмотреть и изучить процесс оценки угроз безопасности информации для последующего применения полученных знаний в построении системы защиты.

Ключевые слова: имитационное моделирование, оценка угроз безопасности информации, anylogic

A. Yu. Soldatov[1], K. A. Ivanov[1], V. V. Selifanov[1]*

Issues of building a model of information security threat management system

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: dglasmann@mail.ru

Abstract. Today, building a threat management system is an important task in the field of information security. To fully ensure the functionality of the entire protection system, it is necessary to ensure the correct operation of the threat management subsystem. This is necessary to update the system configuration in case of new threats to information security for a particular protected system after the introduction of changes to this system. Due to the fact that the assessment of trust and quality of the threat management system is a large-scale and labor-consuming activity, the paper shows the creation of a model of such a system and its evaluation. Simulation modeling and mass service system type model were used as a research method. The results of building a model of threat management system, and variants of its application are given. AnyLogic application software is used to build the model.

Keywords: imitation modeling, information security threat assessment, anylogic

Введение

В настоящее время одним из наиболее приоритетных вопросов стоит вопрос обеспечения информационной безопасности. Для построения системы защиты объекта, в том числе и оптико-электронных приборов и систем, необходимо понимать, от каких угроз строить эту систему защиты. В данном случае требуется построить модель угроз объекта защиты. На текущий момент для оценки угроз безопасности информации можно руководствоваться методикой ФСТЭК 2021 года, в которой поэтапно расписано, как определить угрозы безопасности информации. В результате моделирования угроз составляется перечень актуальных угроз, их сценарии реализации с перечислением тактик и соответствующих техник. Если в информационной системе случается смена или обновление конфигурации, то угрозы необходимо оценивать заново. Это происходит непрерывно в течение всего жизненного цикла информационной системы до момента вывода ее из эксплуатации [1-3].

Прежде чем приступать к решению конкретных задач в области информационной безопасности, необходимо провести предварительное моделирование процессов в математической форме, ведь это представляет собой ценный инструмент для последующего анализа. Построение модели процесса управления угрозами и является текущей задачей [4-6].

В последствии, чтобы понять, насколько системе управления угрозами информационной безопасности можно доверять, необходимо провести оценку ее доверия. Но оценивать систему на реальном объекте считается трудозатратной и дорогостоящей задачей, и, в связи с этим принято решение создать модель данной системы и провести оценку при применении этой модели. Далее в статье дается обоснование применения имитационного моделирования и модели типа «система массового обслуживания» [10-13].

Обоснование применения имитационного моделирования

Перед построением модели стояла задача в выборе типа моделирования. После изучения различных научных методов было выбрано имитационное моделирование. Это метод исследования, при котором изучаемая система заменяется моделью, с достаточной точностью описывающей реальную систему, с которой проводятся эксперименты с целью получения информации об этой системе. Такая модель удобна тем, что в ней можно задавать различные вводные данные, изменять параметры для получения различных результатов, гибко настраивать параметры. Использование имитационного моделирования позволяет провести анализ различных аспектов эффективности, включая производительность, надежность, эффективное использование ресурсов и пропускную способность. Это обеспечивает основу для принятия обоснованных решений на основе данных, полученных в хорошо контролируемой среде, что позволяет минимизировать риски и затраты [14-18].

С использованием метода имитационного моделирования исследуются аналогичные задачи, такие как анализ эффективности методов моделирования рас-

пределенной системы электронного документооборота с целью оптимизации бизнес-процессов. [7, 8].

Построение модели

Для создания модели используется программное обеспечение AnyLogic. Данный инструмент обладает современным графическим интерфейсом и позволяет использовать язык Java для разработки моделей.

В качестве основы для построения модели будет использоваться алгоритм определения угроз безопасности информации в соответствии с Методикой ФСТЭК. На основании данной методики была построена схема алгоритма определения угроз по нотации idef0 (рис. 1)

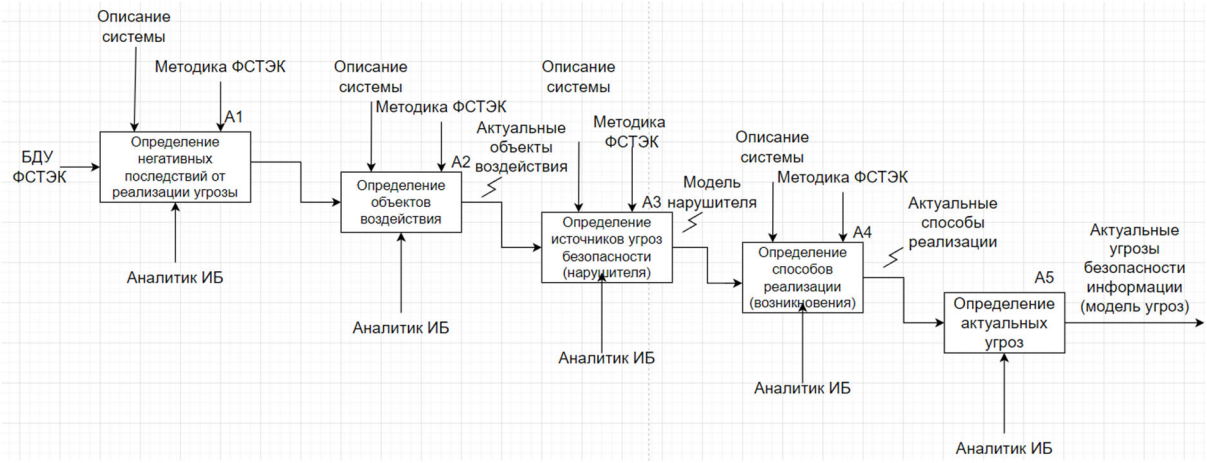

Рис. 1. Блок-схема процесса алгоритма определения угроз по нотации idef0

Сам алгоритм состоит из пяти этапов, с помощью которых выявляются актуальные угрозы безопасности информации [9]:

– определение негативных последствий от реализации угроз безопасности информации;

– определение объектов воздействия угроз безопасности информации;

– определение источников угроз безопасности информации, категории нарушителей и уровень их возможностей;

– оценка способов реализации угроз безопасности информации;

– оценка актуальности угроз безопасности информации.

Для полного представления работы алгоритма разработана схема, на основе которой осуществлена разработка сервиса (рис. 2).

Угроза считается актуальной, если для нее возможен хотя бы один сценарий реализации [9, 19].

Для актуализации угроз безопасности информации в рамках жизненного цикла необходимо принимать во внимание такие характеристики системы, как риски и инциденты безопасности. Для этого информация о них будет включена в математическую модель защиты объекта, в том числе и оптико-электронных приборов и систем.

Применяя всю описанную выше информацию, построена комьютерная модель системы управления угрозами информационной безопасности (рис. 3).

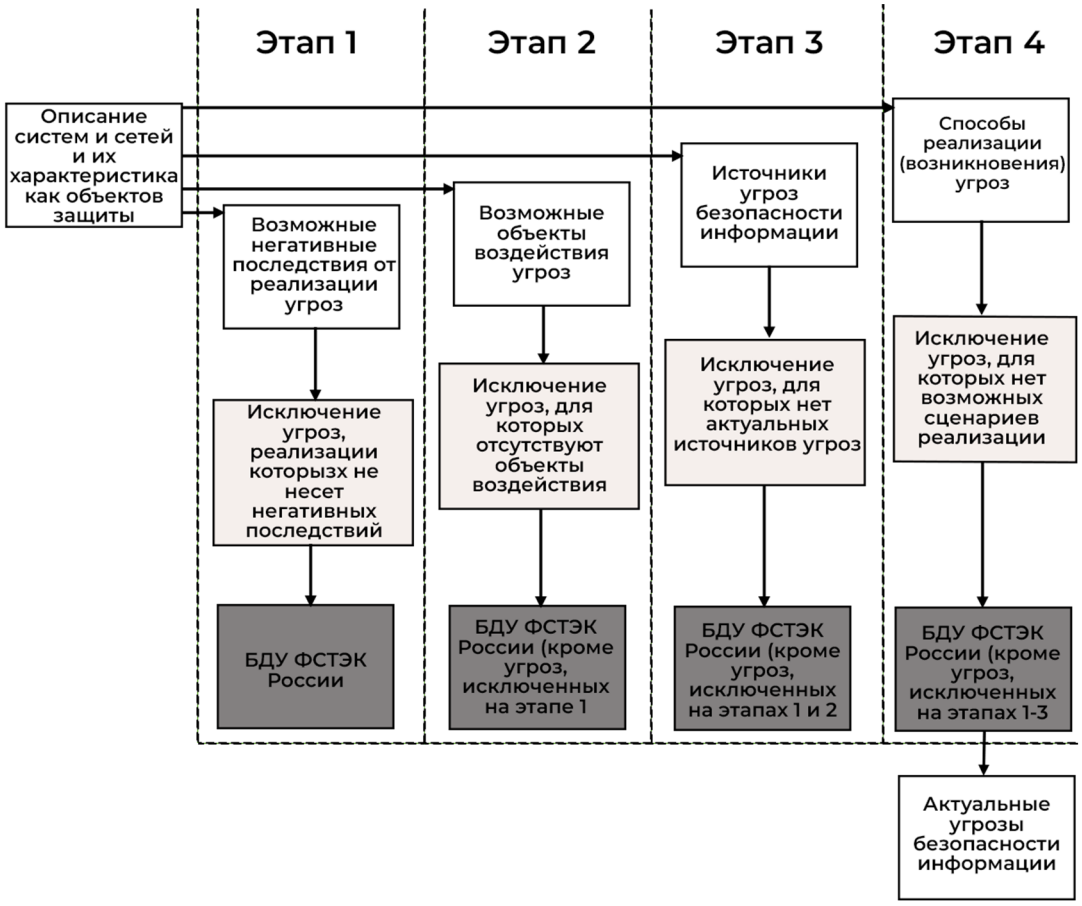

Рис. 2. Детализированное описание алгоритма определения угроз

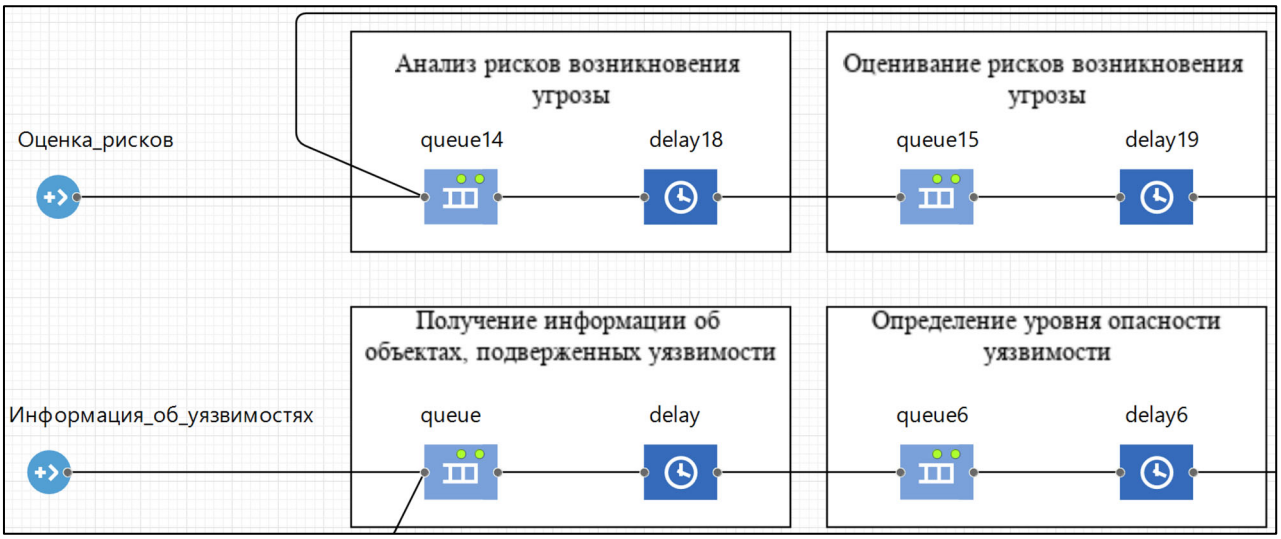

Рис. 3. Фрагмент построенной модели

При запуске системы можно наблюдать поступление агентов и их прохождеие через каждый блок (рис. 4).

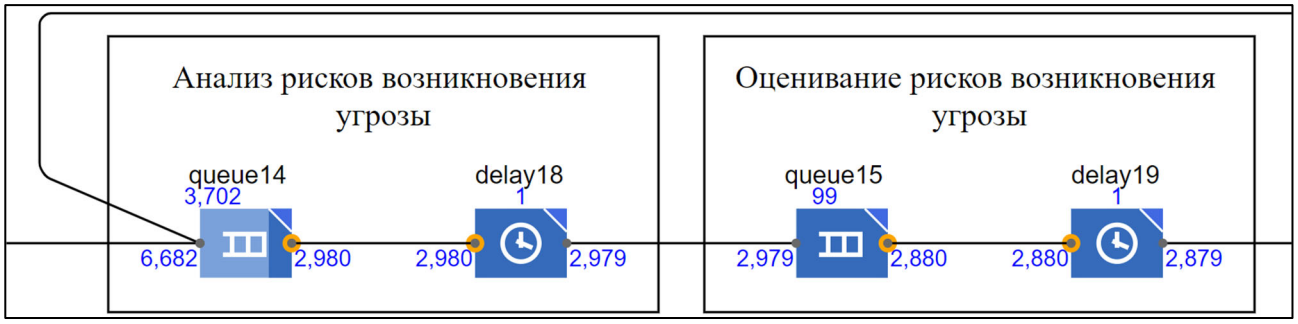

Рис. 4. Демонстрация поступления агентов

Также можно наблюдать наполняемость каждой очереди (рис. 5).

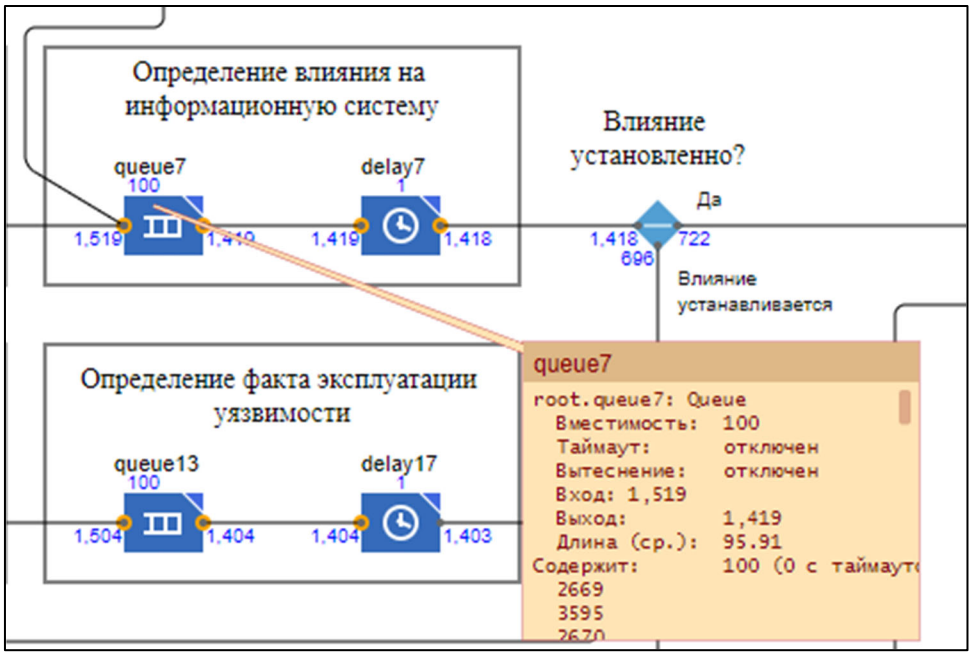

Рис. 5. Характеристики блока очереди

Благодаря возможности изучения каждого узла модели в отдельности, становится возможным проводить детальный анализ воздействия изменений параметров на конкретные элементы системы. Это обеспечивает более точную настройку модели и позволяет улучшить ее точность и реалистичность отражения реальных процессов. Такой подход позволяет более эффективно проводить оптимизацию процессов и принимать обоснованные решения на основе результатов моделирования. Ниже приведен фрагмент кода программы на языке программирования Java (рис. 6).

```
453         } else if (ao == this.selectOutput2) {
454             return "selectOutput2";
455         } else if (ao == this.queue16) {
456             return "queue16";
457         } else {
458             return ao == this.delay20 ? "delay20" : super.getNameOf(ao);
459         }
460     }
461
        no usages
462     public AgentAnimationSettings getAnimationSettingsOf(Agent ao) {
463         return super.getAnimationSettingsOf(ao);
464     }
465
        no usages
466     public String getNameOf(AgentList<?> aolist) { return super.getNameOf(aolist); }
469
        no usages
470     public AgentAnimationSettings getAnimationSettingsOf(AgentList<?> aolist) {
471         return super.getAnimationSettingsOf(aolist);
472     }
473
        no usages
474     protected Source<Agent> instantiate_Аномальная_активность_xjal() {
475         Source<Agent> _result_xjal = new Source(this.getEngine(), this, (AgentList)null);
476         return _result_xjal;
477     }
```

Рис. 6. Фрагмент кода программы

Информация о результатах работы имитационной модели выглядит в виде количественных характеристиках (вместимость очереди, таймаут, средняя длина, количество агентов на входе и на выходе).

Заключение

Построена модель системы управления угрозами безопасности информации. Данная модель может быть полезна перед вводом системы в промышленную эксплуатацию в инфраструктуру и позволяет подробно оценить процесс оценки угроз [20-22].

Компьютерная модель системы управления угрозами информационной безопасности, учитывающая такие характеристики элементов системы, как важность информации об уязвимостях, аномальных активностях в оптико-электронных приборах и системах, а также погрешность при оценке рисков, позволяет наглядно оценить процесс управления угрозами в системе и эффективность управления этими угрозами. Наглядность модели системы управления угрозами информационной безопасности проявляется в возможности визуализации важных характеристик элементов системы и их взаимосвязей. Это позволяет участникам процесса управления угрозами наглядно увидеть динамику изменения уровня рисков, вы-

явить уязвимые места и проследить влияние различных факторов на общую картину безопасности системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аверьянов В. С. О некоторых вопросах, идеях и технологических решениях в области квантового распределения ключей безопасности / В. С. Аверьянов // Информационная безопасность : Сборник докладов Всероссийской Школы молодых ученых, Новосибирск, 14–18 ноября 2022 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – С. 34-39. – DOI 10.55648/978-5-91434-080-0-2022-34-39.

2 . Алексеев А. Л. Об одном способе защиты интерфейса взаимодействия квантовой аппаратуры распределения ключей и средств криптографической защиты информации / А. Л. Алексеев, В. И. Егоров, А. Ю. Щербаков // Вестник современных цифровых технологий. – 2021. – № 9. – С. 15-18.

3. Бобков Е. О. Применение технологии квантового распределения ключей в волоконно-оптических линиях связи / Е. О. Бобков, Е. А. Балашова, А. В. Крыжановский // Научный альманах Центрального Черноземья. – 2022. – № 1-4. – С. 29-36.

4. Габдулхаков И. М. Построение многоканальной системы квантового распределения ключей с частотным кодированием / И. М. Габдулхаков, О. Г. Морозов // Инженерный вестник Дона. – 2020. – № 5(65). – С. 53.

5. Габдулхаков И. М. Принципы построения универсальной системы квантового распределения ключей с частотным кодированиемна основе амплитудной модуляции и фазовой коммутации / И. М. Габдулхаков, О. Г. Морозов // Актуальные вопросы телекоммуникаций : Научно-техническая конференция Росинфоком-2017, Самара, 01 сентября 2017 года / Федеральное агентство связи; Департамент информационных технологий и связи Самарской области; Поволжский государственный университет телекоммуникаций и информатики; Научно-исследовательский институт радио. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. – С. 81-82.

6. Грицкевич Е. В. Компьютерный анализ систем оптотехники и информационной безопасности : учеб. пособие / Е. В. Грицкевич, П. А. Звягинцева. – Новосибирск : СГУГиТ, 2017. – 70 с.

7. Жилин С. В. Квантовое распределение ключей по беспроводному оптическому каналу связи / С. В. Жилин, В. В. Архипенко, Е. С. Басан // Компьютерные и информационные технологии в науке, инженерии и управлении (КомТех-2022) : Материалы Всероссийской научно-технической конференции с международным участием. В двух томах, Таганрог, 08–10 июня 2022 года. – Таганрог: Южный федеральный университет, 2022. – С. 194-200.

8. Луценко С. А. Способ квантового распределения ключей в облачных сетях / С. А. Луценко, П. В. Заика, С. Ю. Козлов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции, Санкт-Петербург, 11–12 октября 2017 года. – Санкт-Петербург: Федеральное государственное казенное военное обра-зовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации, 2017. – С. 218-220.

9. Методика оценки угроз безопасности информации. – Текст : электронный // Федеральная служба по техническому и экспортному контролю : [сайт]. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 20.12.2023).

10. Патент № 2326442 C1 Российская Федерация, МПК G07C 3/00, G06F 17/00. Способ оценки эффективности управления и устройство для его осуществления : № 2007102742/09 : заявл. 24.01.2007 : опубл. 10.06.2008 / В. А. Селифанов, В. В. Селифанов ; заявитель Селифанов Валерий Анатольевич.

11. Патент № 2503985 C2 Российская Федерация, МПК G05B 15/00. Способ двухуровневого управления техническими средствами и система для его осуществления : № 2012105841/08 : заявл. 17.02.2012 : опубл. 10.01.2014 / В. А. Селифанов ; заявитель Федеральное государственное военное образовательное учреждение высшего профессионального образования «Военный авиационный инженерный университет» (г. Воронеж) Министерства обороны Российской Федерации.

12. Патент № 2621605 C Российская Федерация, МПК H04L 9/08, H04B 10/00, G06F 21/60. Сеть квантового распределения ключей : № 2015141966 : заявл. 02.10.2015 : опубл. 06.06.2017 / К. С. Кравцов, С. П. Кулик, С. Н. Молотков [и др.] ; заявитель Российская Федерация, от имени которой выступает Фонд перспективных исследований.

13. Патент № 2665096 C1 Российская Федерация, МПК G05B 15/00. Способ двухуровневого управления и система для его осуществления (варианты) : № 2018113685 : заявл. 13.04.2018 : опубл. 28.08.2018 / В. А. Селифанов ; заявитель Селифанов Валерий Анатольевич.

14. Патент № 2706175 C1 Российская Федерация, МПК H04L 9/08, G06F 21/72. Способ квантового распределения ключей в однопроходной системе квантового распределения ключей : № 2018146854 : заявл. 27.12.2018 : опубл. 14.11.2019 / А. Г. Втюрина, К. А. Балыгин, В. И. Зайцев [и др.] ; заявитель Открытое акционерное общество «Информационные технологии и коммуникаци-онные системы».

15. Патент № 2741264 C1 Российская Федерация, МПК G05B 15/00. Спо-соб двухуровневого управления техническими средствами (варианты) : № 2020122379 : заявл. 07.07.2020 : опубл. 22.01.2021 / В. А. Селифанов, В. В. Селифанов, А. В. Селифанов ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

16. Патент № 2747626 C1 Российская Федерация, МПК G05B 15/02. Способ двухуровневого управления и система управления для его осуществления (варианты) : № 2020114340 : заявл. 22.04.2020 : опубл. 11.05.2021 / В. А. Селифанов, В. В. Селифанов, А. В. Селифанов ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

17. Патент № 2752844 C1 Российская Федерация, МПК H04L 9/08. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты) : № 2020140774 : заявл. 10.12.2020 : опубл. 11.08.2021 / А. Е. Жиляев ; заявитель Акционерное общество «Информационные технологии и коммуникационные системы».

18. Патент № US 5301344 A. Multibus sequential processor to perform in parallel a plurality of reconfigurable logic operations on a plurality of data sets : заявл. 29.01.1991 : опубл. 05.04.1994 / Alexander Kolchinskiy ; заявитель Analogic Corp.

19. Румянцев К. Е. Безопасность режима синхронизации системы квантового распределения ключей / К. Е. Румянцев, А. П. Пленкин // Известия ЮФУ. Технические науки. – 2015. – № 5(166). – С. 135-152.

20. Свидетельство о государственной регистрации программы для ЭВМ № 2022663610 Российская Федерация. Имитационная модель процессов трех-уровневого автоматизированного управления техническими средствами № 2461859-1 : № 2022660418 : заявл. 07.06.2022 : опубл. 18.07.2022 / В. А. Селифанов, А. В. Селифанов, В. В. Селифанов.

21. Свидетельство о государственной регистрации программы для ЭВМ № 2022683792 Российская Федерация. ViPNet Модуль оптоэлектронный клиента квантового распределения ключей : № 2022683156 : заявл. 28.11.2022 : опубл. 08.12.2022 ; заявитель Акционерное общество «Информационные технологии и коммуникационные системы».

22. Kosari A. Unilateral information reconciliation schemes FO quantum key distribution system / A. Kosari // Проблемы инфокоммуникаций. – 2021. – No. 2(14). – P. 44-50.