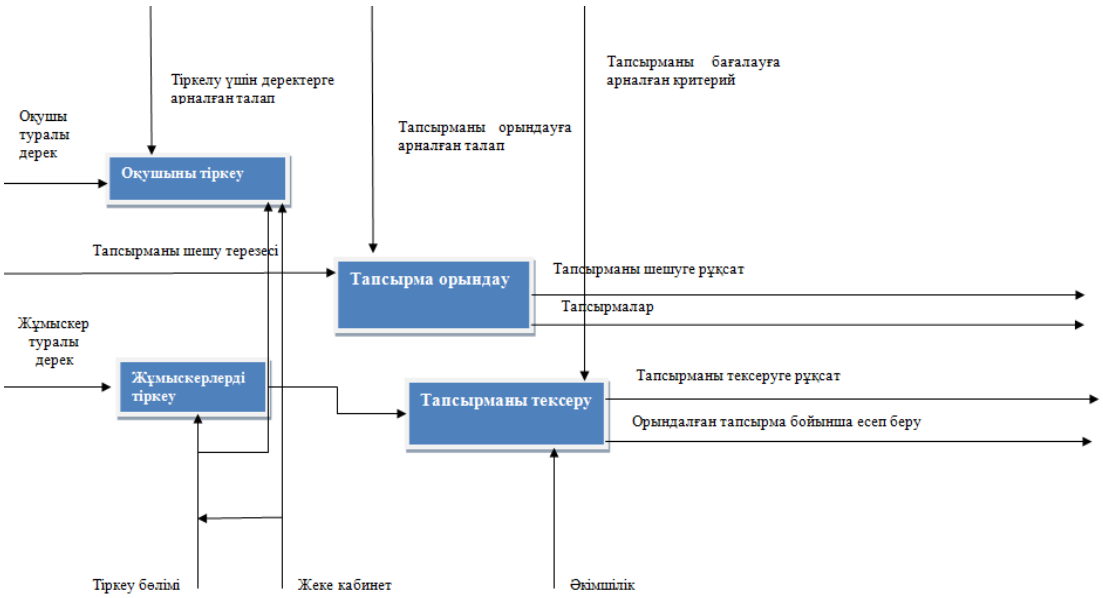

5-сурет. Тапсырманы орындау бизнес-процесінің моделі

«Тапсырманы орындау» процесінің негізгі қатысушылары-оқушылар және қызметкерлер. Сурет 5-те көрсетілгендей оқушы жүйеге кірген жағдайда ең бірінші өзі туралы деректі толтырады, дерек тіркелу процесін қанағаттандыратын талаптарға сай болуы тиіс. Дәл осы процесс жұмыскерлерге де қатысты, яғни олар ең алдымен «тіркеу бөлімі»-нен өтіп, келесі процесске аяқ басады. «Тапсырманы шешу» терезесіне өтіп, оқушы тапсырманы орындауға кіріседі. Бірақ, тапсырманы шешу және тапсырманы тексеру әрекеттері тікелей «әкімшілік» рұқсатымен жүзеге асады. Тапсырманы тексеру әрекеті тапсырманы бағалауға арналған критерийлер арқылы орындалады. Тексерілген тапсырма бойынша есеп беру және бағалауды сақтау орындалуы тиіс.

Қорытындылай келгенде, білім базасына негізделген шешімдерді қабылдауды қолдайтын жүйе процесін модельдеу әр салада, яғни оқу орындарынан бастап үлкен өндіріс орындарының жұмысын оңтайландыру мақсатында қолданылады.

Пайдаланылған әдебиеттер

1. Кулаичев А.П. Методы и средства комплексного анализа данных: Учебное пособие / А.П. Кулаичев. — М.: Форум, 2018. — 160 с.
2. Похилько А.Ф. Case-технология моделирования процессов с использованием средств BPWIN и ERWIN учебное пособие. -Ульяновск: УлГТУ, 2008. -120 с.
3. Халин В.Г., Чернова Г.В. Системы поддержки принятия решений.-Юрайт, 2017. -496 с.
4. Моделирование бизнес-процессов с помощью IDEF0, DFD, BPMN за 7 дней: учеб. пособие / И.В. Миндалѐв; Краснояр. гос. аграр. ун-т. – Красноярск, 2018. – 123 с
5. Цуканова О. А. Методология и инструментарий моделирования бизнеспроцессов: учебное пособие – СПб.: Университет ИТМО

УДК 004.056.55: 003.26

МОДЕЛИ И ТЕХНИКИ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Әбдіраман Әлия Серғалиқызы
a.s.abdiraman@gmail.com

докторант кафедры «системы информационной безопасности» Факультета информационных технологии ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Нурушева А.М.

Объекты информационно-коммуникационной инфраструктуры (ИКИ) при работе с данными сталкиваются с такими атаками информационной безопасности, как подмена, подслушивание, перехват, задержка передачи данных и так далее [1]. Основной задачей обеспечения информационной безопасности объектов ICI является обеспечение конфиденциальности, целостности и доступности данных, передаваемых по их линиям связи. Стоит отметить, что проблема перехвата данных в информационной безопасности все чаще встречается в системах спутниковой связи из-за слабой защиты линий передачи данных [2]. Кроме того, зафиксировано множество фактов перехвата навигационных данных, передаваемых по системам спутниковой связи [3-5].

Система спутниковой навигации является одной из точных систем для обеспечения координации движения судов, самолетов, поездов и других транспортных средств, использующих эту систему. По сравнению с традиционными радионавигационными системами спутниковые навигационные системы обладают рядом преимуществ. Использование спутниковой навигационной системы обеспечивает транспортным средствам высокую точность определения координат. В свою очередь, дальность полета спутников позволяет охватывать большую часть земной поверхности, чем наземные системы связи, использующие простые антенные устройства [6]. Кроме того, при работе со спутниковыми навигационными системами транспортные средства не испытывают помех при передаче сигнала из-за прямой видимости, что снижает вероятность искажения сигнала. Однако из-за низкого уровня информационной безопасности спутниковые навигационные системы подвержены атакам подмены.

Спуфинг – это перехват данных при их передаче с объекта А на объект В. Такого рода атаки часто осуществляются по слабо защищенным линиям связи.

Обсуждение. Чтобы составить модель информационной безопасности для передачи данных через спутник, необходимо определить активы системы. В таблице 1 показаны активы системы и критерий безопасности системы.

Таблица 1 – Активы и критерий безопасности системы

Бизнес-активы	**информация**, передаваемая между пользователями, **резервные данные пользователей**, навигационная информация с самолетов, судов
ИТ-активы	Сегмент заказчика - приемник, Космический сегмент – ретранслятор, наземная станция-передатчик
Критерий безопасности	Конфиденциальность информации пользователей и резервных копий, целостность резервных данных

Результат. В таблице 2 показан примерный сценарий перехвата навигационных данных при передаче по спутнику. Этот сценарий будет использоваться при построении модели безопасности, которая показана на рисунке 1.

Как видно из таблицы 2, при передаче данных необходимо обеспечить конфиденциальность и целостность информации. Сценарий осуществления атаки на координаты средств транспортировки выглядит следующим образом.

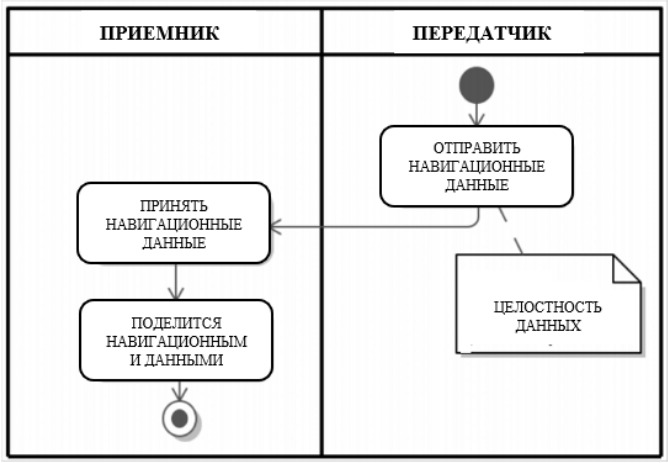

Рисунок 1 – Модель системы

Таблица 2 – Сценарий перехвата навигационных данных

ИТ-актив	Приемник
Уязвимость	откройте доступ к информации, настроив приемник на нужную частоту
Угроза ИБ	злоумышленник может получить доступ к навигационным данным самолетов и судов и при желании изменить их
Метод атаки	1. Установить приемник на правильную частоту 2. Сбор переданной информации
Злоумышлинник	взламывает системы навигации кораблей/самолетов, для этого он должен знать, как шифровать координаты кораблей/самолетов, разбираться в криптографии, может украсть навигационные данные.
Влияние	сводить на нет конфиденциальность информации пользователя Вред ретранслятору, нет информации о транспортировке пользователя Вред получателю – он не может принять информацию
Риск ИБ	Злоумышлинник, который знает, как шифровать координаты кораблей / самолетов. Настраивает приемник на правильную частоту и собирает информацию о связи из-за открытого доступа к информации на желаемой частоте приемника, что приводит к нарушению конфиденциальности информации пользователя и наносит ущерб информации о транспортировке пользователя и самого приемника.

При передаче навигационных данных со спутника на транспортные средства злоумышленник осуществляет атаку подмены (спуфинг), что приводит к перехвату и подмене данных. В свою очередь, подмена навигационных данных приводит к различным авариям транспортных средств и представляет собой потерю человеческих ресурсов. Таким образом, нарушается целостность и конфиденциальность навигационных данных транспортных средств.

Спуфинговые атаки осуществляются на физическом уровне. Для обеспечения конфиденциальности передаваемой информации предлагается использовать шифрование данных перед передачей на транспортные средства. Также предлагается использовать алгоритм верификации для проверки данных. Модель предотвращения рисков

информационной безопасности для спутниковых сетей выглядит следующим образом как представлено на рисунке 2.

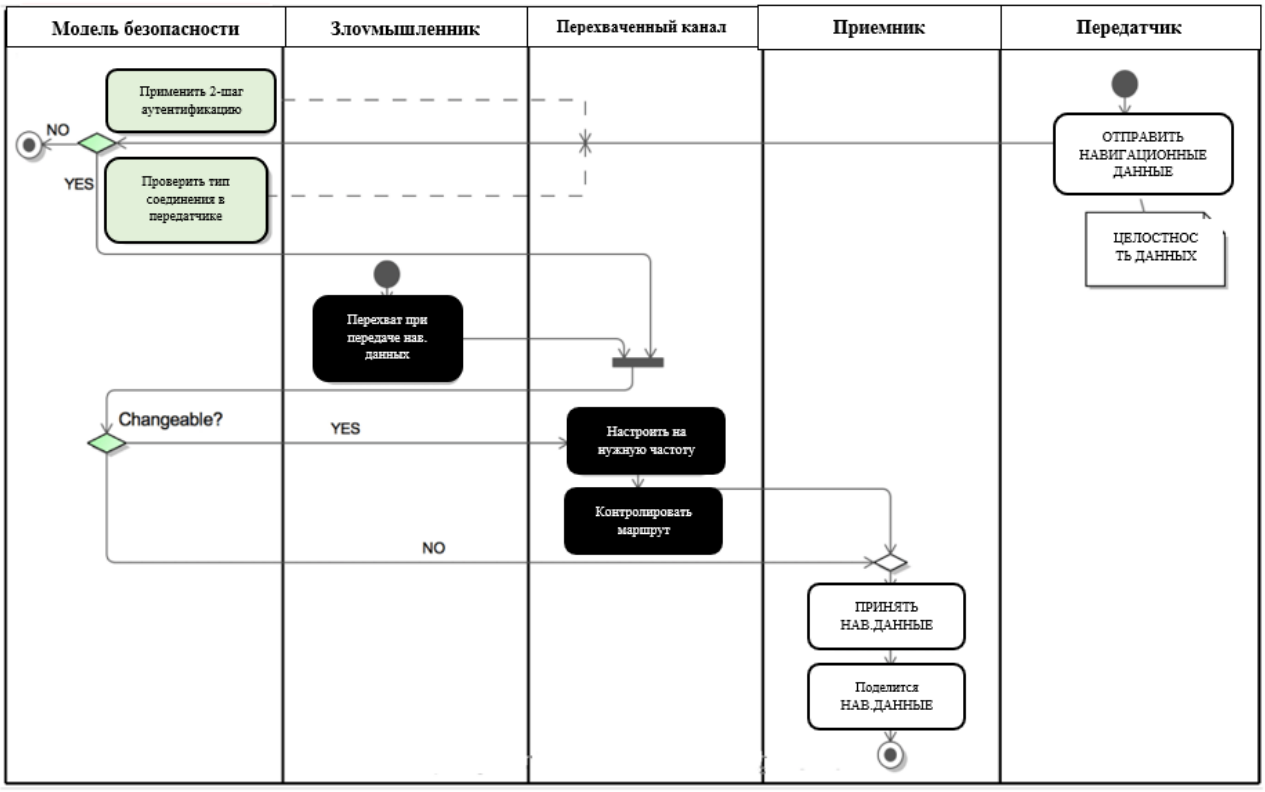

Рисунок 2 – Модель предотвращения рисков информационной безопасности при спуфинговых атаках на спутниковые сети

Вывод. В данной статье представлены модели безопасности передачи навигационных данных через системы спутниковой связи. Кратко описаны существующие проблемы информационной безопасности в спутниковых системах. Был расследован перехват информации во время ее передачи через спутник. Также предложен алгоритм предотвращения такого рода угроз информационной безопасности.

Эта работа была выполнена в рамках проекта с грантовым финансированием Министерства образования и науки Республики Казахстан, номер гранта AP13067916.

Список использованных источников

1 Di, A., Ruisheng, S., Lan, L., & Yueming, L. (2019). On the Large-Scale Traffic DDoS Threat of Space Backbone Network. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)

2 Zhu, Z., Yin, H., Zhang, Z., Li, T., Liu, J., Khoussainov, B., & Xu, C. (2021). Exploring active attacks for three incorrect implementations of the ISO/IEC 9798 in satellite networks. Computer Communications.

3 James Pavur, Daniel Moser, Vincent Lenders, Ivan Martinovic. (2019). Secrets in the sky: on privacy and infrastructure security in DVB-S satellite broadband. WiSec '19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks.

4 James Pavur, Ivan Martinovic. (2021).On Detecting Deception in Space Situational Awareness. ASIA CCS '21: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security.

5 Martin Strohmeier, James Pavur, Ivan Martinovic, Vincent Lenders. (2021) Studying Neutrality in Cyber-Space: a Comparative Geographical Analysis of Honeypot Responses. Critical Information Infrastructures Security: 16th International Conference.
6 Matulevicius, R. (2017). ˇ Fundamentals of secure system modelling. Springer

УДК 004.855.5

СОЗДАНИЕ СИСТЕМЫ МОНИТОРИНГА И КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ РАСПОЗНАВАНИЯ ОБРАЗОВ

Бейсенов Меирбек Канатович
meirbek.b2k@gmail.com
Студент НАО Торайгыров Университет, Павлодар, Казахстан
Научный руководитель – С.Н. Талипов

Введение. В период глобальной пандемии благодаря Covid-19 и его вариации – Omicron, в высоком приоритете является цель – свести шансы заражения вирусами к нулю. И в этом могут помочь сами машины, если обучить их распознавать соблюдает ли человек такую легкую нефармацевтическую меру защиты, как ношение медицинской маски. А также выделить, насколько доступно автоматизировать монотонные задачи при помощи искусственного интеллекта, который все больше и больше применяется для выполнения простых и монотонных задач, и чем больше людей будут в этом заинтересованы, тем быстрее это произойдет. Эксперты в области машинного обучения прогнозируют автоматизацию более половины рабочих мест в ближайшие 20 лет.

Целью данной статьи является внесение вклада в общественное здравоохранение и демонстрация по использованию ИИ для автоматизации повседневных задач, путем разработки специального программного продукта с использованием искусственного интеллекта.

Мною была разработана система мониторинга и контроля доступа на основе распознавания образов, которая распознает маски на лицах в реальном времени. Для разработки были применены наиболее актуальные инструменты в области распознавания объектов:

- Платформа Anaconda с Jupyter Notebook, так как она более удобна для выполнения проектов науки о данных благодаря интерактивному запуску кода, прямому взаимодействию с оболочкой системы и документирования в Markdown;
- Язык программирования Python, так как он обладает наилучшей инфраструктурой/экосистемой для разработки проекта и является самым высоко используемым языком для машинного обучения;
- LabelImg для графической аннотации новых данных для обучения;
- OpenCV – производительная и многофункциональная библиотека компьютерного видения;
- Tensorflow – платформа машинного и глубокого обучения, предоставляющая отдельные пакеты для обучения на центральном процессоре или видеокарте;
- CUDA от NVIDIA – библиотека, позволяющая выполнять обучение нейронных сетей и прочие вычислительные задачи при помощи видеокарты;
- Библиотека cuDNN для значительного ускорения видеокарты при глубинном обучении нейронных сетей на видеокартах, поддерживающих CUDA;
- SSD MobileNet V2 FPNLite 320x320 – предварительно обученная модель обнаружения объектов.

Программа может использоваться во всех помещениях, где требуется обязательное ношение маски, тем самым значительно снижая риск заражения инфекциями.

Искусственный интеллект, компьютерное видение, машинное обучение являются