УДК 004
DOI 10.52575/2687-0932-2023-50-1-203-210

Использование искусственного интеллекта в системах обеспечения комплексной безопасности охраняемого объекта

Офицеров А.И., Сафонов Д.А.
Федеральное государственное казенное военное образовательное учреждение высшего образования
«Академия Федеральной службы охраны Российской Федерации»,
Россия, 302015, Орел, ул. Приборостроительная, д. 35
E-mail: oficerow@mail.ru, daniilsa2020@gmail.com

Аннотация. В данной статье рассматривается возможность повышения эффективности функционирования систем интеллектуального мониторинга и оперативного оповещения в случаях выявления негативных факторов при построении комплексной безопасности охраняемого объекта. Описываются преимущества и недостатки нейронных сетей, а также рассматриваются метод и модель построения самообучающейся нейронной сети с возможностью интеллектуального мониторинга и реагирования на возникающие угрозы системы безопасности. В заключении определена обоснованность и возможность внедрения нейросетевых структур в алгоритм интеллектуального мониторинга состояния охраняемого объекта, применения таких сетей в условиях обеспечения комплексной безопасности охраняемого объекта, что позволит повысить их помехозащищенность и быстроту реагирования на угрозы и, как итог, гарантировать правильное принятие решение оператором.

Ключевые слова: искусственный интеллект, нейронная сеть, охраняемый объект, система обеспечения комплексной безопасности, угрозы, самообучающая среда

Для цитирования: Офицеров А.И., Сафонов Д.А. 2023. Использование искусственного интеллекта в системах обеспечения комплексной безопасности охраняемого объекта. Экономика. Информатика, 50(1): 203–210. DOI 10.52575/2687-0932-2023-50-1-203-210

The Use of Artificial Intelligence in Systems for Ensuring the Integrated Security of a Protected Object

Alexander I. Ofitserov, Daniil A. Safonov
The Federal state government
military educational institution of higher education
«The Academy of the Federal Guard Service of the Russian Federation»,
35 Priborostroitelnaya St, Orel, 302015, Russia
E-mail: oficerow@mail.ru, daniilsa2020@gmail.com

Abstract. This article discusses the possibility of improving the efficiency of the functioning of intelligent monitoring and prompt notification systems in cases of identifying negative factors in the construction of the integrated security of a protected facility. The advantages and disadvantages of neural networks are described, as well as the method and model for building a self-learning neural network with the ability to intelligently monitor and respond to emerging threats to the security system are considered. In conclusion, the validity and possibility of introducing neural network structures into the algorithm for intelligent monitoring of the state of a protected object, the use of such networks in the context of ensuring the integrated security of a protected object, is determined, which will increase their noise immunity and responsiveness to threats and, as a result, to guarantee the correct acceptance the decision the operator.

Keywords: artificial intelligence, neural network, protected object, integrated security system, threats, self-learning environment

For citation: Ofitserov A.I., Safonov D.A. 2023. The Use of Artificial Intelligence in Systems for Ensuring the Integrated Security of a Protected Object. Economics. Information technologies, 50(1): 203–210 (in Russian). DOI 10.52575/2687-0932-2023-50-1-203-210

Введение

В современной цивилизации уровень угроз с каждым годом развивается, исходя из тенденций и вызовов политической, социальной и военной обстановки. Для того, чтобы идти в ногу со временем и успешно отвечать на все те вызовы, которые возникают и наносят ущерб охраняемым объектам, необходимо внедрять высокотехнологичные системы видеонаблюдения с системной аналитикой на базе искусственного интеллекта, которые будут способны выявить и идентифицировать любые потенциальные угрозы. Помимо криминализации различного рода угроз, существуют угрозы техногенного и природного характера, на которые также необходимо быстрое реагирование.

Актуальность использования самообучающихся нейронных сетей сейчас достаточно высока, так как для этого есть все ресурсы [Rashid, 2016; Прохоров, 2021]. Если мы обратимся к недостаткам обычных видеодетекторов, то в своем большинстве они имеют низкую устойчивость к помехам. Это обуславливается, в первую очередь, загруженностью нашего окружающего мира, наличием теней, бликов, а также не исключается факт проблем самой оптики. Вследствие этого оператору технических средств охраны и видеонаблюдения приходится постоянно следить за большим количеством бессмысленных изменений картинки на мониторе. Здесь на помощь в современных условиях приходит нейросеть, так как в хаосе помех она способна отличать по определенным параметрам те или иные явления, процессы и объекты [Yang, 2018]. Многие нейросети сейчас могут классифицировать цели по различным признакам, что значительно облегчает работу оператору и повышает защиту объекта от различного рода уязвимостей. Помимо помех, извещатели обнаружения движения и сигнализации могут сработать в ненастную погоду. Все эти ложные срабатывания системы охраны требуют участия и проверок со стороны человека.

Преимущества и недостатки нейронных сетей

Нейронные сети – это адаптивные системы для обработки и анализа данных, которые представляют собой математическую структуру, имитирующую некоторые аспекты работы человеческого мозга и демонстрирующие его возможности, такие как способность к неформальному обучению, способность к обобщению и кластеризации неклассифицированной информации, способность самостоятельно строить прогнозы на основе уже предъявленных временных рядов.

Главной отличительной чертой и преимуществом нейронных сетей перед традиционными способами является возможность их самообучения [Асадуллаев, 2017]. Сам процесс обучения нейронных сетей происходит путем поиска коэффициентных связей между нейронами. В своем процессе обучения нейросеть может выявлять различные конструктивно-тяжелые зависимости между входными, выходными данными и производить обобщение.

Выделяют некоторые преимущества нейросетей, которые позволяют их использовать в вопросе обеспечения безопасности:

- при успешном и верном обучении сети имеется возможность распознавать те моменты, которые невозможно спрогнозировать при использовании простых систем;
- эффективная коррекция выходных данных путем алгоритмического обучения (таким образом, системы получаются самообучаемы);
- возможность проведения сложного анализа, который на выходе прогнозирует данные с целью выявления новых угроз, возникающих в ходе различных активностей, и производит классификацию событий.

Существует также ряд недостатков использования нейронной сети в системах обеспечения комплексной безопасности:

- значительные затраты вычислительных мощностей в процессе обучения системы;
- дорогостоящее программное обеспечение, а также оборудование, создающие в совокупности систему искусственного интеллекта комплексной системы безопасности;
- обязательное наличие специально обученного оператора на случай сбоев программного обеспечения.

Таким образом, использование нейросетей увеличивает безопасность критически уязвимых охраняемых объектов. При успешном обучении нейросеть может создавать правильный результат на основе предоставленных ей данных, которые отсутствовали, были неполными или на них оказывали действия помехи различного уровня. Благодаря этому использование нейронных сетей в вопросе обеспечения безопасности охраняемых объектов является перспективным и активно входит в практическое использование, так как позволяет минимизировать участие человека в процессе прогнозирования угроз и наблюдения за охраняемым объектом [Perkins, 2015].

Применение самообучающихся нейронных сетей при разработке алгоритма интеллектуального мониторинга состояния охраняемых объектов

Рассмотрим метод обнаружения незаконного лица на территории охраняемого объекта. Схема реализации метода включает тревожный извещатель, блок обработки сигнала (адаптивный фильтр, DSP, нейросетевой анализатор), выход. В данном случае блок обработки сигнала обучаем. При проникновении нарушителя на территорию охраняемого объекта происходят вибрационные процессы, которые представляют собой комбинацию узкополосных составляющих аддитивно смешанных с широкополосным шумом. Так как при изменении условий среды происходит изменение сигнала, а именно увеличение или уменьшение амплитуды и частоты полос, то для определения узкополосных составляющих может использоваться метод EMD или экстремальной фильтрации [Perkins, 2015; Андреев, 2017].

Для классификации и определения сигналов, которые создает лицо, незаконно проникнувшее на охраняемый объект, отдельно от шумов и помех на основе полученных данных происходит анализ, который основывается на принципе нейронной сети. Применение данных сетей уменьшает фактор человеческой ошибки (ошибки оператора) и увеличивает эффективность системы путем исключения ложных срабатываний [Бугорский, 2020]. Среди большого множества нейронных сетей выделяют архитектуру многослойной системы. В ней нейроны располагаются в n-ое количество слоев. Начальные нейроны получают первичные сигналы на входе, преобразовывают их и через точки ветвления посылают их нейронам n-ого слоя. Такой алгоритм происходит циклично, пока сигнал не дойдет до последнего слоя, который даст выходной сигнал. Большую распространенность получили сети, состоящие из трех слоев, где все они имеют наименование: первый является входным, второй – скрытый и третий слой работает на выходные сигналы.

Нужно учитывать тот факт, что нейронные сети являются самообучаемыми, но предварительно требуется их начальное обучение [Асадуллаев, 2017]. Алгоритм обучения нейросети заключается в том, что выход нейронов последнего слоя сравнивается с обучаемой моделью, из разницы между запланированным и действительным происходит сравнение и делается вывод, который определяет связи нейронов крайнего слоя (i) с предыдущем. После этого такой же процесс происходит со слоем (i–1), и так со всеми последующими. В итоге получим таблицу изменения весов связей нейронов. Нейросеть в процессе обучения имеет свои отличительные качества: способность к обучению на определенном количестве примеров, а также стабильность прогнозирования новых ситуаций с высокой точностью. При этом система адекватно реагирует в моменте влияния на нее помех и не утрачивает свою работоспособность. Обучение проводится путем регистрации начальных сигналов от

охранных извещателей, камер видеонаблюдения и других периферийных устройств, установленных на охраняемом объекте. Все полученные сигналы проходят процесс идентификации с помощью анализа по распознаванию и анализа разных параметров. Образы данных сигналов в последующем могут быть использованы, как классификаторы тревожных сигналов с помощью нейросети. Общая настройка может выполняться путем загрузки в базы данных уже известных параметров различных сигналов, при обнаружении которых нейронная сеть сможет быстро реагировать на уже изученные образы [Андреев, 2017].

Также на примере нейронной сети может быть построена схема обнаружения как отдельно стоящего человека, так и группы людей, а также транспортного средства [Андреев, 2015; Полтавский, 2020]. При обнаружении какого-либо транспортного средства сигнал делится на два класса: «сигнал-фон», а при движении одного человека либо группы людей происходит чередование фона и сигнала. Учитывая, что чередование сигналов в зависимости от объекта разное – если проходит один человек, то ритм сигнала четкий в отличии от прохода группы людей, – то такой сигнал носит отличительные черты.

На основе нечеткой логики может быть построена эффективная система охраны на критически уязвимых объектах [Бугорский, 2020]. Если нам требуется определить только транспортное средство и не реагировать на нарушителей, то можно произвести обучение нейроной сети, используя следующие данные: сочетание фона, прохода и проездов. Сигнал выхода должен быть задан следующим образом: на выходе «0», если на входе обнаруживается фон либо проход человека, и «1» – в случае проезда автомобиля.

Таким образом, в данном методе интеллектуального мониторинга, который предназначен для применения в системах обеспечения комплексной безопасности охраняемых объектов, нейросеть является вычислительной системой, алгоритм решения задач которой выражен в виде комбинаций пороговых элементов с перестраиваемыми коэффициентами настройки, независимыми от размерности комбинаций пороговых элементов и их входного пространства.

Описание программы интеллектуального мониторинга состояния охраняемого объекта на основе разработанного алгоритма

Для формирования системы мониторинга за состоянием охраняемого объекта требуется разработка широкого ряда модулей (рис. 1).

Поставленная задача включает в себя использование технологий распознавания объектов с камер системы видеонаблюдения с применением нейросетей, а также дополнительных датчиков для точного опознавания предметов и явлений. Суть данной системы мониторинга заключается в быстрой передаче уведомления оператору для реализации оперативных и четких действий [Ванжа, 2019; Катыс, 2020; Останина, 2020].

База данных является упрощенной, благодаря чему имеется возможность взаимодействия между всеми реализуемыми функциями [Мясникова, 2006; Щеголева, 2016]. Для того, чтобы было понятно, какие объекты определять системе как опасные или нежелательные, необходимо знать их характеристики, в дальнейшем это понадобится для обучения системы. Введем условие, что требуется, чтобы камера видеонаблюдения могла распознавать определенный объект. Для этого необходимо собрать всю информацию о предположительном объекте. Выявленный набор файлов группируется в некую сущность, которая имеет поле, имя, комментарий и тег. Для удобства последующей группировки и выборки все это делается в определенном, необходимом количестве, так как количество объектов и сущностей образов не ограничивается. Таким образом, данной моделью можно провести обучение нейросети. Фактически табличка *neuro_education* позволяет осуществить связь между таблицей заданных нейронных сетей в исследуемых объектах.

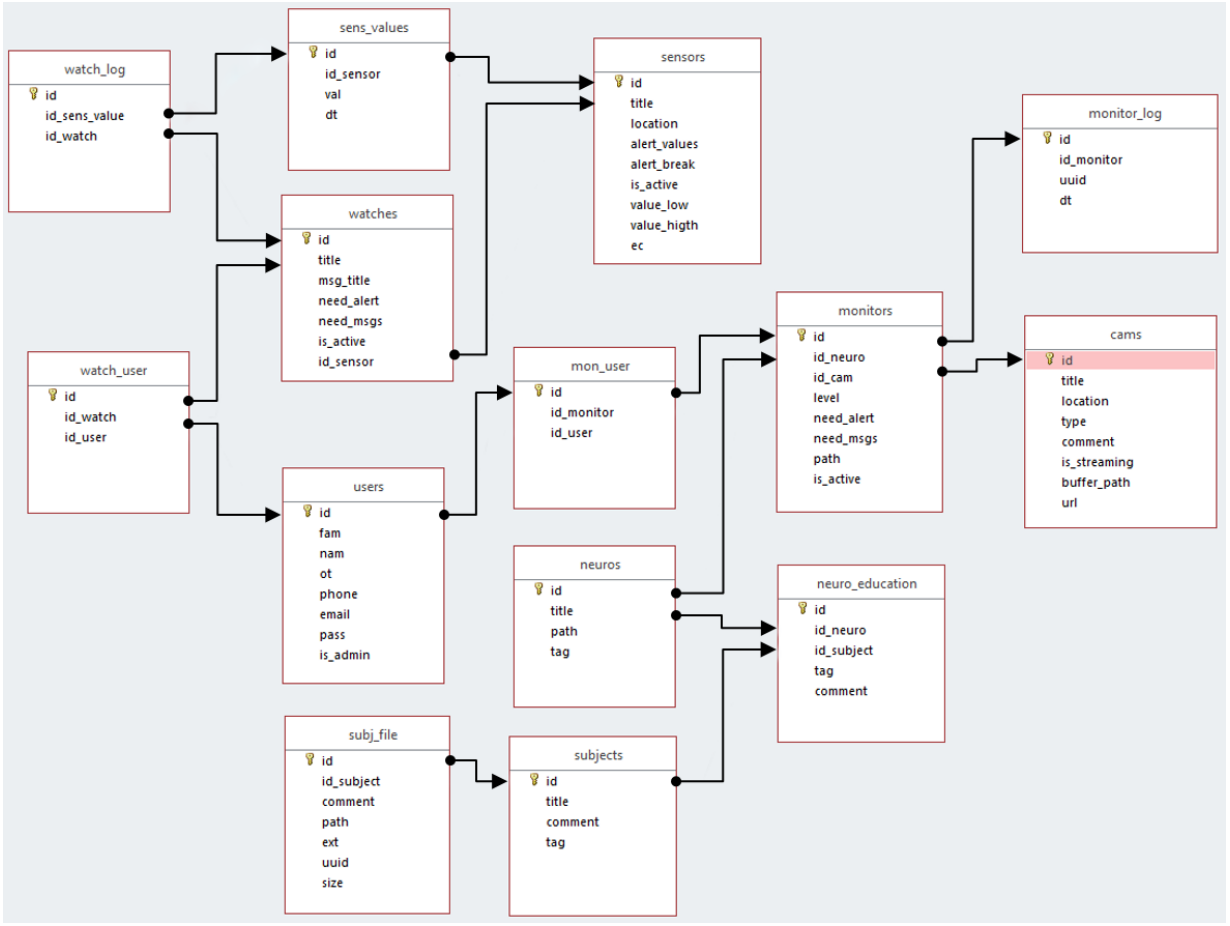

Рис. 1. Алгоритм интеллектуального мониторинга состояния объекта
Fig. 1. Algorithm for intelligent monitoring of the state of an object

После того, как нейронная сеть обучена, возможно сохранение в ней новых полученных знаний. Это особенно актуально, когда оборудование должно быть перезагружено либо проводятся пусконаладочные работы, модернизация, либо требуется перенос системы на другой уровень [Chaudhuri, 2016; Hillar, 2018; Лютикова, 2020]. Табличка *monitors* позволяет соединить знания нейронных сетей и камер видеонаблюдения. Для учета камер предусмотрена сущность *kams*, которая характеризуется наименованием, расположением (можно использовать геокоординаты либо локальные координаты внутри здания с учетом высотности), типом камеры, комментариями в пользовательском поле. Так называемый *urel* для доверенных пользователей определяет, имеется ли возможность с конкретных камер обеспечить запись видео в режиме реального времени либо обеспечивается работа в буферный файл, а в случае *IP*-камеры возможен ли доступ через *Web*-браузер. Задается пороговый уровень распознавания, при этом чем выше этот уровень, тем с большей вероятностью обнаруженный объект будет соответствовать обучающей выборке. Иногда все это устанавливается эмпирическим путем, то есть, как только случаи ложного срабатывания исключаются, вполне можно регулировать данный показатель [Андреев, 2017]. В случае обнаружения фактора угрозы имеется возможность задействовать охранную сигнализацию, уведомления ответственных лиц (это альтернативные варианты: либо то, либо другое, либо все сразу, либо ничего). Результаты распознавания кладутся в каталог, который задается на уровне мониторинга. Все файлы, которые содержат искомый объект, кладутся в этот каталог с именем *uuid*, который прописан в табличке *monitors*. Доступ к данному режиму мониторинга имеют те пользователи, которые на данный момент подключены к нему. Это делается благодаря стыковочной табличке *mon_user*, где в качестве внешних ключей выступает ссылка на *monitors* и *mon_user*. Пользователь, он же ответственное лицо или администратор системы, характеризуется набором полей: фамилия, имя, отчество, телефон, почта, пароль. Почта обычно выступает в качестве логина для доступа в личный кабинет и просмотра состояния системы. В

случае, если пользователь является администратором, он может задавать параметры обучающих выборок в режиме мониторинга. Это что касается ветки алгоритма, отвечающей за слежение и распознавание объектов с камеры видеонаблюдения.

Вторая часть алгоритма – это работа с датчиком, включающая сущность *sensors*, которая также характеризуется наименованием, привязкой к плану, значением сообщений при срабатывании, выходе измерений за пределы допустимого диапазона либо при потере данных с камеры (то есть когда камера перестала работать в штатном режиме). В зависимости от типа датчика, его настройки, некоторые датчики позволяют использовать свое, встроенное программное обеспечение, у некоторых есть кнопки на корпусе. Данная организация позволяет подключать внешние датчики таким образом, чтобы фиксировать те значения, которые измеряются в данный момент времени [Kalnoor, 2018]. Для оптимизации учета в качестве внешнего ключа используется ссылка на сущность датчика.

Итак, для организации режима мониторинга по состоянию датчиков, необходима таблица, которая по аналогии с мониторингом с камер видеонаблюдения будет следить за состояниями сенсора. Для этого необходимо создать табличку наблюдений мониторинга и указать ссылку на сенсор, который будет использовать активность или неактивность для регулирования режима мониторинга без обращения к датчику, то есть напрямую, и формировать сообщение в случае аварии и выхода. Потеря связи в данном случае определяется на уровне сенсора, а логические поля, которые говорят о необходимости включения сигнализации, формируют уведомления согласно информации, содержащейся в полях датчика. Для того, чтобы доступ получили только те пользователи, которым это разрешено, предусмотрена табличка *watch_user*.

В случае, если что-то пошло не так – температура превысила допустимый предел, началось задымление, произошло еще что-то – в табличку *watch_log* пишется соответствующая запись, и ответственные лица получают соответствующие уведомления. В зависимости от настроек может сразу включиться система ликвидации последствий.

Заключение

Неоднозначность, нестабильность современной международной обстановки в связи с проведением специальной военной операции на Украине, обострением международного терроризма, радикальные изменения в методах и принципах защиты охраняемых объектов, повышение роли системы обеспечения комплексной безопасности в организации защиты охраняемого объекта в целом обусловливают необходимость значительного повышения эффективности применения инженерно-технических средств охраны. В качестве основного направления при этом выбрана проблема разработки и оценки системы обеспечения комплексной безопасности охраняемого объекта, наиболее значимой стороной которого становится технология принятия решений. Главным результатом работы является решение проблемы дальнейшего развития подходов и обоснование путей практической реализации и оценки системы обеспечения комплексной безопасности охраняемого объекта на основе интеграции процессов поддержки принятия проектных решений, моделирования рассуждений проектировщика и оптимизации в условиях неопределенности, разработки моделей, методов и алгоритмов оценки уровня защищенности объектов, разработки комплексного подхода при поддержке принятия решений на основе системного анализа и экспертных знаний о процессах разработки и оценки системы обеспечения комплексной безопасности охраняемого объекта.

Внедрение нейросетевых структур в алгоритм интеллектуального мониторинга состояния охраняемого объекта позволит приблизиться к разработке систем обеспечения комплексной безопасности с искусственным интеллектом, повысить их помехозащищенность. При этом повысится как средняя наработка на ложную тревогу, так и вероятность обнаружения с последующей классификацией типа нарушителя. Система обеспечения комплексной безопасности с искусственным интеллектом будет выполнять задачу обнаружения и распознавания автоматически, учитывая при анализе все характеристики исходного сигнала, процесс обработки будет значи-

тельно быстрее и даст более достоверный результат [Демешко, 2020]. Использование интеллектуальных систем обеспечения комплексной безопасности не требует вмешательства оператора для анализа тревожных сигналов и определения признаков реального вторжения или ложной тревоги. Они способны выдать информацию типа да/нет, а также определить тип события – перелаз через ограду, перекус сетчатого полотна заграждения, порыв ветра и т.п. В результате система сама принимает решение – является данный сигнал свидетельством реальной тревоги или обусловлен фактором помехи.

Список литературы

Андреев А.С. 2015. Методика формирования рациональной структуры гибридной интеллектуальной системы обнаружения АСО. Сб. тр. XXXIV межведомственной НТК, Серпухов: ФВА РВСН, 10-13.

Андреев А.С. 2017. Математическая модель процессов обучения нейросетевого канала многоканальной системы обнаружения нарушителя. Сб. тр. XXXVI межведомственной НТК, Серпухов: ФВА РВСН, часть 1: 259-265.

Андреев А.С. 2017. Особенности компенсации помех в интеллектуальных системах охранной сигнализации. Сб. тр. XXXVI межведомственной НТК, Серпухов: ФВА РВСН, часть 1: 240-248.

Асадуллаев Р.Г. 2017. Нечеткая логика и нейронные сети: учебное пособие. Белгород: БелГУ, 309.

Бугорский М.А., Каплин М.А., Остроцкий С.В., Казакова О.В., Селин В.И. 2020. Особенности использования объектов критической информации инфраструктуры с современной системой обнаружения вторжений. Sciences of Europe, 66: 42-46.

Ванжа Т.В. 2019. Статистический анализ современных методов распознавания лиц и эмоций. Информатика и кибернетика, 2 (16): 64-70.

Демешко В.С., Фёдоров А.И. 2020. Применение сверточных нейронных сетей в подсистеме разведки комплексной системы безопасности. Системный анализ и прикладная информатика, 2: 46-53.

Катыс П.Г. 2020. Обработка изображений в системах распознавания лиц. Современная наука: актуальные проблемы теории и практики. Серия: естественные и технические науки, 1: 92-95.

Лютикова Л.А., Ибрагим А.С. 2020. Применение нейросетевого подхода для решения задачи аутентификации пользователя. Известия Кабардино-Балкарского научного центра РАН, 4: 5-10.

Мясникова Н.В. 2006. Теоретические основы экспресс-анализа. Известия высших учебных заведений. Поволжский регион. Технические науки, 6: 117-123.

Останина Е.А. 2020. О некоторых аспектах технологии распознавания лиц. Человеческий капитал, 5 (137): 142-152.

Полтавский А. В., Юрушкина Т. Г., Юрушкин М. В. 2020. Автоматическое распознавание автомобильных номерных знаков. Вестник Донского ГТУ, 1: 93 - 99.

Прохоров А.С. 2021. Применение нейронных сетей для обеспечения безопасности человека в жилых и промышленных помещениях. Символ науки, 1: 25-29.

Щеголева Н.Л. 2016. Концепция построения комплекса программных средств для моделирования систем поиска изображений лиц. Известия СПбГЭТУ "ЛЭТИ", 5: 40-47.

Chaudhuri R., Fiete I. 2016. Computational principles of memory. Nature Neuroscience, 19: 394–403.

Hillar J., Tran N. 2018. Robust Exponential Memory in Hopfield Networks. The Journal of Mathematical Neuroscience, 8: 1-20.

Kalnoor G., Agarkhed J. 2018. Detection of intruder using KMP Pattern Matching Technique in Wireless Sensor Networks. Procedia Computer Science, 125: 187-193.

Perkins C., Muller G. 2015. Using Discrete Event Simulation to Model Attacker Interactions with Cyber and Physical Security Systems. Procedia Computer Science, 61: 221 – 226.

Rashid T. 2016. Make Your Own Neural Network. CreateSpace Independent Publishing Platform, 222.

Yang D., Alsadoon A., Prasad P., Singh A., Elchouemi A. 2018. An Emotion Recognition Model Based on Facial Recognition in Virtual Learning Environment. Procedia Computer Science, 125: 2-10.

References

Andreev A.S. 2015. Metodika formirovaniya ratsional'noy struktury gibridnoy intellektual'noy sistemy obnaruzheniya ASO [Technique for the formation of a rational structure of a hybrid intelligent detection system for ASO]. Sb. tr. XXKhIV mezhvedomstvennoy NTK, Serpukhov: FVA RVSN, 10-13. (in Russian)

Andreev A.S. 2017. Matematicheskaya model' protsessov obucheniya neyrosetevogo kanala mnogokanal'noy sistemy obnaruzheniya narushitelya [Mathematical Model of Learning Processes for a Neural Network

Channel of a Multichannel Intruder Detection System]. Sb. tr. XXKhVI mezhvedomstvennoy NTK, Serpukhov: FVA RVSN, ch. 1: 259-265. (in Russian)

Andreev A.S. 2017. Osobennosti kompensatsii pomekh v intellektual'nykh sistemakh okhrannoy signalizatsii [Features of interference compensation in intelligent security alarm systems]. Sb. tr. XXKhVI mezhvedomstvennoy NTK, Serpukhov: FVA RVSN, ch. 1: 240-248. (in Russian)

Asadullaev R.G. 2017. Nechetkaya logika i neyronnye seti: uchebnoe posobie [Fuzzy Logic and Neural Networks: Tutorial]. Belgorod: BelGU, 309. (in Russian)

Bugorsky M., Kaplin M., Ostrotsky S., Kazakova O., Selin V. 2020. Features of using critical information infrastructure facilities with a modern intrusion detection system. Sciences of Europe, 66: 42 - 46. (in Russian)

Vanzha T. 2019. Statistical analysis of modern methods of recognition of faces and emotions. Computer science and cybernetics, 2 (16): 64-70. (in Russian)

Demeshko V.S., Fedorov A.I. 2020. Application of convolutional neural networks in the intelligence security system subsystem. System analysis and applied information science, 2: 46 - 53. (in Russian)

Katys P.G. 2020. Treatment of images in face recognition systems. Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Seriya: estestvennye i tekhnicheskie nauki [Modern Science: Actual Problems of Theory and Practice. Series: natural and technical sciences], 1: 92-95. (in Russian)

Lyutikova L.A., Ibragim A.S. 2020. Application of a neural network approach to solving user authentication problems. News of the Kabardin-Balkar scientific center of RAS, 4: 5-10. (in Russian)

Myasnikova N.V. 2006. Theoretical foundations of express analysis. Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki [News of higher educational institutions. Volga region. Technical science], 6: 117-123. (in Russian)

Ostanina E.A. 2020. About some aspects of face recognition technology. Human Capital, 5(137): 142-152. (in Russian)

Poltavskii A.V., Yurushkina T.G., Yurushkin M.V. 2020. Automatic license-plate recognition. Vestnik of Don State Technical University, 1:93-99. (in Russian)

Prokhorov A.S. 2021. Primenenie neyronnykh setey dlya obespecheniya bezopasnosti cheloveka v zhilykh i promyshlennykh pomeshcheniyakh [The use of neural networks to ensure human security in residential and industrial premises]. Simvol nauki [Symbol of Science], 1: 25-29. (in Russian)

Shchegoleva N.L. 2016. Conception of software for face retrieval systems modeling. Izvestiya SPbGETU "LETI", 5: 40-47. (in Russian)

Chaudhuri R., Fiete I. 2016. Computational principles of memory. Nature Neuroscience, 19: 394–403.

Hillar J., Tran N. 2018. Robust Exponential Memory in Hopfield Networks. The Journal of Mathematical Neuroscience, 8: 1-20.

Kalnoor G., Agarkhed J. 2018. Detection of intruder using KMP Pattern Matching Technique in Wireless Sensor Networks. Procedia Computer Science, 125: 187-193.

Perkins C., Muller G. 2015. Using Discrete Event Simulation to Model Attacker Interactions with Cyber and Physical Security Systems. Procedia Computer Science, 61: 221 – 226.

Rashid T. 2016. Make Your Own Neural Network. CreateSpace Independent Publishing Platform, 222.

Yang D., Alsadoon A., Prasad P., Singh A., Elchouemi A. 2018. An Emotion Recognition Model Based on Facial Recognition in Virtual Learning Environment. Procedia Computer Science, 125: 2-10.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.

Conflict of interest: no potential conflict of interest related to this article was reported.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Офицеров Александр Иванович, кандидат технических наук, сотрудник Академии ФСО России, г. Орел, Россия

Сафонов Даниил Александрович, сотрудник Академии ФСО России, г. Орел, Россия

INFORMATION ABOUT THE AUTHORS

Alexander I. Ofitserov, Candidate of Technical Sciences, employee of the Academy of the Federal Guard Service of the Russian Federation, Orel, Russia

Daniil A. Safonov, employee of the Academy of the Federal Guard Service of the Russian Federation, Orel, Russia