# СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Е.В. Ким**
Докторант, Гулистанский государственный университет
Преподаватель, Tashkent International University of Education

**Abstract:** This article considers the use of intelligent systems in information security. The introduction highlights the problem of growing threats to information security and introduces the concept of intelligent systems and their potential in this area. It then discusses the definition of intelligent systems, their role in detecting and preventing information security threats, and the benefits of using them. The following are examples of the use of intelligent systems in various areas of information security. It then discusses the challenges and limitations associated with the use of intelligent systems. The conclusion summarizes and summarizes the benefits of using intelligent systems in information security, and also indicates potential directions for the development of this area.
**Keywords:** intelligent systems, information security, information security threats, artificial intelligence, efficiency, automation, machine learning, neural networks, genetic algorithms, challenges, limitations.
**Аннотация:** В статье рассматривается использование интеллектуальных систем в защите информации. Освещается проблема растущих угроз информационной безопасности, дается понятие интеллектуальных систем, анализируются их потенциал, роль в обнаружении и предотвращении угроз информационной безопасности, а также преимущества их использования. Представлены примеры применения интеллектуальных систем в различных областях защиты информации. Обсуждаются вызовы и ограничения, связанные с использованием интеллектуальных систем.
**Ключевые слова:** интеллектуальные системы; защита информации; угрозы информационной безопасности; искусственный интеллект; эффективность; автоматизация; машинное обучение; нейронные сети; генетические алгоритмы; вызовы; ограничения.

Для защиты информации разрабатываются и внедряются высокоэффективные планы по обнаружению сбоев доступа с использованием аппаратной части и программного обеспечения [1]. В последнее десятилетие наблюдается активное развитие нового поколения аналитических систем, которые основаны на передовых технологиях искусственного интеллекта [2].

Они входят в такое понятие, как «интеллектуальные информационные системы». Они имеют большой потенциал в сфере защиты информации благодаря возможности разработки систем, которые обучаются и способны автономно принимать решения, а также обнаружить и классифицировать потенциальные атаки

или угрозы. Понятие интеллектуальных информационных систем (ИИС) сформировалось в результате и прогресса в основах кибернетики, современной теории управления, алгоритмической теории, развития информационных технологий и обобщения накопленных научных знаний, методов и средств в области искусственного интеллекта (ИИ).

Интеллектуальные информационные системы или ИИС, обладают когнитивными способностями благодаря своим функциям обучения. ИИС могут учиться одним из двух основных способов: под наблюдением и без надзора. В упражнении по выявлению мошенничества каждая запись помечается как мошенническая или не мошенническая, и машина идентифицирует другие атрибуты в записи, которые помогают различать две группы. Система ищет наилучшие отличительные признаки для описания одной группы по сравнению с другой. Таким образом, интеллектуальная информационная система (ИИС) – представляет собой разновидность интеллектуальной системы, содержащей комплекс программных, логико-математических, лингвистических средств для решения определенных задач, например, возможность проводить продвинутый диалог на естественном языке и осуществлять поиск информации в этом режиме. На данный момент популярны следующие подходы – технологии иммунных систем, байесовская сеть, генетические алгоритмы, нейронные сети и т. д. Задачи, которые могут быть решены интеллектуальными информационными системами (ИИС):

– Интерпретация данных: определение смысла данных и анализ множества вариантов для достижения согласованности, и корректности результатов.

– Диагностика: соотношение объекта с определенным классом объектов или обнаружение неисправностей в системе.

– Мониторинг: непрерывный анализ данных в режиме реального времени и оповещение о превышении допустимых значений параметров.

– Проектирование: подготовка спецификаций для создания «объектов» с заранее определенными свойствами.

– Прогнозирование: возможность предсказывания последствий определенных событий или явлений на основе данных параметрической динамической модели, при которой значения параметров подбирают под заданную ситуацию.

Планирование: поиск планов действий к конкретным объектам, которые могут выполнять те или иные функции.

Обучение: выявление ошибок в процессе изучения и предоставление правильных решений, на основе накопления знаний о гипотетическом «ученике» и его типичных ошибках. Нейронные сети обладают таким свойством и это их главное преимущество перед другими алгоритмами. Они способны выявлять сложные закономерности между входными и выходными данными, а также осуществлять обобщение. Вследствие чего осуществлять прогнозирование на основе данных, которых не было в обучающем наборе.

Управление: поддержание определенного режима деятельности систем в соответствии с заданными спецификациями. Поддержка принятия решений: помощь специалистам в выборе нужной альтернативы из множества выборов при принятии ответственных решений [5].

Интеллектуальные системы используются в данных системах информационной безопасности:

– Биометрические системы идентификации, применяемые, например, в банковской сфере как полная или частичная замена обычных паролей для контроля и управления доступом. При помощи нейросетевых алгоритмов обработка информации биометрической идентификации проходит в 4 этапа:

– получение биометрических данных пользователя путем использования сенсоров (устройств для преобразования входных сигналов);

– извлечение информативных биометрических характеристик;

– создание биометрического шаблона пользователя с использованием нейронной сети;

– применение решающего правила, основанного на нейронной сети.

Системы обнаружения вторжений (СОВ), основанные на интеллектуальных системах, помогают обнаружить, предупредить и среагировать на инциденты с применением компьютерных атак. СОВ реализуются с использованием разных методов поиска специальных индикаторов того, что передача сетевого трафика проходит в пределах какой-либо атаки на информационную систему. Интеллектуальные системы антивирусной защиты, равно как и СОВ, используют в борьбе с вирусами метод сигнатурного анализа. Антивирусная защита сообщает о «заражении» вирусами, помогает «излечиться» от вирусов и контролирует каналы проникновения вирусов.

Средства анализа и управления информа ционными рисками на базе интеллектуальных систем позволяют определить потенциальный вред от действия атак, использующих уязвимости в системе, а также вероятность реализации таких атак. Для эффективного управления рисками применяется метод когнитивного моделирования, который основывается на использовании ограниченной, нечеткой или противоречивой информации об исследуемом объекте, представленным экспертами. Целью этого подхода является выявление ключевых и значимых взаимосвязей, определение важности каждого фактора, влияющего на проблему [5]. Использование интеллектуальных систем для защиты информации имеет ряд преимуществ. В первую очередь, интеллектуальные системы обладают способностью анализировать большие объемы данных и обнаруживать потенциальные угрозы с большей точностью и эффективностью, чем традиционные методы. Они могут автоматически мониторить и анализировать данные, обнаруживать аномалии и подозрительную активность, которые могут указывать на угрозы и атаки [6]. Также использование интеллектуальных систем позволяет снизить вероятность ошибок, связанных с человеческим фактором. Они могут

проводить комплексный анализ данных, учитывая множество факторов, что способствует более точному и надежному обнаружению угроз и инцидентов безопасности. Еще одним важным преимуществом использования интеллектуальных систем в кибербезопасности является их способность к самообучению на основе полученного опыта. Опыт предыдущих атак поможет улучшить имеющиеся алгоритмы поведения и обеспечить более точное обнаружение угроз в будущем [7].

Помимо этого, интеллектуальные системы могут анализировать и обрабатывать большие объемы данных, чтобы выявлять скрытые закономерности и тенденции. Это позволяет предсказывать потенциальные угрозы и атаки, а также принимать меры по их предотвращению заранее. Благодаря этому повышается эффективность мер по защите информации.

К тому же интеллектуальные системы способны обучаться на основе опыта. Они могут адаптироваться к новым видам угроз и обновлять свои алгоритмы и модели на основе новых знаний. Это позволяет системам постоянно совершенствоваться и эффективнее справляться с постоянно изменяющимися угрозами информационной безопасности.

Интеллектуальные системы могут работать в режиме реального времени, что позволяет оперативно реагировать на угрозы и инциденты безопасности.

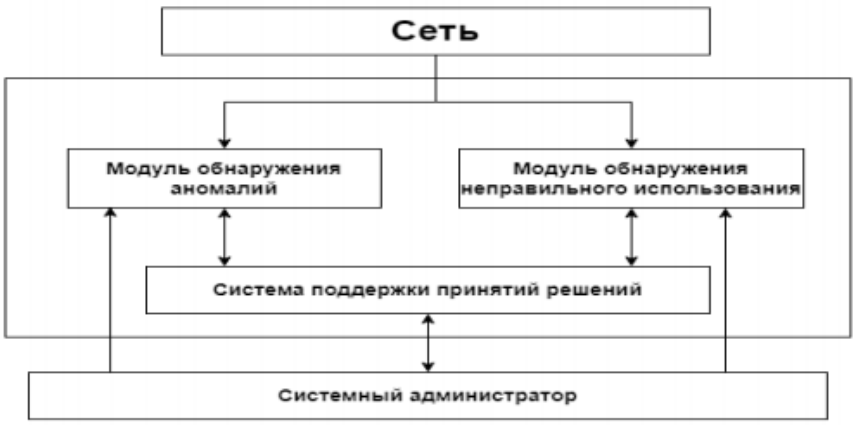


Рисунок 1 – Архитектура гибридной СОВ

Быстрая реакция сокращает время реакции и позволяет своевременно предпринимать необходимые меры по минимизации ущерба от инцидентов. Интеллектуальные системы применяются в различных областях защиты информации. Нейронные сети могут анализировать данные, полученные от СОВ, чтобы идентифицировать фишинговые попытки. Они могут обнаруживать подозрительные письма, веб-страницы, URL-адреса и другие элементы, характерные для фишинговых атак. Это позволяет СОВ предупреждать и блокировать фишинговые атаки, минимизируя риск для пользователей и систем. Нейронные сети могут непрерывно обучаться на основе новых данных о фишинговых атаках, которые обнаруживаются и блокируются СОВ. Это позволяет нейронным сетям обновлять свои модели и алгоритмы, чтобы лучше распознавать и предотвращать

новые виды фишинговых атак. Метод обнаружения аномалий использует алгоритмы для анализа большого объема данных. Он строит картину и сравнивает данные с этой картиной. Если данные не соответствуют картине, то это считается аномалией. В данном случае, используется сетевой трафик в качестве источника данных. Данные сетевого трафика представлены в виде сетевых пакетов, разделенных на уровне IP. Сырые данные используются для анализа. После сбора и анализа данных, каждое действие проверяется на наличие аномалий. Если аномалия обнаружена, появляется уведомление, иначе алгоритм считает действие или данные нормальными (рис. 2).


Рисунок 2. Схема обнаружения сетевых аномалий

Даже у самых сложных систем есть не сетей в сочетании с СОВ для распознавания и предотвращения фишинговых атак [8]. СОВ является средством защиты информации, предназначенным для обнаружения несанкционированного доступа в информационно телекоммуникационную сеть организации, особенно в глобальной сети Интернет. СОВ могут быть реализованы на уровне отдельных узлов, обеспечивая защиту конкретного хоста, или на уровне всей сети организации или ее подсетей, обеспечивая общую защиту. Наиболее распространенные методы обнаружения включают поиск по сигнатурам атак и обнаружение аномалий. На рис. 1 представлена условная схема работы СОВ. Внутри СОВ могут использоваться нейронные сети. С помощью них выполняются многие задачи. Нейронные сети могут быть обучены на основе большого объема данных сетевого трафика для распознавания типичных и аномальных следов активности. Возможно обнаружение необычных трафиковых шаблонов, связанные с фишинговыми атаками, такие как перенаправления, подмены данных или попытки перехвата информации. Это помогает системам обнаружения вторжений раннему распознаванию фишинговых атак. Нейронные сети могут анализировать данные, полученные от СОВ, чтобы идентифицировать фишинговые попытки. Они могут обнаруживать подозрительные письма, веб-страницы, URL-адреса и другие элементы, характерные для фишинговых атак. Это позволяет СОВ предупреждать и блокировать фишинговые атаки, минимизируя риск для пользователей и систем. Нейронные сети могут непрерывно обучаться на основе новых данных о фишинговых атаках, которые обнаруживаются и блокируются СОВ. Что позволяет нейронным сетям обновлять свои модели и алгоритмы, чтобы лучше распознавать и предотвращать новые виды

фишинговых атак. Кроме того, интеллектуальные системы используют машинное обучение для обнаружения аномалий в сетевом трафике. Метод обнаружения аномалий использует алгоритмы для анализа большого объема данных. Он строит картину и сравнивает данные с картиной. Если данные не соответствуют картине, то это считается аномалией. В данном случае, используется сетевой трафик в качестве источника данных. Данные сетевого трафика представлены в виде сетевых пакетов, разделенных на уровне IP. Сырые данные используются для анализа. После сбора и анализа данных, каждое действие проверяется на наличие аномалий. Если аномалия обнаружена, появляется уведомление, иначе алгоритм считает действие или данные нормальными (рис. 2). Также можно добавлять или изменять шаблоны нормального поведения вручную или автоматически [9]. Даже у самых сложных систем есть недостатки. И искусственный интеллект не является исключением из этого правила. Безопасность имеет первостепенное значение в процессе искусственного интеллекта. Она должна быть интегрирована, начиная со стратегического планирования на протяжении всего цикла. Безопасность направлена на защиту конфиденциальности пользователей и их бизнеса от утечек данных [10]. Многие приложения с искусственным интеллектом основаны на огромном количестве данных. И эти данные часто являются конфиденциальными и личными по своей природе. Дело в том, что системы искусственного интеллекта полагаются на данные и не могут обходиться без них. Чем больше искусственный интеллект обучает нейронные сети, тем больше уязвимостей появляется в коде. Системы становятся подверженными утечкам данных и краже личных данных. Чтобы избежать утечек данных, ошибок и репутационных рисков, компаниям необходимо ставить безопасность искусственного интеллекта на первое место. Возможный выход – тщательно протестировать продукты с искусственным интеллектом и устранить недостатки до того, как продукты войдут в практику или выйдут на рынок [10].

Другая проблема связана с тем, что алгоритм искусственного интеллекта анализирует огромные данные, которые требуют огромной вычислительной мощности. До сих пор проблема решалась с помощью облачных вычислений и параллельной обработки. Однако по мере увеличения объема данных и появления более сложных алгоритмов глубокого обучения современных вычислительных мощностей будет недостаточно для удовлетворения сложных требований. Понадобится больше памяти и вычислительных мощностей для обработки огромных объемов данных в эксабайтах и зеттабайтах. Также современные системы искусственного интеллекта могут обучаться не тому, что задумывали разработчики.

Результативность этих систем в большой степени зависит от данных, на которых они обучаются. Если в исходных данных присутствует необычная активность, искусственный интеллект может воспринять ее как обычную и не обнаружить аномалию. Конечно, систему можно дополнительно обучать в процессе использования, но такие сложности необходимо учитывать и не игнорировать.

Проблема отражения новых кибер атак связана с тем, что на данный момент ИИ сложно предугадать действия киберпреступников. В связи с этим в кибербезопасности применяются другие, менее отлаженные алгоритмы искусственного интеллекта. В сфере информационной безопасности использование старых данных для обучения не имеет особого смысла, в то время как в традиционных областях искусственного интеллекта (распознавание лиц и голоса, машинный перевод, управление запасами, автопилоты) такой подход является базовой практикой. Использование алгоритмов на основе сигнатур позволяет обнаружить уже известные атаки без участия искусственного интеллекта [10]. Вышеуказанные проблемы, безусловно, не являются неразрешимыми. Однако это требует быстрого развития технологий и сотрудничества людей. Экспертам предстоит пройти долгий путь по разработке принципов, методологии и рамок, гарантирующих, что мощная технология, такая как искусственный интеллект, не будет использоваться не по назначению, что может привести к непредвиденным последствиям.

## СПИСОК ЛИТЕРАТУРЫ:

1. Авдеева И. Л., Полянин А. В., Головина Т. А. Цифровизация промышленных экономических систем: проблемы и последствия современных технологий // Известия Саратовского ун-та. Нов. сер. Сер. Экономика. Управление. Право. 2019.Т. 19, вып. 3. С. 238–245.

2. Шарапова Т. Н., Селиванов С. А. Анализ угроз информационной безопасности и способы ее защиты // Наукосфера. Экономические науки. 2021. № 1(1).

3. Коровин А. М. Интеллектуальные системы: текст лекций. Челябинск: ЮУрГУ, 2015. 60 с.

4. Классификация задач, решаемых ИИС. URL:https://studfle.net/preview/7411411/page:2/

5. Интеллектуальные системы управления информационной безопасностью / В. А. Табакаева, В. В. Селифанов, В. Р. Ан, С. А. Буларга, А.С. Ворожцов // Сборник научных трудов НГТУ. 2019. № 3–4 (96). С. 165–176. 6. Advantages of AI in Cyber Security. URL: https:// www.analyticssteps.com/blogs/6

7. Роль искусственного интеллекта в кибербезопасности. URL: https://vc.ru/dev/621020-rol iskusstvennogointellekta-v-kiberbezopasnosti

8. Depren O., Topallar M., Anarim E., Ciliz M. K. AnИНДУСТРИАЛЬНАЯ ЭКОНОМИКА № 4, 2023 75 intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks // Expert Systems with Applications. 2021. № 29. С. 173.

9. Котов В. Д., Васильев В. И. Современное состояние проблемы обнаружения сетевых вторжений // Вестник Уфимского государственного авиационного технического университета. 2021. Т. 16. № 3 (48). С. 198-204.
10. Обнаружение аномалий в сетевом трафике, используя методы машинного обучения / И. А. Ушаков, Ф. Х. Исмоилов, А. Э. Федорова [и др.] // Актуальные вопросы современной науки и образования: сборник статей XX Международной научно-практической конференции. В 2 ч., Пенза, 20 июня 2022 года. Ч. 1. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 96-98