n-типа с концентрацией $5 \cdot 10^{15}$–$2 \cdot 10^{16}$ см$^{-3}$. Исследование проводилось методом изотермической релаксации емкости. Измерялось время релаксации заполнения ГЦ (τ), обратное скорости термической эмиссии электронов.

Для объяснения зависимостей τ(ε) учитывалось не только понижение потенциального барьера центра Δφ в электрическом поле, но и зависимость $x_0(\varepsilon)$ для кулоновского (1) и поляризационного потенциала (7). Сечение захвата центра оценивалось, как геометрическое (x_0), величина которого уменьшается коэффициентом, отражающим сложность процесса обмена энергией носителя заряда с решеткой. Такой подход позволил объяснить полевые зависимости скоростей термической эмиссии носителей из кулоновских центров (рис. 2).

Электрополевые зависимости энергии активации, сечения захвата электрона, а также времени релаксации заполнения А-центра в облученном кремнии были объяснены на основе модели поляризационного потенциала с учетом Δφ(ε) и $x_0(\varepsilon)$ при $\alpha = 2{,}5 \cdot 10^{-20}$ см$^{-3}$ (рис. 3). Экстраполированное значение энергии активации центра в нулевом электрическом поле составило 0,18 эВ, что согласуется с литературными данными.

УДК 004.056

МАШИННОЕ ОБУЧЕНИЕ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Глинская Е.В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. В наш век данных данные являются наиболее небезопасным и легкодоступным товаром. В такой ситуации искусственный интеллект может оказать огромную помощь индустрии кибербезопасности, тем более что многие киберпреступники уже используют эту технологию. Рассмотрены методы искусственного интеллекта, которые могут оказать большую помощь в области обнаружения злоумышленников в сфере кибербезопасности.

Ключевые слова: искусственный интеллект, машинное обучение, глубокое обучение, кибербезопасность, фишинг.

MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY

Glinskaya E.

Bauman State Technical University
Moscow, Russian Federation

Abstract. In this age of data, data is the most insecure and easily accessible commodity. In such a situation, artificial intelligence can be of great help to the cybersecurity industry, especially since many cybercriminals are already using this technology. The methods of artificial intelligence are considered, which can be of great help in the field of detecting intruders in the field of cybersecurity.

Key words: artificial intelligence, machine learning, deep learning, cybersecurity, phishing.

Адрес для переписки: Глинская Е.В., ул. Вторая Бауманская, 5, Москва 105005, Российская Федерация
e-mail: Glinskaya@bmstu.ru

В настоящее время много говорят о машинном обучении (МО) и искусственном интеллекте (ИИ). За последние несколько лет эти технологии привлекли внимание специалистов по безопасности, и некоторые из них считают, что ИИ готов трансформировать информационную безопасность.

Искусственный интеллект – это наука о попытках воспроизвести разумное поведение, подобное человеческому. Есть несколько способов добиться этого – машинное обучение – один из них. Например, тип системы искусственного интеллекта, не связанный с машинным обучением, представляет собой экспертную систему, в которой навыки и процесс принятия решений эксперта фиксируются с помощью ряда правил и эвристик.

Машинное обучение – это особый тип ИИ. Система МО анализирует большой набор данных, классифицирует данные и определяет, какие данные относятся к какой категории. Например, машинное обучение можно использовать для анализа данных о поведении сети и классификации их как нормальных или аномальных.

Учитывая эти определения, все системы машинного обучения также являются системами ИИ. Однако не все системы ИИ используют ма-

шинное обучение. Текущая тенденция заключается в том, что используются лишь немногие из методов искусственного интеллекта. В ситуации, когда единственными системами ИИ являются те, которые используют машинное обучение, эти два термина будут синонимами.

Есть две основные ветви машинного обучения: контролируемое и неконтролируемое. Контролируемое машинное обучение включает в себя сопоставление входных переменных с выходными переменными, чтобы делать точные прогнозы об анализируемых данных. Что касается обнаружения угроз, алгоритм машинного обучения может использовать известное подозрительное поведение и присвоение категории «злонамеренных действий» в качестве основы для разработки классификатора угроз. Затем он может использовать этот классификатор для анализа новых образцов.

В неконтролируемом машинном обучении, второй ветви машинного обучения, система пытается сгруппировать группы данных вместе на основе характеристик данных. В этом случае результатом является идентификация групп похожих элементов, что позволяет аналитику, например, обрабатывать большое количество похожих образцов на основе одного решения (например, возможно все электронные письма имеют одинаковые вложения, и они являются вредоносными).

Существует так называемое глубокое обучение, особый тип машинного обучения, который использует нейронные сети вместо статистического анализа для анализа данных. Глубокое обучение особенно хорошо подходит для поиска классификаций в больших объемах данных. Но недостатком глубокого обучения является его ограниченная объяснительная способность в отношении того, почему что-то принадлежит к определенной группе, например, почему исполняемый файл опасен, с точки зрения информационной безопасности.

Машинное обучение сталкивается с одной из проблем информационной безопасности: пытаясь получить наборы данных, отражающие злонамеренное поведение, необходимо предотвратить угрозу. Это и есть обучение, то есть данные, которые намеренно пытаются избежать классификации, особенно когда это что-то злонамеренное, которое пытается не восприниматься как таковое.

Авторы вредоносных программ узнают, какие алгоритмы ищут, и настраивают свои образцы или пытаются переобучить модель до тех пор, пока не будет дана неправильная классификация, чтобы злоумышленники могли избежать обнаружения и заразить больше пользователей. При этом злоумышленники используют то, чему научились алгоритмы, против специалистов по безопасности, а затем и пользователей.

Чтобы учесть эту «враждебную» настройку, специалистам по безопасности необходимо разработать методы машинного обучения, которые ищут выбросы и ложные флаги. Они должны быть особенно осторожны в отношении процесса, который они используют для получения и характеристики данных. В противном случае результаты могут быть непредсказуемыми.

Например, возьмем упаковку исполняемого файла. Многие вредоносные программы используют упаковку, чтобы выглядеть по-новому и избежать обнаружения антивирусными программами, в то время как безопасный код редко использует упаковку (например, в случаях, когда авторы хотят защитить свою интеллектуальную собственность, как это происходит в видеоиграх). Если применяется машинное обучение к программам без предварительной распаковки, алгоритм должен знать, что упаковка «плохая», и алгоритм должен отметить это.

Таким образом методы искусственного интеллекта могут оказать большую помощь в области обнаружения злоумышленников в сфере кибербезопасности. Они могут помочь в обнаружении и защите от любых злоумышленников в системе, используя существующие представления о моделях действий злоумышленников. Например, злоумышленники в системе могут вести себя неестественно, например отправлять и получать большие объемы данных или внезапно менять шаблоны связи. Эти признаки злоумышленников в системе очень сложно уловить специалистам по кибербезопасности, особенно в крупных компаниях, где много сетевого трафика. Здесь системы обнаружения злоумышленников на базе искусственного интеллекта можно использовать для мониторинга сети на предмет любых нежелательных злоумышленников.

Также, внезапные изменения в поведении существующих пользователей могут быть признаком кибератаки в сети. Это может произойти, если злоумышленник украл учетные данные для входа в систему законного пользователя, а затем незаконно вошел в сеть, используя эти учетные данные. Но эти поведенческие изменения чрезвычайно трудно идентифицировать, особенно в большой сети. В такой ситуации искусственный интеллект может использоваться для обнаружения и блокировки скомпрометированных учетных записей пользователей, которые демонстрируют подозрительные изменения в поведении. ИИ может сделать это, создав поведенческий профиль всех пользователей, который включает их шаблоны входа и выхода, шаблоны передачи данных и т. д. Затем анализ поведения пользователей в этих профилях может помочь определить, когда пользователь ведет себя не так, как его обычный

поведенческий профиль, который может использоваться для предупреждения группы кибербезопасности о том, что что-то не так.

Искусственный интеллект также может быть чрезвычайно полезен для предотвращения фишинговых атак на пользователей в определенной сети. Фишинговые атаки чрезвычайно распространены во многих компаниях, где сотрудникам рассылаются мошеннические электронные письма с целью получения конфиденциальной информации их компании, такой как пароли компании, их банковские данные и данные кредитной карты и т. д. Могут использоваться методы искусственного интеллекта, такие как обработка естественного языка. Отслеживать электронные письма сотрудников в их корпоративных учетных записях и проверять, нет ли чего-либо подозрительного, например шаблонов и фраз, которые могут указывать на то, что электронная почта является попыткой фишинга.

Применение и внедрение ИИ в последние годы увеличилось в геометрической прогрессии, исследователи, лаборатории и технологические компании имеют бесчисленное множество применений ИИ во всех сферах жизни, запланированных на будущее.

ИИ способствует прогрессу во всех технологических областях, обеспечивает значительный прогресс в области кибербезопасности, поддерживает средства управления информационной безопасностью в продвинутом и интеллектуальном мире.

Литература

1. Гольдберг, Й. Нейросетевые методы в обработке естественного языка : руководство / Й. Гольдберг; перевод с английского А. А. Слинкина. – Москва: ДМК Пресс, 2019. – 282 с.

2. Бенджамин, Бенгфорт. Прикладной анализ текстовых данных на Python. Машинное обучение и создание приложений обработки естественного языка / Бенджамин Бенгфорт, Ребекка Билбро, Тони Охеда [Электронный ресурс]. – Режим доступа: : https://ibooks.ru/reading.php?short=1&productid=365298.

3. Ганегедара, Т. Обработка естественного языка с TensorFlow : руководство / Т. Ганегедара ; перевод с английского В. С. Яценкова. – Москва: ДМК Пресс, 2020. – 382 с.

УДК 539.1.074.3

ПРИМЕНЕНИЕ ОПТИЧЕСКИХ ВОЛНОВОДНЫХ КОЛЬЦЕВЫХ РЕЗОНАТОРОВ ДЛЯ ИЗМЕРЕНИЯ ПОГЛОЩЕННОЙ ДОЗЫ ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ

Гончаренко И.А., Ильюшонок А.В., Рябцев В.Н.

Университет гражданской защиты МЧС Беларуси
Минск, Республика Беларусь

Аннотация. Проведен анализ воздействия ионизирующего излучения на волноводные микрокольцевые резонаторы и оценка возможности их использования в качестве датчиков поглощенной дозы ионизирующего излучения. Показано, что с точки зрения чувствительности перспективными являются датчики на основе микрокольцевых резонаторов на базе кремниевых волноводов, покрытых фторполимером.
Ключевые слова: оптический волновод, ионизирующее излучение, доза излучения, микрокольцевой резонатор, щелевой волновод.

APPLICATION OF OPTICAL WAVEGUIDE RING RESONATORS FOR MEASUREMENT OF ABSORBED DOSE OF IONIZING RADIATION

Goncharenko I., Il'yushonok A., Reabtsev V.

University of Civil Protection of the Ministry for Emergency Situations of Belarus
Minsk, Republic of Belarus

Abstract. The effect of ionizing radiation on waveguide microring resonators are analysed. The possibility of its application as sensor of absorbed dose of ionizing radiation is estimated. It’s shown that the sensors comprising microring resonators on the base of silicon waveguides coated with fluoropolymer are the most prospective due to the higher sensitivity.
Key words: optical waveguide, ionizing radiation, radiation dose, microring resonator, slot waveguide.

Адрес для переписки: Рябцев В.Н., ул. Машиностроителей, 25, Минск 220118, Республика Беларусь
e-mail: v.reabtsev@ucp.by

В технических устройствах, функционирующих в условиях жесткого излучения, например, на спутниках или в ядерных реакторах, применяются датчики различных физических величин на основе волноводных резонансных структур (резонаторы Фабри-Перо, микрокольцевые резонаторы) [1]. Воздействие ионизирующего излучения вызывает деградацию материала волновода из-за образования дефектов и эффекта ионизации [2, 3]. Дефекты приводят к изменению оптических свойств материала в результате возникновения полос поглощения и центров окраски [4–6].