ларов США, что демонстрирует не только успешность цифровизации бизнес-процессов компаний, но и актуальность разрабатываемой ими продукции – технических средств и средств связи.

Сеть Интернет позволила сформировать новый рынок цифровых услуг и оказала значительное влияние на финансовое благосостояние стран. Так возникла экономика совместного использования (Sharing economy) – переход к платформенным решениям. Изначально базирующиеся на цифровых рынках платформы Google, Facebook (США), Amazon (США), Uber (США), Alibaba (Китай), Яндекс (Россия) являются гигантами цифрового мира и имеют исключительное конкурентное преимущество как на глобальном, так и на местном уровне.

В современных реалиях цифровая экономика стала мощным фундаментом развития государств: страны с более развитой цифровой экономикой получают большую долю своего ВВП за счет высокотехнологичных секторов. Предполагается, что к 2025 г. цифровая экономика может достичь показателя в 50 % глобального ВВП, а в развитых странах превысить его.

Киберугрозы сегодня нацелены на все области, использующие цифровые данные: здравоохранение, образование и науку, банковскую сферу, государственные органы, представителей бизнеса и многое другие. В большинстве случаев цель злоумышленников – хищение персональных данных: номера банковских счетов и кредитных карточек, паспортные данные, медицинские карты, данные об объектах интеллектуальной собственности, а также информация, относящаяся к государственной, коммерческой и военной тайне.

При рассмотрении области киберугроз на уровне государств можно отметить, что кибератакам подвержены как страны с высоким уровнем экономического развития (США, Китай, Канада и т.п.), так и с низким уровнем.

Наиболее актуальными угрозами можно считать:

социальную инженерию – это технологии манипулирования людьми в сети Интернет;

DDoS-атаки или отказ от обслуживания – это поток ложных запросов, блокирующих ресурс;

шифрование данных, которое в основном происходит при установке на компьютер программы-вымогателя (чаще всего через сеть Интернет при введении жертвы в заблуждение методами социальной инженерии). Данные программы блокируют доступ пользователей к их устройствам или блокируют доступ к файлам до тех пор, пока не будет выплачена денежная сумма или выкуп.

киберфизические атаки представляют собой взлом электрических сетей, транспортных систем, водоочистных сооружений и т. д.;

атаки на IoT (Интернет вещей) – это заражение устройства, подключенного к интернету;

киберпропаганду (дезинформация) и хактивизм (форма политической активности, при которой навыки компьютерного взлома широко используются против влиятельных коммерческих институтов и правительств, других целей).

Существующие и вновь возникающие угрозы кибербезопасности сегодня направлены на все структуры, имеющие выход в сеть Интернет: частные и государственные организации, производства, медицинские и образовательные учреждения, учреждения здравоохранения, финансовые и банковские структуры, а также многое другое.

Отсутствие необходимых навыков кибербезопасности активно влияет на ситуацию с киберпреступностью. В результате увеличения пропускной способности устройства, подключенные к Интернету вещей, стали более уязвимыми для кибератак. Многие устройства IoT не разработаны с учетом требований безопасности и могут иметь недостатки и уязвимости, которые легко используют злоумышленники. Если хакеры могут получить контроль над устройствами IoT в организации, они потенциально могут использовать их для доступа к остальной части ИТ-системы.

Таким образом, использование сети Интернет влечет за собой определенные риски, которые необходимо учитывать при проектировании, разработке и внедрении сетевых технологий. Полагается, что не стоит бояться использовать сеть Интернет, однако нужно использовать ее грамотно. Требуется вывести общество из состояния, вызванного опасностью использования сети, сформировать у граждан цифровую грамотность.

УДК 004.056.57; 004.89

М.Н. Сорокин, Д.С. Рябенко

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАЗВИТИИ АНАЛИТИКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В ходе становления информационного общества процесс информатизации является одним из основных факторов его развития на современном этапе. Благодаря процессу информатизации субъект (человек, общество) включается в глобальное информационное пространство, становясь при этом его частью. Наиболее точно данный эффект можно сопоставить с нынешним состоянием технологии ис-

кусственного интеллекта и машинного обучения, когда в основе множества повсеместных технологических процессов содержатся множества приложений искусственного интеллекта. Распространенные приложения искусственного интеллекта в современных технологиях включают распознавание голоса, обнаружение мошенничества, фильтрацию спама в электронной почте, обработку текста, рекомендации по поиску, анализ видео и т. д. Кроме того, эти современные технологии, совершенствуясь ежедневно, подпитываются все более широким анализом данных и получают новые качественные результаты, которые не были заложены их разработчиками.

Невероятные темпы роста данных за последние несколько лет привели к появлению нового термина «большие данные», что может означать много данных, достаточных для специального исследования того, как хранить, передавать, управлять и анализировать информацию, в том числе с применением ставших более доступными облачными вычислениями. Достижения в области облачных вычислений имеют важное значение для обеспечения огромных вычислительных мощностей экономически эффективным способом, помогая решать ресурсоемкие вычислительные задачи.

Наряду с благами объединения субъекта (человека, общества) в единое информационное пространство под управлением искусственного интеллекта, возникают и новые опасности, обусловленные необходимостью обеспечения информационной безопасности. Например, негативное информационное воздействие на сознание человека в результате может привести к изменению его мировоззрения и переориентации ценностей. В связи с этим проблема информационной безопасности должна быть достаточно глубоко осмыслена.

Исследуя проблемы информационной безопасности, возможно определение двух факторов, которые определяют возможность применения технологии искусственного интеллекта для отрасли. Во-первых, сбор и хранение больших объемов данных в области информационной безопасности ведется уже давно. Специалисты по информационной безопасности (далее – специалисты) применяют множество автоматизированных инструментов, предназначенных для сортировки, нарезки и добычи этих данных в целях решения возникающих прикладных задач обеспечения защиты информации. Во-вторых, на настоящий момент существует нехватка квалифицированных, опытных специалистов для успешной защиты информационной инфраструктуры и систем. Кроме того, прогнозируемый спрос на специалистов в сфере информационной безопасности и защиты информации будет продолжать расти. Учитывая эти факторы, технологии искусственного интеллекта отлично подходят для повышения эффективности информационной безопасности.

Обеспечение информационной безопасности представляется сложным, многофункциональным процессом, зависящим от различных внешних и внутренних факторов. Это обусловлено тем, что современный этап развития общества связан с освоением и использованием новых глобальных возможностей информационной сферы, таких как сеть Интернет, виртуальное пространство, новейших беспроводных средств коммуникации и т. д.

Рассмотреть влияние на информационную безопасность применения технологии искусственного интеллекта возможно на примере проведения анализа реагирования специалистом на инцидент взлома информационной сети. Предположим, что с целью несанкционированного получения конфиденциальной информации была взломана информационная сеть и размещено вредоносное программное обеспечение на отдельных вычислительных машинах сети. В этом случае специалист должен решить следующие частные задачи: выяснить, какая именно информация была украдена; каким образом осуществлена кража; восстановить систему, чтобы предотвратить подобные атаки снова.

Сроки физического обнаружения уязвимостей и решения выявленных проблем для специалиста весьма велики. Чтобы выяснить, какая именно информация была украдена, специалисту необходимо проверить журналы доступа к файлам или сетевой трафик, анализируя доступ к конфиденциальным файлам или большим объемам данных, выходящим из сети. Далее может потребоваться анализ диска на наличие вредоносных программ, чтобы попытаться отследить известные образцы вредоносных программ с использованием имеющихся сигнатур. Возможно, в рамках реагирования на инцидент необходим анализ работающей системы с целью поиска необычных процессов или другого аномального поведения информационной сети.

Благодаря технологии искусственного интеллекта большинство из представленных задач могут быть автоматизированы и даже развернуты в режиме реального времени, что позволит установить действия до того момента, как будет нанесен какой-либо ущерб. Например, с помощью хорошо обученной нейронной сети возможно выявление подозрительного трафика в сети и отключение этих соединений по мере их возникновения. Нейронные сети могут идентифицировать новые образцы вредоносного программного обеспечения, ранее не включенные в имеющиеся сигнатуры.

Сегодня подавляющее большинство технологий искусственного интеллекта в информационной безопасности применяется в качестве типа вспомогательной системы «предупреждения». В любом случае окончательное решение принимает человек. Это обусловлено тем, что используемые нейронные сети недостаточно точны по сравнению с типичным аналитиком-человеком.

В сфере информационной безопасности на данный момент ответ на вопрос, следует ли доверять искусственному интеллекту, а не человеческому анализу – часто «нет». В некоторой степени должен произойти сдвиг в том, каким образом мы оцениваем современные технологии и их возможности, прежде чем в полном объеме доверим принятие решения развитым технологиям искусственного интеллекта.

Следующие несколько лет будут интересны в контексте информационной безопасности. Огромные объемы данных, которые могут быть сгенерированы, наряду с проблемами проведения крупномасштабного анализа, для принятия оптимального решения, являются идеальным сочетанием для обширных и успешных архитектур обучаемых нейронных сетей.

УДК 343.3

Н.С. Сорокун, Р.А. Карапетян

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ ПРИЧИН И УСЛОВИЙ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ОСНОВА ПРОФИЛАКТИКИ ТАКИХ ДЕЯНИЙ

В настоящее время наблюдается активное преобразование всех сфер жизнедеятельности граждан. Не остается без внимания и область информационных технологий, развитие которых стремительно возрастает. Становится невозможно уследить за всеми событиями в данной сфере. Создание современной техники, различных программ и приложений приводит к тому, что совершается множество преступлений в информационной среде. Данные обстоятельства ведут к неблагоприятным условиям в обществе. Уровень воспитания и нравственности становится низким, в результате чего падает и уровень развития людей. Современные технологии помогают не только развиваться и совершенствоваться, но и терять те качества, которые необходимы любому человеку для хорошей жизни.

Вопрос раскрытия и расследования преступлений, совершаемых с использованием компьютерных технологий, становится очень остро в последнее время. Прежде всего данный факт обусловлен необходимостью развития и совершенствования существующих методик расследования преступлений. Очевидно, что с развитием информационных технологий возникает необходимость в преобразовании стандартных ме-

тодик и средств. Однако внимание также стоит уделять и предупреждению преступлениям данного вида. В связи с чем видятся актуальными рассмотрение вопросов, связанных с причинами и условиями совершения компьютерных преступлений, а также изучение характеристики личности преступника и потерпевшего.

В настоящее время наблюдается повсеместное внедрение компьютерных технологий во все сферы жизнедеятельности общества. Основное внимание уделяется внедрению в производственные, экономико-финансовые и общественные отношения. Рассматриваемый процесс компьютеризации способствует развитию и совершенствованию жизни общества, а также приводят к появлению новых категорий преступных деяний. Такие преступления совершаются с использованием компьютерной информации и посредством компьютерных технологий.

По общему правилу данные преступления делятся на три категории: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для электронно-вычислительных машин (ЭВМ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Данные противоправные деяния находят свое отражение в нормах Особенной части Уголовного кодекса Российской Федерации.

Рассматриваемые группы преступлений представляют особый интерес, который прежде всего обусловлен характеристикой субъекта совершения компьютерных преступлений. Данный аспект объясняется тем, что обычный гражданин вряд ли способен совершить неправомерный доступ к компьютерной информации или создать вредоносную программу, не обладая специальными знаниями в области информационно-телекоммуникационных систем.

В 2020 г. наиболее распространены мошенничества в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70 % всех хищений, совершенных путем обмана или злоупотребления доверием (+73,4 %, 237,1 тыс.).

В 2021 г. мошенничество в сфере информационно-телекоммуникационных технологий составило 73 % всех хищений (249,2 тыс.), совершенных путем обмана или злоупотребления доверием. При этом существенно замедлились темпы их прироста (с 73,4 % в 2020 г. до 5,1 % в текущем).

За последние пять лет число таких преступлений увеличилось более чем в 11 раз, а удельный вес в структуре преступности возрос с 1,8 % до 25 %. Большинство «киберпреступлений» совершается с использованием сети Интернет (300,3 тыс.) или при помощи средств мобильной связи (218,7 тыс.).

Кроме того, по своей природе компьютерные преступления носят латентный характер. Немаловажным элементом выступает также и харак-