УДК 004.896

ПЕРСПЕКТИВНЫЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК

Скуднев Д.М., Дьяков Н.С., Гулин А.С., Сазонова А.В.

ФГБОУ ВО «Липецкий государственный педагогический университет имени П.П. Семенова-Тян-Шанского», Липецк, e-mail: sdm81@rambler.ru

В статье рассмотрены основные вопросы искусственного интеллекта. Вопрос применения искусственного интеллекта сегодня активно обсуждается во всех отраслях. Потенциал искусственного интеллекта в некоторых областях огромен. Специалисты по информационной безопасности тоже погружаются в эту тему. Но параллельно с работой над искусственным интеллектом большие исследования идут в области изучения физиологии головного мозга человека. Самая значительная по агрегатному ущербу часть утечек данных происходит там, где информация чаще всего создается, используется и хранится: на персональных компьютерах, рабочих станциях и мобильных устройствах обычных пользователей корпоративных ИС. Все эти работы ведутся с целью обеспечения защиты информации и информационных систем, в том числе и облачных. В современном, динамически развивающемся мире происходит эволюция угроз, ежедневно обнаруживаются новые угрозы, большинство из них скрыты и трудно идентифицируются, скрыты и маскируются под обычные приложения, службы, сервисы и т.д. Государства объединились в международное сотрудничество в области информационной безопасности. Искусственный интеллект в сфере защиты информации и информационных систем только начинает своё развитие, но мы уже имеем немало интересных изобретений.

Ключевые слова: искусственный интеллект, мозг человека, вредоносные программы, защита информации, информационные системы, кибератака, факторы риска, киберпространство

PROMISING OPPORTUNITIES FOR USING ARTIFICIAL INTELLIGENCE TO PREVENT CYBER ATTACKS

Skudnev D.M., Dyakov N.S., Gulin A.S., Sazonova A.V.

Lipetsk State Pedagogical P. Semenov-Tyan-Shanskiy University, Lipetsk, e-mail: sdm81@rambler.ru

The article discusses the main issues of artificial intelligence. The issue of using artificial intelligence is currently being actively discussed in all industries. The potential of artificial intelligence in some areas is huge. Information security specialists are also immersed in this topic. But in parallel with the work on artificial intelligence, much research is being done in the field of studying the physiology of the human brain. The most significant part of data leaks in terms of aggregate damage occurs where information is most often created, used, and stored: on personal computers, workstations, and mobile devices of ordinary corporate IP users. All these works are carried out in order to ensure the protection of information and information systems, including cloud-based ones. In the modern, dynamically developing world, threats are evolving, new threats are detected every day, most of them are hidden and difficult to identify, hidden and disguised as ordinary applications, services, services, etc. States have United in international cooperation in the field of information security. Artificial intelligence in the field of information security and information systems is just beginning to develop, but we already have a lot of interesting inventions.

Keywords: artificial intelligence, human brain, malware, information protection, information systems, cyber-attack, risk factors, cyberspace

Вопрос применения искусственного интеллекта сегодня активно обсуждается во всех отраслях. Потенциал искусственного интеллекта (ИИ) в некоторых областях огромен. Специалисты по информационной безопасности также начинают использовать возможности искусственного интеллекта, для повышения защищенности систем. В отличие от отраслей промышленности, непосредственное применение искусственного интеллекта в информационной безопасности не дает необходимого эффекта.

Цель исследования: рассмотреть современные перспективные возможности использования искусственного интеллекта для предотвращения кибератак.

Материалы и методы исследования

На материалах нашумевших кибератак 2017 и 2018 гг. провести исследование, как применять искусственный интеллект в кибербезопасности.

Результаты исследования и их обсуждение

Применение искусственного интеллекта в различных сферах деятельности человека меняет индустриальный ландшафт:

– ИИ ведет к изменению архитектуры вычислений и к дальнейшему изменению отрасли. NVIDIA, Google и Intel борются за доминирующее место в будущем.

– ИИ – следующая главная операционная составляющая предприятия.

– Приложения ИИ для вертикальных отраслей могут предоставляться на основе технологических платформ.

– Стремление быть лидером в области цифрового «мозга» становится стратегическим видением ИТ-гигантов.

– Облачные сервисы будут интегрировать облачные вычисления, большие данные и искусственный интеллект.

Но параллельно с работой над искусственным интеллектом большие исследования идут в области изучения физиологии головного мозга человека.

BrainInitiative: исследование работы мозга человека (с 2013 г., 4,5 мрлд долл. США).

SyNAPSE: разработка крупномасштабных электронных нейроморфных компьютерных прототипов (2008–2016 гг.).

Human Brain Project: исследование ИКТ и здравоохранения в будущем (с 2013 г., 1 млрд евро).

Brain/Minds: исследование мозга мартышки с целью изучения функций и заболеваний мозга (с 2014 г., 270 млн долл. США).

China Brain Project: исследование нервной основы когнитивной функции для улучшения диагностики и профилактики заболеваний головного мозга, (10 млрд юаней), разработка вычислительных систем с когнитивными, обучающими и умственными способностями (под руководством HRL).

Human Brain Project: нейронаука, медицина и вычислительная техника в будущем. Стратегические данные человеческого мозга, когнитивно-поведенческая архитектура, теоретическая нейробиология, нейроинформатика, моделирование мозга, медицинская информатика и другие.

Brain/Minds: определение функции мозга с использованием МРТ и других технологий. Сбор и анализ соответствующей информации, такой как изображение мозга.

Local brain project: исследование алгоритмических моделей, обработки информации и моделирования мозга, разработка систем мозга, которая включает в себя проектирование систем, имитационное моделирование и аппаратные материалы.

Все эти работы ведутся с целью обеспечения защиты информации и информационных систем, в том числе и облачных. В современном, динамически развивающемся мире происходит эволюция угроз, ежедневно обнаруживаются новые угрозы, большинство из них скрыты и трудно идентифицируются, скрыты и маскируются под обычные приложения, службы, сервисы и т.д.

Целевые атаки и уязвимости нулевого дня проникают в сеть при первой возможности. Новые виды вредоносных программ быстро распространяются.

Вот как выглядит гонка со временем для борьбы с целевыми атаками и среднее время атаки на предприятие:

– каждую 81 секунду загружается известное вредоносное ПО;

– каждые 4 секунды происходит загрузка неизвестной вредоносной программы;

– каждые 32 минуты раскрываются ключевые данные;

– каждые 53 секунды хост-зомби подключается к внешнему C&C серверу (Command and Control server);

– каждые 5 секунд Хост посещает вредоносный сайт;

Защита против целевых атак – это гонка со временем.

Вот какую аналогию проводит Илья Медведовский в своей статье «Робот-хакер. Как применять искусственный интеллект в кибербезопасности»: «Один из самых защищенных аэропортов в мире Бен Гурион славится своей многоуровневой системой безопасности, при этом в самом аэропорту сложно встретить вооруженную охрану. При подъезде на первом и единственном внешнем пункте досмотра водитель с пассажирами вынужден снизить скорость почти до нуля, попадая под объективы видеокамер. А далее дорога делает многокилометровый вираж до терминала. Это сделано явно намеренно.

За время, пока машина преодолеет путь от пункта досмотра до терминала, система безопасности успеет проанализировать личности пассажиров и – в случае обнаружения признаков опасности – они будут остановлены до входа в здание аэропорта, не причинив никому вреда. Похожим образом работает система поведенческого анализа аномалий в компьютерной системе на основе искусственного интеллекта. После успешного проникновения злоумышленник не может моментально нанести ущерб – ему нужно время, чтобы разобраться в системе и понять, как она устроена.

Он будет запускать определенные команды, транзакции, пытаться устанавливать специализированный софт и т.п., то есть его поведение будет отличаться от поведения обычного пользователя, а значит, за это время система поведенческого анализа на основе ИИ будет способна обнаружить вторжение и предотвратить его до нанесения ущерба. В этих направлениях мы действительно ждем прорыва. И результаты работы таких систем позволяют рассчитывать на то, что он уже начался» [1].

Рассмотрим возможность отображения пути атаки и полную трассировку атаки.

Полный путь атаки

– Отображение пути атаки на основе цепочки атак.

– Отображение различного поведения атаки на разных узлах.

Интеллектуальный анализ данных на всем пути атаки

– Интеллектуальный анализ угроз.

– Интеллектуальный анализ аномальных событий.

– Интеллектуальный анализ данных трафика.

– Интеллектуальный анализ журналов.

Интеллектуальное обнаружение: интеллектуальная модель обнаружения угроз безопасности на основе больших данных и ИИ.

– Обнаружение аномалии сетевого трафика.

– Обнаружение аномалий передачи почты.

– Обнаружение скрытых каналов.

– Обнаружение соединения C&C.

– Обнаружение аномалий веб-доступа.

– Проверка зашифрованного трафика.

Нашумевшие кибератаки 2017 г. в цифрах

WannaCry (05.2017) [2], Petya (06.2017) [3], Bad Rabbit (10.2017) [4], пострадали 150 стран, > 300 тысяч узлов, > 80 организаций, > $2 млрд ущерба.

2017-05: EternalBlue WannaCry: атака на 19 медицинских учреждений в Англии. Были заражены около 45 000 хостов в 74 странах, сумма выкупа – 13 500 000 долларов США, убытки в миллиарды долларов США.

2017-06: Petya Petya: атака на системы «Роснефти», Государственного сберегательного банка Украины и правительства и компьютер вице-премьера Украины.

2017-10: Bad Rabbit: Bad Rabbit: атака на страны Восточной Европы. Пострадали правительства и бизнес-структуры в России, Украине, Германии и Турции.

Рассмотрим пути проникновения угроз: электронная почта, ссылки на недоверенные ресурсы, съемные носители, прямое подключение из Интернета.

Факторы риска кибератак WannaCry/Petya: архитектура операционной системы (ОС) Windows, уязвимый сервис по умолчанию, распространенность ОС Windows, сетевая архитектура ОС.

Сюда также можно отнести отсутствие процессов управления: обновлениями, уязвимостями, неконтролируемый BYOD (bring your own device, принеси собственное устройство), несовершенство СЗИ (средств защиты информации), человеческий фактор.

Чтобы минимизировать риск кибератак WannaCry/Petya, необходимо: резервное копирование, сетевая архитектура, сегментация, отключение неиспользуемых сервисов ОС.

Организация процессов управления: обновлениями, уязвимостями, контроль доступа в сеть, эшелонированная защита, осведомленность пользователей.

Наиболее значительные факты утечки данных в 2018 г.

Январь 2018 Региональное управление здравоохранения, Норвегия

Злоумышленники взломали систему Регионального управления здравоохранения Южной и Восточной Норвегии (Helse Sør-Øst RHF) и получили доступ к персональным данным и медицинским записям около 2,9 млн норвежцев (более половины всех жителей страны). Похищенные медицинские данные содержали информацию о сотрудниках правительства, секретной службы, военных, политиках и других общественных лицах.

Рособрнадзор, Россия

Утечка информации о дипломах и сопутствующих им прочих персональных данных с вебсайта Федеральной службы по надзору в сфере образования и науки. В сеть утекла база данных о бывших студентах объемом более 5 Гб, с общим количеством записей около 14 млн.

Уязвимость была обнаружена в онлайн-сервисе проверки действительности дипломов о высшем образовании. В поля для реквизитов можно вписать произвольный код (провести SQL-инъекцию), который исполняется сервером. В результате такой SQL-инъекции утекли такие данные, как серия и номер диплома, год поступления, год окончания, СНИЛС, ИНН, серия и номер паспорта, дата рождения, национальность, учебная организация, выдавшая документ.

Апрель 2018 Delta Air Lines, Best Buy и Sears Holding Corp.

Целевая атака специального вредоносного ПО на приложение для онлайн-чата компании [24]7.ai (калифорнийская компания из Сан-Хосе, разрабатывает приложения для онлайн-обслуживания клиентов). Утекли полные данные банковских карт – номера карт, CVV-коды, даты истечения, имена и адреса владельцев.

Известно только примерное количество утекших данных. Для Sears Holding Corp. это чуть менее 100 тыс. банковских карт, для Delta Air Lines это сотни тысяч карт (точнее авиакомпания не сообщает). Количество скомпрометированных карт для Best Buy – неизвестно. Все карты утекли в период с 26 сентября по 12 октября 2017 г.

Компании [24]7.ai потребовалось более 5 месяцев с момента обнаружения атаки на свой сервис, чтобы уведомить клиентов (Delta, Best Buy и Sears) об инциденте.

Самая значительная по агрегатному ущербу часть утечек данных происходит там, где информация чаще всего создается, используется и хранится: на персональных компьютерах, рабочих станциях и мобиль-

ных устройствах обычных пользователей корпоративных ИС [5].

Большинство утечек данных – инсайдерские. Из аналитического отчета Ponemon Institute: «2018 Cost of Data Breach Study» следует, что:

– ошибки сотрудников являются причиной около 27% утечек данных;

– большинство из 48% уязвимостей, связанных с вредоносным ПО или криминальными атаками, используют злоумышленников-инсайдеров или фишинг и социальную инженерию.

Из опроса «Data Protection Risks & Regulations in the Global Economy» можно заключить, что недобросовестные сотрудники и злоумышленники – ключевая причина утечек данных в 69% опрошенных организаций.

Государства объединились в международное сотрудничество в области информационной безопасности.

Основными документами в области информационной безопасности являются:

1. Резолюция по информационной безопасности «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятая ООН 5 декабря 2018 г.

2. «Парижский призыв к доверию и безопасности в киберпространстве» представлен во время Всемирного форума по управлению интернетом в Париже 12 ноября 2018 г. (вместе с речью президента Франции Эмманюэля Макрона).

3. Рекомендации Глобальной комиссии по киберстабильности (Сингапурский пакет, принятый в ноябре 2018 г.).

Все документы отмечают повышение роли государств в процессе управления интернетом вообще и в особенности в вопросах обеспечения информационной безопасности.

Резолюция ООН: Практически все пункты положения призывают государства предпринимать какие-то шаги, только 3 из 25 предусматривают действия со стороны негосударственных.

Парижский призыв: основная роль отводится мультилатеральному подходу, то есть межгосударственному взаимодействию на различных площадках. Другим стейкхолдерам отводится второстепенная роль.

Сингапурский пакет: угрозы со стороны государств признаются наиболее значимыми, и государствам же отводится основная роль по их предотвращению.

Основной механизм сдерживания это ответственное поведение государств (и других участников) в киберпространстве. Государствам предлагается осознанно подойти к выбору инструментов для защиты своих интересов в сети с учетом возможных последствий для «ядра интернета» (Internet public core). Предлагается наделить наднациональные структуры правом следить за тем, как государства соблюдают принципы, изложенные в каждом из документов.

Вместе с угрозами для «публичного ядра интернета» (инфраструктуры) выделяются некоторые сравнительно новые направления:

1. Защита персональных данных.

2. Социально опасный контент (кибербуллинг, призывы к суициду).

3. Вмешательство в выборы, атаки на электронные системы голосования и обработки информации.

4. Атаки на устройства интернета вещей.

5. Атаки на электронные системы, которые обслуживают физическую инфраструктуру поставок различных товаров.

Из этих документов можно сделать вывод, что:

1. Современные документы базируются на одних и тех же предположениях, поэтому в них заявлены настолько похожие подходы к решению проблем информационной безопасности.

2. Главное достижение в вопросах международного сотрудничества по информационной безопасности – это сам факт наличия такого процесса.

Заключение

Искусственный интеллект в сфере защиты информации и информационных систем только начинает своё развитие. Защитить личную информацию и информацию организации становится сложнее. Но время не стоит на месте, а потому будущие массовые атаки на пользователей с применением развитого искусственного интеллекта приведут к появлению нового уровня систем защиты, основанного на искусственном интеллекте, который поможет защитить конфиденциальную информацию.

Список литературы

1. Робот-хакер. Как применять искусственный интеллект в кибербезопасности. Forbes. [Электронный ресурс]. URL: https://www.forbes.ru/tehnologii/354793-robot-haker-kak-primenyat-iskusstvennyy-intellekt-v-kiberbezopasnosti (дата обращения: 20.07.2020).

2. Investigation: WannaCry cyber-attack and the NHS. National Audit Office. [Электронный ресурс]. URL: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/ (дата обращения: 20.07.2020).

3. Petya, NotPetya или Petna. Xakep. [Электронный ресурс]. URL: https://xakep.ru/2017/06/28/petya-write-up/ (дата обращения: 20.07.2020).

4. Россиян и украинцев атаковал новый вирус-вымогатель «Плохой кролик». LENTA.RU. [Электронный ресурс]. URL: https://lenta.ru/news/2017/10/24/bad_rabbit/ (дата обращения: 20.07.2020).

5. Газин А.И., Зияутдинов В.С., Скуднев Д.М., Исаева А.В. Оценка уровня информационно-психологического воздействия различных источников информации на молодую личность // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2019. № 4. С. 152–161.