Опубликовано: 1 декабря 2025 ИСТОЧНИК: НАРОДНАЯ ГАЗЕТА

Белорусские специалисты совершенствуют методики борьбы с вредоносными компьютерными программами

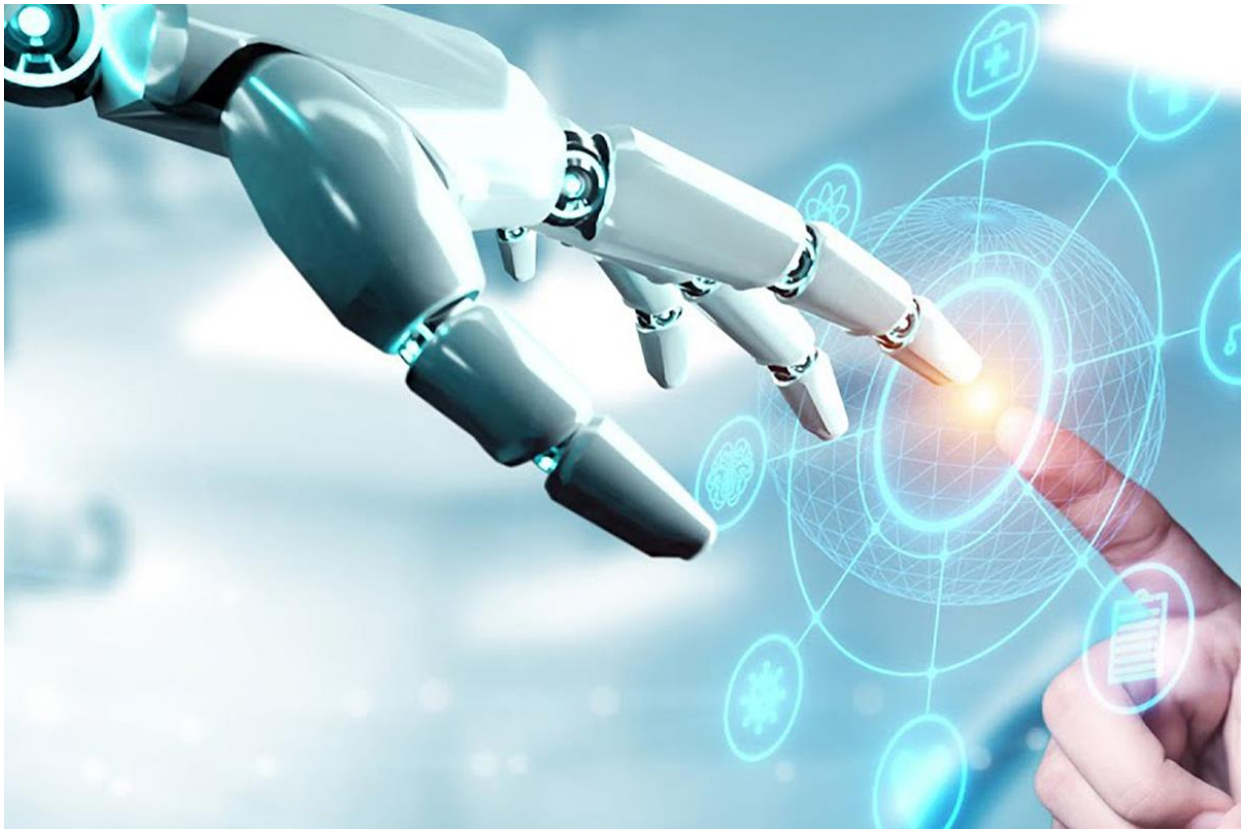
Противостояние в сети

Искусственный интеллект активно используется в бизнесе для автоматизации процессов, улучшения принятия решений и повышения эффективности. Умные технологии помогают в маркетинге, финансах, производстве, логистике, HR, продажах и других областях экономики. Однако чем глубже ИИ интегрируется в бизнес-процессы, тем серьезнее становятся связанные с этим риски. Чего от них ждать и как противостоять — об этом наша беседа с заведующей кафедрой защиты информации БГУИР кандидатом технических наук Ольгой Бойправ.

Хакер или защитник?

— Ольга Владимировна, известно о первом вирусе, созданном искусственным интеллектом. Это начало новой массовой тенденции?

— Искусственный интеллект сейчас инструментарий не только в руках разработчиков средств защиты информации, но и в руках киберпреступников. ИИ уже успешно справляется с написанием программных кодов. Между тем вредоносное ПО — это тот же самый программный код.



Помимо этого, благодаря искусственному интеллекту сейчас формируются базы для реализации парольных кибератак. Современные алгоритмы, обученные на огромных базах утекших данных, позволяют предсказывать сложные комбинации паролей. Даже надежные на первый взгляд пароли, если они следуют популярным шаблонам, становятся уязвимыми.

— Вместе с этим ИИ помогает обнаруживать атаки и защищать систему?

— Верно, ряд антивирусных программ создан с использованием технологий искусственного интеллекта. Они называются эвристические. Суть в чем? Программа обнаруживает вредоносное ПО, анализируя его «поведение», а не только сверяясь с базой известных вирусов (как это делали более ранние антивирусы). Этот метод позволяет находить неизвестные угрозы, ища подозрительные признаки, такие как попытки самоскрытия, внедрение в другие процессы или использование опасных функций. И в принципе, можно сказать, что алгоритм функционирования этих средств уже предполагает самообучение.

Не все подряд

— Если говорить о бизнесе, который применяет нейросети каждый день, какие правила должны стать базовыми для сотрудников?

— Важно понимать, какие данные вы «скармливаете» нейросети. Например, у вас база пациентов и стоит задача определить статистику заболеваемости по месяцам. Прежде чем дать нейросети весь пласт данных, в котором информация о том, какой пациент, когда обращался, с какой жалобой, как долго пробыл на больничном, надо бы это все обезличить. Иными словами, убрать из этого массива данных те атрибуты, по которым точно можно сказать, что данные о заболевании характерны для конкретного человека. В первую очередь это Ф.И.О., дата рождения, адрес.

Наряду с персональными данными стоит помнить, что не должна утечь в нейросеть информация, которая относится к коммерческой тайне. Не говоря уже о госсекретах и служебной информации ограниченного распространения. В противном случае это трансграничная передача данных, которая является нарушением закона.

Если говорить о случаях, когда ИИ используют для того, чтобы разработать ПО, рисков не так много. Например, когда нейросети «скармливают» код в целях поиска ошибки. Угроза утечки не столь велика за счет того большого массива программных кодов, который искусственный интеллект постоянно обрабатывает.

Внезапный удар

— С какими атаками компании сталкиваются чаще всего?

— Пока разновидности кибератак из года в год остаются прежними. Все они нацелены либо на то, чтобы снизить конкурентоспособность организации на рынке, либо на то, чтобы добыть какие-то данные из информационной системы.

ФОТО GETTYIMAGES

В первую очередь речь о DDoS-атаках, которые направлены на то, чтобы вызвать отказ в обслуживании. Сервер обрабатывает массу бесполезных запросов, поступающих от ботнета, и перестает отвечать реальным пользователям. Это удар по репутации и работе компании. К слову, недавно самой масштабной DDoS-атаке за 2025-й подверглась облачная платформа Microsoft Azure. Мощность достигала 15,72 терабита в секунду, атаковали более чем 500 тысяч IP-адресов.

Фишинг

Вторая форма атаки — фишинговая рассылка. Она нацелена на то, чтобы перехватить пароли от учетных записей пользователей информационной системы, дальше, уже применяя эти данные, планировать другие кибератаки на эту систему. Классика жанра — в письме ссылка на внешний ресурс. С виду он может быть похож, например, на ту же самую страницу для ввода логина и пароля в системе Google либо корпоративной почтовой системе. Никаких подозрений у пользователя это, к сожалению, как правило, не вызывает, он вводит свои учетные данные, а они попадают к мошеннику.

Рассылки

Пример другого варианта «вредоносной» почты — письмо с текстом «срочно проверить дебиторскую задолженность, информация в прикрепленном файле», где как раз таки вредоносный программный код, который шифрует активы информационной системы. Такая форма

«вредоносной» рассылки придумана для того, чтобы вымогать с организации деньги.

Человеческий фактор

И конечно, нельзя не упомянуть про классический подход к добыванию ценных сведений. В этом случае целью злоумышленников является именно человек. Преступники ищут сотрудника, которого можно подкупить или запугать, а взамен получить искомую информацию (и никакие кибератаки не нужны). Чаще всего выбирают тех, кто переживает трудности, недоволен зарплатой или ощущает несправедливость.

С их помощью можно получить доступ к данным быстрее, чем с помощью технических средств. Поэтому специалист по безопасности должен работать не только с железом, но и с людьми. Иногда важно просто вовремя заметить, что сотрудник демотивирован или устал, и реагировать на это. Поэтому на первом курсе наши студенты изучают дисциплину «Социально-психологические аспекты информационной безопасности», в рамках которой учим в том числе и премудростям работы с людьми.

На страже цифровых интересов

— Насколько сегодня востребованы специалисты в области кибербезопасности?

— Несмотря на то что второй год подряд на 30 % увеличиваем набор, мы не в силах удовлетворить все заявки на специалистов. Почему вырос спрос? Есть Указ № 40 «О кибербезопасности», подписанный Президентом в 2023-м, согласно которому в ряде организаций должны быть созданы киберцентры. Они работают 24/7, соответственно, их необходимо комплектовать кадрами. Пока у нас в стране идет процесс насыщения рынка этими специалистами. Когда он закончится, во многом востребованность в работниках будет зависить от масштабов кибератак, реализуемых на информационные системы.

— Угрозы совершенствуются, и обновлять быстро и часто учебные пособия очень сложно. Удается ли готовить специалистов, которые на выходе из вуза подкованы в своем деле?

— Ключевые угрозы пока неизменны. В связи с этим у сотрудников

должны быть развиты базовые компетенции: поиск уязвимостей в информационной системе, анализ процессов, которые могут ассоциироваться с исполнением вредоносного ПО, резервное копирование данных. С этого начинается кибербезопасность. Когда планируется атака, преступник ищет слабые места в системе. Одна из задач, которая решается в этом поиске, — сбор информации о том, какое ПО используется в информационной системе организации. А уж если известно, какое оно, можно понять и слабые места. Ключевая базовая задача безопасника — эти уязвимости своевременно закрывать.

Разобраться с актуальным ландшафтом киберугроз нам помогают наши партнеры. Сейчас совершенствуем учебные программы в тесном взаимодействии с вендорами современных программных средств, которые применяются для защиты информации в информационных системах. На базе университета работает две совместные лаборатории, первую открыли с организацией «Код безопасности», вторую — с «Лабораторией Касперского». Благодаря работе с ними мы можем актуализировать подходы к подготовке наших специалистов.

Александра ЯНКОВИЧ

Фото: Дарья ТИТОВА