УДК 004.8
DOI: 10.33764/2618-981X-2021-6-131-135

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ ПРИ ПОМОЩИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Василий Сергеевич Кизин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел. (909)534-64-77, e-mail: pikachy159@gmail.com

Сергей Николаевич Новиков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, профессор кафедры информационной безопасности, тел. (383)269-22-45, e-mail: snovikov@ngs.ru

По мере того, как виртуальные рабочие среды становятся все более сложными, задача защиты конфиденциальных данных организации от случайного или преднамеренного раскрытия и соблюдения нормативных требований становится всё сложнее. С помощью решений безопасности на базе искусственного интеллекта, специально созданных для мониторинга платформ совместной работы, организации могут выявлять и реагировать на риски в режиме реального времени, чтобы защитить свои данные и данные своих сотрудников.

Ключевые слова: видеоконференция, искусственный интеллект, информационная безопасность

IMPROVING VIDEO CONFERENCE SECURITY WITH ARTIFICIAL INTELLIGENCE

Vasily S. Kizin
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, phone: (909)534-64-77, e-mail: pikachy159@gmail.com

Sergei N. Novikov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor, Department of Information Security, phone: (383)269-22-45, e-mail: snovikov@ngs.ru

As virtual workspaces become more sophisticated, the challenge of protecting an organization's sensitive data from accidental or intentional disclosure and compliance is becoming more challenging. With AI-powered security solutions specifically designed to monitor collaboration platforms, organizations can identify and respond to risks in real time to protect their data and that of their employees.

Keywords: video conferencing, artificial intelligence, information security

Введение

Инструменты видеоконференцсвязи, такие как Zoom [1], получили глобальную базу пользователей во время пандемии в прошлом году. Для миллионов профессионалов COVID-19 резко ускорил изменения в работе [2]. Инструменты видеоконференцсвязи и совместной работы, такие как Microsoft

Teams [3], Zoom и Google Meet [4], стали основой повседневной рабочей жизни. Многие из нас проводят дни, переключаясь между несколькими различными видеоконференциями, демонстрацией экрана, каналами чата и службами обмена сообщениями в реальном времени, когда мы виртуально координируем свою работу с нашими коллегами.

Рост использования этих инструментов сотрудничества был астрономическим. Этот внезапный переход к работе из любого места и появление современных платформ для видео-сотрудничества повысили эффективность и позволили многим людям безопасно работать во время глобальной пандемии. Однако это также повысило необходимость безопасности данных, соответствие нормативным требованиям и юридические риски для любой организации, использующей эти платформы для совместной работы. Те, кому поручено следить за этими рисками безопасности и соответствия, изо всех сил стараются не отставать.

Материалы

Видеоконференции, совместное использование файлов, совместное использование приложений, совместное использование экрана, чат, веб-камеры и цифровые доски — все это потенциальные средства защиты данных или нарушения нормативных требований. Риски, несомненно, велики - от взлома Zoom до закрытых собраний, случайного чрезмерного распространения конфиденциальной информации на экране и неприятных инцидентов с персоналом, которые могут привести к жалобам со стороны персонала и репутационному ущербу.

Поскольку корпоративные организации регистрируют тысячи часов совещаний с помощью этих инструментов, для сотрудников службы безопасности практически невозможно гарантировать, что все, что отображается на экране, о чем говорится, передается при загрузке файла или набирается в окне чата, обеспечивает конфиденциальность и соблюдение нормативных требований. Традиционные методы мониторинга коммуникаций, такие как сбор и последующее сканирование записей, основанные на простом поиске слов, упускают важные визуальные подсказки и нехватку контекстного понимания, что может привести к пропуску инцидентов с высоким риском или, наоборот, к выявлению ложных срабатываний. К счастью, достижения в области искусственного интеллекта (ИИ) [5], машинного обучения (МО) [6] и обработки естественного языка (ОЕЯ) [7] позволяют специалистам по безопасности эффективно управлять сложными приложениями для совместной работы, отслеживать их и составлять отчеты, а также помогают защитить конечных пользователей от совершая дорогостоящие ошибки.

Результаты

Искусственный интеллект изменит способы, которыми организации могут улучшить безопасность и соответствие требованиям для современных платформ для совместной работы, вот три основных способа, которыми они могут это сделать.

Определить масштаб риска.

При таком количестве цифрового контента, который создается на платформах для совместной работы, сотрудники по безопасности не могут контролировать и проверять все, что передается, отображается, набирается или говорится в сообщениях сотрудников. Современные решения для обеспечения безопасности и соблюдения нормативных требований, разработанные специально для этих платформ для совместной работы, используют не только искусственный интеллект и глубокое обучение, но и тщательно подобранные средства обнаружения рисков, созданные экспертами для быстрого анализа всех данных с целью выявления любых инцидентов или действий, которые могут представлять риск для организации.

Эти обнаружения могут использовать и имеют смысл из нечеткого сопоставления неточного текста, а также анализа изображений, оптического распознавания символов (OPC) [8], транскрипции и многого другого, чтобы идентифицировать и отмечать инциденты, которые беспокоят специалиста по безопасности. Используя ИИ и анализируя различные фрагменты контента разговора, эти технологии могут учитывать контекст и намерения ситуации, чтобы более точно определять, какие ситуации представляют собой риск, а какие нет. По сути, ИИ помогает быстро и эффективно сузить кругозор от огромных объемов данных до тех инцидентов, которые необходимо проанализировать.

Расставить приоритеты по уровням риска.

Во-вторых, ИИ помогает автоматизировать процесс проверки, эффективно расставляя приоритеты и упорядочивая инциденты, которые представляют наибольший риск, и передает их в группы безопасности и соответствия для немедленного рассмотрения. Понимая контекст и цель разговора, а также то, что потенциально плохое произошло или каких хороших результатов не было в разговоре, на экране или в чате, решения на основе искусственного интеллекта могут фильтровать сигнал от шума и назначать риск оценка конкретных действий и поведения в течение сеанса. Отмеченные инциденты отображаются на визуальной панели управления, что упрощает для проверяющих точный момент в записи, когда происходит инцидент, для более быстрого и эффективного реагирования. Более того, системы искусственного интеллекта и машинного обучения учатся на предыдущих инцидентах и становятся лучше обученными с каждым событием, пока в конечном итоге они не смогут заранее рекомендовать соответствующие действия на основе предыдущих ответов. Назначая оценки рисков, расставляя приоритеты для инцидентов для немедленного рассмотрения и рекомендуя действия, которые необходимо предпринять, ИИ может помочь специалистам в области безопасности и соблюдения требований более эффективно выявлять и устранять ситуации с высоким риском, прежде чем они станут более серьезной проблемой или приведут к серьезной утечке данных.

Предупреждать конечных пользователей о рисках в режиме реального времени.

Способность ИИ улучшать безопасность и соответствие на платформах видеосвязи не имеет ничего общего с оптимизацией работы специалиста по безопасности. Скорее, он помогает предупреждать и информировать конечного пользователя (сотрудника организации) в режиме реального времени о рискованном или потенциально несоответствующем поведении, которое он может совершить. Консультанты по соблюдению нормативных требований на базе искусственного интеллекта, встроенные в современные инструменты безопасности, поддерживают сотрудников во время сеансов видеоконференций и чатов с предупреждениями и напоминаниями в реальном времени, снижающими риск [9]. Например, когда пользователь участвует в собрании и предоставляет общий доступ к своему экрану, система напоминает ему о том, что необходимо принять меры предосторожности, чтобы не «поделиться» сообщением на этом собрании, которое также напоминает им о безопасности совместной работы и мониторинге соответствия.

Благодаря этой способности понимать контекст встреч, помощники по соответствию на базе искусственного интеллекта могут автоматически предупреждать пользователей и напоминать им о передовых методах обеспечения безопасности данных и соответствия требованиям при участии в потенциально рискованных действиях или разговорах.

Заключение

Переход к работе из любого места и развитие современных инструментов видеоконференцсвязи и совместной работы продолжатся в ближайшие месяцы и годы. Недавний опрос показал, что 55 процентов работников хотят иметь возможность продолжать работать из дома даже после того, как мы победим COVID-19 [10]. Таким образом, сотрудники по безопасности не могут должным образом контролировать эти сложные унифицированные коммуникационные платформы и платформы для совместной работы без использования ИИ и машинного обучения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Видеоконференции и чат Zoom [Электронный ресурс]. URL: https://zoom.us/ru-ru/meetings.html/ (дата обращения: 05.03.2021).

2. Жуков Р. Обеспечиваем кибербезопасность удалённой работы сотрудников во время пандемии COVID-19 - Anti-Malware [Электронный ресурс]. URL: https://www.anti-malware.ru/practice/methods/Employee-Remote-Work-Cybersecurity/ (дата обращения: 05.03.2021).

3. Платформа для собраний, чатов, звонков и совместной работы Microsoft Teams [Электронный ресурс]. URL: https://www.microsoft.com/ru-ru/microsoft-teams/group-chat-software/ (дата обращения: 05.03.2021).

4. Сервис защищённых видеоконференций Google Meet [Электронный ресурс]. URL: https://meet.google.com// (дата обращения: 05.03.2021).

5. Шабанов А. Применение технологий искусственного интеллекта в информационной безопасности – Anti-Malware [Электронный ресурс]. URL: https://www.anti-

3. Платформа для собраний, чатов, звонков и совместной работы Microsoft Teams [Электронный ресурс]. URL: https://www.microsoft.com/ru-ru/microsoft-teams/group-chat-software/ (дата обращения: 05.03.2021).

4. Сервис защищённых видеоконференций Google Meet [Электронный ресурс]. URL: https://meet.google.com// (дата обращения: 05.03.2021).

5. Шабанов А. Применение технологий искусственного интеллекта в информационной безопасности – Anti-Malware [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security/ (дата обращения: 10.03.2021).

6. Машинное обучение в информационной безопасности - Kaspersky [Электронный ресурс]. URL: https://www.kaspersky.ru/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity/ (дата обращения: 10.03.2021).

7. Милютин И. Что такое обработка естественного языка - NeuroHive [Электронный ресурс]. URL: https://neurohive.io/ru/osnovy-data-science/5-metodov-v-nlp-kotorye-izmenjat-obshhenie-v-budushhem// (дата обращения: 10.03.2021).

8. Лобков И. Оптическое распознавание символов - Habr [Электронный ресурс]. URL: https://habr.com/ru/post/330936// (дата обращения: 13.03.2021).

9. Меры по обеспечению информационной безопасности - SearchInform [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/mery-po-obespecheniyu-informatsionnoj-bezopasnosti/ / (дата обращения: 22.03.2021).

10. Логинов Д. М. Портал социологических данных РАНХиГС [Электронный ресурс]. URL: https://social.ranepa.ru/novosti/item/issledovanie-sociologov-ranhigs-vyyavilo-otnoshenie-rossiyan-k-rabote-v-udalennom-rezhime/ (дата обращения: 08.04.2021).