В настоящее время правоохранительные органы обладают различными не связанными между собой базами данных, хранящими множество информации из различных источников в разных форматах, которые не всегда имеют возможность подвергнуть анализу. Так, например, нет возможности подвергнуть анализу системным образом сведения о личности или характеристике преступников, описании места происшествия и иных сведений, между которыми сложно провести какие-либо взаимосвязи для установления неочевидных закономерностей, при этом CatBoost обладает необходимыми возможностями в анализе указанной информации.

В рамках данного исследования был изучен метод машинного обучения CatBoost для определения его положительных и отрицательных сторон и возможного использования его в своей служебной деятельности.

Метод машинного обучения CatBoost является разработкой IT-компании «Яндекс» и применяется ею в работе своих сервисов. Разработка уже нашла первое применение за пределами «Яндекса» в Европейском центре ядерных исследований (ЦЕРН). CatBoost используется для обработки данных эксперимента LHCb, который проходит на одноименном детекторе Большого адронного коллайдера. Для системы Министерства внутренних дел (МВД) метод проведения анализа CatBoost может предоставить ряд преимуществ, но также сопряжен с определенными ограничениями и недостатками.

Так, основным преимуществом использования CatBoost в правоохранительной деятельности является возможность обработки категориальных данных, т. е. способность автоматически обрабатывать категориальные признаки без необходимости их предварительного кодирования или преобразования в числовые значения. Используя CatBoost, не будет упущены текстовые данные, различные описания событий, места происшествий и многое другое.

Положительной стороной CatBoost также является его точность предсказаний, которая обладает потенциалом и может использоваться в прогнозировании преступлений, на основании изучения исторических и иных данных о преступлениях с выявлением неочевидных или даже нестандартных элементов, которые позволяют под другим углом рассмотреть имеющиеся данные. К этому можно добавить, что в основу метода заложен механизм борьбы «с переобучением», который реализуется в предотвращении излишнего «запоминания» тренировочных данных для прекращения обучения на определенном цикле изучения данных и последующей успешной обработки новых данных.

Положительной стороной CatBoost является также его скорость обучения, реализуемая в построении работы модели на анализе больших объемов разнообразных данных (количественных показателей, сведений о преступлениях, местах преступлений, сведений о преступнике и многом другом), которые обрабатываются в реальном времени. Составленная модель гибко реагирует при работе пополнения данных, что может эффективно использоваться при принятии управленческих решений.

CatBoost является свободно распространяемым и постоянно обновляемым компанией «Яндекс» программным обеспечением, которое имеет большое сообщество разработчиков, предоставляющих техническую и обучающую документацию по изучению данного метода. После установки на локальный компьютер работа с библиотекой не требует подключения к сети Интернет, в связи с этим соблюдается конфиденциальность анализируемых данных, и следовательно, она применима в системе МВД.

Рассмотрим недостатки в использовании CatBoost, которые выходят из положительных сторон метода. Для проведения эффективного анализа различных данных они должны быть приведены к определенному единообразному виду, т. е. для примера при описании места происшествия необходимо придерживаться определенных норм отражения обстановки, для успешного категорирования этих данных программой и пр. Стоит также учитывать, что эффективный анализ данных будет проведен при наличии большого количества развернутых данных по каждому анализируемому событию. Следовательно, заинтересованным подразделениям необходимо проработать порядок учета и описания событий, подвергаемых анализу в базах данных МВД.

Для эффективного использования CatBoost требуются опыт и понимание работы с методами машинного обучения. Это может потребовать наличия квалифицированных сотрудников в области анализа данных со знанием программирования на языках программирования Python или R, на подготовку которого также потребуется время и финансовые затраты, при этом следует учитывать о дополнительном финансировании на приобретение компьютерного оборудования.

Недостатком CatBoost является также возможность в переобучении модели анализа и искажении результатов, что потребует от сотрудника контроля за работой модели и получаемого результата.

Таким образом, из описанного выше можно сделать вывод, что использование сотрудниками правоохранительных органов CatBoost в своей служебной деятельности может обеспечить возможности для улучшения прогнозирования, выявления закономерностей и оперативного реагирования на угрозы. Учитывая имеющиеся ограничения и требования к качеству предоставляемых данных, а также компетентности сотрудников, использование CatBoost позволит создавать более точные модели, которые способствуют более эффективному принятию решений и обеспечивают дополнительные инструменты для обеспечения безопасности общества.

УДК 342

Н.В. Михайленко

КОД НАСТОЯЩЕГО И БУДУЩЕГО ИНФОРМАЦИОННОГО ОБМЕНА И СОТРУДНИЧЕСТВА В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Проблема киберпреступности не ограничивается границами страны или континента, преступники действуют в международном масштабе, используя сложные технические методы и сети. Сложная и интернациональная природа киберпреступности создает уникальные вызовы для правительств, правоохранительных органов и частных компаний в борьбе с этой угрозой.

Киберпреступники не придерживаются государственных границ и могут нападать на объекты в разных странах, что создает потребность в совместных усилиях для защиты от таких атак. Международное сотрудничество в области кибербезопасности становится ключевым фактором в предотвращении и противодействии киберугрозам, поскольку способствует обмену опытом между странами и регионами, что позволяет учиться на ошибках других и создавать более эффективные стратегии борьбы. Партнерство между государствами и частным сектором также играет важную роль, так как бизнес часто является объектом кибератак, и его участие в обеспечении безопасности данных и информационных систем критически важно.

Таким образом, международное сотрудничество в области кибербезопасности необходимо для создания устойчивой и безопасной цифровой среды, где данные и технологии могут развиваться, не подвергаясь постоянным угрозам со стороны киберпреступников.

Международное сотрудничество в области кибербезопасности охватывает ряд основных направлений. Прежде всего это обмен информацией, который позволяет своевременно реагировать на киберугрозы, выявлять схемы атак и предотвращать их распространение.

Не менее важны обучение и экспертиза. В рамках данного направления целесообразны такие мероприятия, как обмен знаниями и опытом, повышение квалификации кадров, создание образовательных инициатив: международные партнеры могут поддерживать создание образовательных и исследовательских инициатив в области кибербезопасности, включая курсы, семинары и мастер-классы. Чрезвычайно полезны обмен экспертами для участия в совместных проектах, расследованиях инцидентов и разработке стратегий кибербезопасности, создание центров компетенции и исследовательских лабораторий, где ученые и специалисты могут совместно работать над решением сложных кибербезопасностных проблем, а также международные учения и симуляции, позволяющие странам проверить свои навыки и готовность к кибератакам в условиях, приближенных к реальным.

Международное сотрудничество включает в себя взаимоинформирование о новых угрозах и уязвимостях, разработку совместных методов анализа и реагирования на кибератаки, создание международных норм и стандартов в области кибербезопасности, а также предполагает совместные учения и тренировки, направленные на повышение квалификации профильных специалистов.

В современном мире, где цифровые технологии проникают во все сферы нашей жизни и бизнеса, обеспечение информационной безопасности (ИБ) становится критически важной задачей. Однако интеграция новых технологий в области ИБ несет с собой ряд сложностей и вызовов. Эти проблемы могут усложнить внедрение инновационных методов защиты данных и систем, оставляя организации уязвимыми перед киберугрозами.

Интеграция технологий в области информационной безопасности (ИБ) сталкивается с рядом серьезных проблем, затрудняющих эффективное обеспечение кибербезопасности в современном цифровом мире. Среди них:

1. Несовместимость технологий: различные продукты и решения ИБ могут быть несовместимыми между собой. Это усложняет интеграцию систем и может привести к неполной защите из-за разрывов в сетевой безопасности.

2. Сложность систем: для современных информационных систем характерны сложность и многоуровневость. Интеграция новых технологий в такие системы может вызвать конфликты и нестабильность.

3. Недостаток обученного персонала: дефицит специалистов в области ИБ, способных эффективно внедрять новые системы и управлять ими.

4. Бюджетные ограничения: ограниченные финансовые ресурсы могут стать препятствием для внедрения дорогостоящих систем ИБ, даже если они могут значительно улучшить кибербезопасность.

5. Динамичность киберугроз, которые постоянно эволюционируют: технологии, которые эффективны сегодня, могут оказаться устаревшими завтра. Это требует постоянного обновления и адаптации систем ИБ.

6. Соблюдение законодательства и стандартов в области ИБ: компании обязаны соблюдать и их. Интеграция технологий должна соответствовать различным нормативам, в противном случае могут возникнуть дополнительные сложности.

7. Человеческий фактор: пользователи могут стать уязвимостью в системах ИБ из-за слабых паролей, неосторожного поведения в сети и других ошибок. Технологии должны учитывать и компенсировать этот человеческий фактор.

Решение вышеуказанных проблем требует комплексного подхода, информационного обмена, включая тщательное планирование, обучение персонала, выбор подходящих технологических решений и постоянное обновление стратегий ИБ в соответствии с меняющейся угрозовой картиной.

Россия активно участвует в международных инициативах, совместных учениях и обмене информацией о киберугрозах, внедряя собственные разработки в СНГ и дальнем зарубежье. Важно отметить, что сотрудничество России с другими странами в сфере кибербезопасности способствует не только защите национальных интересов, но и обеспечивает общеглобальную киберустойчивость. Это значительно повышает международный авторитет России в сфере информационной безопасности и борьбы с киберпреступностью.

Однако, несмотря на позитивные тенденции, еще предстоит преодолеть ряд вызовов, включая несовместимость методов защиты, быстрое развитие кибератак и необходимость обучения специалистов в сфере кибербезопасности.

Таким образом, международное сотрудничество в борьбе с киберпреступностью для России имеет важное стратегическое значение. Оно способствует обмену передовым опытом в сфере кибербезопасности, что позволяет учиться на чужих ошибках и разрабатывать более эффективные стратегии противодействия преступлениям в сфере информационно-телекоммуникационных технологий. В сложившейся ситуации немаловажную роль играют возможности использования образовательного процесса: обмен знаниями и опытом, повышение квалификации кадров, создание образовательных инициатив, обмен экспертами, создание центров компетенции, международные учения. Россия, как и другие страны, продолжает развивать свои стратегии борьбы с киберпреступностью, поддерживая открытый и доверительный диалог с мировым сообществом и совместно работая над созданием безопасного цифрового будущего для всех.