Стохастические модели, основанные на модификации моделей эпидемиологического типа, прогнозируют макродинамику процессов.

Системно-динамические модели через систему взаимосвязанных дифференциальных уравнений синтезируя ключевые процессы распространения дискредитирующей информации, учитывают нелинейные обратные связи.

Модели инсайдерских угроз интегрируют модели машинного обучения с моделями системной динамики.

Однако единая методологическая система моделей пока не реализована. Комплексная модель, которая бы объединила качества всех рассмотренных подходов, еще не обоснована и не построена.

Представляется, что наиболее адекватной инструментальной основой для решения такой актуальной задачи является системно-динамическое моделирование в имитационной среде типа AnyLogic. Ее использование позволит построить целостную модель, учитывающую взаимодействие человеческого фактора, технологической среды и институциональных ограничений, и обеспечивающую раннюю диагностику и активное противодействие дискредитирующим кампаниям в социальных медиа.

Макушко А.А.

Московский Ордена почета университет МВД России им. В.Я. Кикотя

Биометрические технологии в деятельности дорожной полиции

Используемые подразделениями ГИБДД автоматизированные системы (АС) обеспечивают сбор, обработку и хранение значительных объемов информации, в том числе персональных данных. Защита вышеуказанных сведений имеет первостепенное значение, так как неправомерный доступ к ним и их разглашение могут повлечь очень серьезные негативные последствия.

Одним из перспективных направлений повышения информационной безопасности данных при эксплуатации АС является использование биометрических технологий. Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» биометрические персональные данные – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Биометрия позволяет идентифицировать пользователей на основе их уникальных биологических характеристик (отпечатки пальцев, радужная оболочка глаза, голос, лицо и т. д). Внедрение биометрических методов защиты информации может значительно повысить надежность АС, эксплуатируемых в подразделениях ГИБДД.

Обеспечение информационной безопасности автоматизированных систем ГИБДД

Современные базы данных АС ГИБДД содержат сведения о транспортных средствах, владельцах транспортных средств, дорожно-транспортных происшествиях (ДТП). Используются для решения задач:

– регистрации транспортных средств и выдачи водительских документов;

– контроля за соблюдением правил дорожного движения;

– выявления и пресечения правонарушений, связанных с использованием транспортных средств;

– расследования ДТП.

К АС, эксплуатируемым в подразделениях ГИБДД, относятся:

– федеральная информационная система ГИБДД-М (ФИС ГИБДД-М), обеспечивающая сбор и обработку информации в масштабах всей страны;

– система «Безопасный город» – комплексная система, использующая видеонаблюдение, распознавание номерных знаков и другие технологии для обеспечения безопасности на дорогах[1];

– система «Паутина» – информационно-поисковая система, обеспечивающая оперативный поиск информации о транспортных средствах и водителях, находящихся в розыске;

– различные региональные и локальные системы, используемые для решения специальных задач в рассматриваемой сфере.

Вышеуказанные АС входят в состав Единой системы информационно-аналитического обеспечения деятельности МВД России – ИСОД МВД России

Согласно приказу МВД России от 05.02.2016 № 60 «О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции» защита данных от несанкционированного доступа в вышеуказанных системах обеспечивается средствами подсистемы информационной безопасности, включая:

– доступ администраторов, пользователей и операторов к системе путем авторизации;

– защиту информации в каналах связи;

– разграничение прав доступа администраторов, пользователей и операторов к информационным ресурсам, программным средствам обработки, передачи и защиты информации;

– ведение учета работы администраторов и пользователей.

В состав подсистемы входят средства защиты инфраструктуры, средства защиты сервисов и средства защиты автоматизированных рабочих мест

[1] О Концепции построения и развития аппаратно-программного комплекса «Безопасный город» : распоряжение Правительства РФ от 03.12.2014 № 2446-р.

(АРМ) сотрудников МВД России. В системе защиты АРМ выделяются базовые средства, приведенные на рис.

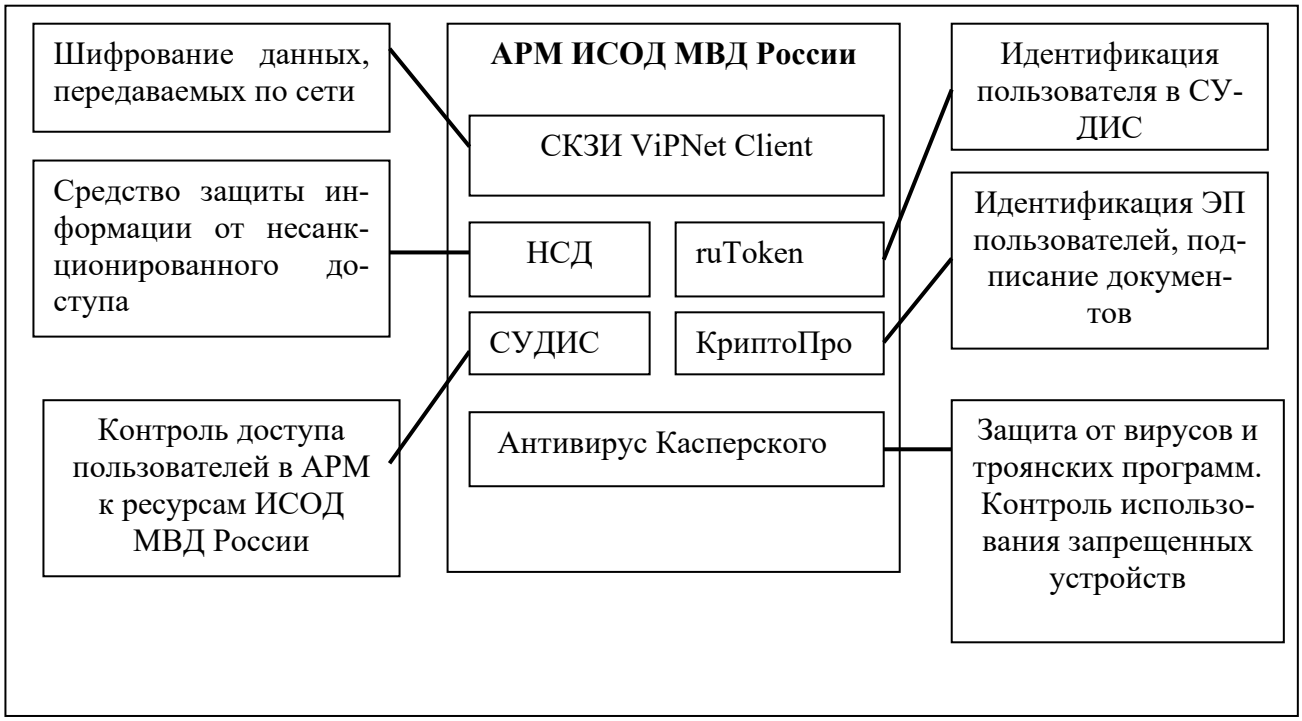

Рис. Состав системы защиты АРМ[1]

Как видно из представленной схемы, сервис управления доступом к информационной системе (СУДИС) играет ключевую роль в обеспечении безопасности. Он отвечает за управление доступом пользователей к системе и сервисам ИСОД МВД России, предоставляя единую точку входа и регистрируя события безопасности. Он позволяет управлять полномочиями пользователей и сервисов, а также обеспечивает доступ к ресурсам с использованием электронной подписи, что делает его одним из ключевых элементов подсистемы информационной безопасности ИСОД МВД России. Однако, несмотря на имеющиеся достоинства, методы защиты информации, применяемые в АС, пока имеют ряд недостатков:

– не уделяется достаточно внимания мерам, направленным на комплексность защиты данных, что оставляет систему, уязвимой их к утечкам;

– система защиты информации не всегда вовремя адаптируется к постоянно изменяющимся методам атак со стороны злоумышленников, по этой причине не имея достаточных средств для оперативного обнаружения и анализа потенциальных угроз;

– существенная зависимость от СУДИС создает риски для доступности информации в случае сбоев в ее работе.

[1] Особенности технических средств защиты информации электронного документооборота. URL: https://student-servis.ru/spravochnik/osobennosti-tehnicheskih-sredstv-zashhity-informatsii-elektronnogo-dokumentooborota/ (дата обращения: 27.10.2025).

Кроме того, следует отметить, что недостаточная интеграция вышеотмеченных сервисов, используемых в деятельности ГИБДД, создает значимые препятствия для оперативной работы сотрудников ГИБДД. Разрозненность информационных баз данных и отсутствие единой платформы для доступа к комплексному профилю водителя и транспортного средства существенно снижает оперативность принятия решений и увеличивает время, затрачиваемое на проверку информации.

Таким образом, перечисленные выше аспекты позволяют сделать вывод о том, что информационная система, обладая перечисленными недостатками, становится уязвимой к утечкам, неспособна оперативно реагировать на новые угрозы и зависима от стабильности отдельных компонентов, что в конечном итоге снижает эффективность работы сотрудников ГИБДД и повышает риски для безопасности.

В то же время используемые в настоящее время биометрические технологии демонстрируют стремительный рост и все чаще интегрируются в самые различные сферы деятельности. Это обусловлено их надежностью, удобством использования и способностью эффективно предотвращать несанкционированный доступ.

Среди наиболее распространенных биометрической технологий следует отметить[1]:

– распознавание лица (Face ID) используется для быстрой идентификации лиц;

– сканирование отпечатков пальцев (Touch ID) для подтверждения личности при оформлении документов;

– сканирование радужной оболочки глаза (Iris Scan) возможно использовать как дополнительный уровень защиты в критически важных системах;

– голосовая идентификация (Voice ID) используется для удаленной проверки личности пользователя;

– биометрия, основанная на поведенческих характеристиках, использует уникальные особенности поведения человека для идентификации.

Каждая из представленных технологий предлагает уникальные преимущества и уровни безопасности.

Биометрические системы безопасности представляют собой один из самых современных подходов к обеспечению защиты информации.

В частности, появилась возможность контролировать доступ к информации с использованием биометрических методов. В США, по статистике, более 87% таких систем защищают важные машинные залы ЭВМ, исследовательские центры, хранилища ценной информации и военные учреждения.

[1] Современные методы биометрической идентификации. URL: https://www.azone-it.ru/sovremennye-metody-biometricheskoy identifikacii?ysclid= ls62v1ifjy175552977 (дата обращения: 18.10.2025).

Биометрические системы доступа устанавливаются в местах массового скопления людей, таких как аэропорты и крупные торговые центры[1].

За рубежом активно внедряют биометрию в работу дорожной полиции для повышения эффективности и безопасности[2]. В частности, системы сканирования отпечатков пальцев в Испании позволяют быстро идентифицировать водителей, исключая подделку документов и выявляя находящихся в розыске лиц. Активно разрабатываются и тестируются системы, анализирующие видеозапись лица водителя для выявления признаков усталости или опьянения, что способствует предотвращению ДТП. Системы автоматического распознавания номерных знаков, широко используемые в Великобритании, США и Австралии, помогают выявлять угнанные автомобили и нарушителей ПДД, сопоставляя данные с базами данных, в Китае разработана система распознавания жестов регулировщика, которая призвана повысить эффективность управления дорожным движением при перегрузках, биометрические технологии позволяют правоохранительным органам повысить точность и оперативность идентификации. Кроме того, биометрические системы в сочетании с другими технологиями контролируют соблюдение ПДД, автоматически фиксируя нарушения и повышая безопасность на дорогах.

В эпоху цифровой трансформации правоохранительные органы, в частности ГИБДД, не могут эффективно функционировать без активного внедрения информационных технологий, среди которых особое место занимает биометрия. Обширный круг задач, возложенных на сотрудников ОВД, указывает на перспективность использования именно биометрических решений. В свете стремления к совершенствованию безопасности дорожного движения, ГИБДД должно быть в числе лидеров во внедрении современных биометрических технологий, оперативно решая задачи контроля, надзора и идентификации участников дорожного движения. Ориентируясь на инновации и передовой опыт, правоохранительные органы смогут в полной мере раскрыть потенциал биометрии для обеспечения безопасной и комфортной среды на дорогах.

Принимая во внимание недостаточную защищенность существующих АС дорожной полиции и опираясь на мировой опыт использования биометрической идентификации и аутентификации, можно сделать вывод о

[1] Бойко А.А., Милевская Ю.С. Обзор биометрических систем безопасности. Применение биометрических систем контроля доступа в деятельности сотрудников органов внутренних дел // Вестник Московского университета МВД России имени В.Я. Кикотя. 2017. № 5. С. 291-293.

[2] Wang B., Yuan T. Traffic Police Gesture Recognition using Accelerometers. URL: https://warwick.ac.uk/fac/sci/eng/research/grouplist/sensorsanddevices/mbl/database/ieeesensors08/PDFs/Papers/275_6240.pdf (дата обращения: 30.10.2025); Utegen D., Rakhmetov B. Zh. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. https://doi.org/10.21202/jdtl.2023.36 (дата обращения: 30.10.2025).

необходимости развития и внедрения подобных технологий в нашей стране. Это позволит не только повысить надежность доступа пользователей к АС дорожной полиции, но и внести значительный вклад в повышение безопасности дорожного движения.

Бондарь К.М.,

кандидат технических наук, доцент
Дальневосточный юридический институт МВД России им. И.Ф. Шилова (г. Хабаровск)

Аспект виктимности в современной киберпреступности России

Развитие информационных технологий стало ключевым фактором в возникновении и распространении киберпреступности. Анализ показывает, что большинство киберпреступников – это высококвалифицированные специалисты, обладающие глубокими знаниями в области IT. Они используют свои навыки для совершения различных преступлений, от мошенничества до угроз национальной безопасности, при этом часто скрывая свое местоположение и действуя из любой точки мира.

Установление личности преступников в сфере интернет-преступности затруднено в связи с дистанционным характером совершаемых деяний[1]. Сложность в этой борьбе заключается в ее скрытом характере, что приводит к низкой раскрываемости. Эффективность раскрытия и расследования таких преступлений напрямую определяется оперативностью обнаружения, а также особенностями и следами, которые, как правило, существуют только в виртуальном пространстве.

Современные информационные технологии открывают широкие горизонты, позволяя использовать инновационные методы торговли и предоставления услуг. Но возможно и попадание на мошенников, маскирующихся под добросовестных продавцов. В Интернете мошенники не всегда сразу стремятся украсть деньги, не всегда все сводится к прямому обогащению. Нередко их цель – это ваши личные данные-логины, пароли, файлы. Получив к ним доступ, они могут шантажировать, вымогать деньги или просто использовать информацию в своих интересах.

При этом используются различные программы, которые предназначены для тайного доступа к носителю информации, без уведомления владельца. К ним можно отнести различные рекламные, троянские, вирусы. Все они нацелены на захват и контролирование информации.

Процесс виктимизация населения на сегодняшний день является одной из актуальных проблем. Потенциальные жертвы сами идут на поводу у

[1] Устинов А.А. Основные проблемы раскрытия и расследования интернет-преступлений // Молодой ученый. 2020. № 49 (339). С. 338-340.