веденческие признаки), позволяющая устанавливать и подтверждать личность человека на основе его уникальных биометрических характеристик.

К системам информационной безопасности относятся:

антивирусные программы и межсетевые экраны, способствующие предотвращению несанкционированный доступ к данным и защищающие информацию от киберугроз;

системы обнаружения и предотвращения вторжений (мониторинг сетевого трафика для выявления и блокировки подозрительных действий);

шифрование данных (инструменты для защиты информации при передаче и хранении).

Эти средства в комплексе создают надежную защиту, минимизируя риски и предотвращая инциденты безопасности.

УДК 004.05

Л.В. Степанов, Н.П. Сергеев

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ И ТЕХНОЛОГИЙ

В настоящее время существует тенденция проникновения современных информационных технологий во все сферы деятельности человека, включая критически важные силовые блоки, такие как уголовно-исполнительная система России (УИС). Вместе с этим появляется проблема обеспечения безопасности функционирования исправительных учреждений и систем контроля, предотвращения утечек конфиденциальных данных и защиты информации особой важности. Постоянно нарастающая угроза реализации злоумышленниками кибератак на критически важные элементы информационного пространства УИС делает вопросы безопасности крайне актуальными и первостепенными. Данная проблема требует от системы постоянного мониторинга, своевременного оперативного реагирования на угрозы и инциденты, а также внедрения современных технологий в сфере защиты информации.

Направление информационной безопасности (далее – ИБ) является важнейшим вектором в обеспечении общей безопасности УИС. Он направлен на защиту конфиденциальной информации, предотвращение несанкционированного доступа злоумышленников к важным секторам и минимизацию рисков, связанных с киберугрозами и инсайдерскими действиями. Методы и технологии, применяемые для защиты инфор-

мации в УИС должны учитывать особенности работы системы и требования к обеспечению сохранности данных, а также гарантировать безопасность информации на всех уровнях.

Информационная безопасность, как правило, включает в себя защиту конфиденциальности, целостности и доступности данных. В современных условиях основные угрозы информационной безопасности можно разделить на несколько категорий:

кибератаки – целенаправленные негативные действия злоумышленников, целью которых является получение доступа к защищенным системам и данным (фишинг, вирусы, атаки типа DDoS и др.);

утечки данных – получение доступа к конфиденциальной информации злоумышленниками не только через недостаточную защиту сетей или устройств, но и ввиду человеческого фактора персонала;

инсайдерские угрозы – действия сотрудников компании, которые имеют доступ к данным и используют их в личных целях или передают третьим лицам.

Эти угрозы демонстрируют необходимость надежной защиты информационных систем. Технические средства и технологии, применяемые в этой области, направлены на минимизацию рисков и предотвращение инцидентов безопасности.

Для обеспечения безопасности информации используются различные технические средства и решения. Рассмотрим некоторые из них.

Одной из ключевых технологий информационной безопасности являются системы обнаружения и предотвращения вторжений (Intrusion Detection Systems/Intrusion Prevention Systems). Эти системы анализируют трафик сети, выявляют подозрительные действия и сообщают о возможных угрозах. IDS позволяют обнаружить попытки вторжения, а IPS – блокировать их.

Такие системы работают на основе анализа сетевого трафика в реальном времени и могут выявлять сигнатуры известных атак или анализировать аномальное поведение в сети. Это позволяет оперативно реагировать на угрозы и предотвращать их развитие.

Еще одной из наиболее эффективных технологий информационной безопасности является шифрование данных, которое обеспечивает сохранность конфиденциальной информации при ее хранении и передаче. В настоящее время для защиты информации широко применяются современные криптографические алгоритмы, такие как AES (Advanced Encryption Standart), RSA и др.

При передаче информации через сеть Интернет важным аспектом является использование таких протоколов шифрования, как SSL/TLS.

При работе этих протоколов информация, передаваемая между клиентом и сервером, становится недоступной для перехвата злоумышленниками.

Для обеспечения безопасности информации важно, чтобы доступ к ней имели только авторизованные и доверенные пользователи. Так, современные методы аутентификации включают в себя:

многофакторную аутентификацию (MFA) – технологию, требующую от пользователя подтверждения своей личности несколькими способами одновременно (ввод пароля и SMS-кода или биометрических данных);

биометрическую аутентификацию, использующую уникальные физические характеристики пользователя (отпечатки пальцев, сканирование сетчатки глаза и другие) с целью разрешения его доступа к данным;

систему управления доступом (Access Control), позволяющую разграничить доступ различных пользователей к определенным данным, где важными элементами являются ролевое распределение прав и динамическое управление доступом в зависимости от контекста.

Важную роль в защите периметра сети играют брандмауэры, фильтрующие входящий и исходящий трафик на основе заданных правил. Брандмауэры могут быть реализованы как в виде программных, так и аппаратных средств, обеспечивая защиту как на уровне отдельных устройств, так и на уровне всей сети. Современные брандмауэры зачастую работают в совокупности с другими системами защиты, что позволяет создавать многоуровневую систему безопасности.

Брандмауэры нового поколения (Next-Generation Firewalls, NGFW) обладают расширенными возможностями: глубокий анализ поступающих пакетов данных, контроль приложений и предотвращение появляющихся угроз.

Значимыми элементами защиты информационных систем от вредоносного программного обеспечения (далее – ПО) продолжают оставаться антивирусные программы. Современные антивирусы не только сканируют файлы на наличие известных вирусов и угроз, но и используют эвристические методы анализа для выявления новых, ранее неизвестных типов вредоносного ПО.

Интеграция антивирусных решений с облачными сервисами позволяет получать обновления сигнатур в режиме реального времени, что значительно увеличивает эффективность защиты.

Информационная безопасность в условиях стремительного развития технологий становится важнейшей задачей для всех участников информационного пространства. Системы IDS/IPS, шифрование, аутентификация и управление доступом, брандмауэры, антивирусы и прочие современные технические средства обеспечивают высокий уровень защиты данных.

Для обеспечения эффективной защиты информации необходимо постоянно следить за новыми разработками и внедрять комплексные решения, включающие как традиционные, так и инновационные технологии.

Важно отметить, что обеспечение информационной безопасности в УИС является большим шагом к укреплению безопасности системы в целом. Внедрение современных технологий защиты информации, таких как системы обнаружения вторжений, шифрование и управление доступом, будет способствовать созданию надежной и устойчивой к угрозам среды, обеспечивающей не только сохранность данных, но и бесперебойную работу УИС, как целостной системы.

УДК 351.74

Ю.А. Сурженко, Я.В. Крупский

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ОБЕСПЕЧЕНИЮ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Обеспечение общественной безопасности является актуальным направлением для всех развитых стран мира. В данной сфере различными организациями проводится постоянный мониторинг с опубликованием рейтингов, результаты которых имеют существенное влияние при выборе места проживания, привлечения туристов, инвесторов и др. На помощь правоохранительным органам приходит стремительно развивающийся искусственный интеллект (далее – ИИ), который уже успел стать частью жизни многих людей.

Целесообразно рассмотреть способствование ИИ правоохранительным органам Республики Беларусь и других стран в обеспечении общественной безопасности.

Для того, чтобы понять, как он может помочь, необходимо определить, где правоохранительным органам нужна помощь.

Первой проблемой являются дипфейки, создаваемые ИИ. Дипфейк (англ. deepfake) – методика синтеза изображения или голоса, основанная на ИИ. В 2024 г. ИИ так сильно развился, что сейчас человеческому глазу становится все сложнее и сложнее отличить, где реальность, а где дипфейк. С помощью дипфейков можно распространять фейковые новости, например, о руководстве МВД, Главе государства и т. д., что может привести к массовому недовольству или перерасти во что-то большее. Дипфейк используется для шантажа людей, которые, опасаясь за свою