

легчит работу сотрудникам компании и позволит снизить расходы минимум на 30%. Система raven cruizer нужна для выполнения параллельного вождения сельскохозяйственной техники. Точность находится в пределах 3 – 20 см., а зависит этот параметр от вида установленного GPS-навигатора. Если же обработка земли осуществляется на пересеченной местности, рекомендуется дополнить систему особыми датчиками, определяющими наклон. Имеется возможность модернизации автопилотом механического типа с установкой на руль или же гидравлического типа, который позволит управлять техникой с высокой точностью на скорости примерно 40 км/ч.

Предлагаемая система raven cruiser отличается точностью, доступностью. Ее покупка позволит значительно повысить эффективность выполнения различных сельскохозяйственных задач. В данной модели решены две главные проблемы систем предыдущего поколения, а именно сложность контроля, высокая цена. Установка данного оборудования значительно упрощает работу, открывает ряд возможностей за счет автоматизированного рулевого контроля, управления секциями штанги.

УДК 004.056

Алёна Тюленева

(Российская Федерация)

Научный руководитель О.В. Пшеничникова, к.э.н., доцент
ФГБОУ ВО Финансовый университет при Правительстве
Российской Федерации Курский филиал

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

В современном мире информация играет ключевую роль в деятельности любой организации, будь то коммерческая компания, государственное учреждение или частное лицо. В условиях стремительного развития информационных технологий и роста объемов данных, вопрос защиты информации становится одним из важнейших аспектов обеспечения безопасности. Угрозы информационной безопасности могут быть разнообразными: от несанкционированного доступа к данным до утечек конфиденциальной информации и киберугроз. Поэтому разработка и внедрение эффективных методов и

средств защиты информации являются приоритетными задачами для всех, кто работает с информационными системами и сетями.

В данной статье рассматривается классификация методов и средств защиты информации, которая является важным инструментом для понимания и выбора оптимальных решений для обеспечения безопасности данных в информационных системах и сетях. Она помогает систематизировать подходы и технологии, используемые для защиты информации от несанкционированного доступа, изменения, уничтожения или кражи. В рамках этой классификации выделяются четыре основных группы методов и средств: организационные, технические, программные и криптографические. Каждая из этих групп содержит разнообразные инструменты и методики, направленные на достижение разных целей и решение определенных задач.

1. Организационные методы

Организационный метод защиты информации направлен на создание и поддержание структуры и процессов, обеспечивающих безопасность данных в организации. Этот метод акцентируется на управлении человеческими ресурсами, разработке и внедрении политик безопасности, а также контроле за соблюдением установленных правил. Одним из ключевых элементов организационного метода является политика информационной безопасности, которая формулирует основные принципы и процедуры обращения с информацией. Эта политика описывает обязанности сотрудников, определяет меры контроля доступа к данным и регламентирует действия в случае возникновения инцидентов.

2. Технические методы

Технический метод защиты информации основан на использовании специализированных устройств и технологий для обеспечения безопасности данных в информационных системах и сетях. Этот метод включает в себя широкий спектр аппаратных и программных решений, направленных на предотвращение несанкционированного доступа, мониторинг активности и защиту от вредоносного программного обеспечения.

3. Программные методы

Программный метод защиты информации заключается в использовании специального программного обеспечения, направленного на обеспечение безопасности данных в информационных сис-

темах и сетях. Этот метод охватывает широкий спектр программных решений, которые работают на уровне операционной системы и прикладных программ, обеспечивая защиту от несанкционированного доступа, утечек данных и других угроз.

Основные компоненты программного метода включают:

- Антивирусные программы
- Системы управления доступом (АСУ)
- Средства резервного копирования и восстановления данных
- Средства защиты от утечек данных (DLP)

4. Криптографические методы

Криптографический метод защиты информации базируется на использовании математических алгоритмов для шифрования данных, что делает их недоступными для чтения посторонними лицами. Этот метод играет центральную роль в обеспечении конфиденциальности и целостности информации, особенно при передаче данных через ненадежные каналы связи, такие как Интернет. Основные компоненты криптографического метода включают: симметричное шифрование, асимметричное шифрование, цифровые подписи, хэш-функции.

5. Комплексный подход

Также стоит отметить, что для максимальной эффективности защиты информации рекомендуется использовать комбинацию всех вышеперечисленных методов. Комплексный подход подразумевает создание многослойной системы защиты, где каждый уровень усиливает следующий. Такой подход значительно повышает надежность всей системы безопасности.

Подводя итог вышесказанному, можно сделать вывод о том, что методы и средства защиты информации играют немаловажную роль в обеспечении безопасности информационных систем и сетей. Современные условия требуют комплексного подхода к защите данных, который включает в себя организационные, технические, программные и криптографические меры. Эти методы позволяют предотвратить, обнаружить и устранить различные угрозы информационной безопасности.

Эффективная защита информации требует постоянного обновления и адаптации защитных мер, поскольку угрозы постоянно эволюционируют. Важно интегрировать различные методы и средства в единую систему, чтобы обеспечить многоуровневую защиту

данных. Это позволит минимизировать риски и гарантировать безопасность информации в условиях растущего объема данных и усложнения информационных технологий.

УДК 004.4:631

Станислав Хамутовский, Елена Передня

(Республика Беларусь)

Научный руководитель А.В. Лукашевич, ст. преподаватель
Белорусский государственный аграрный технический университет

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Искусственный интеллект (ИИ) в современном агропромышленном комплексе (АПК) представляет собой одну из самых перспективных технологий, способных значительно улучшить эффективность сельскохозяйственного производства. В данной статье подробно рассматриваются два основных направления применения ИИ в АПК: прогнозирование урожаев и мониторинг полей.

Прогнозирование урожаев с использованием ИИ базируется на анализе огромного массива данных, который включает в себя погодные условия, состав почвы, уровень влажности и другие агрономические параметры. В Республике Беларусь, как и во многих других странах, сельское хозяйство сильно зависит от погодных условий. Частые колебания температуры, осадков и другие климатические изменения могут существенно влиять на урожайность. Алгоритмы машинного обучения позволяют обрабатывать и анализировать эти данные, выявляя скрытые закономерности и зависимости, которые невозможно обнаружить традиционными методами.

Основной принцип работы таких алгоритмов заключается в обучении моделей на исторических данных. Модель получает информацию о прошлых сезонах, включая параметры, связанные с урожайностью, и обучается предсказывать будущие результаты на основе текущих условий. Например, анализируя данные о количестве осадков, температуре и состоянии почвы за последние несколько лет, ИИ может предсказать, как изменение этих факторов в текущем году скажется на урожае. В результате фермеры получают