Цель работы: определить, какие из современных материалов, использующихся в магнитопорошковой дефектоскопии, оптимально подходят для использования на объектах железнодорожного транспорта.

При выборе магнитопорошковых материалов для контроля на объектах железнодорожного транспорта (например, на железнодорожных путях) основным параметром является разрешающая способность, которая напрямую зависит от размера частиц порошка или суспензии. Рассмотрим основные виды материалов с учетом данного параметра.

Порошки. Примером порошка может стать магнитный порошок Диагма-1100 производства РФ. Из плюсов можно выделить его небольшую цену, а также огнестойкость. Основные минусы: большой размер частиц – не менее 30 мкм, что ограничивает минимальный размер обнаруживаемых дефектов, а также, что касается всех порошков в принципе – сложность использования по сравнению с суспензиями.

Суспензии. Среди суспензий можно выделить несколько самых распространенных, а именно: Magnaflux 7HF, Элитест ЧС2 и Helling NRS 103 (рис. 1). Рассмотрим характеристики каждой из них.

а *б* *в*

Рис. 1. Рассматриваемые магнитные суспензии: Magnaflux 7HF (*а*); Элитест ЧС2 (*б*); Helling NRS 103 (*в*)

Magnaflux 7HF – суспензия американского производства. Среди основных характеристик можно выделить высокую температуру вспыхивания (> 93 ºС), температуру использования от –5 ºС до 50 ºС и средним размером частиц 2–6 мкм. Элитест ЧС2 – суспензия российского производства. Температура вспыхивания также составляет > 93 ºС, температура использования от –10 ºС до 90 ºС, размер частиц составляет не более 2 мкм. Helling NRS 103 – суспензия немецкого производства. Температура вспыхивания производителем не указана, рабочая температура от –10 ºС до 50 ºС, размер частиц составляет не более 4 мкм.

Таким образом, для магнитопорошковой дефектоскопии объектов железнодорожного транспорта стоит использовать магнитные суспензии, за счет их упрощенного использования и частиц в несколько раз меньших, чем у магнитных порошков. Из рассмотренных нами суспензий российский Элитест ЧС2 по соотношению цена-качество обладает наилучшими параметрами, однако предпочтительными являются суспензии фирм Magnaflux и Helling за счет высокого качества и надежности. Указанные выше фирмы поставляют свою продукцию в Республику Беларусь длительное время, и вся нормативная документация по их применению уже разработана.

УДК 339.54.012

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Магистранты Куликова А. В., Богословский Ф. И.
Ст. преподаватель Левиев Д. О.
Московский государственный технический университет имени Н. Э. Баумана, Москва, Россия

В современном мире, где цифровые технологии проникают во все сферы жизни, защита персональных данных становится все более актуальной проблемой. В связи с этим, исследование методов защиты персональных данных в эпоху цифровой трансформации приобретает особую важность.

Целью данного исследования является анализ существующих методов защиты персональных данных в условиях цифровой трансформации с целью выявления их эффективности и возможных улучшений.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить основные принципы защиты персональных данных в цифровой среде.
2. Проанализировать существующие методы защиты персональных данных и их применимость в современных условиях.
3. Выявить основные угрозы и риски для персональных данных в эпоху цифровой трансформации.
4. Предложить рекомендации по улучшению методов защиты персональных данных с учетом современных тенденций развития информационных технологий.

Основные понятия и законодательство в области защиты персональных данных. Международные и национальные стандарты в области защиты персональных данных [1] играют ключевую роль в обеспечении конфиденциальности и безопасности информации.

Законодательство в области защиты персональных данных направлено на защиту прав человека на конфиденциальность его личных данных и обязывает организации соблюдать определенные стандарты безопасности. Однако, в эпоху цифровой трансформации, когда объемы информации растут экспоненциально, возникают новые вызовы и угрозы для защиты персональных данных.

Для анализа методов защиты персональных данных в условиях цифровой трансформации необходимо учитывать как основные принципы защиты данных, так и существующие стандарты и законодательство. Важно рассмотреть как традиционные методы защиты данных, такие как шифрование, аутентификация и контроль доступа, так и новые технологии, включая блокчейн, искусственный интеллект и машинное обучение.

Угрозы для персональных данных и их классификация. Угрозы для персональных данных [2] могут быть классифицированы на внутренние и внешние. Внутренние угрозы возникают изнутри организации и могут быть вызваны недобросовестными сотрудниками, ошибками в управлении данными или слабой кибергигиеной. Эти угрозы могут привести к утечке конфиденциальной информации, несанкционированному доступу к данным или неправомерной обработке персональных данных.

Внешние угрозы, с другой стороны, исходят извне и могут включать в себя хакерские атаки, кибершпионаж, вирусы и мошенничество. Эти угрозы могут быть направлены на похищение личных данных, шантаж, финансовые мошенничества или нарушение конфиденциальности.

Угрозы для персональных данных также могут быть классифицированы по степени опасности. Например, низкой степенью опасности могут быть считаться случайные ошибки или утраты данных, средней – несанкционированный доступ к данным или вредоносное программное обеспечение, а высокой – целенаправленные хакерские атаки или утечки конфиденциальной информации.

Методы и технологии защиты персональных данных. Для эффективной защиты конфиденциальной информации используются различные методы и технологии [3]. В данном списке рассмотрим основные подходы к защите персональных данных, включая технические средства, организационные мероприятия, юридические аспекты и роль государства в обеспечении безопасности информации.

Технические средства защиты. В рамках технических средств защиты персональных данных широко используются методы шифрования, аутентификации и контроля доступа. Шифрование данных позволяет обезопасить информацию от несанкционированного доступа путем преобразования ее в недоступный для посторонних вид. Аутентификация предоставляет возможность проверить личность пользователя перед предоставлением доступа к данным. Контроль доступа позволяет управлять правами доступа к информации в зависимости от роли и полномочий сотрудников.

Организационные мероприятия по защите персональных данных. Организационные меры включают в себя обучение сотрудников по вопросам безопасности данных, разработку политики безопасности информации, регулярные аудиты и мониторинг защиты данных, а также управление рисками, связанными с обработкой персональных данных.

Юридические меры защиты. Юридические меры включают в себя соблюдение законодательства о защите персональных данных, заключение соответствующих договоров с третьими сторонами, которые имеют доступ к данным, а также проведение оценки влияния на защиту данных (DPIA) для оценки рисков и разработки мер по их устранению.

Роль государства в обеспечении защиты персональных данных. Государство играет ключевую роль в обеспечении защиты персональных данных путем принятия соответствующего законодательства, контроля за его соблюдением, разработки стандартов безопасности и поддержки развития технологий для защиты данных.

Практические примеры защиты персональных данных. Одним из ключевых аспектов защиты персональных данных является использование технических средств, таких как криптографические методы шифрования, механизмы аутентификации и контроля доступа [4]. Крупные компании, такие как Яндекс, Сбербанк и другие, активно внедряют передовые технологии для защиты информации своих пользователей. Примерами могут служить двухфакторная аутентификация, шифрование конфиденциальных данных и мониторинг безопасности сетей.

Государственные органы также не остаются в стороне и принимают меры по обеспечению безопасности персональных данных граждан. Здесь важными являются законодательные меры, регулирующие сбор, хранение и обработку информации, а также создание специализированных служб по защите информации.

Медицинские учреждения также сталкиваются с необходимостью обеспечения безопасности персональных медицинских данных пациентов. Здесь важно использование защищенных баз данных, шифрования медицинских записей и строгого контроля доступа к чувствительной информации.

Оценка эффективности методов защиты персональных данных и проблемы их реализации. Одной из основных сложностей реализации методов защиты персональных данных на практике является постоянное развитие технологий и угроз в области кибербезопасности. Это требует постоянного обновления и модернизации средств защиты, что может быть затруднительно для многих организаций из-за финансовых и организационных ограничений.

Проблема выбора оптимальных методов защиты персональных данных для различных организаций заключается в необходимости учитывать специфику деятельности, объем обрабатываемых данных, уровень угроз и другие факторы. Не всегда можно найти универсальное решение, которое подойдет всем организациям, поэтому требуется индивидуальный подход к выбору методов защиты.

Оценка эффективности существующих методов защиты персональных [5] данных должна проводиться с учетом затрат на их внедрение и поддержание, а также полученных результатов. Не всегда самые дорогостоящие методы являются наиболее эффективными, поэтому важно проводить анализ и выбирать оптимальные решения с учетом баланса между затратами и результатами.

Заключение. В современном мире цифровой трансформации защита персональных данных становится все более актуальной и важной задачей. Анализ методов защиты персональных данных позволяет оценить их эффективность, сложности внедрения и проблемы, с которыми сталкиваются организации.

Одной из основных тенденций развития методов защиты персональных данных в будущем является углубление интеграции технологий искусственного интеллекта и машинного обучения для обнаружения и предотвращения киберугроз. Автоматизация процессов анализа и реагирования на инциденты безопасности позволит повысить эффективность защиты данных.

Другой важной тенденцией является усиление фокуса на защите конечных точек и облачных решений. С увеличением числа мобильных устройств и облачных сервисов растет необходимость обеспечения безопасности данных на всех уровнях доступа.

Рекомендации по выбору и применению методов защиты персональных данных включают в себя несколько ключевых аспектов. Во-первых, необходимо проводить анализ уровня угроз и специфику деятельности организации для выбора оптимальных методов защиты. Во-вторых, важно учитывать баланс между затратами на внедрение и поддержание методов и получаемой защитой данных.

Кроме того, рекомендуется уделять внимание обучению сотрудников по вопросам кибербезопасности, так как человеческий фактор часто является слабым звеном в цепи защиты данных. Регулярное обновление программного обеспечения и мониторинг событий безопасности также играют важную роль в обеспечении надежной защиты персональных данных.

Таким образом, развитие методов защиты персональных данных в будущем будет направлено на использование передовых технологий, повышение автоматизации процессов и укрепле-

ние защиты на всех уровнях доступа. Следует учитывать рекомендации по выбору и применению методов защиты для обеспечения эффективной защиты персональных данных в условиях цифровой трансформации.

Литература

1. Латухина, В. С. Международные и национальные стандарты уголовно-правовой защиты персональных данных // Экономика, социология и право. – 2017. – № 4. – С. 76–80.

2. Докучаев, В. А. Классификация угроз безопасности персональных данных в информационных системах / В. А. Докучаев, В. В. Маклачкова, В. Ю. Статьев // T-Comm-Телекоммуникации и Транспорт. – 2020. – № 1.

3. Параскевов, А. В. Защита персональных данных в информационных обучающих системах / А. В. Параскевов, А. А. Каденцева, М. В. Филоненко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2016. – № 122. – С. 1085–1098.

4. Приезжевой А. А. Федеральный закон «О персональных данных»: научно-практический // Редакция «Российской газеты. – 2015. – № 11. – С. 37.

5. Мищенко, Е. Ю. Моделирование процессов обезличивания персональных данных и оценка эффективности используемых методов на основе модели нарушителя: диссертация на соискание ученой степени кандидата технических наук: 2.3.6: дис. – 2022.

УДК 681

УСТРОЙСТВО ПОДКЛЮЧЕНИЯ И КОНТРОЛЯ ПОСТОЯННОТОКОВЫХ ШЛЕЙФОВ ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПКП

Студенты гр. 11301121 Купреенко К. В., Адамович К. А.
Ст. преподаватель Василевский А. Г.
Белорусский национальный технический университет, Минск, Беларусь

Основная цель работы – разработка более совершенного устройства подключения и контроля постояннотоковых шлейфов и ПКП пожарной сигнализации [1].

В состав этого устройства входят: блок коммутации шлейфов, блок контроля шлейфов, блок обработки сигналов, блок индикации, блок контроля напряжения питания (рис. 1) и разъемы для подключения шлейфа и ПКП.

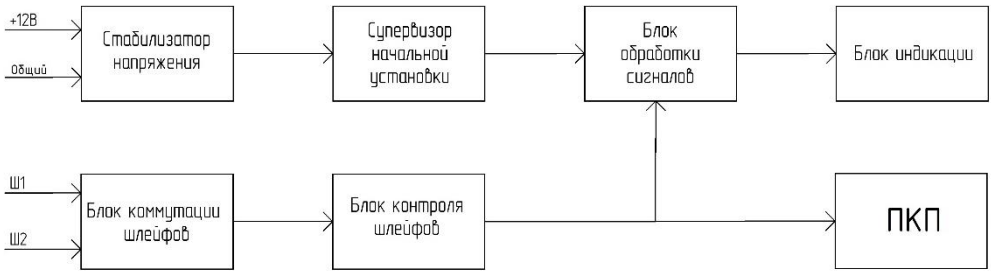

Рис. 1. Структурная схема устройства

Функционирование прибора: Устройство подключается последовательно в шлейф ПКП. На устройство подается питание от источника ПКП. Далее идет инициализация микроконтроллера устройства. В процессе инициализации может иметь место индикация «Неисправность», при этом необходимо перезапустить устройство вручную. Если напряжение питания микроконтроллера устройства недостаточно для обеспечения его нормальной работы, то микроконтроллер будет удерживаться с помощью супервизора в состоянии сброса до тех пор, пока напряжение питания не стабилизируется на уровне, достаточном для корректной работы устройства. После инициализации микроконтроллера, проверяется состояние шлейфа. Микроконтроллер формирует запрос на блок контроля шлейфов, который производит проверку шлейфа на различные состояния, передавая значения на блок обработки сигналов. Далее блок обработки сигналов производит сравнение значений токов в шлейфах с токами, соответствующих различным режимам работы, после чего загорается индикация в соответствии с установленными режимами работы шлейфа, а именно: «КЗ», «Обрыв», «Норма», «Внимание», «По-