Кибербезопасность технической документации железнодорожной автоматики и телемеханики

М. Н. Василенко,
д-р техн. наук, профессор Петербургского государственного университета путей сообщения Императора Александра I (ПГУПС)

Д. В. Зуев,
канд. техн. наук, руководитель НТЦ САПР ПГУПС

Проблема кибербезопасности технической документации железнодорожной автоматики и телемеханики становится все более актуальной в связи с внедрением безбумажных технологий электронного документооборота на базе АРМ-ВТД. При этом необходимо решать задачи анализа вариантов кибератак и методов защиты от них.

Сегодня вопросы кибербезопасности программно управляемых систем автоматики с элементами искусственного интеллекта стали особо актуальными. В системах железнодорожной автоматики и телемеханики (ЖАТ) используется импортное системное и прикладное программное обеспечение (ПО) в сочетании с сетевыми протоколами иностранных государств, которые создают и развивают военные ведомства, ориентированные на действия в киберпространстве **[1]**.

В полной мере сказанное относится и к современным микропроцессорным системам ЖАТ. По поводу разработки и реализации комплексных мер обеспечения кибербезопасности микропроцессорных систем управления ОАО «РЖД» выпущено распоряжение ОАО «РЖД» № 2300р от 28.10.2013 г., а головной организацией определен ОАО «НИИАС» **[2]**. Однако в этой программе не отражено очень важное, на наш взгляд, направление, связанное с кибербезопасностью технической документации (ТД) ЖАТ. Поясним этот тезис.

Объекты кибератак

Жизненный цикл технической документации ЖАТ включает ряд этапов (*рис. 1*) от проектной технической документации (ПТД) до исполненной технической документации (ИТД). Понятие ИТД определено инструкцией ЦШ-617 по содержанию ТД ЖАТ как документации, отражающей фактическое исполнение проектных решений. Иными словами, ИТД однозначно должна соответствовать реальному объекту ЖАТ. Это эталонная модель объекта, на основе которой организуется его эксплуатация (техническое обслуживание, мониторинг состояния, диагностика отказов и т. п.).

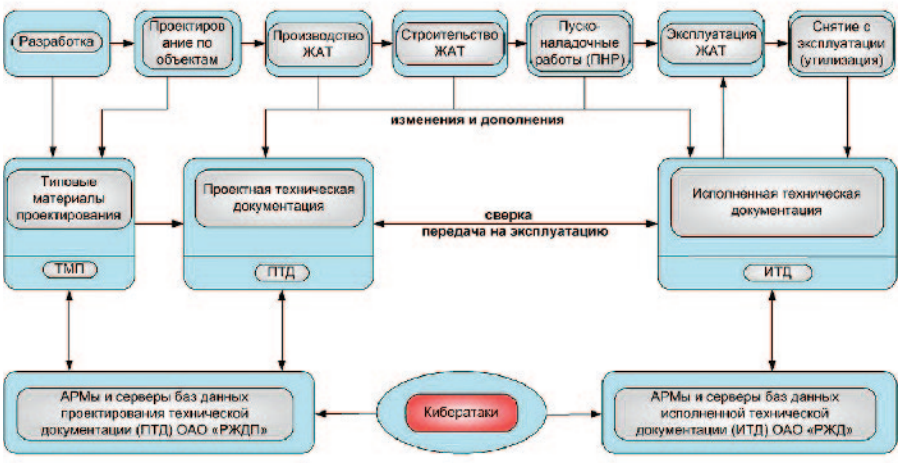

Рис. 1. Этапы жизненного цикла технической документации ЖАТ и потенциальные объекты кибератак

Рис. 2. Классификация ошибок в электронной технической документации ЖАТ

Ошибки, внесенные в ТД на любом этапе ее жизненного цикла (от разработки до утилизации), могут приводить, а подчас и приводят к серьезным материальным потерям, срыву графика движения, авариям и крушениям поездов. Особенно опасны умышленные ошибки, преследующие определенные цели, например ошибки, внесенные в результате кибератак на электронные базы данных ТД (БДТД).

Конечно, «сгенерировать» такие ошибки в ТД могут только квалифицированные специалисты в области ЖАТ: в проекты нужно вносить изменения, нарушающие проверку условий безопасности движения поездов. Отметим, что кибератаку на проекты ТД, находящиеся в АРМ многочисленных пользователей (*рис. 1*) и на серверах баз данных проектных институтов и дорог, организовать проще, чем атаку на действующую систему ЖАТ вследствие применения в действующих системах специальных методов резервирования и избыточного кодирования на уровне микрокоманд.

Способы кибератак и концепция безопасности

Следует отметить, что переход на электронные безбумажные технологии проектирования и ведения ТД ЖАТ идет интенсивно. В проектных институтах, на заводах-изготовителях и при строительстве объектов активно внедряются технологии автоматизации проектирования с использованием АРМ-ПТД. Внедрение безбумажной технологии ведения ТД ЖАТ выполнено на базе АРМ-ВТД отечественной разработки. Процент заполнения БДТД неуклонно растет. Это веление времени. Именно поэтому вопрос кибербезопасности ТД весьма актуален и требует быстрого и эффективного решения.

Такие решения должны приниматься на основе Концепции корпоративной безопасности ОАО «РЖД» в условиях реформирования, утвержденной распоряжением ОАО «РЖД» № 2628р от 20.12.2010 г. В концепции указывается, что при проектировании информационной инфраструктуры ОАО «РЖД», в которую входят и БДТД, должны быть проанализированы способы кибератак, к которым можно отнести следующие:

• несанкционированный просмотр защищаемой информации на экране монитора администраторов или пользователей информационной системы;

• вывод защищаемой информации на неучтенные носители;

• подбор аутентифицирующей информации администраторов или пользователей информационной системы;

• доступ к функционирующим штатным средствам ведения ТД лиц, не допущенных к ним (несанкционированный доступ, НСД);

• несанкционированное изменение конфигурации (настроек) программно-технических средств;

• модификация ведущихся в электронном виде регистрационных протоколов (журналов регистрации);

• несанкционированное подключение к техническим средствам информационных систем устройств, способных накапливать или каким-либо способом передавать защищаемую информацию;

• несанкционированная модификация программных средств;

• использование недекларированных возможностей (НДВ) программного обеспечения;

• блокирование или уничтожение информации, а также разрушение или искажение данных, в том числе путем внедрения вирусов программного обеспечения различных типов;

• модификация защищаемой информации, хранящейся на съемных носителях информации;

• перехват защищаемой информации при ее передаче по каналам связи, расположенным за пределами защиты;

• перехват защищаемой информации путем несанкционированного подключения к кабельным системам, коммутационному и серверному оборудованию, размещенному в пределах систем защиты;

• целенаправленное искажение или уничтожение защищаемой информации, а также навязывание ложной (специально сформированной нарушителем) информации при ее передаче по каналам связи;

• перенаправление потоков данных путем воздействия через каналы связи;

• целенаправленное искажение или навязывание ложных (специально сформированных нарушителем) команд управления, передаваемых по каналам связи;

• нарушения в каналах связи вследствие преднамеренной загрузки трафика ложными сообщениями.

Концепция также рекомендует поэтапный подход к обеспечению информационной безопасности:

• обеспечение базового уровня безопасности в результате внедрения первоочередных организационных процедур и технических мер защиты информации для эксплуатируемых ЖАТ,

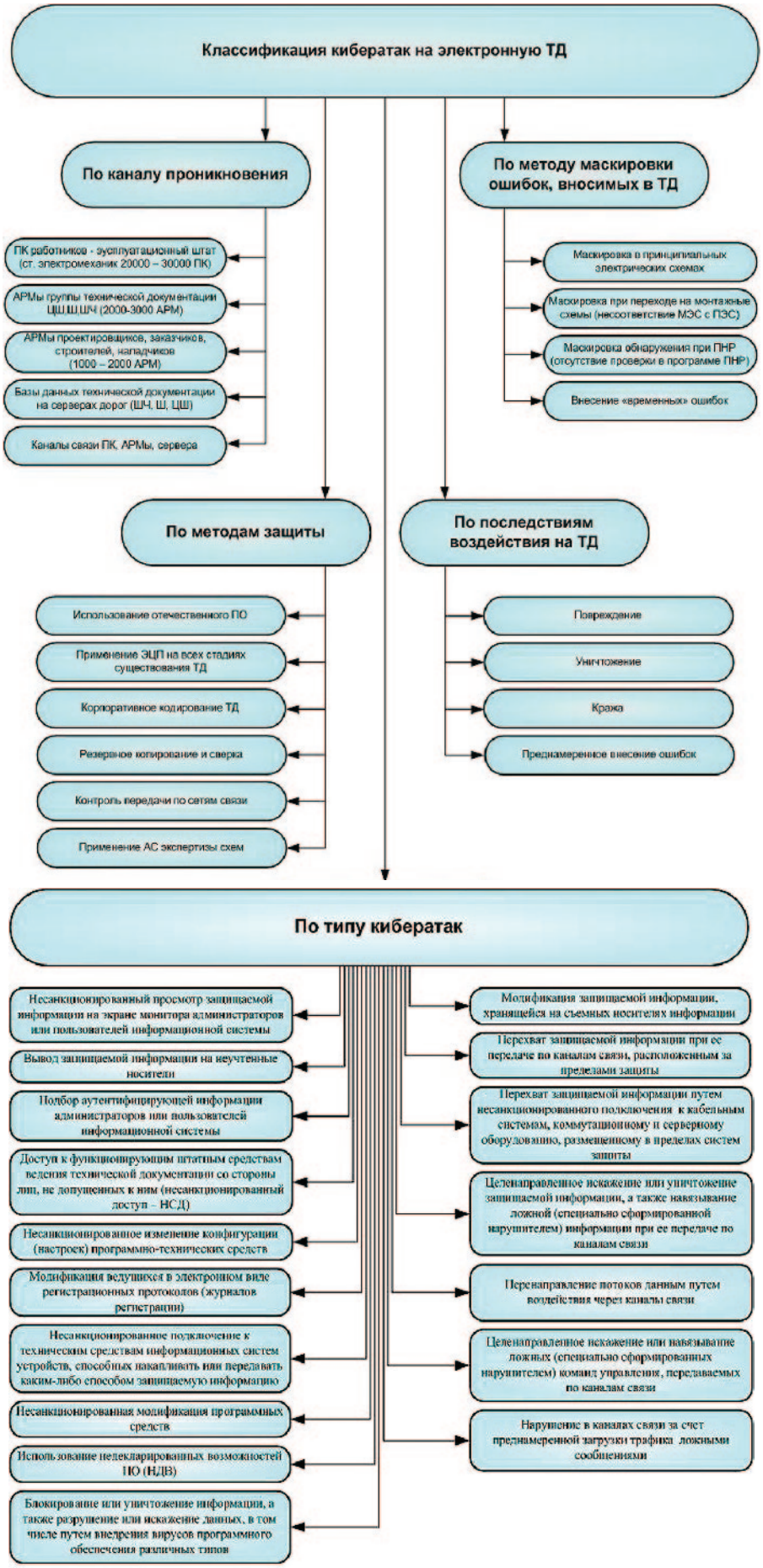

Рис. 3. Классификация вариантов организации и последствий кибератак на техническую документацию ЖАТ

преимущественно на основе встроенных механизмов общесистемного программного обеспечения;

• реализация полномасштабного комплекса организационно-технических мер обеспечения информационной безопасности для проектируемых и эксплуатируемых ЖАТ, формирование и обеспечение функционирования системы управления информационной безопасностью;

• проектирование и внедрение в информационную инфраструктуру ОАО «РЖД» систем защиты информации;

• реализация документооборота в ОАО «РЖД» с учетом требований безопасности информации.

Работа над ошибками

Для анализа вариантов кибератак на электронную ТД необходимо определить понятие ошибки в ТД и дать классификацию ошибок. Под ошибкой в ТД будем понимать любое отклонение от ГОСТов, ОСТов, типовых материалов проектирования, утвержденных нормативов и инструкций, отраслевого формата представления ТД в электронном виде.

Классификация ошибок в электронной ТД приведена на *рис. 2*; классификация вариантов организации и последствий кибератак на техническую документацию – на *рис. 3*.

Необходимо также учитывать особенности проведения кибератак на ТД ЖАТ, обеспечивающую безопасность движения поездов.

К таким особенностям можно отнести:

• атаки на утвержденную ТД, на основе которой выполняются изготовление, строительство, пусконаладочные работы и эксплуатация систем (контрольный экземпляр схем ЖАТ);

• атаки, которые приводят к нарушению проверки условий безопасности движения поездов; например, при включении на входном светофоре зеленого сигнального показания, разрешающего проследование станции с максимально разрешенной скоростью, проверяются 29 условий обеспечения безопасности, нарушение любого из них (отсутствие проверки) может привести к опасному отказу ЖАТ; под опасным отказом ЖАТ понимается:

1. перевод стрелки под составом в процессе его движения;

2. задание маршрута с включением разрешающего показания на светофоре, враждебного заданному;

3. включение на светофоре более разрешающего показания, чем установленная категория маршрута (например, включение зеленого огня при установке маршрута на боковой путь);

4. задание маршрута на пути с нарушением целостности (излом рельса, обрыв соединительного стыка и т. п.);

5. задание маршрута по стрелкам (стрелочным приводам), у которых нарушены нормативные параметры эксплуатации;

6. ошибки, внесенные в монтажные схемы ЖАТ (типа «короткое замыкание», пропуск контакта и т. д.) и не отраженные на принципиальных электрических схемах;

7. кратные ошибки, обнаружение которых весьма трудоемко при проведении пуско-наладочных работ;

8. ошибки на период производства, строительства или монтажа оборудования.

В настоящее время специалисты ПГУПС и ООО «ИМСАТ» разрабатывают комплекс мер защиты ТД ЖАТ:

• использование отечественного ПО (АРМ-ПТД, АРМ-ВТД) для проектирования и ведения ТД;

• использование электронной цифровой подписи на всех стадиях жизни ТД (от проектирования до эксплуатации);

• корпоративное кодирование ТД, предназначенной для служебного пользования, контроль создания копий ТД;

• резервное копирование ТД с возможностью последующей сверки различных документов;

• контроль специальными средствами передаваемых и принимаемых файлов по сетям передачи данных;

• разработка АС экспертизы схемных решений для полной функциональной проверки ТД с учетом специфики документации.

Программные средства защиты (специализированное ПО) на этапе внедрения должны быть дополнены блоком организационно-технических мероприятий, включая:

• разработку дополнения к инструкции ЦШ-617 по ведению электронных копий ТД;

• обучение персонала основам безопасной работы с ТД в современных условиях;

• введение электронного документооборота и ЭЦП на всех этапах существования ТД;

• внесение изменений и дополнений, касающихся безопасности, информации в должностные инструкции всех участников электронного документооборота (ЭДО);

• внедрение средств ЭДО для контроля исполнительской дисциплины участников;

• разработку и применение специальных технических средств защиты серверов, баз данных и каналов связи.

Успешная реализация проекта кибербезопасности на полигоне Октябрьской железной дороги позволит обобщить результаты и распространить полученный опыт на другие дороги и на другие виды ТД (системы связи, энергоснабжения и т. п.) ОАО «РЖД» .

Литература

1. Шубинский И. Б. Безопасность информации в ключевых системах // Автоматика, связь, информатика. 2005. № 33. С. 22–23.
2. Ампилов М. В. Функциональная безопасность в среде интегрируемых систем // Автоматика, связь, информатика. 2005. № 33. С. 24–27.