УДК 004.056

О. О. Матусевич

Система захисту інформаційних повідомлень телемеханічних комплексів керування пристроями тягового електропостачання залізниць

Запропоновано методику побудови системи захисту інформації комплексів керування тяговим електропостачанням електрифікованих залізниць.

Вирішення першочергових задач, які стоять перед електрифікованими залізницями України, неможливе без забезпечення стійкої і надійної роботи тягового електропостачання електричного транспорту. Тому при ускладненні технологічних процесів і режимів роботи залізниць у сучасних умовах експлуатації необхідно удосконалення та підвищення надійності комплексів керування системою тягового електропостачання, що функціонують в умовах внутрішніх та зовнішніх загроз, під якими розуміються потенційно можливі події, дії, процеси, які можуть привести до відмов комплексу.

На електрифікованих залізницях України в даний час застосовуються сучасні інформаційно-керуючі телемеханічні комплекси «Граніт-мікро», «Дніпро – 2000», «Лоза – 2000» та інші. Дані комплекси керування тяговим електропостачанням залізниць побудовані на новій технологічній основі і сучасних технологічних засобах. Вказані системи забезпечують не тільки автоматизацію керування технологічним процесом, але і дозволяють вирішити питання організаційно-економічного управління, діагностики устаткування тягових підстанцій, аналізу інформації і формування енергооптимальних рішень при управлінні [1]. Широкомасштабне використання обчислювальної техніки і телекомунікаційних систем в даних комплексах, збільшення об'ємів оброблюваної інформації і розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до їх високої уразливості. Ефективність механізмів захисту інформаційних активів (команди телекерування, телесигналізації, телевимірювань, обліку електроенергії, реєстрації аварійної інформації, організації автоматизованих робочих місць диспетчерів, тощо) в значній мірі залежить від реалізації ряду принципів [2]:

1. Механізми захисту слід проектувати одночасно з розробкою інформаційно-керуючих телемеханічних комплексів, а це дозволить забезпечити їх своєчасну інтеграцію в обчислювальне середовище систем керування тяговим електропостачанням і скорочення витрат на організацію та забезпечення захисту.

2. Питання захисту слід розглядати комплексно в рамках єдиної системи захисту інформаційних активів систем керування тяговим електропостачанням залізниць.

Інформація, як сукупність знань про фактичні дані і залежності між ними, стала стратегічним ресурсом, вона – основа для вироблення будь-якого рішення. Тому захист інформаційних активів телемеханічних комплексів керування тяговим електропостачанням, будучи складною, наукоємкою і багатогранною проблемою по суті, в умовах впровадження сучасних інформаційних технологій, створення розподілених обчислювальних систем і мереж зв'язку керуванням електропостачанням електрифікованих залізниць, набуває особливої гостроти.

Сучасні обчислювальні системи можуть працювати в мультипрограмному режимі (одночасно вирішується декілька завдань керування тяговим електропостачанням залізниць), в мультипроцесорному режимі (створюються умови для вирішення програми завдання декількома паралельно працюючими ПЕОМ, процесорами, число яких визначається кількістю контрольованих пунктів), а також в режимі розділення часу, коли до інформаційних ресурсів одночасно може звертатися велика кількість абонентів (багаторівнева система керування тяговим електропостачанням). При таких режимах роботи в пам'яті комп'ютерів одночасно можуть зберігатися програми і масиви даних різних користувачів або серверами одночасно підтримуватиме зв'язок значне число абонентів. В цьому випадку необхідне вирішення як проблем фізичного захисту інформації, так і захист її від користувачів, які несанкціоновано уклинюються в обчислювальний процес. В той же час, циркулююча в територіально розподілених системах і мережах керування тяговим електропостачанням залізниць інформація стає уразливою у зв'язку із зростанням різноманіття загроз несанкціонованого її отримання і використання.

Необхідно враховувати, що під захистом інформації розуміють захист не тільки комп'ютерної інформації, але і безліч інших аспектів, наприклад: захист каналів телемеханічного зв'язку, захист фізичних об'єктів інформаційної системи(диспетчерські і контрольовані пункти), технічний захист інформації на об'єктах інформаційної системи (диспетчерські і контрольовані пункти), придушення побічних електромагнітних випромінювань і багато інше [3].

– по-перше, зрозуміти, що є інформаційна система, яку необхідно захищати, які пред'являються вимоги до її захисту, а також необхідно розглянути існуючий досвід створення подібних систем і причини порушення їх безпеки.

– по-друге, необхідно визначити, які функції захисту і яким чином повинні бути реалізовані, і як вони

протидіють погрозам і усувають причини порушення безпеки стійкої і надійної роботи тягового електропостачання електричного транспорту.

Проте, великий об'єм наявних публікацій про захист інформації не дозволяє сформувати чітке уявлення про те, як же приступити до створення системи захисту інформаційних повідомлень комплексів керування тяговим електропостачанням залізниць з урахуванням властивих ним особливостей і умов функціонування. Поняття системності полягає не просто в створенні відповідних механізмів захисту, а є регулярним процесом, здійснюваним на всіх етапах життєвого циклу інформаційної системи. При цьому всі засоби, методи і заходи, використані для захисту інформації, об'єднуються в єдиний цілісний механізм – систему захисту.

Відомо, що основою або складовими частинами практично будь-якої системи (у тому числі і системи захисту інформації) є [4]:

– нормативно-правова і наукова база;
– структура і завдання органів;
– організаційні заходи і методи;
– програмно-технічні способи і засоби.

Далі виділимо основні напрями в загальній проблемі забезпечення безпеки інформаційних технологій. Напрями формуються виходячи з конкретних особливостей інформаційної системи як об'єкту захисту. Згідно проведеного аналізу експлуатаційної надійності комплексів керування різних поколінь розробку системи захисту комплексів необхідно проводити з наступних основних напрямів [5]:

– захист каналів зв'язку;
– захист центрально прийомо-передавальної станції (ЦППС) диспетчерського пункту (ДП), ПЕОМ контрольованих пунктів (КП) та програмного продукту;
– захист функціональних модулів (ФМ) комплексу;
– захист системи керування від внутрішніх та зовнішніх силових дій;
– захист об'єктів інформаційної системи ДП (ЦППС), КП.

Але оскільки кожен з цих напрямів базується на перерахованих вище основах, то ці основи і напрями нерозривно зв'язані один з одним.

Автором запропонована методика (послідовність кроків) побудови системи захисту інформації комплексів керування тяговим електропостачанням електрифікованих залізниць. Ця методика в рівній мірі може бути застосована для всіх вище вказаних напрямів захисту інформації сучасних телемеханічних комплексів і припускає наступну послідовність дій, дивись рис. 1.

Вказана послідовність дій повинна здійснюватися безперервно по замкнутому циклу з проведенням відповідного аналізу стану системи захисту інформації і уточненням вимог до неї після кожного кроку.

Висновки

Для керування системою електропостачання на електрифікованих залізницях України в даний час застосовуються сучасні інформаційно-керуючі телемеханічні комплекси, які побудовані на новій технологічній основі і сучасних технологічних засобах. Широкомасштабне використання обчислювальної техніки і телекомунікаційних систем в даних комплексах

Рис. 1. Безперервний цикл створення системи захисту інформації комплексів керування тягового електропостачання залізниць

приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до їх високої уразливості. В цьому випадку необхідне вирішення як проблем фізичного захисту інформації, так і захист її від користувачів, які несанкціоновано уклинюються в обчислювальний процес. Для вирішення цього питання:

1. Автором розроблена методика побудови системи захисту інформації комплексів керування тяговим електропостачанням електрифікованих залізниць.

2. Для забезпечення захисту комплексу керування тяговим електропостачанням від загроз необхідне узгоджене застосування різнорідних заходів захисту (організаційно – правових, технічних, програмних). Обґрунтоване поєднання цих заходів і є системою захисту комплексу керування тяговим електропостачанням електричного транспорту від внутрішніх та зовнішніх загроз.

Перелік посилань

1. Аналіз роботи господарства електрифікації та електропостачання в 2006 році [Текст] / Міністерство транспорту та зв'язку України. Державна адміністрація залізничного транспорту. Головне управління електрифікації та електропостачання. – К. : ТОВ «НВП Поліграфсервіс», 2007. – 197 с.
2. Яковлев В. В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта [Текст] / В. В. Яковлев, А. А. Корниенко. – М. : УМК МПС России, 2002. – 327 с.
3. Матусевич А. А. Основные направления и методы повышения надежности аппаратуры и защиты информации телемеханических комплексов тягового электроснабжения железных дорог [Текст] / А. А. Матусевич // Вісник Дніпропетровського національного університету залізничного транспорту. – 2007. – № 15. – С. 32–35.
4. Хорошко, В. А. Методы и средства защиты информации [Текст] / В. А. Хорошко, А. А. Чекатков – К. : «ЮНИОР», 2003. – 501 с.
5. Матусевич А. А. Анализ надежности существующей системы телемеханики на Приднепровской железной дороге [Текст] / А. А. Матусевич, В. Г. Кузнецов // Залізничний транспорт України. – 2007. – № 5. – С. 72–73.

Поступила в редакцию 25.03.09 г.

Предложена методика построения системы защиты информации комплексов управления тяговым электроснабжением электрифицированных железных дорог.

The author proposed the method of protective system construction for management complexes of traction power supply railways.

УДК 621.313

А. А. Петков

Особенности формирования испытательного импульса тока при его идентификации набором контролируемых параметров и интегралом действия

Рассмотрен вопрос формирования испытательных импульсов тока, заданных амплитудно-временными параметрами и интегралом действия. Предложен метод выбора элементов генератора при нечетком определении контролируемых параметров формируемого импульса тока.

Введение

Процесс совершенствования электротехнического, электронного и микропроцессорного оборудования обязательно включает аспект повышения его устойчивости к воздействиям различных электромагнитных факторов, сопровождающих все жизненные циклы оборудования. Одним из наиболее значимых факторов этого класса является разряд молнии. Особая важность проверки устойчивости авиационного оборудования на прямое поражение молнией нашла отражение в разработке ряда международных и национальных нормативных документов, например [1, 2].

Особенностью воздействия разрядов молнии является то, что имеющие при этом место процессы (электромагнитные, электротермические и электродинамические), наряду с амплитудно-временными параметрами (АВП) импульса тока, определяются такой его характеристикой, как интеграл действия [2, 3]. Это влечет за собой ряд проблем при разработке и создании генераторов импульсов тока (ГИТ), моделирующих ток прямого поражения разрядом молнии. Одной из задач, возникающих на стадии проектирования ГИТ, является выбор параметров разрядной цепи, позволяющей формировать импульс тока при его идентификации АВП и интегралом действия.

Выбор элементов традиционной схемы ГИТ для формирования импульса тока, заданного только на-