УДК 681.3.06

А. А. МАТУСЕВИЧ (ДИИТ)

ПОСТРОЕНИЕ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ ТЕЛЕМЕХАНИЧЕСКИХ КОМПЛЕКСОВ ЭЛЕКТРОСНАБЖЕНИЯ ЖЕЛЕЗНЫХ ДОРОГ

Запропоновано модель захисту інформації телемеханічних комплексів керування пристроями електропостачання залізниць. Обрано раціональний варіант побудови системи захисту інформації.

Предложена модель защиты информации телемеханических комплексов управления устройствами электроснабжения железных дорог. Выбран рациональный вариант создания системы защиты информации.

A model of protecting the information of telecontrol complexes for operating railway power supply devices has been offered and a rational option of creating the system of information protection has been selected.

Четкая организации перевозного процесса на железных дорогах предъявляет повышенные требования к системам автоматики и телемеханики управления устройствами электроснабжения. Основными определяющими требованиями являются: обеспечение безопасности движения, непрерывное электроснабжение, надежность устройств и систем управления, обеспечение высоких скоростей движения. Для автоматизации управления устройствами электроснабжения железных дорог Украины сегодня применяются в основном старые системы телемеханики, созданные в 60–70 гг. прошлого столетия.

В последние пять лет на отдельных участках электрифицированных железных дорог Украины начали применять современные информационно-управляющие телемеханические комплексы (ИУТК). За базовую в Украине принята интегрированная система управления устройствами электроснабжения «Гранит-микро», которая построена на новой технологической основе и современных технологических средствах. Система обеспечивает не только автоматизацию управления технологическим процессом, но и позволяет решить вопросы организационно-экономического управления, диагностики оборудования тяговых подстанций, анализа информации и формирования энергооптимальных управляющих решений. Системные и схемные решения «Гранит-микро» защищены 20 патентами [3; 4].

Современные ИУТК, в том числе «Гранит-микро», строятся по принципам SCADA systems (Supervisory Control and Data Acquisition) – диспетчерских систем с супервизорным управлением при сборе данных. Аппаратные и программные средства ИУТК образуют автоматизированный оперативно-информационный комплекс (АОИК) со вставками для реализации автоматизированных рабочих мест диспетчера (АРМ-Д) и обслуживающего персонала (АРМ-ОП). Обрабатывающий центр (ОЦ) ЦППС выполняется на ПЭВМ [5]. Следовательно, в такой автоматизированной системе управления (АСУ) формируется информационная система (ИС), которая должна быть защищена от случайных или преднамеренных воздействий [1; 2].

Система информационной безопасности должна представлять собой регулярный процесс, осуществляемый на всех этапах жизненного цикла информационной системы. При построении такой системы необходимо объединить все средства, методы и мероприятия, используемые для защиты информации, в единый целостный механизм – систему защиты информации (СЗИ) [6–8].

Однако необходимость системного подхода к вопросам обеспечения безопасности информационных технологий современных ИС пока еще не находит должной поддержки и понимания со стороны руководства железных дорог. В настоящее время нет руководящих документов и методических указаний по созданию СЗИ, а также методик по организации проведения комплексных мероприятий защиты информации в автоматизированных системах управления устройствами электроснабжения железных дорог Украины [3; 11; 12].

Сегодня специалисты из самых разных областей знаний занимаются вопросами обеспечения информационной безопасности. Это обусловлено тем, что мы живем в обществе (среде) информационных технологий, куда переходят все социальные проблемы человечества, в том числе и вопросы информационной безопасности. Каждый из указанных специалистов по-

своему решает задачу обеспечения информационной безопасности и применяет свои способы и методы для достижения заданных целей и каждый из них в своем конкретном случае находит свои совершенно правильные решения. Но, как показывает практика, совокупность таких правильных решений не дает в сумме положительного результата – система безопасности в общем и целом работает неэффективно. Такое положение дел обусловлено отсутствием системного подхода, который определил бы взаимные связи (отношения) между существующими понятиями, определениями, принципами, способами и механизмами защиты. Все сказанное касается и проблем защиты информации в АСУ электроснабжения железных дорог Украины при применении современных ИУТК.

Система защиты информации лишь тогда станет системой, когда будут установлены логические связи между всеми ее составляющими. Следовательно, для обеспечения информационной безопасности и надежности аппаратуры информационно-управляющих телемеханических комплексов электроснабжения железных дорог необходимо создавать модель СЗИ. Существует многообразие вариантов построения информационных систем и каждая из них порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время, большой объем имеющихся публикаций не позволяет сформировать четкое представление о том как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования.

Практическая задача обеспечения информационной безопасности и надежности аппаратуры ИУТК состоит в разработке модели представления системы (процессов) информационной безопасности (ИБ), которая на основе научно-методического аппарата, позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих ИС ИУТК управления устройствами электроснабжения железных дорог.

Из анализа существующего многообразия вариантов построения моделей СЗИ (международные, европейские, американские, украинские, российские стандарты), основной задачей модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации [2; 9; 10]. Исходя из вышеизложенного, упрощенный вид создаваемой модели системы информационной безопасности (СИБ) ИУТК может иметь вид, представленный на рис. 1.

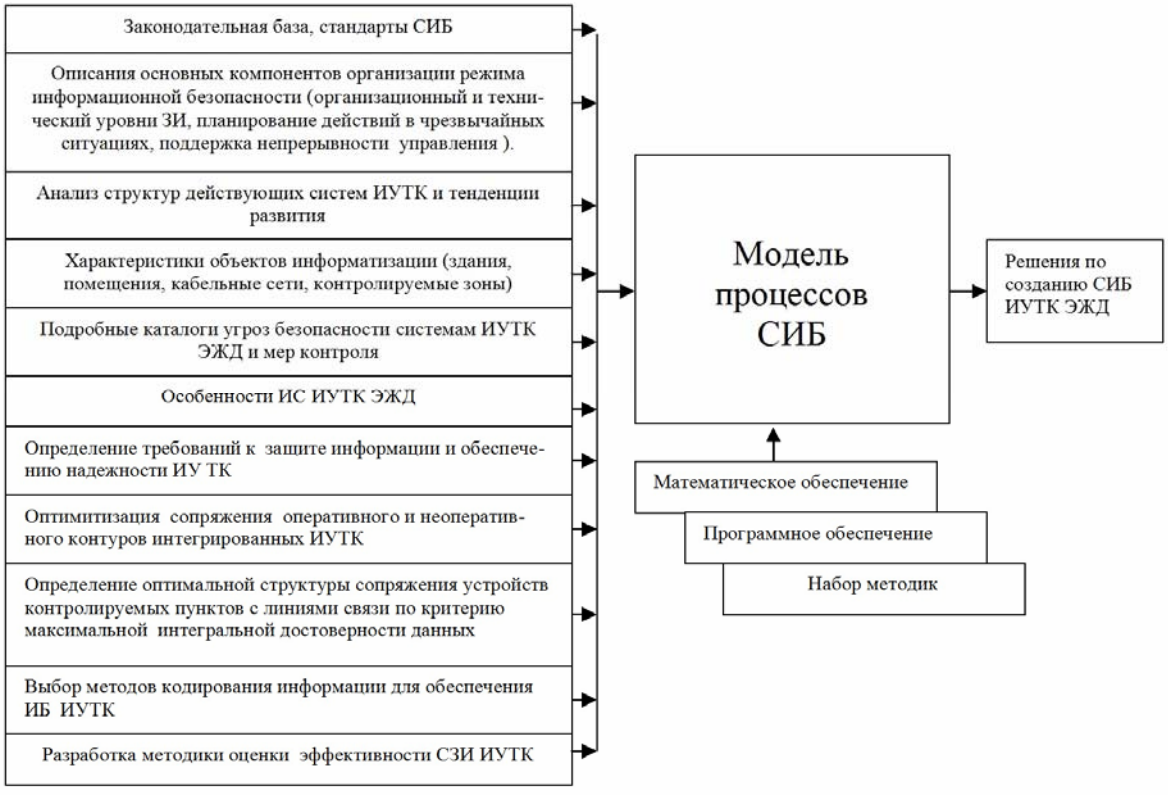

Рис. 1. Упрощенный вид модели СИБ ИУТК

Предлагаемая модель может использоваться для разработки методических указаний по созданию СИБ ИУТК, а также методик оценки ИБ и надежности ИУТК, создания модели для проведения исследований.

Для решения этой задачи модель должна обладать следующими свойствами: функционировать в условиях высокой неопределенности исходной информации; простота использования, универсальность, комплексность, наглядность, практическая направленность, возможность наращивания знаний. Возможности модели должны позволять: оперативно реагировать на изменения условий функционирования ИУТК и задавать различные уровни защиты; контролировать состояние СИБ ИУТК; объединить усилия различных специалистов единым замыслом; установить взаимосвязь между показателями СИБ и надежности ИУТК; применять различные методики оценок СИБ и надежности ИУТК управления устройствами электроснабжения ж. д.

Формирование имитационной модели для исследования различных систем дискретных параллельных асинхронных процессов разрабатываются на основе различных подходов. Наиболее распространенными являются системы и сети массового обслуживания (СМО), в последнее время виден рост интереса к таким моделям и методам: стохастические автоматы, сети Мерлина, стохастические сети Петри, семантические схемы (с позиций структурной иерархии, функциональной иерархии, причинно-следственной иерархии) и т. д. В последнее время появились публикации построения различных имитационных моделей на основе матриц знаний.

Этот метод отличается своей наглядностью и дает возможность: оперативно реагировать на изменения условий функционирования ИС; задавать различные уровни защиты; регулировать взаимные связи между элементами защиты; применять существующие программы автоматизации создания СЗИ и разрабатывать новые.

Для применение этого метода необходимо охватить все основные аспекты СЗИ, а это возможно только при рассмотрении проблемы с разных сторон (объемное построение системы информационной безопасности), в этом случае человек получает наиболее полное представление об интересующем его явлении.

В этом направлении проведенный анализ существующих методик (последовательностей) работ по созданию СЗИ позволяет выделить три группы составляющих модели [6; 8; 12].

Первая группа – основные методы создания СЗИ: организационные; технические; программные.

Вторая группа – направления создания СЗИ: защита диспетчерских (ДП) и контролируемых пунктов (КП) как объектов ИС; защита каналов связи; повышение надежности ИУТК; защита автоматизированного оперативно-информационного комплекса (АОИК) ПУ и ПЭВМ КП; защита ИС ИУТК от силовых воздействий и подавление побочных ЭМИ.

Третья группа – последовательность (этапы) создания СЗИ: определение информации, подлежащей защите, и предполагаемых отказов аппаратуры ИУТК; выявление угроз и каналов утечки информации, обнаружение факта отказа аппаратуры; оценка угроз и рисков для информационных ресурсов (информации); определение требований к СЗИ; выбор способа и средств защиты аппаратуры и информации; применение выбранных мер, способов и средств защиты; контроль целостности СЗИ, управление защитой. Если рассмотреть составляющие модели второй группы, то каждое направление создания СЗИ базируется на составляющих первой группы модели. К примеру, направление под названием «Защита каналов связи» необходимо рассматривать по всем методам создания СЗИ, а именно: организационные методы защиты каналов связи; технические и программные методы защиты каналов связи.

Аналогично можно рассматривать остальные направления по всем методам создания СЗИ.

Следовательно, для формирования общего представления о конкретной системе защиты необходимо ответить минимально на

$$K = M_i \cdot N_j$$

самых простых вопросов. Здесь M_i – количество составляющих первой группы; N_j – количество составляющих второй группы. В нашем случае $M_i = 3$, $N_j = 5$, следовательно,

$$K = 3 \cdot 5 = 15 .$$

Однако в разрабатываемой модели СЗИ необходимо рассмотреть также последовательность (этапы) создания СЗИ – третья группа составляющих модели. Составляющие этой группы необходимо реализовать в равной степени для каждого в отдельности метода создания СЗИ с учетом второй группы составляющих модели.

Таким образом, количество рассматриваемых вопросов может быть определено из соотношения

$$K = M_i \cdot N_j \cdot P_k , \qquad (1)$$

где P_k – количество составляющих третьей группы. Следовательно, при $M_i = 3$, $N_j = 5$, $P_k = 7$

$$K = 3 \cdot 5 \cdot 7 = 105 \qquad (2)$$

Из анализа существующих методик по созданию СЗИ, рассматриваемые вопросы можно представить в виде элементов матрицы (рис. 2.) [8].

<<< Последовательность	Направления >>>	010 Защита объектов ИС			020 Защита каналов связи			030 Защита ПВЭМ и программ			040 Защита от СВ и ЭМИ			050 Повышение надежности		
	Методы >>>	Организационные	Технические	Программные	Организационные	Технические	Программные	Организационные	Технические	Программные	Организационные	Технические	Программные	Организационные	Технические	Программные
		011	012	013	021	022	023	031	032	033	041	042	043	051	052	053
100	Определение информации, подлежащей защите	111	112	113	121	122	123	131	132	133	141	142	143	151	152	153
200	Выявление угроз и каналов утечки инф., отказа аппарат.	211	212	213	221	222	223	231	232	233	241	242	243	251	252	253
300	Оценка уязвимости, факт. отказа аппаратуры и рисков	311	312	313	321	322	323	331	332	333	341	342	343	351	352	353
400	Определение требований к СЗИ	411	412	413	421	422	423	431	432	433	441	442	443	451	452	453
500	Выбор способов и средств защиты аппар. и информац.	511	512	513	521	522	523	531	532	533	541	542	543	551	552	553
600	Внедрение и использование выбранных способов и средств	611	612	613	621	622	623	631	632	633	641	642	643	651	652	653
700	Контроль полноты и управление защитой	711	712	713	721	722	723	731	732	733	741	742	743	751	752	753

Рис. 2. Матрица взаимосвязи составляющих создаваемой СЗИ

В нашем случае общее количество элементов матрицы равно 105. Элементы матрицы имеют соответствующую нумерацию. Знакоместо (X00) – соответствует номерам составляющих третьей группы, знакоместо (0X0) – соответствует номерам составляющих второй группы, знакоместо (00X) – соответствует номерам составляющих первой группы.

Информация каждого элемента матрицы описывает взаимосвязь составляющих модели СЗИ. Круг вопросов создания СЗИ, оценки ее возможности рассматриваются путем анализа различных групп элементов матрицы в зависимости от поставленных целей и решаемых задач. Например, рассматривая элементы матрицы 111–711, 121–721, 131–731, 141–741, 151–751, можно отдельно оценить качество нормативной базы организационных мероприятий, создаваемой (созданной) СИБ. Рассматривая элементы 211–253, можно оценить качество мероприятий по выявлению угроз и каналов утечки информации. Рассматривая элементы 131–733, можно оценить защищенность ПЭВМ, процессов и программ и т. д. Можно рассматривать также содержание информации в отдельных элементах матрицы.

Для описания каждого элемента матрицы создан перечень вопросов и проведены необходимые математические расчеты, а для сложных элементов дополнительно созданы свои матрицы знаний. Чтобы оценить защищенность существующей СИБ и в случае определения требований для разработки новой системы необходимо проводить оценку защищенности ИУТК по всем направлениям.

Для автоматизации процессов создания и оценки процессов СЗИ можно использовать программу «Протект» (рис. 3.) [8]. Автором статьи разработана программа оценки эффективности СЗИ в виде таблиц Excel.

Рис. 3. Интерфейс ввода данных

Выводы

Предложенная модель СЗИ позволяет оперативно реагировать на изменения условий функционирования ИУТК и задавать различные уровни защиты, регулировать взаимные связи между элементами защиты, а также может выступать в роли руководства по созданию СЗИ.

На базе модели возможно проводить оценку эффективности принимаемых решений и выбрать рациональный вариант технической реализации системы защиты информации ИУТК управления устройствами электроснабжения железных дорог.

Модель может использоваться для разработки методических указаний по созданию СИБ ИУТК, а также методик оценки ИБ и надежности ИУТК, создания модели для проведения исследований. Данным вопросам будут посвящены следующие статьи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Закон України «Про захист інформації в автоматизованих системах».
2. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. ДСТУ 3396.0-96.
3. Корниенко В. В. Электрификация железных дорог. Аналитический обзор / В. В. Корниенко, А. В. Котельников, В. Т. Доманский. – К.: Транспорт Украины, 2004. – 195 с.
4. Портнов М. Л. Современные средства телемеханики, организация рабочих мест и щитов управления: Доклад на пятом специализированном семинаре – выставке. – М., 2004.
5. Информационный материал по проектированию применению информационно-управляющего телемеханического комплекса «Гранит-микро» (товарный знак МИКРОГРАНИТ). Редакция 5, 2004 г. Научный руководитель СНПП «Промэкс», канд. техн. наук Портнов М. Л. – 93 с.
6. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – К.: Юниор, 2003. – 501 с.
7. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800. – CCITT, Geneva, 1991.
8. Домарев В. В. Безопасность информационных технологий. – М., DiaSoft, 2004. – 975 с.
9. http://www.intuit.ru. Интернет университет информационных технологий. Стан охорони державної таємниці та технічного захисту інформації в Україні.
10. http://www.intuit.ru. Интернет университет информационных технологий. Методические основы защиты информационных активов компании. Сергей Петренко.
11. Матусевич А. А. Повышение информационной безопасности и достоверности данных систем управления устройствами электроснабжения железных дорог: Доклад на 65 Международной НПК / А. А. Матусевич, М. Л. Портнов. – Д.: Изд-во Днепропетр. нац. ун-та ж.-д, трансп. им. акад. В. Лазаряна. 2005.
12. Матусевич А. А. Основные направления и методы защиты аппаратуры автоматики и телемеханики железных дорог от внутренних и внешних воздействий: Доклад на третьем Международном симпозиуме eltrans 2005 ПГУПС, Санкт-Петербург, 2005.

Поступила в редколлегию 27.06.2006.