УДК 681.518 + 004.056 Вестник УрФО № 1(31) / 2019, с. 69–74

Московченко В. М., Шилина А. Н., Гайдаревский А. А.

DOI: 10.14529/secur190111

ИМИТАЦИОННЫЕ МОДЕЛИ ПРОЦЕССОВ НЕГАТИВНОГО ВОЗДЕЙСТВИЯ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОТИВОДЕЙСТВИЯ ИМ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

В работе представлены предложения по созданию эффективных комплексных систем обеспечения безопасности противодействия негативным воздействиям на автоматизированные системы управления технологическими процессами на основе имитационного моделирования процессов.

Описаны схема исследования качества обеспечения безопасности защищаемых объектов и алгоритм негативных воздействий на автоматизированные системы управления технологическими процессами. Рассмотрены основные принципы построения имитационной моделирующей системы, порядок ее разработки и вопросы реализации.

Результаты работы могут использоваться для получения количественных оценок показателей качества (эффективности) обеспечения безопасности защищаемых объектов.

Ключевые слова: *информационная безопасность, автоматизированные системы управления производственными и технологическими процессами, модель негативного воздействия, система обеспечения безопасности.*

IMITATING MODELS OF NEGATIVE IMPACT PROCESSES ON AUTOMATED CONTROL SYSTEMS OF TECHNOLOGICAL PROCESSES AND COUNTERING SAFETY SYSTEMS

The work offers suggestionsfor creation effective complex safety systems for counteraction to negative impacts on technologicalprocesses automated process control systems on thesimulation modeling of processes basis.

Research plan of the quality protected objects safety and negative impacts algorithm on the automated process control systems aredescribed. The main principals of an imitating analog system creation, order of its development and questions of realization are considered in this work.

Work results can be used for receiving quality (effectiveness) assessments of indexes of the protected objects safety.

Keywords: *information security, production and technological processes automated control systems, negative impact model, safety system.*

Современные тенденции повышения эффективности деятельности и качества управления путем упорядочения и ускорения информационных процессов, оптимизации и ускорения оперативно-технических расчетов, научного обоснования принимаемых решений неразрывно связаны с автоматизацией в профессиональной деятельности и определяются ролью и местом в системе управления, спецификой решаемых задач и уровнем в иерархии управления. Комплекс программных и технических средств, предназначенных для создания систем автоматизации управления технологическим оборудованием и производственными процессами на предприятиях (автоматизация производства) — это автоматизированные системы управления в производственных и технологических процессах (АСУ ТП) [1].

Особую роль АСУ играют в автоматизации технологических процессов в критических информационных инфраструктурах (КИИ), а так же сетях электросвязи, используемых для организации и функционирования таких объектов [2]. Нарушение или прекращение их функционирования приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению, разрушению или ущербу определенного вида и масштаба. Такое преднамеренное или непреднамеренное, организованное или случайное действие, событие или явление различной природы и характера в общем виде определяется как негативное воздействие (НВ) на объект АСУ ТП.

Одним из важнейших условий успешного решения задач по противодействию различного вида НВ на защищаемые объекты является создание эффективных комплексных систем обеспечения их безопасности (СОБ). Создание и развитие таких систем в современных условиях при закономерном усложнении задач по обеспечению безопасности невозможно без наличия соответствующих научно-методических основ. Отсутствие или недостаточный уровень основ, построенных

без использования положений моделирования сложных систем [4], приводит к принятию необоснованных и неэффективных решений по защите АСУ ТП от НВ.

Применительно к проблеме обеспечения безопасности в качестве исследовательских моделей должны выступать модели процессов НВ на АСУ ТП и противодействия им СОБ.

Общая схема таких процессов может быть описана моделью (1), которая вместе с соответствующей методикой обеспечит возможность получения количественных оценок показателей качества (эффективности) обеспечения безопасности защищаемых объектов (рис. 1)

$$A^{НВ}_{э} \leftrightarrow A^{СОБ}_{э} (э = 1,2,\ldots, Э), \quad (2)$$

а его многоэтапность – набором этапов (э = 1,2,…,Э), характерных для процесса функционирования объекта безопасности при данном НВ.

Случайный (вероятный) характер процесса определяется наличием множества неопределенностей $\boldsymbol{H_{BF}}$.

Следует подчеркнуть особую важность прогнозирования алгоритма $A^{НВ}_{э}$ (в том числе алгоритма поведения нарушителя при реализации им акта незаконного вмешательства (АНВ)), под которым обычно понимается время, место и характер протекания процесса НВ на АСУ ТП.

Рис. 1. Схема исследования качества обеспечения безопасности защищаемых объектов

В представляемой модели $\boldsymbol{B}$ – множество негативных воздействий на АСУ ТП; $\boldsymbol{F}$ – множество факторов, способствующих НВ на АСУ ТП; $\boldsymbol{H_{BF}}$ – множество неопределенностей, сопровождающих негативные воздействия; $\boldsymbol{A^{НВ}_{э}}$ и $\boldsymbol{A^{СОБ}_{э}}$ – соответственно алгоритм НВ на АСУ ТП (в том числе действия нарушителя – «модель нарушителя») на этапе процесса реализации этого воздействия и алгоритм СОБ защищаемого объекта (модель противодействия негативному воздействию); $\boldsymbol{Э}$ – количество этапов многоэтапного процесса реализации НВ на АСУ ТП; $\boldsymbol{S}$ – дуальное состояние АСУ ТП («негативное воздействие реализовано» или «негативное воздействие предотвращено (в том числе, «нарушитель обнаружен и обезврежен»)»; $\boldsymbol{U}(\boldsymbol{U^{нд}})$ – множество величин ущерба (недопустимого ущерба), полученных АСУ ТП в результате реализации НВ; $\boldsymbol{W}$ – значение показателей эффективности обеспечения безопасности защищаемого объекта, которое определяется по соответствующей методике с использованием информации, получаемой с помощью модели (1).

Антагонистический характер процесса противоборства СОБ с НВ в модели (1) учитывается алгоритмами противоборства:

Применительно к АНВ это, в частности, касается совокупности сведений о численности, оснащенности, подготовленности, осведомленности и тактике действий потенциального нарушителя, его мотивации и преследуемых целях при совершении АНВ в деятельность АСУ ТП.

Знание указанного алгоритма является необходимым условием рациональной организации соответствующего алгоритма $A^{СОБ}_{э}$ функционирования СОБ защищаемого объекта.

С учетом специфики защищаемого объекта, системы обеспечения его безопасности и характерных для него НВ моделирование процессов НВ на АСУ ТП и противодействия им СОБ, должно осуществляться с использованием физических, математических, алгоритмических моделей и их комбинаций.

Одной из особенностей процесса реализации НВ на АСУ ТП является участие в них человека (наличие так называемого «человеческого фактора») и сложность его формального описания. Поэтому можно с уверенностью утверждать, что ни один из перечисленных видов моделей в одиночку не обеспечит получения необходимой информации для

исследования безопасности защищаемых объектов и количественной оценки качества (эффективности) этой защиты.

Выход заключается в создании имитационной (человеко-машинной) моделирующей системы с участием экспертов для моделирования элементов исследуемого процесса, которые по тем или иным причинам не могут быть формализованы.

Понятие «имитационная система» не следует отождествлять с термином «имитационная модель» (модель Монте-Карло») [5]. Имитационная система должна составлять основу научно-методического аппарата исследований безопасности защищаемых объектов.
Имитационная моделирующая система (модель ***M***) позволяет языком моделирования реализовать не описываемую формально символическую форму (1). Необходимость ее разработки обусловлена также тем обстоятельством, что использование для принятия решений по совершенствованию СОБ защищаемых объектов имеющейся статистики по различным происшествиям только фиксирует результаты работы существующих (существовавших) систем.

Между тем необходима разработка опережающих мер по борьбе с НВ, связанных с прогнозированием развития как алгоритмов реализации этих воздействий (в том числе, постоянно совершенствующихся способов и средств осуществления нарушителями АНВ), так и способов и средств борьбы с ними.

Основными принципами построения имитационной моделирующей системы (модели ***M***) должны быть:

1) Модульность построения, позволяющая набором стандартных модулей формировать модель ***M*** и проводить автономную отладку ее отдельных модулей;

2) Открытость и гибкость структуры, позволяющая производить наращивание (корректировку) модели ***M*** (пополнение баз данных, подключение или отключение отдельных модулей) без коренной перестройки ее структуры и принципиального изменения содержания отдельных стандартных модулей;

3) Соответствие вида и количества моделируемой информации данному уровню иерархии модели.

4) Имитационный характер модели ***M***, который, как уже отмечалось выше, позволяет вводить отдельным «блоком» эксперта (специалиста-оператора) для моделирования процессов, некоторые элементы которых по тем или иным причинам не могут быть формализованы.

Отметим важность принципа 3, который вытекает их иерархической структуры «АСУ ТП – СОБ».

Реализация этого принципа, во-первых, позволит создать модель ***M***, соответствующую содержанию процессов функционирования СОБ, и, во-вторых, обеспечит возможность проведения моделирования при приемлемых затратах времени и вычислительных ресурсов (что особенно важно при проведении многократных «прогонов» задач для получения устойчивых статистических результатов).

Как следует из символической формы (1), исходной информацией для моделирования процесса НВ на *i*-ю АСУ ТП являются:

– множество $\boldsymbol{B}_i$ видов негативных воздействий, характерных для *i*-ой АСУ ТП;

– множество $\boldsymbol{F}_{ij}$ факторов, способствующих реализации *j*-го НВ на *i*-ой АСУ ТП;

– прогнозируемые алгоритмы $\boldsymbol{A}_{ij}^{НВ}$;

– существующие алгоритмы $\mathbf{A}_{ij}^{СОБ}$ СОБ *i*-го защищаемого объекта.

Множества $\boldsymbol{B}_i$, $\boldsymbol{F}_{ij}$ определяются экспертным методом, исходя из имеющегося опыта борьбы с НВ, глубокого знания структуры, состава и особенностей защищаемого объекта и его СОБ, а также прогноза состояния элементов этих множеств на рассматриваемом временном интервале.

На основе этих исходных данных соответствующими специалистами экспертным методом разрабатываются прогнозные сценарии развития процесса.

С использованием этих сценариев моделирование алгоритмов $\boldsymbol{A}_{ij}^{СОБ}$ реализуется следующим образом:

$$\boldsymbol{A}_{ij}^{СОБ}: \boldsymbol{И}_{ij} \times \boldsymbol{H}_{BF} \rightarrow \boldsymbol{P}_{ij},$$

где $\boldsymbol{И}_{ij}$ – информация, располагаемая персоналом защищаемого объекта и его СОБ применительно к *j*-му НВ на *i*-ю АСУ ТП на некотором временном интервале; $\boldsymbol{P}_{ij}$ – решения, принимаемые и осуществляемые персоналом защищаемого объекта и его СОБ на этом временном интервале.

Неопределенности $\boldsymbol{H}_{BF}$ при моделировании учитываются случайным образом в соответствии с их содержанием для конкретных сценариев реализации алгоритмов $\boldsymbol{A}_{ij}^{НВ}$ и $\boldsymbol{A}_{ij}^{СОБ}$ (для экспертов – существующими «вводными», для математических моделей – реализацией распределений соответствующих случайных величин (функций)).

Отрицательные последствия некачественных решений P_{ij}, как уже отмечалось выше, могут выражаться:

- в несвоевременности принятия решения (хотя и правильного, которого требовала создавшая ситуация);

- принятии решения, не позволяющего использовать все имеющиеся возможности СОБ;

- непринятии какого-либо решения вообще (отсутствие реагирования на создавшуюся ситуацию).

В зависимости от специфики конкретной структуры «АСУ ТП – СОБ» модель ***M*** может реализовываться следующими методами:

– проведением учений и тренировок персонала СОБ защищаемого объекта (аналогично командно-штабным учениям в силовых структурах государства);

– физическим моделированием на реальных элементах АСУ ТП и его СОБ;

– математическим (интерактивным) моделированием;

– их различными комбинациями.

Отличительной особенностью моделирования процесса является возможность и целесообразность использования метода физического моделирования, так как его исследование можно проводить на реальных АСУ ТП. Роль нарушителя при интерактивном моделировании должны выполнять высококвалифицированные специалисты СОБ защищаемого объекта.

Способом получения устойчивых обобщенных результатов моделирования при реализации модели ***M*** является метод статистических испытаний. Модель ***M*** кроме ее основного предназначения может использоваться также:

– для выявления и последующей ликвидации имеющихся технологических и эксплуатационных уязвимостей АСУ ТП;

– для тренировки персонала СОБ с целью получения и совершенствования им соответствующих навыков производственной деятельности.

Таким образом, разработка модели ***M*** представляет собой самостоятельную научную задачу и должна осуществляться в зависимости от особенностей конкретной исследуемой АСУ ТП, прогнозируемого алгоритма $A^{НВ}_{э}$, состава СОБ и используемого ею алгоритма $A^{СОБ}_{э}$ *(э= 1.2.…. Э)*. Порядок ее разработки представляется следующим:

- обследование АСУ ТП (изучение ее топологии, выполняемых задач, кадрового и технического состава, алгоритмов и режимов функционирования и т.п.);

- обследование существующей на нем СОБ (изучение ее кадрового состава и показателей его квалификации, инженерно-технических средств, режимов функционирования и используемых алгоритмов $A^{СОБ}_{э}$ противодействия НВ;

– прогнозирование множества ***B*** возможных видов НВ в функционирование АСУ ТП, их конечных результатов, а также алгоритмов их реализации $A^{НВ}_{э}$;

– разработка типовых сценариев функционирования СОБ защищаемого объекта;

– алгоритм модели ***M***;

– программная реализация модели ***M***;

– тестирование модели ***M*** с использованием имеющейся статистики по реализации НВ и противодействию им.

Не останавливаясь на очевидных элементах приведенного порядка, сделаем несколько замечаний по двум из них.

Разработка типовых сценариев НВ на АСУ ТП на основе ее обследования и СОБ является (с учетом частоты использования этих сценариев) оперативной основой создания модели ***M***.

Указанные сценарии содержат описание способов применения СОБ, наиболее полно характеризующих их возможности в определенных условиях, и представляют собой также базу для создания методик оценки их качества (эффективности). Эти сценарии должны обеспечивать согласование исследований, проводимых различными научно-техническими коллективами в интересах разработки проектов СОБ и программ их развития.

Имеющийся опыт и создания больших систем различного назначения говорит о принципиальной необходимости и важности наличия подобных типовых сценариев, разработка которых требует, как правило, проведения специальных научно-исследовательских работ.

Литература

1. Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных систе-

мах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а так же объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природы».

2. Федеральный закон от 26 июлю 2017 г. № 187-ФЗ «О безопасности информационной инфраструктуры Российской Федерации».

3. Ю.В.Михайлов. Научно-методические основы обеспечения безопасности защищаемых объектов. – М-: Горячая линия – Телеком, 2016. – 322 с.

4. О.И.Шелухин. Моделирование информационных систем. – М-: Горячая линия – Телеком, 2016. – 214 с.

5. А.В.Войтишек. Основы метода Монте-Карло: Учеб. пособие/Новосиб. гос. ун-т. Новосибирск, 2010 г.

References

1. Prikaz Federal'noy sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 14 marta 2014 g. № 31 «Ob utverzhdenii Trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"yektakh, potentsial'no opasnykh ob"yektakh, a tak zhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirody».

2. Federal'nyy zakon ot 26 iyulyu 2017 g. № 187-FZ «O bezopasnosti informatsionnoy infrastruktury Rossiyskoy Federatsii».

3. YU.V.Mikhaylov. Nauchno-metodicheskiye osnovy obespecheniya bezopasnosti zashchishchayemykh ob"yektov. – M-: Goryachaya liniya – Telekom, 2016. – 322 s.

4. O.I.Shelukhin. Modelirovaniye informatsionnykh sistem. – M-: Goryachaya liniya – Telekom, 2016. – 214 s.

5. A.V.Voytishek. Osnovy metoda Monte-Karlo: Ucheb. posobiye/Novosib. gos. un-t. Novosibirsk, 2010 g.

МОСКОВЧЕНКО Валерий Михайлович, доктор экономических наук, профессор, профессор кафедры «Информационная безопасность» Южно-Российского государственного политехнического университета (НПИ) имени М.И.Платова. Россия, 346428, Ростовская область, г. Новочеркасск, улица Просвещения, 132. E-mail: fvo.urgpu.npi@yandex.ru

ШИЛИНА Анна Николаевна, кандидат технических наук, доцент учебного военного центра Южно-Российского государственного политехнического университета (НПИ) имени М.И. Платова. Россия, 346428, Ростовская область, г. Новочеркасск, улица Просвещения, 132. E-mail: kurnevakatya@mail.ru

ГАЙДАРЕВСКИЙ Алексей Александрович, преподаватель учебного военного центра Московского государственного технического университета им. Н.Э. Баумана (Калужский филиал). Россия, 248000, Калужская область, г. Калуга, ул. Баженова 2. E-mail: Aleksey-gaidarevski@yandex.ru.

MOSKOVCHENKO Valery, doctor of Economics sciences, Professor of the Department of Information Security of the South-Russian State Polytechnic University (NPI) named after M. Platov. Russia, 346428, Rostov Region, Novocherkassk, Prosveshenia street, 132. E-mail: fvo.urgpu.npi@yandex.ru

SHILINA Anna, candidate of technical Sciences, associate Professor at the military training center South-Russian state Polytechnic University (NPI) named after M. I. Platov. Russia, 346428, Rostov Region, g. Novocherkassk, street of Enlightenment, 132. E-mail: kurnevakatya@mail.ru.

GAYADAREVSKY Aleksey, Bauman Moscow State Technical University (Kaluga branch) military training center teacher, Russia, 248000, Kaluga Region, Kaluga, Bazhenova street 2. E-mail: kurnevakatya@mail.ru