ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП С ИСПОЛЬЗОВАНИЕМ МЕТОДА ПРЕДИКТИВНОЙ ЗАЩИТЫ

Гарбук С.В.[1], Правиков Д.И.[2], Полянский А.В.[3], Самарин И.В.[4]

В статье рассмотрены подходы к управлению информационной безопасностью АСУ ТП промышленного объекта. Предложен метод предиктивной защиты, построенный на прогнозировании последствий реализации команд управления и основанный на активно развивающихся в настоящее время «сквозных цифровых технологиях»: искусственного интеллекта, сенсорики и робототехники, а также использующий современные вычислительные средства. Представлена комплексная модель технического объекта автоматизации. Описаны последствия от реализации угроз информационной безопасности на разных уровнях комплексной модели объекта автоматизации. Рассмотрен один из методов классификации интеллектуальных SCADA-систем, по признаку использования методов искусственного интеллекта для решения задач поддержки принятия решений оператором сложного объекта контроля и управления. Для каждого из классов представлены соответствующие примеры существующих реализаций SCADA.

В качестве преимущества предложенного метода предиктивной защиты, являющимся новым поколением интеллектуальных методов управления технологическими процессами, выделяется возможность управления в ситуациях с неизвестными видами помех и деструктивными воздействиями.

Ключевые слова: *АСУ ТП, интеллектуальная система управления, искусственный интеллект, критическая инфраструктура, объект управления, предиктивная защита, цифровая модель, SCADA.*

DOI: *10.21681/2311-3456-2019-3-63-71*

Введение

В декабре 2016 года состоялось заседание «круглого стола» Комитета Государственной Думы по энергетике на тему: «Перспективы развития вопросов информационной безопасности топливно-энергетического комплекса и законодательные аспекты обеспечения безопасности информационных систем объектов топливно-энергетического комплекса». В ходе заседания представителями экспертного сообщества задача, вынесенная на обсуждение, была признана актуальной. Фактической реализацией поставленной задачи стало принятие Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ и ряда детализирующих подзаконных актов.

Вместе с тем, несмотря на очевидный прогресс в нормативном обеспечении, задача практического обеспечения информационной безопасности информационных систем критически важных объектов, в первую очередь обеспечения безопасности АСУ ТП, на настоящий момент не имеет удовлетворительного решения. Обратной стороной динамичного развития информационных технологий является постоянное пополнение арсенала средств, используемых злоумышленниками для реализации информационных атак, в том числе, на объекты критически важной инфраструктуры и другие важные объекты защиты. В этих условиях традиционные подходы, основанные на формулировании модели угроз и реализации стандартных защитных мер, направленных на нейтрализацию угроз, являются неэффективными, что подтверждается мнением ведущих специалистов, в частности, в работе [1], которую уже сейчас можно считать канонической.

В качестве примера можно привести массовые атаки в 2017 году на критическую инфраструктуру различных государственных структур – подразделений МВД России, Следственного комитета, крупнейших телекоммуникационных компаний и т.п. Атака осуществлялась вирусом-шифровальщиком WannaCry. Во многих случаях атака была успешной, несмотря на существующие системы защиты. Резонансным инцидентом ИБ, приведшим к выведению инфраструктурного объекта из строя на продолжительное время, стала атака на подвесную канатную дорогу в Москве 28 ноября 2018 года. Неизвестный прислал на отвечающий за работу фуникулера компьютер сообщение о блокировке всех файлов с требованием перевести биткойны на указанную электронную почту.

Управление объектами критически важной инфраструктуры, объектами интернета вещей и другими техническими объектами осуществляется с использованием АСУ технологическими процессами (АСУ ТП), в состав которых входят SCADA-системы (реализация базовой логики управления процессом, взаимодействие с внешними системами), человеко-машинные интерфейсы (HMI), программируемые логические контроллеры (передача

1 Гарбук Сергей Владимирович, кандидат технических наук, директор по научным проектам, НИУ ВШЭ, г. Москва, Россия. E -mail: garbuk@list.ru

2 Правиков Дмитрий Игоревич, кандидат технических наук, директор НОЦ Новые информационно-аналитические технологии, РГУ нефти и газа (НИУ) имени И.М. Губкина. г. Москва, Россия. E -mail: dip@gubkin.pro

3 Полянский Алексей Вадимович, генеральный директор, НТЦ «Станкоинформзащита», г. Москва. Россия. E -mail: polyansky@ntcsiz.ru

4 Самарин Илья Вадимович, кандидат технических наук, РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва, Россия. E-mail: fkb-info@gubkin.ru

Таблица 1.

Поколения АСУ технологическими процессами

Поколение	Системы управления	Объекты управления	Показатели эффективности управления
I (1970)	Аналоговые, с минимальной адаптивностью	Отдельные агрегаты	Скалярные регулировочные характеристики
II (1990)	Цифровые на базе микропроцессоров, адаптивные. Человеко-машинные интерфейсы (HMI)	Сложные технические системы	Матричные регулировочные характеристики
III (2010)	Цифровые с элементами ИИ (обучение на прецедентах)	Технологические процессы	Показатели качества функционирования системы
IV (2020)	Системы с предиктивной аналитикой	Бизнес-процессы	KPI на уровне интегральных бизнес-процессов

управляющих сигналов непосредственно к исполнительным устройствам) и другие компоненты. Актуализация угроз информационной безопасности, связанных с воздействием на технические объекты автоматизации, связана, прежде всего, с совершенствованием функциональных возможностей АСУ ТП и расширением сферы их применения.

Основные этапы эволюционирования АСУ ТП представлены в табл.1. На начальном этапе создания АСУ ТП объектами управления являлись отдельные параметры, установки, агрегаты. Системы автоматического регулирования обеспечивали решение задач стабилизации, программного управления, слежения, в то время, как за человеком были сохранены функции расчета задания и параметры настройки регуляторов.

Второй этап развития АСУ ТП был связан с бурным развитием аппаратных платформ на основе микропроцессоров, обеспечившим внедрение в управление технологическими процессами вычислительной техники. Первоначальное применение микропроцессоров на отдельных фазах управления привело в последующем к широкому применению человеко-машинных систем управления, развитию методов инженерной психологии, методов и моделей исследования операций, а затем – к диспетчерскому управлению на основе использования автоматических информационных систем сбора данных и современных вычислительных комплексов.

Приблизительно с 2010 года начали активно применяться так называемые «интеллектуальные» системы управления, характеризующиеся возможностью обучения на прецедентах, что, в свою очередь, позволило управлять сложными технологическими процессами в условиях отсутствия детерминированных алгоритмов управления. Основной сложностью при создании таких систем является формирование обучающей выборки исходных данных требуемого объёма. В условиях динамически изменяющихся внешних условий (включая изменение модели угроз информационной безопасности) и вариативности характеристики объектов управления сформировать такую выборку за практически приемлемое время далеко не всегда представляется возможным, что существенно ограничивает возможность применения интеллектуальных методов в АСУ.

Важно отметить, что с точки зрения задач информационной безопасности средства защиты информации (СЗИ) для АСУ ТП первых трёх поколений представляют собой отдельную систему, ориентированную на фильтрацию поступающего управляющего трафика в соответствии с предопределённой или адаптивной логикой «чёрных» и «белых» списков, определяющих запрещённые и разрешённые команды. При этом отличительными признаками фрагментов управляющего трафика могут являться отдельные сигнатуры, поведенческие (эвристические) признаки или их совокупность. Так или иначе, «чёрные» и «белые» списки формируются операторами безопасности, исходя из своего понимания угроз ИБ, в то время, как эксплуатация АСУ ТП осуществляется инженерами-технологами, не являющимися, как правило, специалистами в области защиты информации. Такое разделение сфер ответственности является одной из системных причин недостаточной эффективности функционирования СЗИ АСУ ТП на современном этапе.

Метод предиктивной защиты объектов автоматизации

В работе [2] был сформулирован новый критерий защищённости АС, используемой в замкнутом контуре управления объектом (функциональной подсистемой): система является защищённой, если под воздействием факторов, влияющих на информацию, передаточная функция АС меняется таким образом, что качество управления объектом управления остаётся в заданных пределах. При этом под передаточной функцией W под-

разумевается зависимость сигнала S(t), подаваемого на вход объекта управления, от структуры управляющего информационного трафика I(t), поступающего на вход АС. Деструктивное воздействие информационной атаки x(t) приводит к изменению как управляющего трафика $I'(t)=I(t)\oplus x(t)$, так и самой управляющей функции $W'=W\oplus x(t)$, в результате чего на объект поступает искажённый сигнал управления:

$$S'(t)=W'(I'(t)). \quad (1)$$

Как уже было отмечено выше, система считается защищённой, если для всех возможных $x:S\rightarrow S'$ качество управления объектом управления остаётся приемлемым. В соответствии со стандартами в области менеджмента качества ИСО 9000 под качеством управления здесь целесообразно понимать степень соответствия параметров управления требованиям, предъявляемым потребителем.

В [3-5] было показано, что подобный подход наиболее эффективен для АСУ ТП, что обусловлено, прежде всего, возможностью автоматизированной оценки влияния изменений передаточной функции, вызванных информационной атакой, на способность объекта управления выполнять задачи в соответствии со своим целевым назначением. Подобная автоматизированная оценка может быть выполнена с использованием цифровой модели объекта управления, позволяющей прогнозировать поведение объекта при подаче на него различных управляющих сигналов S(t). В этом случае решение о легитимности (безопасности) поступающего на вход АС управляющего трафика I(t) принимается, исходя из допустимости прогнозируемого поведения объекта управления. Соответственно, подобный подход к управлению безопасностью может быть назван методом предиктивной защиты.

Отметим, что адекватная модель объекта управления в большинстве случаев может быть разработана именно для АСУ ТП, осуществляющих управление техническими объектами. Для других АСУ, используемых, например, для управления организационно-техническими и социальными системами (ERP, BPMS), возможность и целесообразность создания адекватной модели объекта управления представляется намного более проблематичной.

Необходимо учитывать, что реализация технологического процесса осуществляется в реальном времени. Соответственно, задержки, вносимые работой системы защиты т, должны быть такими, чтобы не приводить к сбоям в работе АСУ ТП. Характерное допустимое время задержки для большинства объектов управления составляет единицы микросекунд.

Таким образом, в отличие от стандартных подходов, ориентированных на обеспечение информационной безопасности АС как таковой, предлагаемый метод предиктивной защиты [2,4] направлен на обеспечение безопасности комплексной технической системы, включающей как АС, так и объект управления. Важно отметить, что при таком подходе управление безопасностью осуществляется с учётом целевых задач, решаемых комплексной системой.

Комплексная модель технического объекта автоматизации

Модель комплексной технической системы, включающей АСУ ТП и объект автоматизации, представлена на рис.1. Как и прежде предполагается, что на вход АСУ поступает управляющий трафик I(t), который преобразуется в электрический сигнал управления $S(t)=W_1(I(t))$. Сигнал S(t) подаётся на управляющее устройство, осуществляющее физическое воздействие (механическое, тепловое, электромагнитное и др.) $R(t)=W_2(S(t))$ непосредственно на объект управления, реализующий полезный технологический процесс. Результаты выполнения технологического процесса $F(t)=W_3(R(t))$ на интервале времени ΔT определяют глобальные экономические, социальные, экологические и иные последствия

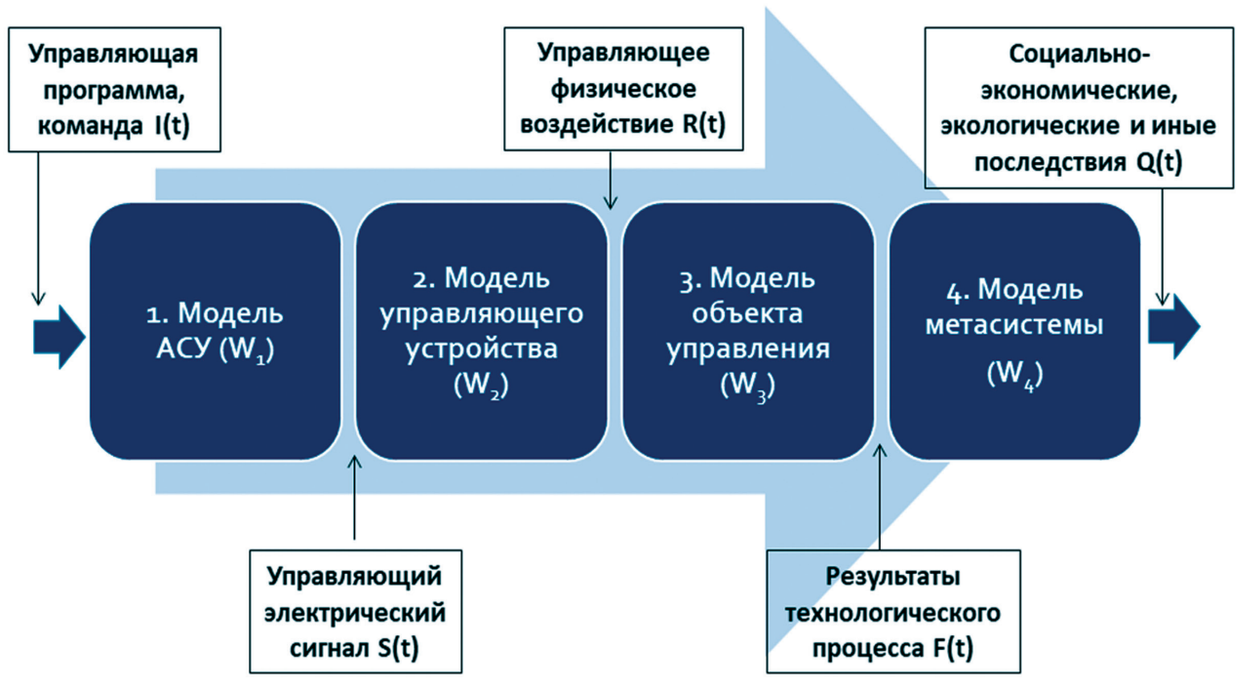

Рис.1. Комплексная модель технического объекта автоматизации

Рис.2. Последствия от реализации угроз информационной безопасности на разных уровнях комплексной модели объекта автоматизации

тервале времени ΔT определяют глобальные экономические, социальные, экологические и иные последствия с учётом состояния окружающей среды и иных внешних факторов: $Q=W_4(F(t),\Delta T)$.

Задача предиктивной защиты заключается в выборе такой управляющей характеристики W_1^*, при которой достигается оптимальное значение итоговых макропараметров, определяющих интегральную эффективность реализации технологического процесса при заданных характеристиках управляющего устройства, объекта управления и внешней среды:

$$W_1^*=\text{argopt}\{W_4(W_3(W_2(W_1(t)))),\Delta T\}. \quad (2)$$

Подобная структура модели объекта автоматизации представляется оправданной в связи с тем, что разные компоненты модели предполагают использование различных инструментов моделирования.

В частности, моделирование работы АСУ ТП W_1 может быть выполнено с использованием аналитических и имитационных моделей конечных автоматов, соответствующих отдельным элементам автоматизированной системы (SCADA, программируемый логический контроллер, интерфейсное устройство и др.). В зависимости от логики работы, заложенной в основу АСУ ТП, такие модели могут быть детерминированными или стохастическими.

Создание моделей исполняющего устройства W_2 и объекта управления W_3 основывается на активно развивающихся в настоящее время технологиях создания «цифровых двойников» [6] сложных технических систем, позволяющих создавать комплексные (мультифизические, т.е., учитывающие различные физические свойства: конструктивные, теплофизические, электромагнитные, трибологические и другие) модели объектов. В некоторых случаях, представляется возможным использовать мультифизическую модель, соответствующую не классу объектов некоторого типа, а конкретному экземпляру объекта. Такие, ещё более точные, модели принято называть «цифровыми тенями» [1,6].

Моделирование технологических и бизнес-процессов W_4 может быть выполнено с использованием нотации eEPC (extended Event-driven Process Chain) в соответствии с универсальной методологией ARIS (Architecture of Integrated Information Systems). Широко применяются также методология функционального моделирования $IDEF_0$, нотация документирования технологических процессов $IDEF_3$, средства моделирования компании Business Genetics (BusinessGenetics W5 Modeler), описательная методология POEM (Process Oriented Enterprise Modelling) и другие средства моделирования.

Таким образом, может быть выделено три основных уровня, на которых последствия реализации угрозы ИБ проявляются принципиально по-разному (рис.2):

– информационный уровень – нарушение целостности, доступности и конфиденциальности технологической информации, обрабатываемой в АСУ ТП. Отметим, что для защиты технологических объектов наиболее важным является обеспечение целостности и доступности управляющего трафика, в то время, как конфиденциальность передаваемой информации, имеющая для большинства систем первостепенное значение, в АСУ ТП не так существенна. В то же время, в случае реализации предиктивной защиты принципиальным является вопрос обеспечения конфиденциальности (равно как и целостности и доступности) модели объекта

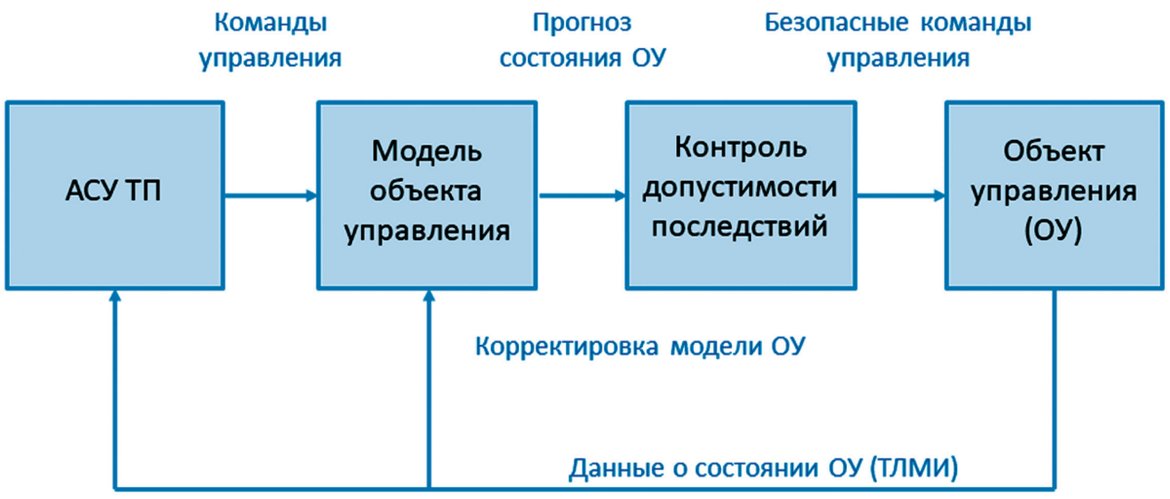

Рис.3. Значимость разных аспектов ИБ при защите информации, обрабатываемой в АСУ ТП

можности прогнозировать поведение системы защиты (рис.3). Так, например, в работе «Black-box Adversarial Attacks with Limited Queries and Information» показано, что если в системе управления используются нейросетевые модели W1-W_4, то знание структуры нейронных сетей или даже возможность анализировать отклик на различные значения исходных данных позволяет в тысячи раз ускорить подбор параметров эффективной функциональной атаки (Adversarial Intelligence) на подобную систему;

– физический уровень – аварии на объекте автоматизации, сбои в работе отдельных управляющих узлов и агрегатов;

– макроуровень – интегральные негативные последствия экономического и иного характера.

Для реализации метода предиктивной защиты поступающий управляющий трафик I^' (t) должен быть разбит на фрагменты:

$$I'(t)=I_1'(t) \cup I_2'(t) \cup \ldots \cup I_L'(t), \quad (3)$$

где $I_l'(t)$ соответствует фрагменту управляющего трафика на промежутке времени $t \in (t_{l1};t_{l2})$, достаточно продолжительном для того, чтобы на модели $W=W_1 \cup W_2 \cup W_3 \cup W_4$ можно было принять достоверное решение о допустимости или нежелательности прогнозируемого поведения объекта управления; L – количество временных фрагментов, на которые разбивается период наблюдения системы ΔT.

Относительно выбора размера фрагментов $I_l'(t)$ необходимо отметить, что они должны быть достаточно продолжительными, чтобы позволять прогнозировать поведение объекта управления, и короткими настолько, чтобы задержка $\tau=(t_{l2}-t_{l1})+t_0$, вносимая работой системы предиктивной защиты, не препятствовала управлению технологическим процессом в реальном масштабе времени (t_0 – среднее время прогнозирования поведения объекта управления).

Тогда согласно (2) оптимальный сигнал управления S* (t) на l-том интервале времени $t \in (t_{l1};t_{l2})$ формируется в соответствии со следующим правилом:

$$S^*(t)=\begin{cases} W'(I'(t)), \text{если прогнозируемое поведение объекта является допустимым;} \\ argopt\left\{W_4\left(W_3\left(W_2(S(t))\right)\right)\right\}, \text{при недопустимом прогнозе поведения.} \end{cases} \quad (4)$$

Выражение (4) означает, что если прогнозируемое поведение системы является допустимым (качество управления является приемлемым), то l-й фрагмент управляющего трафика выполняется. В противном случае фрагмент трафика $I'(t \in (t_{l1};t_{l2}))$ считается недопустимо искажённым и игнорируется, а сигнал управления S*(t) формируется, исходя из накопленного ранее и зафиксированного в моделях W_2-W_4 опыта управления технологическим процессом, (управление объектом становится разомкнутым). Если количество последовательно игнорируемых фрагментов управляющего трафика превышает некоторый заранее заданный порог, управление объектом начинает осуществляться по определённому сценарию, предполагающему безопасную остановку технологического процесса.

Созданию моделей, необходимых для реализации метода предиктивной защиты (в особенности, моделей W_2 и W_3), способствует развитие следующих т.н. «сквозных цифровых технологий» [7,8]:

– большие данные (построение моделей с использованием эмпирических данных, собираемых на стадии эксплуатации объектов автоматизации);

– нейротехнологии и искусственный интеллект (построение моделей сложных объектов управления с использованием методов искусственного интеллекта, включая нейросетевые алгоритмы);

– новые производственные технологии (формирование и актуализация «цифровых двойников» и «цифровых теней» технических объектов);

– промышленный интернет (сбор данных о состоянии промышленных объектов с использованием специализированных протоколов обмена информацией);

– компоненты робототехники и сенсорика (использование информативных и дешёвых сенсоров для

4 Введение в «интеллектуальные» SCADA-системы для построения АСУТП трубопроводных систем. Материалы компании ООО «Трансэнергострой». URL: http://transenergostroy.ru/blog/_scada-.html

– технологии беспроводной связи (передача данных о состоянии промышленных и иных технических объектов в условиях отсутствия проводной коммуникационной инфраструктуры).

Кроме того, развитие средств микропроцессорной техники позволяет реализовывать вычисления, необходимые для расчёта прогноза поведения объекта управления в соответствии с его моделью $W=W_1UW_2UW_3UW_4$, за приемлемо короткий промежуток времени. Как было отмечено выше, для АСУ ТП, работающих в реальном масштабе времени, это требование является принципиальным.

Предиктивная защита как способ интеллектуального управления технологическим процессом

Как уже было отмечено, одно из наиболее перспективных направлений развития информационных систем заключается в их «интеллектуализации» за счёт использования т.н. «интеллектуальных» методов обработки данных, разработанных в ответ на необходимость решения ряда вычислительных задач, которые ранее могли быть решены исключительно человеком, благодаря его естественным интеллектуальным способностям [9,10]. В полной мере эта тенденция справедлива и для АСУ ТП [11].

Один из методов классификации интеллектуальных SCADA-систем предложен в статье[5]. Предлагается такие системы разделить на две группы по признаку использования методов искусственного интеллекта для решения задач поддержки принятия решений оператором сложного объекта контроля и управления. В первую группу входят SCADA-системы, реализующие традиционные функции мониторинга и управления процессами и использующие интеллектуальные алгоритмы для анализа состояний оборудования и режимов контролируемой системы:

– ведение базы данных реального времени;

– выполнение расчетов;

– графическое представление данных и параметров в виде мнемосхем, графиков, диаграмм и т.д.;

– предупредительная сигнализация;

– архивирование информации;

– генерирование отчетов.

Типичными представителями являются продукты: WinCC (Siemens), RTAP/Plus (Industrial Defender), SCADA NPT Expert (ООО «ЭнергопромАвтоматизация») и другие.

Вторую группу составляют SCADA-системы, использующие методы обработки и представления информации, основанные на знаниях. В функции таких систем входит интеллектуальная информационная поддержка человека-оператора при управлении процессами. К числу этих функций относятся:

– ситуационный анализ состояния объекта контроля и управления;

– оперативный поиск действий оператора-управленца при возникновении аномальных и критических ситуаций;

– диагностика состояния технологического оборудования;

– диагностика состояния технологического процесса;

– логический анализ событий;

– логический анализ аномальных ситуаций;

– прогноз поведения процесса во времени и другие;

– защита от несанкционированных технологическим регламентом действий оперативного персонала;

– ведение баз данных и знаний реального времени;

– ведение гипертекстовых баз эксплуатационных и регламентных знаний.

Наиболее известными представителями такого класса систем являются системы G2 (Gensym)[6], «СПРИНТ-РВ» (ООО «ТАСМО-БИТ» совместно с МЭИ) [12-14].

Gensym G2 является платформой для разработки экспертных систем реального времени в системах управления критически важными процессами, управления аварийными сигналами и сложными имитационными приложениями.

СПРИНТ-РВ включает набор программных инструментов для проектирования систем информационной поддержки операторов АСУ ТП. Технология построения систем информационной поддержки основана на выполнении последовательности шагов, определяющих процесс проектирования от технического задания на проектирование АСУ ТП до внедрения на технологическом объекте управления. При проектировании АСУ ТП программное и информационное обеспечения, устанавливаемые на технических средствах, объединяются в рабочее пространство, которое не только содержит всю необходимую для работы информацию и программные модули, реализующие соответствующие функции АСУ ТП, но и определяет связи между ними.

Еще один вариант решения проблемы интеллектуализации управления и информационного обеспечения предложен в работах [15-19] на основе концепции и методологии интеллектуальных сред. Термин «интеллектуальная среда» (дословно: «окружающий интеллект» – Ambient Intelligence [20]) служит для обозначения искусственных сред, чувствительных к присутствию людей и реагирующих на это присутствие. Сформулирована концепция построения искусственной интеллектуальной среды как гибридного мета-агента с распределенной системой восприятия и централизованной исполнительной системой. Общая архитектура интеллектуальной среды как гибридного интеллектуального агента включает 4 основных компонента:

1) средства обработки знаний и рассуждений;

2) искусственные сенсорные системы;

3) искусственные средства осуществления действий;

4) программно-аппаратные средства реализации повсеместных вычислений (Ubiquitous Computing).

Ключевую роль при создании интеллектуальных сред призваны сыграть средства проведения автоматизированных измерений и оценок, относящиеся к классу SCADA-систем.

5 Введение в «интеллектуальные» SCADA-системы для построения АСУТП трубопроводных систем. Материалы компании ООО «Трансэнергострой». URL: http://transenergostroy.ru/blog/_scada-.html

6 G2 Overview. URL: http://www.gensym.com/platforms/g2-enterprise/

Из приведённого анализа видно, что главным отличием предлагаемого метода предиктивной защиты от существующих интеллектуальных АСУ ТП является использование адекватной мультифизической модели объекта управления и модели бизнес-процесса, позволяющих реализовывать предиктивное управление. В контексте рассматриваемой задачи это означает, что решение о легитимности той или иной команды управления будет приниматься не на основе анализа команды как таковой (как это делается в существующих СЗИ) и не на основе значений управляющих сигналов, формируемых АСУ ТП и подаваемых на объект управления (как это делается в известных SCADA-системах с интеллектуальным управлением), а на основе прогнозируемого поведения самого объекта управления и влияния этого поведения на макропоказатели реализуемого бизнес-процесса. В этом случае автоматизированная система повторяет ключевое свойство естественного интеллекта человека: способность действовать в непредвиденных ситуациях, исходя из приемлемости прогнозируемых последствий выбранной стратегии поведения (управления).

Выводы

Таким образом, в статье предложен способ предиктивного управления информационной безопасностью объекта, основанный на прогнозировании последствий реализации той или иной команды управления. Показано, что данный способ может быть реализован на основе активно развивающихся в настоящее время «сквозных цифровых технологий»: искусственного интеллекта, сенсорики и робототехники, а также с использованием современных вычислительных средств. Метод предиктивной защиты может рассматриваться как новое поколение интеллектуальных методов управления технологическими процессами, высокая эффективность которого основывается на возможности управления в непредвиденных ситуациях, исходя исключительно из предопределённых целей реализуемого с использованием АСУ ТП бизнес-процесса.

Литература:

1. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 2 (26). С.2-15
2. Правиков Д.И. Об одном подходе к обеспечению информационной безопасности автоматизированных систем // Вопросы защиты информации. 2007. №3. С.17-19.
3. Гарбук С.В., Бурцев А.Г. Методические основы исследования уязвимостей компонентов АСУ ТП // Защита информации. Inside. 2012. №3. С.34-38
4. Гарбук С.В. Перспективы применения интеллектуальных технологий для решения задач безопасности // Национальная безопасность / nota bene. 2016. №4. С.451-457
5. Гарбук С.В. Интеллектуальные автоматизированные средства тематической обработки информации в системах безопасности// Искусственный интеллект и принятие решений. 2017. №1. С.95-104.
6. Боровков А.И. «Умные» цифровые двойники – основа новой парадигмы цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения. Трамплин к успеху// Журнал АО «ОДК». 2018. №13. С.12-18.
7. Башлыков А.А., Еремеев А.П. Методы и программные средства конструирования интеллектуальных систем поддержки принятия решений для объектов энергетики // Вестник МЭИ. 2018. № 1. С. 72—85.
8. Новиков Д.А. Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития. – М.: ЛЕНАНД, 2016. 160 с.
9. Гарбук С.В. Интеллектуальные автоматизированные средства тематической обработки информации в системах безопасности// Искусственный интеллект и принятие решений. 2017. №1. С.95-104.
10. Гарбук С.В., Бакеев Р.Н. Конкурентная оценка качества технологий интеллектуальной обработки данных // Проблемы управления. 2017, №6. С.50-62.
11. Гордейчик С.В. Миссоцентрический подход к кибербезопасности АСУ ТП. // Вопросы кибербезопасности № 2 (10). 2015. стр. 56 – 59.
12. Башлыков А.А., Еремеев А.П. Методы и программные средства конструирования интеллектуальных систем поддержки принятия решений для объектов энергетики // Вестник МЭИ. 2018. № 1. С. 72—85.
13. Башлыков А.А. СПРИНТ-РВ — интеллектуальная SCADA-система для построения средств человеко-машинного управления сложными и экологически опасными объектами и технологиями // Автоматизация, телемеханизация и связь в нефтяной промышленности. 2012. № 12. С. 8—20.
14. Lange T. Intelligent SCADA Systems// Engineer IT. Automation and Technical.Control April 2007. P. 26-30.
15. Тарасов В. Б., Святкина М. Н. Интеллектуальные SCADA-системы: истоки и перспективы // Наука и образование. Научное издание МГТУ им.Н.Э.Баумана. 2011. №10. URL: http://technomag.edu.ru/doc/224479.html (дата обращения: 01.12.2018)
16. Ковалев С.М. Тарасов В.Б. Проблемы развития интеллектуальных технологий на транспорте и производстве // Автоматизация и механизация технологических процессов на сортировочных станциях. Труды 1-й международной научно-практической конференции (Москва, 24-25 ноября 2010 г). С. 68-72.
17. Тарасов В.Б. От информационного общества к интеллектуальной экономике // Реинжиниринг бизнес-процессов на основе современных информационных технологий. Системы управления знаниями. Сборник научных трудов XIV-й научно-практической конференции (РБП-СУЗ-2011, Москва, МЭСИ, 28-29 апреля 2011 г.). - М.: МЭСИ, 2011. С. 286-298.
18. Кудж С.А., Цветков В.Я. Сетецентрическое управление и киберфизические системы. // Образовательные ресурсы и технологии. № 2 (19), 2017, стр. 86-92.
19. Андрюхин Е.В., Ридли М.К. Анализ сетевого трафика для выявления критических состояний систем автоматизации в условиях индустриальных промышленных сетей. // Безопасность информационных технологий. Том 25, № 3. 2018, стр. 79-87.
20. Aarts E., Harwig R., Schuurmans M. Ambient Intelligence // The Invisible Future: The Seamless Integration of Technology into Everyday Life / Ed. by P.J.Denning. – New York: McGraw-Hill Companies, 2001. Pp. 235-250

ENSURIN APCS INFORMATION SECURITY USING THE PREDICTIVE PROTECTION METHOD

Garbuk S.V.[7], Pravikov D.I.[8], Polyansky A.V.[9], Samarin I.V.[10]

The article discusses approaches to the management of information security of an industrial facility's APCS. A predictive protection method is proposed that builds on predicting the consequences of implementing control commands and on now actively developing "end-to-end digital technologies" (artificial intelligence, sensory capabilities and robotics), and uses advanced computing facilities. An integrated model of a technical automation object is presented. Information security implications at different levels of the automation object's integrated model are described. One of the classification methods for intelligent SCADA systems is considered, which builds on the use of artificial intelligence methods to handle tasks of supporting decision making by the operator of a complex control and monitoring facility. Examples of the existing SCADA implementations are presented for each of the classes.

The controlling capability in situations with unknown types of interference and ravages was pointed out as an advantage of the proposed predictive protection method pertaining to the new generation of intelligent process control methods.

Keywords: *ICS, intelligent control system, artificial intelligence, critical infrastructure, control object, predictive protection, digital model, SCADA.*

References:

1. Zegzhda D.P., Vasil'ev YU.S., Poltavceva M.A., Kefeli I.F., Borovkov A.I. Kiberbezopasnost' progressivnyh proizvodstvennyh tekhnologij v ehpohu cifrovoj transformacii // Voprosy kiberbezopasnosti. 2018. № 2 (26). S.2-15
2. Pravikov D.I. Ob odnom podhode k obespecheniyu informacionnoj bezopasnosti avtomatizirovannyh sistem // Voprosy zashchity informacii. 2007. №3. S.17-19.
3. Garbuk S.V., Burcev A.G. Metodicheskie osnovy issledovaniya uyazvimostej komponentov ASU TP // Zashchita informacii. Inside. 2012. №3. S.34-38
4. Garbuk S.V. Perspektivy primeneniya intellektual'nyh tekhnologij dlya resheniya zadach bezopasnosti // Nacional'naya bezopasnost' / nota bene. 2016. №4. S.451-457
5. Garbuk S.V. Intellektual'nye avtomatizirovannye sredstva tematicheskoj obrabotki informacii v sistemah bezopasnosti// Iskusstvennyj intellekt i prinyatie reshenij. 2017. №1. S.95-104.
6. Borovkov A.I. «Umnye» cifrovye dvojniki – osnova novoj paradigmy cifrovogo proektirovaniya i modelirovaniya global'no konkurentosposobnoj produkcii novogo pokoleniya. Tramplin k uspekhu// ZHurnal AO «ODK». 2018. №13. S.12-18.
7. Bashlykov A.A., Eremeev A.P. Metody i programmnye sredstva konstruirovaniya intellektual'nyh sistem podderzhki prinyatiya reshenij dlya ob»ektov ehnergetiki // Vestnik MEHI. 2018. № 1. S. 72—85.
8. Novikov D.A. Kibernetika: Navigator. Istoriya kibernetiki, sovremennoe sostoyanie, perspektivy razvitiya. – M.: LENAND, 2016. 160 s.
9. Garbuk S.V. Intellektual'nye avtomatizirovannye sredstva tematicheskoj obrabotki informacii v sistemah bezopasnosti// Iskusstvennyj intellekt i prinyatie reshenij. 2017. №1. S.95-104.
10. Garbuk S.V., Bakeev R.N. Konkurentnaya ocenka kachestva tekhnologij intellektual'noj obrabotki dannyh // Problemy upravleniya. 2017, №6. S.50-62.
11. Gordejchik S.V. Missocentricheskij podhod k kiberbezopasnosti ASU TP. // Voprosy kiberbezopasnosti № 2 (10). 2015. str. 56 – 59.
12. Bashlykov A.A., Eremeev A.P. Metody i programmnye sredstva konstruirovaniya intellektual'nyh sistem podderzhki prinyatiya reshenij dlya ob»ektov ehnergetiki // Vestnik MEHI. 2018. № 1. S. 72—85.
13. Bashlykov A.A. SPRINT-RV — intellektual'naya SCADA-sistema dlya postroeniya sredstv cheloveko-mashinnogo upravleniya slozhnymi i ehkologicheski opasnymi ob»ektami i tekhnologiyami // Avtomatizaciya, telemekhanizaciya i svyaz' v neftyanoj promyshlennosti. 2012. № 12. S. 8—20.
14. Lange T. Intelligent SCADA Systems// Engineer IT. Automation and Technical.Control April 2007. P. 26-30.
15. Tarasov V. B., Svyatkina M. N. Intellektual'nye SCADA-sistemy: istoki i perspektivy // Nauka i obrazovanie. Nauchnoe izdanie MGTU im.N.EH.Baumana. 2011. №10. URL: http://technomag.edu.ru/doc/224479.html (data obrashcheniya: 01.12.2018)
16. Kovalev S.M. Tarasov V.B. Problemy razvitiya intellektual'nyh tekhnologij na transporte i proizvodstve // Avtomatizaciya i mekhanizaciya tekhnologicheskih processov na sortirovochnyh stanciyah. Trudy 1-j mezhdunarodnoj nauchno-prakticheskoj konferencii (Moskva, 24-25 noyabrya 2010 g). S. 68-72.

7 Sergey Garbuk, Ph.D., Director for Research Projects, National Research University Higher School of Economics, Moscow, garbuk@list.ru
8 Dmitry Pravikov, Ph.D., Director of the REC of new information and analytical technologies, Gubkin Russian State University of Oil and Gas (NRU), Moscow, dip@gubkin.pro
9 Alexey Polyansky, General Director, STC «Stankoinformzaschita», Moscow, polyansky@ntcsiz.ru
10 Ilya Samarin, Ph.D., associate professor, Gubkin Russian State University of Oil and Gas (National Research University), fkb-info@gubkin.ru

17. TarasovV.B.Otinformacionnogoobshchestvakintellektual'nojehkonomike//Reinzhiniringbiznes-processovnaosnovesovremennyh informacionnyh tekhnologij. Sistemy upravleniya znaniyami. Sbornik nauchnyh trudov XIV-j nauchno-prakticheskoj konferencii (RBP-SUZ-2011, Moskva, MEHSI, 28-29 aprelya 2011 g.). - M.: MEHSI, 2011. S. 286-298.
18. Kudzh S.A., Cvetkov V.YA. Setecentricheskoe upravlenie i kiberfizicheskie sistemy. // Obrazovatel'nye resursy i tekhnologii. № 2 (19), 2017, str. 86-92.
19. Andryuhin E.V., Ridli M.K. Analiz setevogo trafika dlya vyyavleniya kriticheskih sostoyanij sistem avtomatizacii v usloviyah industrial'nyh promyshlennyh setej. // Bezopasnost' informacionnyh tekhnologij. Tom 25, № 3. 2018, str. 79-87.
20. Aarts E., Harwig R., Schuurmans M. Ambient Intelligence // The Invisible Future: The Seamless Integration of Technology into Everyday Life / Ed. by P.J.Denning. – New York: McGraw-Hill Companies, 2001. Pp. 235-250