3. *Хэррис Ф. Дж.* Использование окон при гармоническом анализе методом дискретного преобразования Фурье.// ТИИЭР: 1978. – Т. 66. – №1. – С. 60-96.
4. *Рабинер Л., Гоулд Б.* Теория и применение цифровой обработки сигналов.- М.: Мир, 1978. – 523 с.
5. *Хемминг Р.В.* Цифровые фильтры: Пер. с англ./ под ред. А.Хойнен. Измерение матрицы рассеяния цели // ТИИЭР: 1965. – Т. 53. – № 8. – С. 1074-1076.
6. *Шахтарин Б.И., Ковригин В.А.* Методы спектрального оценивания случайных процессов. М.: Гелиос АРВ, 2005. – 248 с.
7. *Chengge Z., Yeshu Y., Xinchao Z., Xin W.* A method for target estimation of level radar // International conference of radar proceedings. ICR'96. – Beijing. China. – 1996. – P.270-273.

Поступила 17.02.2014р.

УДК 004.056.5

Т. Л. Щербак, г. Киев

ЗАДАЧИ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Рассмотрены задачи комплекса средств защиты технологических процессов, которые на ряду с классическими задачами защиты аппаратно-программных ресурсов процесса объединены в единую последовательность задач защиты и инженерно-технических ресурсов процесса, включая задачи охранной и пожарной безопасности.

Введение. Широкое использование современных информационных технологий в науке, технике, отраслях промышленности и областях производства является известным фактом. В каждом конкретном случае такое использование имеет свою специфику и характерные особенности. В полной мере это относится и к технологическим процессам. Если рассматривать предметные области проведения таких процессов, то они практически охватывают весь диапазон промышленного и других видов производства, а сами процессы разнообразны и разноплановы. В настоящее время технологические процессы реализуются на базе использования широкого ассортимента изготавливаемых промышленностью аппаратно-программных средств. Возникает актуальная научно-техническая проблема защиты технологических процессов, в первую очередь, аппаратных и информационных ресурсов для обеспечения эффективного их проведения. На сегодня это стало, по сути, аксиомой, поскольку введение в мире рыночной экономики существенно реформировало социально-экономические отношения между производителями и странами, способствовало созданию конкурентных

отношений.

В данной работе предпринята попытка рассмотреть общие задачи использования средств защиты, как аппаратных, информационных, так и инженерно-технических ресурсов при проведении технологических процессов. При таком рассмотрении будут использованы результаты публикаций по защите информации, в том числе [1-4].

Постановка задания. На основании современных подходов повышения эффективности технологических процессов сформулировать задачи средств защиты информации при проведении технологических процессов.

Перейдем к изложению результатов данной работы.

При рассмотрении подобного рода задач возникают определенные трудности, суть которых состоит в обосновании на множестве разнородных и разноплановых технологических процессов наиболее типовые задачи средств защиты информации.

Факторы, которые действуют при проведении технологических процессов можно условно разделить на три группы:

а) обеспечивающие штатное функционирование процесса;

б) природного характера, как прогнозируемые, так и непрогнозируемые;

в) факторы несанкционированных действий злоумышленников (нарушителей), а в ряде случаев неумышленных действий сотрудников и работников процесса, направленных на нарушения штатного режима функционирования процесса; норм, требований, инструкций охраны производственных сооружений, конструкций, помещений, используемых при проведении технологического процесса; несанкционированного отбора, съема информации.

В зависимости от специфики функционирования объекта защиты, в основном это телекоммуникационные системы передачи и обработки информации, факторы группы в) разделяют еще на две следующие подгруппы:

- факторы несанционированного отбора и съема информации;
- факторы несанционированного нарушения функционирования объекта защиты.

Учитывая тот факт, что в большинстве случаев технологические процессы проводятся в местах пространственной компактности, целесообразно рассматривать задачи защиты в комплексе от всей группы факторов в) путем создания единого комплекса средств защиты проведения технологического процесса (далее *комплекс средств защиты информации*).

Известно [2], что комплексная программа защиты технологического процесса – это совокупность организационных и инженерных мероприятий, аппаратно-программных средств, которые обеспечивают штатный режим технологического процесса.

Такая программа мероприятий, реализация которой обеспечивает определенный уровень защиты (безопасности), в первую очередь комплекса

защиты информации, и соответствующих гарантий при проведении технологических процессов.

Для того, чтобы в рейтинг комплекса мог быть включен определенный уровень защиты и гарантий, должны быть выполнены все требования, перечисленные в критериях для данного уровня защиты и гарантий [3, 4].

Выбор средств защиты в соответствии с проблемами и угрозам защиты провеления технологического процесса можно использовать следующим образом [1].

Первый шаг - определить и оценить проблемы защиты (безопасности). Надо рассмотреть требования к конфиденциальности, целостности, доступности, наблюдаемости, подлинности и надежности информации процесса. Функциональное обеспечение и количество выбранных средств защиты должны соответствовать оцененным проблемам защиты [3].

Второй шаг - для каждой проблемы защиты определяют типовые угрозы и для каждой угрозы предлагают соответствующие средства защиты технологического процесса. Таким образом возможно удовлетворить специфические потребности защиты.

Оценка проблем защиты должна охватывать как всю имеющуюся информацию комплекса средств защиты информации, так и операции, которые производятся в процессе проведения технологического процесса. Это оценка определяет цели выбранных средств защиты. Различные средства комплекса или информация могут иметь различные проблемы защиты. Важно связывать проблемы защиты непосредственно с ценностями, поскольку это влияет на угрозы, которые могут появляться, и, таким образом, на выбор средств защиты [1-4].

Значимость проблем защиты может быть оценена в зависимости от того, какие из нарушений наносят серьезные повреждения или наносят легкий вред, или не влияют совсем.

Основными задачами комплексной программы защиты технологического процесса является предотвращения:

- несанкционированного доступа к аппаратным средствам процесса, нарушающих его штатный режим функционирования;
- несанкционированного доступа к информационным ресурсам процесса и нарушения целостности, конфиденциальности и достоверности информации технологического процесса;
- воздействия различных видов физических излучений на функционирование аппаратно-программных ресурсов процесса, включая информационные каналы передачи, обработки, управления, регистрации и представления данных измерений, контроля операторам;
- нарушения функционирования или вскрытия аппаратно-программных средств защиты;
- неправомерных действий как пользователей, так и обслуживающего персонала.

К основным этапам, а соответственно и конкретным задачам создания единого комплекса средств защиты информации, как аппаратных, так и информационных ресурсов конкретного технологического процесса относят следующие [3, 4]:

- базируясь на современных тенденциях защиты информации, используя развитую номенклатуру комплектующих, модулей и средств защиты информации в целом, интеллектуальные ресурсы заказчиков и изготовителей комплекса, производственные и финансовые ресурсы, разработать техническое задание на создание комплекса средств защиты информации, адаптированной к конкретному технологическому процессу для реализации комплекса программ для защиты технологического процесса;
- разработать конструктурскую, технологическую и техническую документацию на создание комплекса;
- произвести в случае необходимости подготовку производства и изготовить необходимые модули комплекса с последующими их испытаниями;
- откорректировать необходимую документацию для создания серийного образца комплекса;
- создать с использованием серийных комплектующих, модулей и изготовленных устройств серийный образец комплекса средств защиты информации;
- выполнить необходимый комплекс испытаний, сертификации и передать серийный образец системы в эксплуатацию.

Более подробно остановимся на этапах создания комплекса средств защиты информации. В отличие от всех технических систем, жизненный цикл такого комплекса имеет свою специфику и характерные особенности. Это связано с тем, что по сути недорогой по стоимости комплекс обеспечивает защиту в большинстве случаев очень дорогих и важных технологических процессов [2, 3].

Кроме функциональных критериев работы средств защиты требуется определить критерии гарантий, которые дают возможность оценить корректность реализации защиты. Критерии гарантий включают требования к архитектуре комплекса средств защиты, организации и уровня разработки, последовательности разработки, испытаний комплекса средств защиты, создания технической и эксплуатационной документации.

Иерархия уровней гарантий отображает постепенно возрастающую меру уверенности в том, что реализованные средства защиты позволяют противостоять определенным видам угроз. Механизмы средств защиты корректно реализованы и могут обеспечить ожидаемый уровень безопасности (защищенности) в процессе проведения технологического процесса.

Порядок оценки средств защиты на соответствия критериям гарантии определяется соответствующими нормативными документами. Экспертная комиссия, которая проводит оценку комплекса средств защиты информации

определяет какие функции защиты и на каком уровне они реализованы, каким образом обеспечиваются требования гарантий.

Результатом оценки является рейтинг, который согласно нормативным документам представляет собой упорядоченный ряд буквенно-числовых комбинаций, которые определяют уровень реализованной защиты в совокупности с уровнем гарантий [2].

Используя опыт создания подобного рода комплексов средств защиты информации [1-4], приведем некоторые практические рекомендации разработки такого комплекса.

Реализация разработанного и адаптированного для конкретного технологического процесса проекта создания комплекса средств защиты информации в большинстве случаев использует проверенные на практике принципы построения, управления и функционирования современных аппаратно-программных средств, систем и комплексов.

Принцип построения комплекса базируется на совокупности отдельных автономных подсистем, например:

- подсистема средств защиты аппаратных ресурсов процесса;
- подсистема средств защиты информационных ресурсов процесса;
- подсистема видеонаблюдения за помещениями, оборудованием проведения процесса;
- подсистема охранно-тревожной сигнализации;
- подсистема пожарной сигнализации;
- подсистема автоматического пожаротушения и др.

В целом комплекс средств защиты информации технологического процесса представляет автоматизированную систему с участием оператора с использованием широкого спектра аппаратных и программных средств. А сетевые решения этой системы допускают свободную топологию, в том числе такие соединения, как «звезда», «кольцо», «шина» и др.

Аппаратно-программная реализация комплекса использует номенклатуру комплектующих, модулей, средств, например различного рода сенсоров (датчиков), видеокамер, контроллеров, интерфейсных модулей, выпускаемых промышленностью различных стран, а также известные программные продукты по защите информации.

Принцип управления комплексом основан на децентрализации, когда архитектура управления комплексом представляет собой пирамиду. На нижних уровнях этой пирамиды находятся сенсоры (датчики), затем контроллеры, а на верхнем – многооконный графический интерфейс автоматизированного рабочего места оператора.

Выводы. Сформулированы основные задачи комплекса средств защиты информации при проведении технологического процесса. При этом наряду с традиционными задачами защиты информации – обеспечения конфиденциальности, целостности и доступности – при проведении технологического процесса необходимо в комплексе решать и другие задачи,

включая задачи защиты инженерно-технических ресурсов процесса, включая задачи охраны помещений, конструкций, сооружений и оборудования процесса, обеспечения пожаробезопасности проведения технологического процесса.

1. *Бабак В.П.,* Теоретические основы защиты информации: учебник / В.П. Бабак, А.А. Ключников. – Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2012. – 776 с.
2. *Домарев В.В.* Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД ДС», 2004. – 992 с.
3. *Зайцев А.П.* Технические средства и методы защиты информации: учеб. / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков: под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Машиностроение, 2009. – 508 с.
4. *Ленков С.В.* Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко: под ред. В.А. Хорошко. – К.: Арий, 2008. – Т.1. Несанкционированное получение информации. – 464 с. Т.2. Информационная безопасность. – 344 с.

Поступила 12.02.2014р.

УДК 621.311

О.Тимченко[1 2], А. Вовк[2]

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ АГРЕГОВАНИМИ ОБ'ЄКТАМИ ВИРОБНИЧИХ ПОЛІГРАФІЧНИХ СИСТЕМ

Анотація. В статті розглянуто методи забезпечення функціональної стійкості агрегованих об'єктів управління на підставі використання інформаційних і інтелектуальних моделей підтримки прийняття рішень. Розглядаються механізми логічного виводу в системі управління, як інтерпретатори правил продукції. В правила закладають знання про стратегії дій і умови їх можливих реалізацій, алгоритмів дій.

Аннотация. В статье рассмотрены методы обеспечения функциональной устойчивости агрегированных объектов управления на основе использования информационных и интеллектуальных моделей поддержки принятия решений. Рассматриваются механизмы логического вывода в системе управления, как интерпретаторы правил продукции. В правила закладывают знания о стратегии действий и условия их возможных реализаций, алгоритмов действий.

Abstract. The article describes the methods of providing functional stability of aggregated objects management based on the use of information and intelligent decision support models. The mechanisms of inference in the control system, as interpreters of production rules. These regulations lay knowledge about the strategy and the conditions of their possible implementations of algorithms action.

[1] Uniwersytet Warmińsko-Mazurski w Olsztynie
[2] Українська академія друкарства