УДК 51-74

СОВРЕМЕННЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И МЕТОДЫ АНАЛИЗА ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ

Можаева И.А., к.т.н., **Струков А.В.** доцент, к.т.н. (АО «СПИК СЗМА»)

Введение

До недавнего времени организации, создававшие и обслуживавшие информационные системы (ИС) и системы промышленной автоматики и контроля IACS (IACS – Industrial Automation and Control Systems), существовали и развивались в двух взаимоисключающих областях. Профессиональный опыт, знания и требования каждой отдельной организации не учитывались другими организациями. Анализ современного состояния решения задач обеспечения безопасности промышленного производства в целом предполагает необходимость взаимодействия между этими организациями.

Понятия кибербезопасности интегрированы с понятиями информационной безопасности, но с позиций IACS расширяются за счет анализа средств и методов обеспечения безопасности в широком смысле слова, в том числе и за счет необходимости решения задач анализа и управления рисками. Риск-ориентированная методология, согласно современным нормативным документам в сфере деятельности Ростехнадзора, опирается на традиционные методы теории надежности, сочетающие как качественные, так и количественные аспекты решения задач. Анализ опыта развития методов количественной оценки показателей функциональной безопасности систем, связанных с безопасностью, показывает, что и в области информационной безопасности может быть реализовано не только качественное оценивание. В настоящее время, наряду с широким использованием средств защиты информации, актуальной становится задача оценки надежности функционирования IACS, в частности автоматизированных систем управления, с учетом надежности самих средств защиты информации.

1 Терминология в области функциональной и информационной безопасности

Следует учесть, что еще в недавнем прошлом надзорные органы запрещали использовать любое программируемое оборудование в системах, критичных с точки зрения безопасности. Ситуация изменилась с введением международных стандартов МЭК 61508 и МЭК 61511. Эти стандарты, разработанные в ТК МЭК 65, обеспечили технический и научный подход к формулированию требований и спецификаций при проектировании систем, связанных с безопасностью, позволили более точно и обосновано оценивать риски.

В том же Техническом комитете МЭК 65 разработана серия стандартов МЭК 62443, объектом стандартизации которой является безопасность систем промышленной автоматики и контроля. Под термином «безопасность» в стандартах данной серии понимается предотвращение незаконного или нежелательного проникновения, умышленного или неумышленного вмешательства в штатную и запланированную работу, или получения ненадлежащего доступа к конфиденциальной информации в IACS.

Учитывая рост рисков кибербезопасности, многие организации руководствуются упреждающим подходом при устранении рисков безопасности своих информационно-технических систем и сетей. Организации начинают осознавать, что решение вопросов, связанных с кибербезопасностью, – это непрерывная деятельность или процесс, а не проект с четко обозначенным стартом и финишем. При этом ясно видна необходимость синтеза различных научных направлений анализа безопасности, что дает возможность применения наработанных научных и методических инструментариев. Условно взаимодействие различных направлений анализа безопасности систем промышленной автоматизации показано на рис.1 [1].

Если, например, промышленная безопасность опасных производственных объектов есть состояние защищенности жизненно важных интересов личности и общества от аварий на этих производствах, то технологическая безопасность рассматривает внутренние и внешние угрозы при реализации используемых или проектируемых технологий, а также защищенность научно-технической и технологической информации от несанкционированного использования и воздействия. Объектами технологической безопасности являются научно-техническая деятельность и образование, информация, природоохранные технологии, промышленное производство, сельское хозяйство, энергетика, транспортная инфраструктура.

Функциональная безопасность – часть общей безопасности, обусловленная применением объекта управления (ОУ) и системы управления ОУ и зависящая от правильности функционирования Э\Э\ЭП систем, связанных с безопасностью, и других средств по снижению риска [2,3].

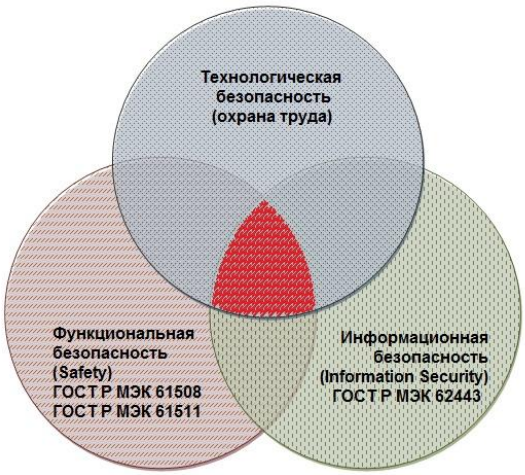

Рисунок 1 – Направления анализа безопасности систем промышленной автоматизации

Согласно ГОСТ Р ИСО МЭК 13335 информационная безопасность охватывает все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки [4]. На наш взгляд, по отношению к системам промышленной автоматики и контроля, особенно к автоматизированным системам управления технологическими процессами (АСУ ТП), больше подходят термины и определения серии ГОСТ МЭК 62443. В частности – термин кибербезопасности определяет действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов [5]. В этом случае рассматривается не только сама по себе информация, но и качество функционирования объекта управления. В настоящее время эти термины используются практически как синонимы.

В табл.1 приведено сравнение некоторых терминов стандартов серии МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» и серии МЭК 62443 «Сети промышленной коммутации. Безопасность сетей и систем».

Таблица 1– Сравнение терминов стандартов серий МЭК 61508 и МЭК 62443

ГОСТ Р МЭК 61508-4	ГОСТ Р МЭК 62443-1-1
Функциональная безопасность: Часть общей безопасности, обусловленная применением объекта управления (ОУ) и системы управления ОУ, и зависящая от правильности функционирования Э\Э\ЭП систем, связанных с безопасностью, и других средств по снижению риска.	**Кибербезопасность:** Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов.
Риск: Сочетание вероятности события причинения вреде и тяжести этого вреда.	**Риск**: Ожидание ущерба, выраженное как вероятность того, что определенный источник угрозы воспользуется определенной уязвимостью системы, и это приведет к определенным последствиям.
Остаточный риск: Риск, остающийся после принятий защитных мер.	**Остаточный риск**: Риск, сохраняющийся после реализации мер защиты или контрмер.
Безопасность: Отсутствие неприемлемого риска.	**Безопасность**: Отсутствие недопустимого риска.
Система, связанная с безопасностью – Система, которая реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния …	**Автоматизированная система безопасности** (safety-instrumented system): Система, используемая для реализации одной или нескольких функций технологической безопасности.
Уровень полноты безопасности (safety integrity level): Дискретный уровень (принимающий одно из четырех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.	**Уровень целостности безопасности** (safety integrity level): Дискретный уровень (один из четырех) для определения требований к целостности безопасности, предъявляемых к функциям технологической безопасности, которыми наделяются автоматизированные системы безопасности.
Функция безопасности: функция, реализуемая Э\Э\ЭП, системой, связанной с безопасностью, или другими мерами по снижению риска, предназначенная для достижения или поддержания безопасного состояния ОУ по отношению к конкретному опасному событию.	**Функция безопасности**: Функция зоны или тракта, направленная на предотвращение несанкционированного электронного вмешательства, которое способно нарушить или повлиять на нормальное функционирование устройств и систем в пределах данной зоны или тракта.
Полнота безопасности: Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного интервала времени.	**Уровень безопасности**: Степень необходимой эффективности контрмер и внутренне присущих свойств безопасности устройств и систем для зоны или тракта, основанная на оценке риска для данных зоны или тракта.
Электрическая\электронная\программируемая электронная система – Э\Э\ЭП система – система управления, защиты или мониторинга, основанная на использовании одного или нескольких Э\Э\ЭП устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие коммутационные магистрали, исполнительные устройства и другие устройства вывода.	**Системы промышленной автоматики и контроля (**IACS): Группа персонала, а также совокупность аппаратного и программного обеспечений, которые могут регулировать или воздействовать иным образом на безопасное, защищенное и надежное функционирование производств. процесса, включающие в себя распределенные системы управления (РСУ), программируемые логические контроллеры (PLC), пульты дистанционного управления, интеллектуальные электронные устройства, системы диспетчерского контроля и сбора данных (SCADA), объединенные системы электронного детектирования и контроля, а также системы мониторинга и диагностики.

2 Показатели функциональной безопасности

Системы физической безопасности, например, АСУ ТП, используют концепцию УПБ – уровень полноты безопасности (SIL – Safety Integrity Level) уже почти двадцать лет. Это позволяет представить потенциальную целостность физической безопасности того или иного компонента или уровень целостности физической безопасности применяемой системы одним числом, которое характеризует коэффициент защищенности, необходимый для обеспечения охраны труда и безопасности людей или среды на основе вероятности отказа этого компонента или системы.

В стандартах серии МЭК 61508 одним из показателей функциональной безопасности (ПФБ) является вероятность (частота) отказа на запрос выполнения функции безопасности (ФБ). Значения этой вероятности (частоты) соотносятся с определенными УПБ, как показано на рис.2.

Уровень безопасности (SIL)	**Режим с низким уровнем требований по требованию функции безопасности** (средняя вероятность отказа в выполнении заданной функции безопасности по требованию)	**Режим с высоким уровнем требований по требованию функции безопасности** (вероятность опасного отказа в течении одного часа в режиме непрерывной работы)
4	$\geq 10^{-5}$ PFD $< 10^{-4}$	$\geq 10^{-9}$ PFH $< 10^{-8}$
3	$\geq 10^{-4}$ PFD $< 10^{-3}$	$\geq 10^{-8}$ PFH $< 10^{-7}$
2	$\geq 10^{-3}$ PFD $< 10^{-2}$	$\geq 10^{-7}$ PFH $< 10^{-6}$
1	$\geq 10^{-2}$ PFD $< 10^{-1}$	$\geq 10^{-6}$ PFH $< 10^{-5}$

Рисунок 2– Показатели функциональной безопасности в стандартах МЭК 61508

Процесс определения необходимого фактора защищенности для системы физической безопасности хоть и сложен, но осуществим, поскольку вероятность отказа компонента может быть измерена в количественном отношении. В компании АО «СПИК СЗМА» разработана методика оценки показателей функциональной безопасности АСУ ТП [6], основанная как на использовании моделей стандартов МЭК 61508-6 [3], так и на методологии автоматизированного структурно-логического моделирования, реализованной в ПК АРБИТР [7].

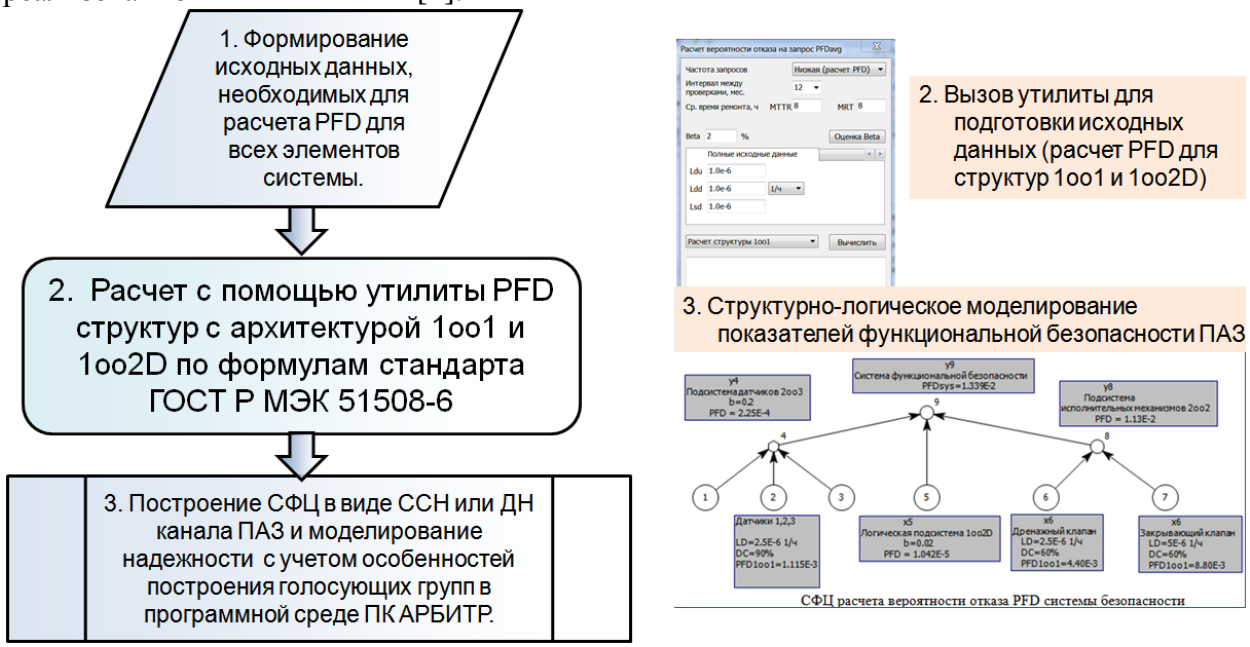

Рисунок 3 – Алгоритм определения показателей функциональной безопасности

На рис.3 показан алгоритм определения ПФБ и элементы его реализации – утилита для расчета показателей функциональной безопасности для простейших структур 1oo1 и 1oo2D и схема функциональной целостности (СФЦ) для моделирования ПФБ системы безопасности.

3 Уровни информационной безопасности

Системы информационной безопасности характеризуются значительно более широким набором последствий и значительно большим набором возможных обстоятельств, ведущих к возможному событию. Подразумевается, что системы информационной безопасности служат для защиты HSE (HSE – Health, Safety& Environment – здоровье, охрана труда и окружающей среды), проприетарной информации организации, общественного доверия и государственной безопасности, в ситуациях, когда случайные отказы оборудования не могут быть основной причиной. В одних случаях виновником может быть благонамеренный сотрудник, допускающий ошибку, а в других – злоумышленник, стремящийся спровоцировать событие и скрыть улики. Возрастающая сложность систем информационной безопасности значительно затрудняет описание фактора защищенности одним числом.

На современном уровне развития методологии оценки информационной безопасности применяется качественный метод определения уровня безопасности (SL). По мере доступности новых данных и разработки математических моделей риска, угроз и инцидентов безопасности эта концепция уступит место количественному подходу к выбору и верификации SL .

SL разбиты на три различных типа: целевые, достигнутые и потенциальные. Эти типы, будучи взаимосвязаны, затрагивают разные аспекты жизненного цикла безопасности [8]:

- **целевые SL (SL-T)** – это желаемые уровни безопасности для отдельно взятой системы. Эти уровни обычно определяются посредством выполнения оценки рисков для системы и установления того, что она нуждается в конкретном уровне безопасности для гарантированного обеспечения корректного функционирования;
- **достигнутые SL (SL-A)** – это фактические уровни безопасности для отдельно взятой системы. Эти уровни измеряются после того, как система введена в действие. Они служат для установления того, что система безопасности отвечает целям, которые были с самого начала обозначены в целевых SL;
- **потенциальные SL (SL-C)** – это уровни безопасности, которые могут обеспечивать компоненты или системы, будучи корректно сконфигурированными. Эти уровни указывают, что тот или иной компонент или система изначально способны соответствовать целевым SL без помощи дополнительных компенсационных контрмер, будучи корректно сконфигурированными и интегрированными.

Как определено в МЭК 62443-1-1, существует семь фундаментальных требований информационной безопасности (FR):

1) управление идентификацией и аутентификацией (УИА-IAC);
2) контроль использования (КИ-UC);
3) целостность системы (ЦС-SI);
4) конфиденциальность данных (КД-DC);
5) ограничение потока данных (ОПД-RDF);
6) своевременный отклик на события (СО-TRE);
7) работоспособность и доступность ресурсов (РД-RA).

Вместо сведения уровней SL к общему знаменателю стандарты серии МЭК 62443 используют вектор уровней SL. При этом используется пять разных уровней (0,1, 2, 3 и 4) по степени возрастания безопасности.

В формулировках для каждого SL используются такие термины, как «случайный», «непредумышленный», «простой», «изощренный» и «обширный». Эти формулировки умышленно абстрактны, чтобы одни и те же базовые формулировки можно было использовать для всех документов серии МЭК 62443. Тем не менее, имеется общая методологическая основа к разграничению уровней SL.

Уровень SL 0 не требует специальных требований или защиты безопасности.

Уровень SL 1 предполагает защиту от случайного или непредумышленного нарушения безопасности, что чаще всего является следствием не совсем строгой реализации политик безопасности. Примером нарушения может быть изменение уставки оператором инженерной станции.

Уровень SL 2 предполагает защиту от умышленного нарушения безопасности с использованием простых средств при незначительных ресурсах, посредственных навыках и низкой мотивации. Простые средства не требуют обширных познаний со стороны злоумышленника, не требуется досконального знания безопасности, домена или отдельно взятой системы, на которую совершается атака.

Уровень SL 3 предполагает защиту от умышленного нарушения безопасности с использованием изощренных средств, при умеренных ресурсах, наличии специальных познаний в АСУ и умеренной мотивации. Изощренные средства подразумевают продвинутые знания безопасности, продвинутые знания доменов, продвинутые знания целевой системы или любую их комбинацию. Злоумышленник, скорее всего, будет использовать векторы атаки, которые приспособлены к конкретной системе. Для нарушения безопасности системы злоумышленник может использовать эксплойты в операционных системах, которые недостаточно распространены, уязвимости в промышленных протоколах, специальную информацию о конкретной цели или другие средства, требующие наличия мотивации. Примером изощренных средств могут быть инструменты для взлома паролей или ключей, основанные на хеш-таблицах. Эти инструменты доступны для загрузки, но их применение требует знания системы (например, хеша взламываемого пароля).

Уровень SL 4 предполагает защиту от умышленного нарушения безопасности с использованием изощренных средств, при обширных ресурсах, наличии специальных познаний в АСУ и высокой мотивации. Примером изощренных средств при обширных ресурсах будет использование супер-ЭВМ или кластеров ЭВМ для осуществления взлома паролей методом перебора с использованием обширных хеш-таблиц. Другим примером будет ботнет, используемый для атаки на систему одновременно с помощью нескольких векторов атак. Третьим примером будет организованная преступная группировка, имеющая достаточную мотивацию и ресурсы, чтобы несколько недель подряд пытаться анализировать систему и разрабатывать собственные эксплойты «нулевого дня».

В общем виде вектор SL может иметь следующую структуру:

{тип SL; домен; FR: IAC UC SI DC RDF TRE RA}.

Пример вектора потенциальных уровней SL для рабочей станции инженера:

тип SL	домен	IAC (УИА)	UC (КИ)	SI (ЦС)	DC (КД)	RDF (ОПД)	TRE (СО)	RA (РД)
SL-C	рабочая станция инженера	**3**	**0**	**3**	**2**	**2**	**1**	**3**

В табл.2 представлен иллюстративный пример уровней безопасности для фундаментального требования УИА.

Таблица 2 – Уровни безопасности для фундаментального требования УИА.

	Управление идентификацией и аутентификацией (УИА): *идентифицировать и аутентифицировать всех пользователей (людей, программные процессы и устройства) посредством механизмов, которые препятствуют осуществлению:*
SL1	**случайного или непредумышленного доступа** неаутентифицированными субъектами
SL2	**умышленного** неаутентифицированного доступа субъектами **с использованием простых средств**, при **незначительных ресурсах**, **посредственных навыках и низкой мотивации**
SL3	умышленного неаутентифицированного доступа субъектами с использованием **изощренных средств**, при **умеренных ресурсах**, **наличии специальных** познаний в АСУ и **умеренной** мотивации
SL4	умышленного неаутентифицированного доступа субъектами с использованием **изощренных средств**, при **обширных ресурсах**, **наличии специальных** познаний в АСУ и **высокой** мотивации

4 Оценка надежности АСУ с учетом надежности СЗИ

В настоящее время ведутся активные разработки и внедрение средств защиты информации (СЗИ) в АСУ ТП. Это связано в первую очередь с требованиями Приказа ФСТЭК №31 и Федерального закона №187.

Одним из важных вопросов внедрения СЗИ является оценка их влияния на надежность выполнения функций АСУ ТП. На рис.4 представлены варианты и схемы подключения СЗИ к АСУ ТП, предложенные компанией InfoWatch [9].

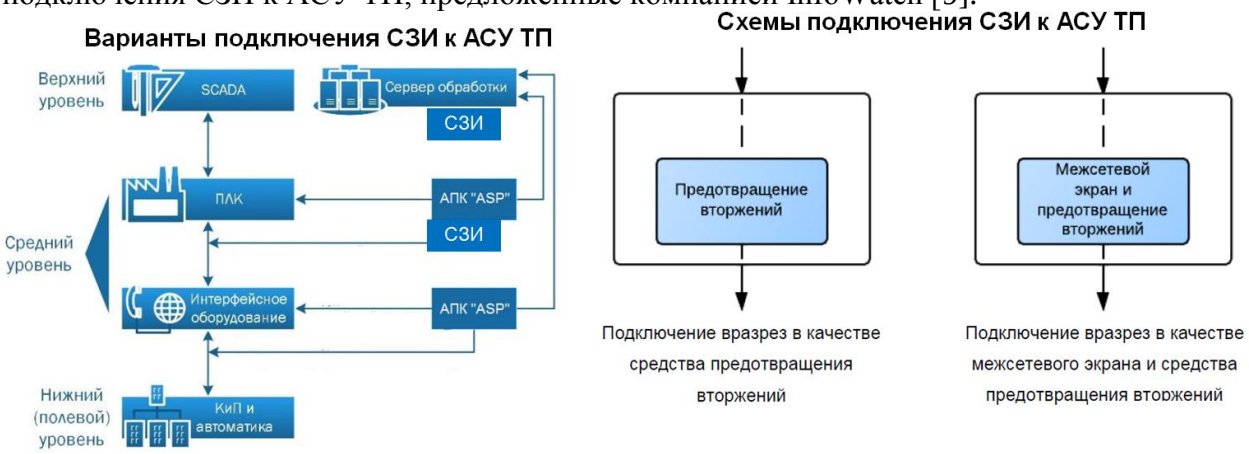

Рисунок 4 – Варианты и схемы подключения СЗИ к АСУ ТП

Как видно из рис.4, СЗИ могут подключаться к разным уровням АСУ ТП – как на верхнем уровне связи АСУ ТП с заводской сетью, так и на уровне связи ПЛК с рабочими станциями и на полевом уровне.

Возможность подключения СЗИ по схеме подключения вразрез требует рассмотрения влияния надежности как аппаратных средств защиты информации, так и алгоритмов выполнения ФБ на надежность АСУ.

Для решения этой задачи предлагается структурно-логическая модель в виде СФЦ, представленная на рис.5.

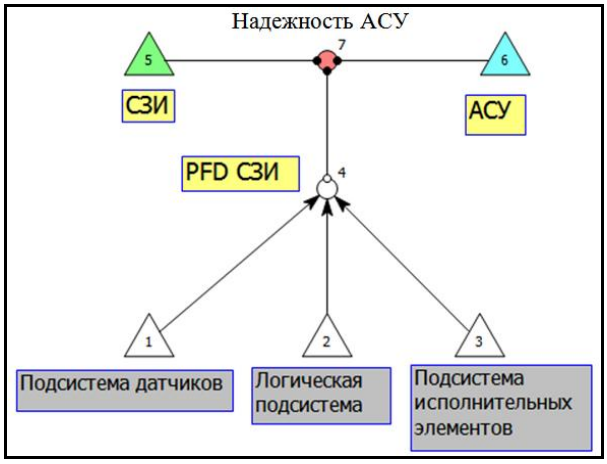

Рисунок 5 – СФЦ для моделирования надежности АСУ с учетом надежности СЗИ

По аналогии с инструментальными средствами безопасности, например, системами противоаварийной защиты (ПАЗ), в реализации алгоритмов информационной защиты могут применяться такие подсистемы, как подсистема датчиков для получения исходной информации для проведения анализа защищенности АСУ, логическая подсистема для принятия решения о возможной атаке (вторжении) и подсистема исполнительных механизмов, которая решает вопросы регистрации и индикации вторжений, формировании сигналов для принятия решения по информационной защите АСУ. Примерами перечисленных выше подсистем являются модули обнаружения и предупреждения вторжений, межэкранные модули и сервер обработки информации АПК «ASAP» компании InfoWatch [9].

На рис.5 фиктивная вершина 7 представляет логическое условие работоспособности АСУ, которое является конъюнкцией (логическим произведением) следующих событий:

1. работоспособности аппаратных средств АСУ (эквивалентированная вершина 6);
2. работоспособности аппаратных СЗИ (эквивалентированная вершина 5);
3. отсутствие отказа на запрос функции безопасности (PFD СЗИ) в случае возникновения угрозы (инверсия относительно фиктивной вершины 4).

Использование эквивавлентированных вершин 1, 2, 3, 5 и 6 вызвано тем, что эти элементы схемы сами могут быть сложными техническими системами и иметь собственную внутреннюю структуру. При необходимости внутренняя структура эквивалентированных вершин может быть конкретизирована.

Например, на рис.6 представлена внутренняя структура подсистемы датчиков, реализующая архитектуру 2oo3, для которой используется β-модель отказа по общей причине, β = 0.05.

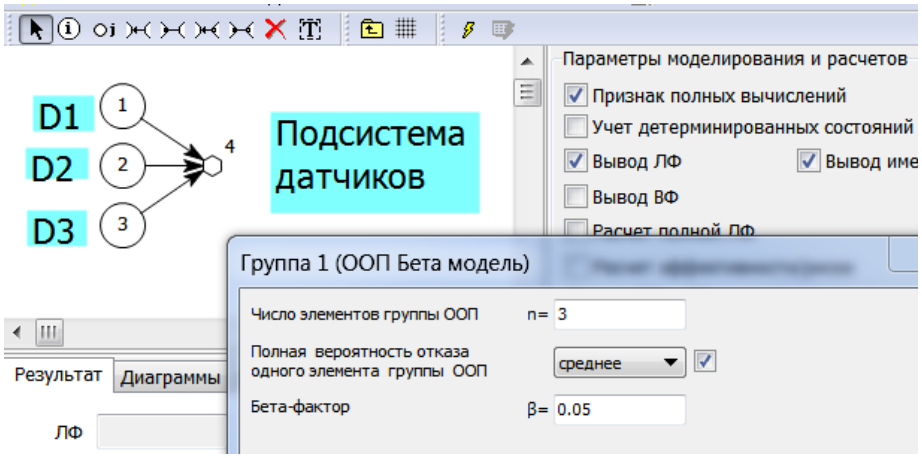

Рисунок 6 – СФЦ внутренней структуры подсистемы датчиков

Пусть для примера вероятность безотказной работы аппаратной части АСУ ТП составляет за некоторый промежуток времени $R_{АСУТП}(t)=0.95$, аппаратной части СЗИ – $R_{СЗИ}(t)=0.99$.

В качестве исходных данных для элементов 1, 2 и 3, реализующих функции безопасности, используем результаты расчетов показателей PFD для датчиков, ПЛК и исполнительных механизмов, выполненных с помощью утилиты (рис.3). Пусть, например, эти показатели будут иметь значения 10E-3, 3E-5 и 2E-4 соответственно.

На рис.7 представлен фрагмент отчета результатов моделирования надежности АСУ относительно критерия *y7*.

Результаты моделирования всей системы

Логический критерий Yc= y7

Логическая функция содержит 1 конъюнкций

№ кон.	Ркон.	Знач.кон по F_V	ЛФ
1	0.94005549	1	Датчики" Логика" ИМ" СЗИ АСУ

P = **0.940055489681** - вероятность реализации критерия

Таблица характеристик элементов

Номер эл-та	P эл-та	Значимость эл-та	Отрицательн. вклад	Положительн. вклад	Наименование
1	5.2706E-5	-0.94011	4.9549E-5	0.94006	Датчики
2	3E-5	-0.94008	2.8203E-5	0.94006	Логика
3	0.00038996	-0.94042	0.00036673	0.94006	ИМ
5	0.99	0.94955	0.94006	0.0094955	СЗИ
6	0.95	0.98953	0.94006	0.049477	АСУ

Рисунок 7 – Фрагмент отчета ПК АРБИТР

На рис.7 отрицательные величины значимостей датчиков, логики и исполнительных механизмов объясняются тем, что для этих элементов для расчета вероятности отказа на запрос формируется схема дерева неисправностей, которая входит в структурную схему надежности АСУ инверсно.

Если, например, безотказность СЗИ будет равна безотказности АСУ, то есть снизится до значения $R_{СЗИ}(t)=0.95$, то надежность всей системы снизится с 0.94 до 0.92.

Схема моделирования, приведенная на рис.5, отражает крайний случай, когда отказ СЗИ приводит к отказу АСУ. Но это не снижает важности учета надежности СЗИ, например, при проектной оценке надежности, когда необходимо подтверждать весьма высокие требования по надежности АСУ ТП, применяемых на опасных производственных объектах.

Литература

1. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУТП // Вопросы кибербезопасности. 2015. №2 (10). С.56-59.
2. ГОСТ Р МЭК 61508-4-2013 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения.
3. ГОСТ Р МЭК 61508-6-2013 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководства по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р 61508-3.
4. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
5. ГОСТ Р 56205-2014 (IES/TS 62443-1-1:2009). Сети коммутационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.
6. Можаева И.А., Струков А.В. Программно-методическое обеспечение проектной оценки показателей функциональной безопасности систем противоаварийной защиты опасных производственных объектов // Сборник трудов XX Всероссийской научно-практической конференции «Актуальные проблемы защиты и безопасности» Том 2, «Технические средства противодействия терроризму», РАРАН-Москва, НПО СМ-СПб., 2017, С.70–83.
7. Можаев А.С. Аннотация программного средства «АРБИТР» (ПК АСМ СЗМА) // Вопросы атомной науки и техники. Серия «Физика ядерных реакторов». Раздел «Аннотации программных средств, аттестованных Ростехнадзором РФ»: науч.-техн. сб.– М.: РНЦ «Курчатовский институт», 2008. – Вып. 2/2008. – С. 105-116.
8. ГОСТ Р МЭК 62443-3-3:2016). Сети промышленной коммутации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности.
9. ПАК Infowatch ASAP. Электронный ресурс https://www.infowatch.ru/products/asap (Дата обращения 04.04.2018).