УДК 004.056
DOI: 10.53403/9785951505460_533

РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ВЕРХНЕГО УРОВНЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ АТОМНОЙ ЭЛЕКТРОСТАНЦИИ

Павлин Артём Юрьевич (niiis@niiis.nnov.ru), Акимов Николай Николаевич

Филиал РФЯЦ-ВНИИЭФ «НИИИС им. Ю. Е. Седакова», г. Нижний Новгород

Работа посвящена описанию модели управления событиями информационной безопасности системы верхнего уровня автоматизированной системы управления технологическими процессами атомной электростанции (СВУ АСУ ТП АЭС). Особое внимание уделяется организации мониторинга событий информационной безопасности СВУ АСУ ТП АЭС. В работе представлена модель управления и алгоритмы работы программной модели событиями информационной безопасности.

Ключевые слова: события информационной безопасности; кибербезопасность; АСУ ТП; система верхнего уровня; АЭС.

DEVELOPMENT OF INFORMATION SECURITY EVENT MANAGEMENT MODEL OF THE UPPER-LEVEL SYSTEMS OF THE AUTOMATED CONTROL SYSTEM FOR TECHNOLOGICAL PROCESSES OF A NUCLEAR POWER PLANTS

Pavlin Artem Yurievich (e-mail: pavlin.artem@mail.ru), Akimov Nikolay Nikolaevich

Branch RFNC-VNIIEF «NIIIS named after Yu. Ye. Sedakov», Nizhny Novgorod, Russia

The work presents information security event management model of the upper-level systems automated process control system for nuclear power plants (ULS APCS NPP). Particular attention is paid to organizing monitoring of ULS APCS NPP information security events. The work presents the information security event management model and algorithms of the software model operation.

Keywords: information security events, cybersecurity, APCS, upper-level system, NPP.

В настоящее время в атомной энергетике предъявляются высокие требования по кибербезопасности систем верхнего уровня (СВУ) автоматизированной системы управления технологическими процессами (АСУ ТП) атомной электростанции (АЭС). Обеспечение кибербезопасности СВУ АСУ ТП АЭС регламентируется обширной международной и национальной (российской) нормативной базой [1, 2]. Основными нормативными документами являются приказы федеральной службы по техническому и экспортному контролю (ФСТЭК) и стандарты международной электротехнической комиссии:

– приказ ФСТЭК России № 31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [1];

– приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию системы безопасности значимых объектов КИИ РФ и обеспечение их функционирования» [2];

– приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ» [3];

– IEC 62645:2019 Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements [4].

– IEC 63096:2020 Nuclear power plants – Instrumentation, control and electrical power systems – Security controls [5].

За последние десятилетия в АСУ ТП атомной энергетики произошло широкое внедрение компьютерных технологий, которое кроме явных преимуществ привело к возникновению ряда проблем, связанных с информационной безопасностью, компьютерной безопасностью, кибербезопасностью. Перед разработчиками систем контроля и управления сложными техноло-

гическими процессами встала задача обеспечить в АСУ ТП возможность своевременного обнаружения событий и инцидентов информационной безопасности (ИБ) и последующее реагирование на них для обеспечения защищенного функционирования этих систем [6–9].

Особое внимание предлагается уделить организации мониторинга событий ИБ СВУ АСУ ТП АЭС.

Для решения задачи организации мониторинга событий ИБ необходимо было разработать:

– модель управления событиями ИБ;

– архитектуру программной модели управления событиями ИБ;

– алгоритмы работы программной модели управления событиями ИБ;

– программную модель управления событиями ИБ.

При формировании программной модели управления событиями ИБ предполагается использование методов структурного анализа сложных технических систем на основе логических правил продукционной модели представления знаний.

На рис. 1 представлена разработанная концептуальная модель управления событиями ИБ.

Концептуальная модель управления событиями ИБ содержит следующие сущности (концепты): событие ИБ, сигнал, инцидент ИБ, способ реагирования.

В рамках данной работы под указанными сущностями подразумевается следующее.

Событие – изменение состояния контролируемого дискретного сигнала, выход за уставки аналогового сигнала, информация о деятельности пользователя (квитирование, управление, снятие блокировки) [6].

Примечание: к событиям относятся команды управления, действия оператора, изменения состояний объектов управления, моменты выхода параметров за допустимые пределы, действия устройств сигнализации, неисправности, действия устройств релейной защиты и автоматики, переключения режимов работы оборудования.

Существует несколько определений для термина событие ИБ.

Событие ИБ – это изменение состояния элементов инфраструктуры, которое может являться причиной возникновения инцидента ИБ [6].

Событие ИБ – выявленное наступление состояния системы, сервисов или вычислительной сети, указывающее на возможное нарушение политики ИБ, на сбой или отсутствие необходимых мер защиты или на прежде неизвестную ситуацию, относящейся к обеспечению безопасности [6].

Сигнал – это оповещение лица принимающего решение (ЛПР) о том, что произошло событие ИБ.

Инцидент ИБ – это событие ИБ или совокупность событий ИБ, приводящих к реализации угрозы ИБ [6].

Среди основных типов событий присутствуют:

– отказ оборудования по любым причинам, как технического, так и программного характера;

– нарушение работы программного обеспечения;

– нарушение любых правил обработки, хранения, передачи информации, как электронной, так и документов;

– неавторизированный или несанкционированный доступ третьих лиц к информационным ресурсам;

– выявление вирусов или других вредоносных программ;

– любая компрометация системы, например, попадание пароля от учетной записи в открытый доступ.

Все эти события должны быть классифицированы, описаны и внесены во внутренние документы, регламентирующие порядок обеспечения ИБ. Следует учитывать, что существенная часть инцидентов малозаметны, они происходят вне периметра внимания должностных лиц. Такие события должны быть описаны особо, и определены меры для их выявления в режиме постфактум.

Предполагая, что инцидентом является недозволенное, несанкционированное событие, в работе нужно опираться на механизм, разделяющий события и действия на разрешенные и запрещенные. Кроме того, регламент определяет методы и способы классификаций событий, прямо не обозначенных в документах в качестве значимых, и механизм выявления таких событий, их описания и последующего внесения в регламентирующие документы.

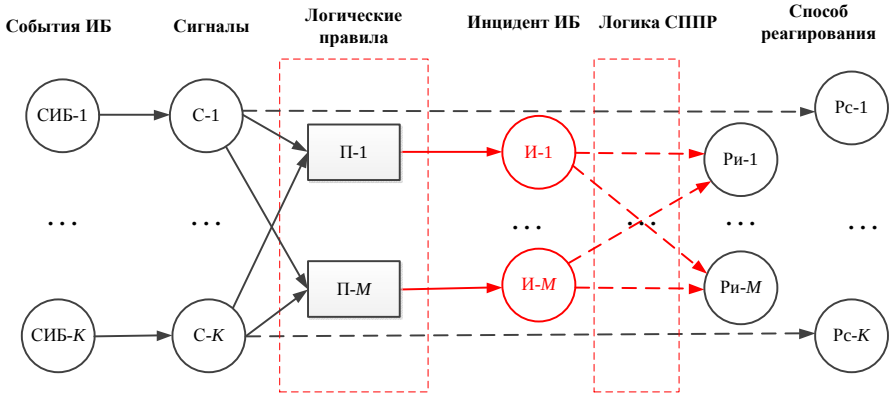


Рис. 1. Концептуальная модель управления событиями ИБ

Управление инцидентами ИБ основано на следующих действиях:

– определение;
– оповещение о возникновении;
– регистрация;
– меры реагирования на инциденты;
– устранение причин и последствий;
– расследование;
– реализация превентивных мер;
– аналитика.

Способ реагирования – это задокументированная политика, процедура, инструкция или сценарий реагирования, по которым ЛПР будет принимать решение в случае возникновения события ИБ или инцидента ИБ.

Для работы программной модели управления событиями ИБ были разработаны следующие алгоритмы:

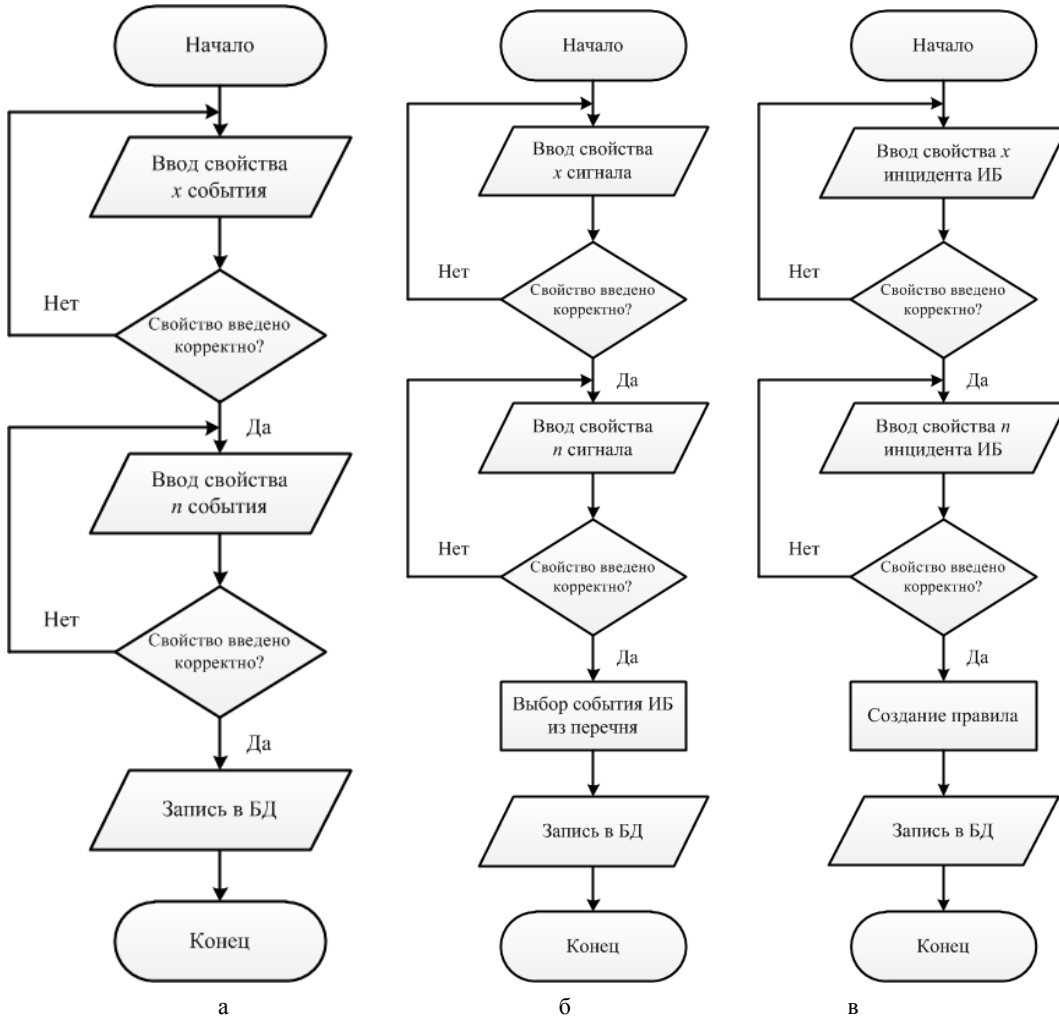
– алгоритм создания перечня событий ИБ, рис. 2,а;
– алгоритм ввода перечня сигналов, рис. 2,б;
– алгоритм ввода перечня инцидентов ИБ, рис. 2,в;
– алгоритм ввода правил «если-то» реагирования на события информационной безопасности, рис. 3;
– алгоритм создания перечня способов реагирования на событие информационной безопасности, рис. 4;
– алгоритм трассировки принятого решения по способу реагирования на событие ИБ, рис. 5.

Проектирование программной модели управления событиями ИБ разделено на 3 этапа:

– разработка вариантов использования программной модели;
– разработка экранных форм программной модели;
– разработка архитектуры программной модели управления событиями ИБ.

В рамках разработки вариантов использования программной модели разработаны следующие сценарии:

– сценарий создания перечня событий ИБ;
– сценарий создания перечня сигналов;
– сценарий создания перечня инцидентов ИБ;
– сценарий создания логических правил;
– сценарий создания способов реагирования на событие ИБ;
– сценария трассировки принятого решения по способу реагирования на событие ИБ.



а б в

Рис. 2. Алгоритмы создания перечней событий, сигналов и инцидентов ИБ: а – создание перечня событий, б – ввод перечня сигналов, в – ввод перечня инцидентов

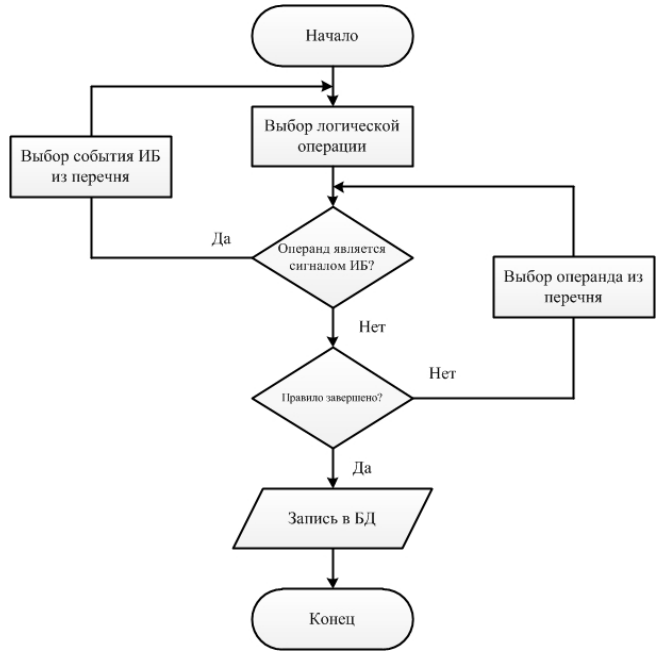


Рис. 3. Алгоритм ввода правил «если-то» реагирования на события ИБ

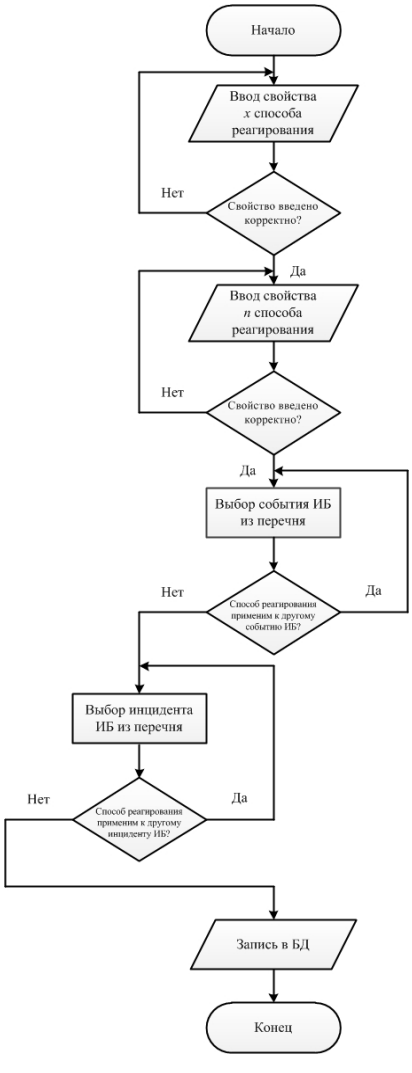


Рис. 4. Алгоритм создания перечня способов реагирования на событие ИБ

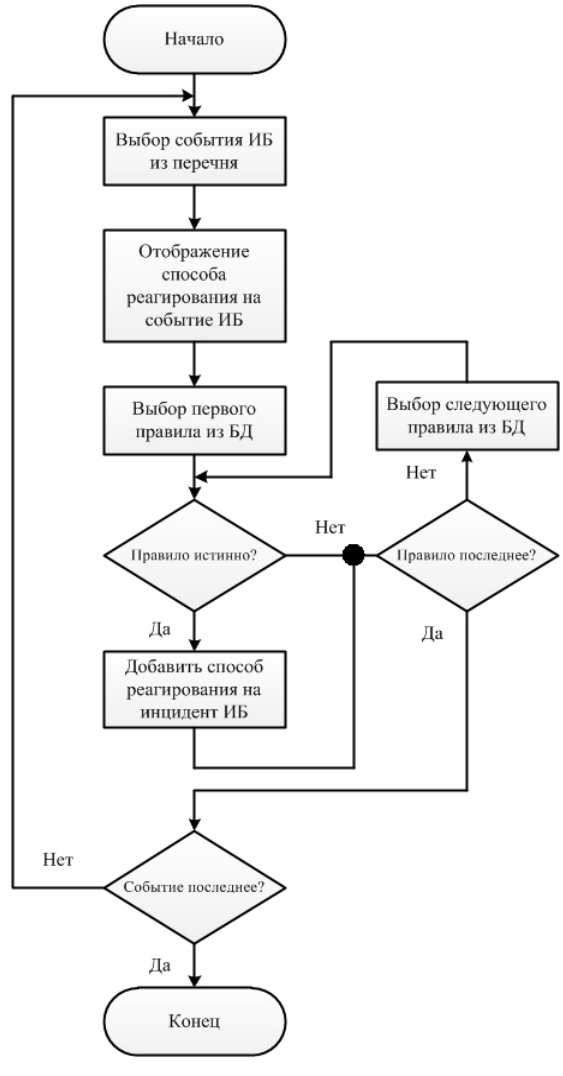


Рис. 5. Алгоритм трассировки принятого решения по способу реагирования на событие ИБ

В рамках разработки экранных форм программной модели разработаны следующие формы:

– экранная форма основного окна;

– экранная форма для ввода перечня событий ИБ;

– экранная форма для ввода перечня сигналов;

– экранная форма для ввода перечня инцидентов ИБ;

– экранная форма для ввода правил «если-то» реагирования на события ИБ;

– экранная форма для ввода способов реагирования на событие ИБ;

– экранная форма для трассировки принятого решения по способу реагирования на событие ИБ.

Архитектура программной модели управления событиями ИБ представляет собой модель, предполагающую наличие трех типов уровней (слоев):

– слой представления (графический интерфейс пользователя);

– слой логики (обработка сигналов, событий ИБ, инцидентов ИБ, способов реагирования и логических правил);

– слой данных (база данных и хранилище данных).

Архитектура программной модели управления событиями ИБ представлена на рис. 6.

Слой представления – это интерфейсный компонент, предоставляемый конечному пользователю. Этот уровень не имеет прямых связей с базой данных, не нагружен основной логикой и хранит состояние программы.

Слой логики (средний слой, связующий слой) располагается на втором уровне, на нём сосредоточена большая часть логики программы. Вне его остаются только фрагменты, экспортируемые на слой представления, а также элементы логики, погруженные в базу данных (хранимые процедуры и правила).

Рис. 6. Архитектура программной модели управления событиями ИБ

Слой данных обеспечивает хранение данных и выносится на отдельный уровень, реализуется, как правило, средствами систем управления базами данных, подключение к этому компоненту обеспечивается только со второго уровня.

В рамках разрабатываемой конфигурации программной модели управления событиями ИБ все компоненты совмещены на одном вычислительном узле.

Модель управления событиями ИБ в дальнейшем планируется применять при разработке системы контроля событий ИБ, которая впоследствии найдет свое применение на АЭС в составе поставляемого АСУ ТП.

В результате предложена модель управления событиями ИБ, разработаны алгоритмы работы программной модели событий ИБ, выполнено проектирование программной модели и определены пути дальнейшего развития в обеспечении ИБ СВУ АСУ ТП АЭС. Программная реализация модели управления событиями ИБ в виде информационной системы контроля событий ИБ СВУ АСУ ТП АЭС – это значительный вклад в обеспечении защищенности АСУ ТП АЭС.

Список литературы

1. Приказ ФСТЭК России № 31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

2. Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию системы безопасности значимых объектов КИИ РФ и обеспечение их функционирования».

3. Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ».

4. IEC 62645:2019 Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements.

5. IEC 63096:2020 Nuclear power plants – Instrumentation, control and electrical power systems – Security controls.

6. Безкоровайный М. М., Лосев С. А., Татузов А. Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. 2011. № 6. С. 27–33.

7. Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук. Концепция нового поколения систем верхнего уровня АСУ ТП АЭС. Полетыкин А. Г., Жарко Е. Ф., Менгазетдинов Н. Э., Промыслов В. Г. Москва 2017 г. [Электронный ресурс] Режим доступа: http://nics.sicpro.org/doc/conception.pdf.

8. Казарин О. В., Тарасов А. А. Современные концепции кибербезопасности ведущих зарубежных государств // Вестник Российского государственного гуманитарного университета. 2013. № 14. С. 58–74.

9. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Современные методы обеспечения безопасности в атомной энергетике. Монография под редакцией Астайкина А. И. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014.