УДК 681.3

Б.М. ГЕРАСИМОВ, П.В. ХУСАИНОВ

Военный институт телекоммуникаций и информатизации Национального технического университета «Киевский политехнический институт», Украина

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ПРИ ЦЕНТРАЛИЗОВАННОЙ ОБРАБОТКЕ СОБЫТИЙ

В статье рассматривается актуальная научно-практическая задача повышения эффективности работы оператора системы централизованной обработки событий – администратора безопасности – в процессе управления инцидентами и подход к её решению за счет информационной поддержки оператора.

инцидент безопасности, информационная поддержка, принятие решений, эргономика

Обеспечение безопасности бизнес-процессов, автоматизированных функций управления, реализуемых с применением современных информационных технологий и *Internet*, требует внедрения процесса оценки влияния текущего состояния информационной системы (ИС) на ведение бизнеса. Сложность технической реализации систем защиты обуславливает участие человека с целью устранения неопределенности и принятия качественного решения по оценке текущего состояния безопасности ИС для бизнес-процессов на основе интеллектуальных способностей, опыта, субъективных представлений. Участие человека связано со значительными временными задержками на информационную подготовку решений, что обуславливает необходимость решения актуальной научно-практической задачи автоматизации информационной подготовки принятия решений в рассматриваемой предметной области.

Комплексный подход к обеспечению безопасности ИС рассматривается в рамках системы управления информационной безопасностью (СУИБ), определяемой стандартом *ISO/IEC 27001:2005 Information security management system. Requirements*. Описываемый стандартом процессный подход (рис. 1) выделяет прагматически важную задачу определения влияния состояния ИС на безопасность бизнес-процессов организации в отдельный компонент СУИБ – управление инцидентами. В соответствии с тематикой проводимых исследований, безопасность бизнес-процессов обеспечивается безопасным состоянием используемых информационных активов или соблюдением следующих свойств: конфиденциальность, целостность, доступность. Инцидент ин-

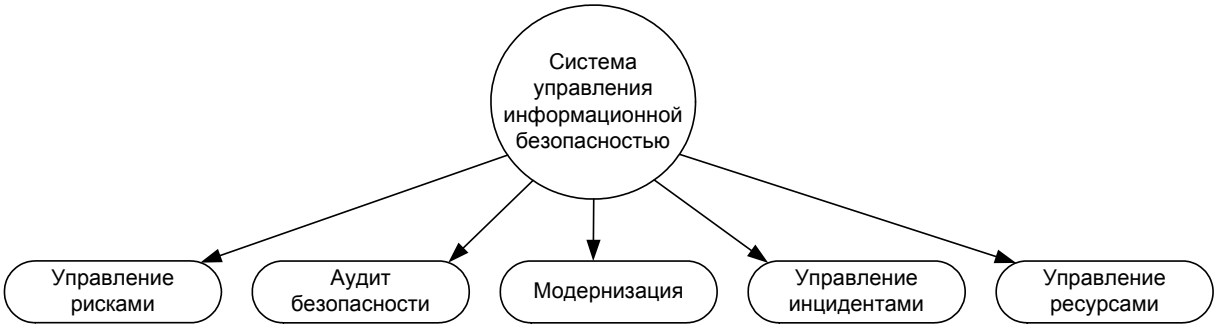

Рис. 1. Компоненты системы управления информационной безопасностью

формационной безопасности – единичное событие или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации информации и угрозы информационной безопасности. Событие информационной безопасности – идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности.

Управление инцидентами рассматривается стандартом *ISO/IEC TR 18044 Information security incident management*. Обработка и анализ событий безопасности с целью обнаружения и идентификации инцидентов безопасности бизнес-процессов обеспечивается организацией в СУИБ процесса реагирования на инциденты. Он включает: обнаружение и идентификацию инцидента; предварительный анализ инцидента; начальное реагирование на инцидент; реагирование на инцидент. Решение частных задач этапов реагирования на инциденты составляет процесс принятия решения по факту инцидента безопасности бизнес-процесса.

Организационной основой управления инцидентами является группа по расследованию инцидентов организации, технологической – система централизованной обработки событий (ЦОС) (рис. 2). Система ЦОС позволяет собирать и анализировать сообщения о событиях безопасности, поступающих от систем обнаружения вторжений, межсетевых экранов, операционных систем, приложений, антивирусных программ и др. [1]. Данная информация собирается в едином центре, обрабатывается и подвергается анализу в соответствии с заданными правилами по обработке событий, связанных с безопасностью. Результаты анализа в удобном виде предоставляются лицу, принимающему решение (ЛПР) по факту обнаружения инцидента безопасности.

Математическое обеспечения ЦОС включает методы и алгоритмы: нормализации, агрегирования, корреляции, визуализации (рис. 3). Нормализация – удаление избыточной информации, приведение регистрационных данных к единому виду и времени. Рассматривая процесс нормализации данных, отдельное направление посвящено исследованию методов и алгоритмов фильтрации, т.е. выделения из хранилищ данных событий по некоторому шаблону. Агрегирование подразумевает группирование однотипных событий, что немаловажно, учитывая особенности реализации сетевых вторжений. Корреляция – установление зависимости между частными событиями безопасности с целью обнаружения и идентификации инцидентов безопасности. С использованием методов и алгоритмов визуализации осуществляется отображение текущей информации ЛПР с учётом требований эргономики и обеспечения качества принимаемых решений. Важным вопросом визуализации является определение последовательности выдачи информации о событиях

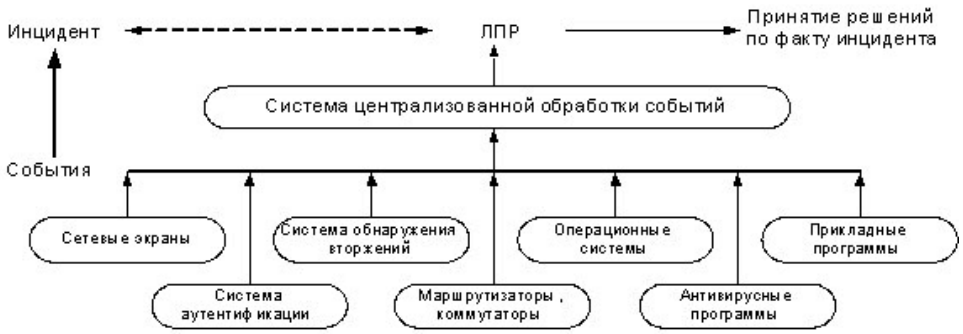

Рис. 2. Обобщенная схема реагирования на инциденты

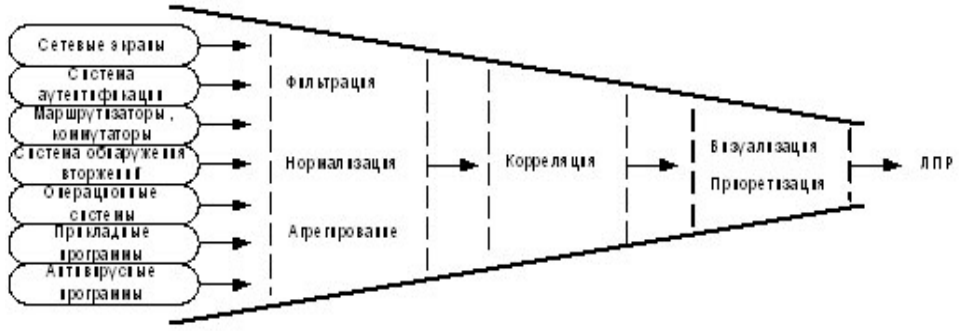

Рис. 3. Состав математического обеспечения ЦОС

безопасности с учётом её важности для реагирования на инциденты и повышения величины предотвращенного ущерба.

Обеспечение правильности и своевременности решений ЛПР из состава группы расследования инцидентов требует разработки соответствующих алгоритмов математического обеспечения ЦОС и заключается в автоматизации функций информационной поддержки: идентификации событий и инцидентов безопасности; формирования и корректировки информационной модели; синтеза плана разрешения ситуаций [2].

В процессе реагирования на инциденты безопасности возникают задачи различной интенсивности, которые определяют содержание деятельности администратора безопасности и его загруженность. В этих условиях организация взаимодействия осуществляется путем выбора оптимальной структуры информационной модели, временных параметров визуализации инцидентов безопасности. Особенности решения задач обнаружения и идентификации инцидентов, эргономические и временные требования к деятельности оператора обуславливают выбор формулярного способа отображения [3].

При разработке методик, алгоритмов визуализации, проектировании пользовательского интерфейса ЛПР, в части касающейся отображения текущей информации обнаружения и идентификации инцидентов безопасности, следует придерживаться следующих требований:

– состав отображаемой информации должен определяться согласно структуре алгоритмов задач обнаружения и идентификации инцидентов безопасности;

– объем предоставляемой информации должен соответствовать пропускной способности ЛПР;

– соответствие количества типов формуляров возможностям долговременной памяти человека;

– соответствие количества информационных элементов на одновременно анализируемом участке области отображения не должно превышать возможностей кратковременной памяти оператора;

– компоновка формуляров безопасности должна производиться с учётом логической связности в алгоритме выполнения задачи;

– обеспечение стандартного вида формуляров безопасности.

Предложенные алгоритмы являются основой работы функциональных блоков системы информационной поддержки оператора (рис. 4) и являются частью математического обеспечения ЦОС.

Блок визуализации и комментария предназначен для отображения текущей информации о событиях безопасности в информационной системе согласно структуры информационной модели и плана отображения информации. Блок синтеза плана предоставляет рациональную последовательность отображения информации о текущих событиях безопасности. Блок логического вывода осуществляет идентификацию событий и инцидентов безопасности пу-

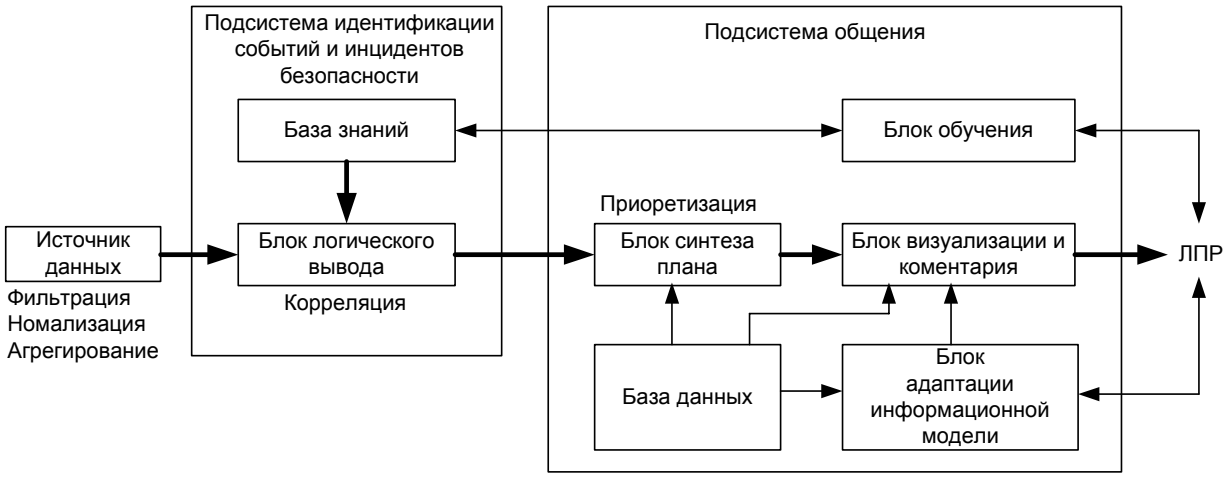

Рис. 4. Структурная схема системы информационной поддержки в составе ЦОС

тем корреляции предоставляемых источником данных информации о частных событиях. Блок адаптации информационной модели предназначен для выполнения совокупности операций связанных с определением (изменением) структуры информационной модели, введения соответствующего диалога с пользователем. С использованием блока обучения осуществляется формирование, ввод и корректировка содержимого базы знаний. База знаний содержит описания распознаваемых ситуаций (событий, инцидентов безопасности) на основе экспертной информации. База данных предназначена для хранения необходимых данных при функционировании системы информационной поддержки: временные характеристики и важность ситуаций; структуру и состав информационной модели; комментарий и др.

Создание системы информационной поддержки требует решения ряда частных научных задач, постановки которых, заключаются в разработке методик и алгоритмов для определения:

– оптимального состава и объема отображаемой информации об инциденте безопасности;

– структуры формуляров безопасности;

– приоритетного отображения информации об инцидентах безопасности;

– текущих событий безопасности для отображения в составе информационной модели.

Предварительный анализ показал повышение вероятности своевременного и правильного принятия решений в задачах обнаружения и идентификации инцидентов безопасности с участием оперативного состава системы защиты информационной системы.

Литература

1. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети: анализ технологий и синтез решений. – М.: ДМК-Пресс, 2004. – 616 с.

2. Герасимов Б.М., Дивизинюк М.М., Субач И.Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. – Севастополь.: СНИЯЭиП, 2004. – 319 с.

3. Герасимов Б.М., Тарасов В.А., Токарев И.В. Человеко-машинные системы принятия решений с элементами искусственного интеллекта. – К.: Наук. думка, 1993. – 184 с.

Поступила в редакцию 12.01.2007

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.