УДК 004.58
DOI 10.21685/2587-7704-2018-3-2-10

Open Access | RESEARCH ARTICLE

Среда тестирования обработки инцидентов информационной безопасности

А. Ю. Щербакова
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В статье рассматривается среда тестирования обработки инцидентов информационной безопасности, разрабатываемая с помощью средств виртуализации для использования в учебном процессе при подготовке специалистов по защите информации. Приводятся основные цели создания, этапы разработки среды тестирования обработки инцидентов информационной безопасности и возможные типы заданий, выполняемых с ее помощью.

Ключевые слова: событие информационной безопасности, инцидент информационной безопасности, обработка инцидентов информационной безопасности, система тестирования, виртуализация.

Testing environment for information security incident handling

A. Yu. Shcherbakova
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article discusses testing environment for information security incident handling developed using virtualization tools for educational process in training information security specialists. There are main objectives of the creation, development stages of testing environment for information security incident handling, and possible types of tasks performed with its help.

Keywords: information security event, information security incident, information security incident handling, testing system, virtualization.

Частота появления и количество инцидентов, связанных с информационной безопасностью (ИБ), – один из наглядных показателей того, правильно ли функционирует система ее управления. Реагирование на инциденты информационной безопасности и их расследование является неотъемлемой частью обеспечения информационной безопасности. Именно во время расследования и реагирования на инцидент проявляются уязвимости информационной системы, обнаруживаются признаки атак и вторжений, проверяется работа защитных механизмов, качество архитектуры системы ИБ и управления ею.

Инцидент информационной безопасности – одно или серия нежелательных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операций и угрожают информационной безопасности [1]. В [2] особое внимание обращается на необходимость создания процедуры управления инцидентами информационной безопасности: очевидно, что без своевременной реакции на инциденты безопасности и устранения их последствий невозможно эффективное функционирование системы управления информационной безопасностью.

Немаловажной задачей при подготовке специалистов по защите информации является формирование профессиональных навыков, выражающихся в готовности к совершенствованию информационной безопасности организации посредством осуществления мониторинга событий ИБ в информационной системе, а также управлению инцидентами ИБ. Для выработки таких навыков в рамках

практических занятий по дисциплинам «Управление инцидентами информационной безопасности защищенных автоматизированных систем» специальности 10.05.03 «Информационная безопасность автоматизированных систем» и «Управление инцидентами информационной безопасности телекоммуникационных систем» специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» может быть использована среда тестирования обработки инцидентов ИБ.

Под средой тестирования понимается информационная система, построенная в среде виртуализации, которая воспроизводит структуру и поведение реальной системы объекта и позволяет выполнять в ней следующее:

– операции, связанные с деятельностью определенного объекта;

– действия по реализации инцидентов ИБ;

– обнаружение событий и потенциальных инцидентов ИБ;

– процедуры обработки инцидентов ИБ.

Под операциями, связанными с деятельностью объекта, подразумеваются действия с активами объекта, направленные на достижение его бизнес-целей. В качестве объекта может быть рассмотрена организация или ее часть, использующая автоматизированную систему для реализации бизнес-процессов. Для выполнения таких операций в среде тестирования должны быть установлены, например, офисный пакет программ, включающий текстовый редактор и табличный процессор, графические приложения и др.

Действия по реализации инцидентов ИБ – действия в соответствии с определенными сценариями инцидентов ИБ [3]. Это операции, которые приводят к нежелательным для объекта последствиям, компрометации бизнес-процессов, прерыванию деятельности. В среде тестирования должна быть обеспечена возможность реализации сценариев инцидентов ИБ, например, установлены приложения с известными уязвимостями, программные средства удаленного доступа, допущены ошибки в настройке средств защиты от несанкционированного доступа и несоответствующего использования и др.

Обнаружение событий ИБ и потенциальных инцидентов ИБ возможно при наличии в среде тестирования специализированных программных средств, позволяющих детектировать отклонения от нормальной работы системы, например системы обнаружения вторжений, антивирусного программного обеспечения, межсетевого экрана, средств защиты от несанкционированного доступа и др. Должны быть детектируемыми ошибки установленных прикладных программных средств, изменения настроек безопасности, данных учетных записей пользователей.

Выполнение действий, связанных с обработкой инцидентов ИБ, представляет собой реагирование на инциденты – обнаружение события ИБ и оповещение о нем уполномоченных лиц, анализ события, идентификация его как инцидента ИБ, сдерживание, устранение инцидента ИБ и восстановление системы после него или принятие «антикризисных» мер в соответствии с [1]. Последовательность данных процедур приведена на рис. 1.

Для реализации процедур обработки инцидентов в среде тестирования должны быть предусмотрены средства администрирования системы, инструменты для расследования инцидентов ИБ [4], обеспечен доступ к системным настройкам, журналам, резервным копиям операционных систем, программ и файлов.

Разработка и создание среды тестирования обработки инцидентов ИБ состоит из следующих процессов:

– планирование информационной системы, состава компонентов для определенного объекта, выбор программного обеспечения, устанавливаемого на компоненты системы;

– выбор среды виртуализации и создание виртуальной автоматизированной системы, установка операционных систем и программного обеспечения на узлы виртуальной системы;

– разработка и подготовка сценариев инцидентов ИБ, установка инструментальных средств для их реализации;

– разработка руководства пользователя по использованию среды тестирования обработки инцидентов ИБ.

Среда тестирования обработки инцидентов ИБ позволяет выполнять задания, связанные с выработкой практических навыков по реагированию на инциденты информационной безопасности, применению инструментальных средств обработки инцидентов ИБ, оповещению о событиях ИБ, оформлению документации, связанной с инцидентами ИБ, идентификации уязвимостей системы и недостатков в стратегиях обработки инцидентов, оценке информационной безопасности объекта, разработке предложений по совершенствованию системы управления ИБ и системы управления инцидентами ИБ объекта [5].

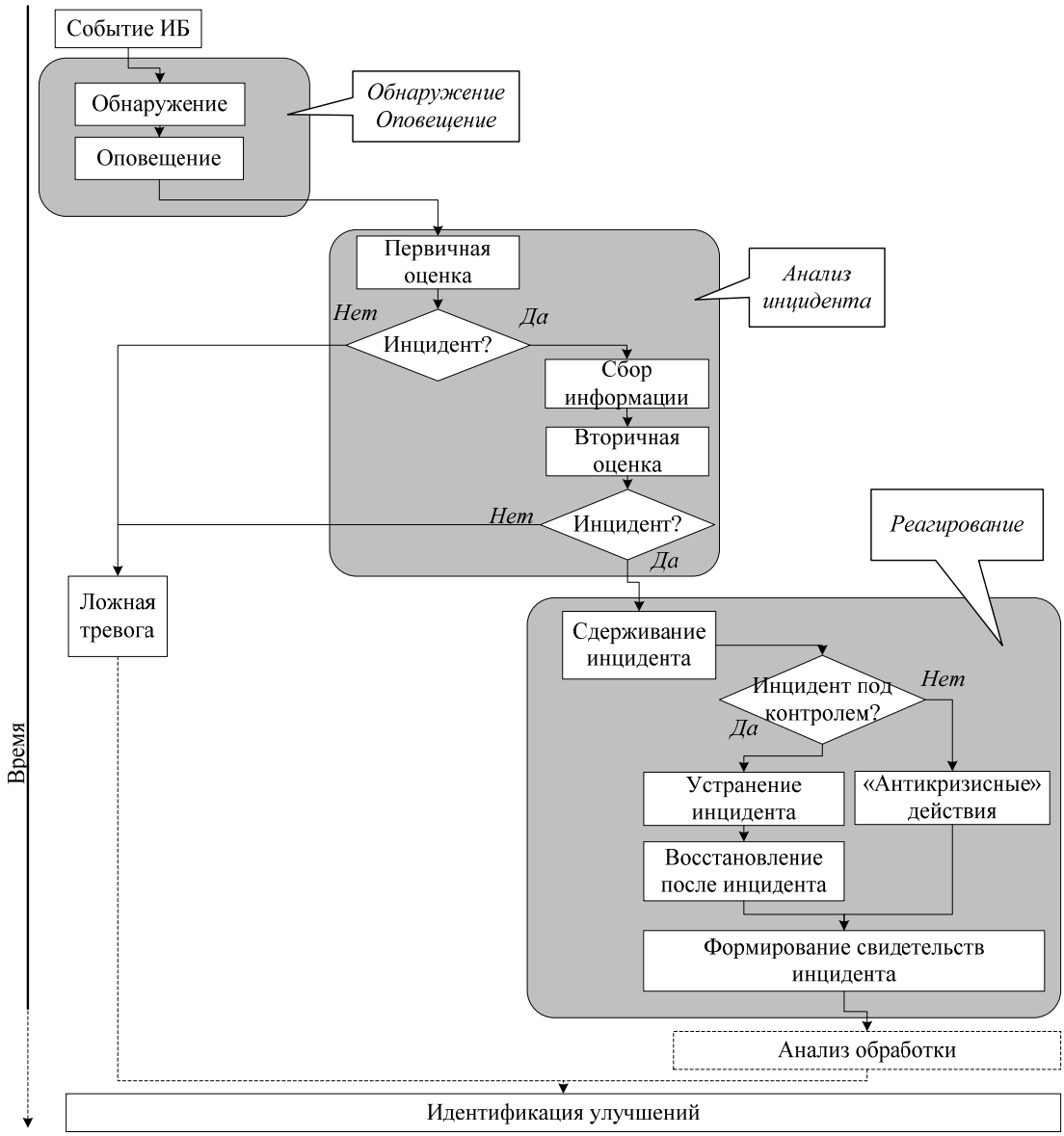

Рис. 1. Последовательность процедур обработки инцидентов ИБ

Практические занятия с использованием среды тестирования могут быть реализованы в виде деловой игры, в рамках которой формируются навыки по организации работы малых коллективов исполнителей, принятию управленческих решений в сфере профессиональной деятельности. Задания, выполняемые в среде тестирования, могут быть, например, следующими:

– идентифицировать события ИБ, произошедшие в системе определенного объекта, заполнить форму «Отчет о событии ИБ» [1];

– провести анализ отчета о событии ИБ, собрать дополнительную информацию о событии ИБ, в случае идентификации инцидента ИБ заполнить форму «Отчет об инциденте ИБ» [1];

– идентифицировать инцидент ИБ в автоматизированной системе объекта, оценить возможные последствия, произвести выбор стратегии по обработке инцидента ИБ;

– идентифицировать инцидент ИБ в автоматизированной системе объекта, произвести выбор и реализацию стратегии по обработке инцидента ИБ, завершить заполнение формы «Отчет об инциденте ИБ»;

– в рамках деловой игры сформировать группу реагирования на инциденты ИБ [1], произвести обработку идентифицированных инцидентов ИБ и др.

Ввиду доступности и широкого применения средств виртуализации, создание среды тестирования обработки инцидентов ИБ является выполнимой в рамках реализации образовательной программы задачей. На базе созданной виртуальной автоматизированной системы возможно выполнение процедур по управлению ИБ объектов, принятие управленческих и проектных решений, тестирова-

ние средств защиты информации, исследование влияния человеческого фактора на работоспособность систем и других. Таким образом, среда тестирования обработки инцидентов ИБ является функциональным средством для формирования навыков, необходимых будущим специалистам по защите информации в профессиональной деятельности.

Библиографический список

1. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
2. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы обеспечения информации. Системы менеджмента информационной безопасности. Требования.
3. Зефиров, С. Л. Оценка инцидентов информационной безопасности / С. Л. Зефиров, А. Ю. Щербакова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 2 (32). – С. 77–81.
4. 23 бесплатных инструмента расследования инцидентов для специалиста по информационной безопасности // habr. – 2006–2018 «TM». 15.11.2016. – URL: https://habr.com/company/hosting-cafe/blog/315278/ (дата обращения: 14.10.2018).
5. Зефиров, С. Л. Инциденты информационной безопасности. Совершенствование защитных мер / С. Л. Зефиров, А. Ю. Щербакова // Информационные технологии в науке и образовании. Проблемы и перспективы : сб. науч. ст. IV ежегод. межвуз. науч.-практ. конф. / под ред. Л. Р. Фионовой. – Пенза : Изд-во ПГУ, 2017. – С. 247–248.

Щербакова, А. Ю.

Среда тестирования обработки инцидентов информационной безопасности / А. Ю. Щербакова // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-10.