ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

КНИГА 3

Н. Г. Милославская,
М. Ю. Сенаторов, А. И. Толстой

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 – «Информационная безопасность» (уровень – магистр)

2-е издание, исправленное

Москва
Горячая линия - Телеком
2014

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
М60

Рецензенты: кафедра защиты информации НИЯУ МИФИ (зав. кафедрой кандидат техн. наук, профессор *А. А. Малюк*); академик РАН *И. А. Соколов*; доктор техн. наук, профессор *П. Д. Зегжда*; доктор техн. наук, профессор *А. Г. Остапенко*

Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.

М60 Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия–Телеком, 2014. – 170 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 3»

ISBN 978-5-9912-0363-0.

В учебном пособии изучается процесс управления инцидентами информационной безопасности (ИБ), для чего вводятся понятия события и инцидента ИБ и выделяются цели и задачи управления инцидентами ИБ. Описывается система управления инцидентами ИБ. Анализируются этапы процесса управления инцидентами ИБ. Исследуются подпроцессы обнаружения событий и инцидентов ИБ и оповещения о них; обработка событий и инцидентов ИБ, включая первую оценку и предварительное решение по событию ИБ и вторую оценку и подтверждение инцидента ИБ; реагирования на инциденты ИБ. Описывается документация системы управления инцидентами ИБ, включая политику и программу. Анализируется деятельность группы реагирования на инциденты ИБ. Значительное внимание уделяется сохранению доказательств инцидента ИБ. Далее вводятся определения непрерывности бизнеса, управления ею и системы управления непрерывностью бизнеса (УНБ). Рассматривается применение цикла PDCA к этой системе управления. Детально описывается жизненный цикл УНБ. Определяется состав документации в области непрерывности бизнеса, в частности, политика УНБ и планы управления инцидентом, обеспечения непрерывности и восстановления бизнеса. Анализируются готовность информационных и телекоммуникационных технологий (ИТТ) к обеспечению непрерывности бизнеса (ОНБ) и интеграция процессов готовности ИТТ и ОНБ в рамках цикла PDCA.

Для студентов высших учебных заведений, обучающихся по программам магистратуры направления 090900 – «Информационная безопасность», будет полезно слушателям курсов переподготовки и повышения квалификации и специалистам.

ББК 32.973.2-018.2я73

ISBN 978-5-9912-0363-0

ПРЕДИСЛОВИЕ

Учебное пособие «Управление инцидентами информационной безопасности и непрерывностью бизнеса» является третьей частью серии учебных пособий «Вопросы управления информационной безопасностью».

При подготовке данного учебного пособия были поставлены следующие задачи:

1) описать процесс управления инцидентами информационной безопасности (ИБ);

2) определить особенности системы управления инцидентами ИБ и рассмотреть ее основные характеристики;

3) дать основные определения, относящиеся к проблеме обеспечения непрерывности бизнеса (ОНБ);

4) рассмотреть основные аспекты управления непрерывностью бизнеса (УНБ).

Исходя из поставленных задач, была определена структура учебного пособия «Управление инцидентами информационной безопасности и непрерывностью бизнеса», которое состоит из введения, трех глав, заключения, приложения и списка литературы из 30 наименований.

Во введении обоснована актуальность темы учебного пособия.

В первой главе кратко анализируется нормативное обеспечение вопросов управления инцидентами ИБ и ОНБ.

Во второй главе изучается процесс управления инцидентами ИБ, для чего вводятся понятия события и инцидента ИБ и выделяются цели и задачи управления инцидентами ИБ. Описывается система управления инцидентами ИБ. Анализируются этапы процесса управления инцидентами ИБ, разбиваемого на планирование и подготовку, использование, анализ и улучшение. Отдельно исследуются подпроцессы обнаружения событий и инцидентов ИБ и оповещения о них, а также обработка событий и инцидентов ИБ, включая первую оценку и предварительное решение по событию ИБ и вторую оценку и подтверждение инцидента ИБ. Детально исследуется подпроцесс реагирования на инциденты ИБ и его составляющие: немедленное реагирование, контроль, последующее реагирование, антикризисные действия, правовая экспертиза, передача информации, расширение области принятия решений, регистрация деятельности и контроль за внесением изменений и техническая поддержка реагирования на инциденты ИБ. Описывается документация системы управления инцидентами ИБ, включая политику и программу. Анализируется деятельность группы реагирования на инциденты ИБ. Подчеркивается необходимость обеспечения осведомленности и обучения в области инцидентов ИБ. Значительное внимание уделяется сохранению

доказательств инцидента ИБ и кратко определяются функции инструментальных средств управления событиями ИБ.

В третьей главе вводятся определения, относящиеся к ОНБ, управления ею и системы УНБ. Рассматривается применение циклической модели улучшения процессов PDCA (от англ. *Plan-Do-Check-Act* – планируй–выполняй–проверяй–действуй) к этой системе управления (сама модель описана в первой части серии учебных пособий). Детально описывается жизненный цикл УНБ, включающий шесть элементов: управление программой УНБ, анализ непрерывности бизнеса (НБ) организации, определение стратегии УНБ, разработка и внедрение в УНБ ответных мер на инциденты, меры по применению, поддержке и анализу УНБ и внедрение УНБ в культуру организации. Определяется состав документации в области НБ, в частности, политика УНБ и планы управления инцидентом, обеспечения непрерывности и восстановления бизнеса. Анализируются готовность информационных и телекоммуникационных технологий (ИТТ) к ОНБ и интеграция процессов готовности ИТТ и ОНБ в рамках цикла PDCA.

В заключении кратко выделяется взаимосвязь изученных понятий, относящихся к управлению инцидентами ИБ и НБ, а также устанавливается связь между материалом учебного пособия и составляющими профессиональных компетенций.

В приложении приводится информация справочного характера в виде примеров инструментальных средств управления событиями ИБ.

Освоение материалов данного учебного пособия лежит в основе формирования у обучающихся следующих профессиональных компетенций:

- способность участвовать в управлении ИБ объекта (в части управления инцидентами ИБ и НБ);
- способность участвовать в проектировании и разработке системы управления ИБ (СУИБ) объекта (в отношении подсистем управления инцидентами ИБ и НБ);
- способность участвовать в проведении контрольных мероприятий по определению эффективности и результативности СУИБ объекта (в части эффективности и результативности управления инцидентами ИБ и НБ).

Эти профессиональные компетенции необходимы для решения задач, относящихся к таким видам профессиональной деятельности в сфере управления ИБ, как проектная и организационно-управленческая.

После изучения учебного пособия «Управление инцидентами информационной безопасности и непрерывностью бизнеса» обучающиеся будут:

Знать:

- принципы построения СУИБ объекта в части систем управления инцидентами ИБ и НБ;

- современные подходы к управлению инцидентами ИБ и НБ объекта и направления их развития;
- особенности отдельных процессов управления инцидентами ИБ в рамках СУИБ и УНБ;
- основные международные и российские стандарты, регламентирующие управление инцидентами ИБ и НБ;
- принципы разработки процессов управления инцидентами ИБ и НБ;
- принципы создания основных документов, регламентирующих вопросы управления инцидентами ИБ и НБ.

Уметь:

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления инцидентами ИБ и НБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления инцидентами ИБ и НБ;
- применять процессный подход к управлению инцидентами ИБ и НБ;
- используя современные методы и средства, разрабатывать процессы управления инцидентами ИБ и НБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления инцидентами ИБ и НБ;
- разрабатывать документальное обеспечение для процессов управления инцидентами ИБ и НБ, включая различные политики и применять его на практике.

Владеть:

- терминологией и процессным подходом построения систем управления инцидентами ИБ и систем управления НБ;
- навыками построения как отдельных процессов управления инцидентами ИБ и НБ, так и систем процессов в целом.

Материалы, вошедшие в учебное пособие «Управление инцидентами информационной безопасности и непрерывностью бизнеса» обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к управлению ИБ. Однако в полной мере данное учебное пособие может быть востребовано при подготовке профессионалов в области управления ИБ. Поэтому оно может быть рекомендовано студентам высших учебных заведений, обучающимся по программам магистратуры направления 090900 – «Информационная безопасность».

Кроме этого учебное пособие «Управление инцидентами информационной безопасности и непрерывностью бизнеса» из серии «Вопросы управления информационной безопасностью» может быть полезным при реализации программ дополнительного образования (курсы повышения квалификации или переподготовки кадров).

Важно подчеркнуть, что для приступающих к ознакомлению с данным учебным пособием есть определенные требования по предварительной подготовке. Например, следует знать основы теории ИБ и комплексный подход к обеспечению ИБ (ОИБ), уязвимости и угрозы ИБ в информационной среде. Следует рекомендовать предварительное ознакомление с материалом первых двух частей серии учебных пособий «Вопросы управления информационной безопасностью»: «Часть 1. Основы управления информационной безопасностью» и «Часть 2. Управление рисками информационной безопасности».

Авторы признательны коллегам по факультету «Кибернетика и информационная безопасность» НИЯУ МИФИ, а также всем рецензентам.

Авторы, естественно, не претендуют на исчерпывающее изложение всех названных в работе аспектов проблем управления инцидентами ИБ и НБ организации, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

ВВЕДЕНИЕ

Основополагающей частью СУИБ является система управления инцидентами ИБ (СУИИБ). Данные, аккумулируемые в рамках процессов управления инцидентами ИБ, являются необходимыми для работы достаточно большого количества других процессов управления ИБ, например для корректного проведения оценки рисков ИБ мониторинга/аудита, управления изменениями, доступом и непрерывностью бизнеса (НБ), оценки эффективности существующих защитных мер. Другими словами, процесс управления инцидентами ИБ является своеобразным «мотором» жизненного цикла СУИБ.

Разработка и реализация процесса управления инцидентами ИБ в соответствии с лучшими практиками обеспечивает следующее:

- четкое определение ролей и ответственности всех специалистов за качественное и своевременное реагирование на инциденты ИБ;
- предоставление оперативной информации для мониторинга эффективности принимаемых защитных мер;
- предоставление необходимой информации для корректного проведения анализа рисков ИБ;
- предотвращение инцидентов ИБ в будущем благодаря оперативному предоставлению сведений об имеющихся инцидентах ИБ, эффективности реагирования на них, анализу динамики инцидентов ИБ.

Таким образом, можно сделать вывод, что внедрение процесса управления инцидентами ИБ в СУИБ способствует решению проблем, с которыми сталкиваются динамично развивающиеся организации: увеличение ущерба от инцидентов ИБ, а также выбор и принятие адекватных решений, минимизирующих последствия от возможной реализации угроз ИБ.

Возникновение какого-либо неожиданного или нежелательного инцидента ИБ и неэффективное функционирование самой СУИБ способны негативно воздействовать на непрерывность важных функций бизнеса организации и поддерживающих его элементов. В данном случае актуальным является планирование обеспечения непрерывности бизнеса (ОНБ) как гарантии восстановления функционирования организации в случае любого инцидента, включая и инциденты ИБ. Процесс ОНБ также обеспечивает уверенность в том, что восстановление всех функций бизнеса в исходное состояние достигается с учетом заданных очередностей и интервалов времени и за счет применения необходимых плановых мер и средств. Поэтому перед каждой организацией рано или поздно встают следующие вопросы:

- насколько применим и критичен для нее тот или иной риск прерывания бизнеса;

- как избежать данного риска или минимизировать его негативные последствия;
- что нужно сделать заранее;
- как найти «золотую середину» между приемлемыми инвестициями в превентивные меры (по предотвращению прерываний и минимизации их последствий) и возможными потерями.

На решение всех поставленных вопросов и направлен процесс управления непрерывностью деятельности, или как его чаще называют, процесс управления непрерывностью бизнеса (УНБ) – важный элемент надлежащего управления всей деятельностью организации, предоставления ее услуг и производства продукции, а также предпринимательской дальновидности и конкурентоспособности. В свою очередь ИБ является важнейшей составляющей НБ.

Все это доказывает необходимость внимательного изучения вопросов управления инцидентами ИБ и ОНБ. Актуальность определенных выше проблем, наличие непосредственной связи между инцидентами ИБ и ОНБ и важность при этом роли СУИБ объясняет выбор тематики и структуры данного учебного пособия.