

ПРЕДИСЛОВИЕ

При подготовке данного учебного пособия были поставлены следующие задачи:

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

2) определить особенности системы управления инцидентами ИБ (СУИИБ) и рассмотреть ее основные характеристики.

Исходя из поставленных задач, была определена структура учебного пособия «Управление инцидентами информационной безопасности», которое состоит из введения, трех глав, заключения, приложения, глоссария и списка литературы из 59 наименований.

Во введении обоснована актуальность темы учебного пособия.

В первой главе кратко анализируется нормативное обеспечение вопросов управления инцидентами ИБ (УИИБ).

Во второй главе изучается процесс управления инцидентами ИБ (ПУИИБ), для чего вводятся понятия события и инцидента ИБ и выделяются цели и задачи УИИБ. Описывается СУИИБ. Анализируются этапы ПУИИБ, 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 первичную оценку и предварительное решение по событию ИБ и вторичную оценку и подтверждение инцидента ИБ. Детально исследуется подпроцесс реагирования на инциденты ИБ и его составляющие: немедленное реагирование, контроль, последующее реагирование, антикризисное управление, передача информации, мониторинг возможностей реагирования на инциденты ИБ и извлечение опыта из УИИБ.

В третьей главе рассматриваются три вида обеспечения УИИБ: кадровое документальное и техническое. Анализируется

деятельность группы реагирования на инциденты ИБ. Подчеркивается необходимость обеспечения осведомленности и обучения в области инцидентов ИБ. Описывается документация СУИИБ, включая политику УИИБ и план реагирования на инциденты ИБ. Определяются функции инструментальных средств управления событиями ИБ. Подробно описываются SIEM- системы, предназначенные для автоматизации управления информацией и событиями ИБ.

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

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

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» обучающиеся будут:

Знать:

- принципы построения СУИБ объекта в части СУИИБ;
- современные подходы к УИИБ объекта и направления их развития;
- особенности отдельных процессов УИИБ в рамках СУИБ;
- основные международные и российские стандарты, регламентирующие УИИБ;
- принципы разработки процессов УИИБ;
- принципы создания основных документов, регламентирующих вопросы УИИБ.

Уметь:

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

Владеть:

- терминологией и процессным подходом построения СУИИБ;
- навыками построения как отдельных процессов УИИБ, так и систем процессов в целом.

Материалы, вошедшие в учебное пособие «Управление инцидентами информационной безопасности», 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 10.04.01 — «Информационная безопасность».

Кроме того, учебное пособие «Управление инцидентами информационной безопасности» 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 НИЯУ МИФИ, а также всем рецензентам.

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