

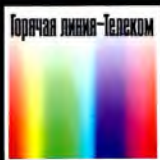
# УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ



## УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Н. Г. МИЛОСЛАВСКАЯ  
А. И. ТОЛСТОЙ

# Оглавление

|  |           |
|--|-----------|
| Предисловие .....  | 3         |
| Введение .....   | 7         |
| <b>1. Нормативная база управления инцидентами информационной безопасности .....</b>  | <b>10</b> |
| 1.1. ГОСТ Р ИСО/МЭК 18044-2007 — инфраструктура управления инцидентами ИБ в рамках циклической модели PDCA .....                               | 12        |
| 1.2. NIST SP Rev 2 800-61 — обработка инцидентов компьютерной безопасности .....   | 14        |
| 1.3. РС БР ИБВС-2.5-2014 — управление инцидентами ИБ .....   | 15        |
| 1.4. Стандарты, посвященные свидетельствам инцидентов ИБ, представленным в цифровой форме .....  | 18        |
| 1.5. СТО БР ИБВС-1.3-2016 — инциденты ИБ при осуществлении переводов денежных средств .....  | 33        |
| 1.6. Серия стандартов ISO/IEC 27035 об управлении инцидентами ИБ .....   | 35        |
| Выводы .....   | 43        |
| Вопросы для самоконтроля .....   | 44        |
| <b>2. Управление инцидентами информационной безопасности .....</b>   | <b>45</b> |
| 2.1. Событие и инцидент ИБ .....   | 46        |
| 2.2. Цели и задачи управления инцидентами ИБ .....   | 60        |
| 2.3. Система управления инцидентами ИБ .....   | 68        |
| 2.4. Этапы процесса управления инцидентами ИБ .....  | 77        |
| 2.4.1. Планирование и подготовка процесса управления инцидентами ИБ .....  | 80        |
| 2.4.2. Использование и анализ процесса управления инцидентами ИБ согласно ГОСТ Р ИСО/МЭК ТО 18044-2007 ..                                      | 82        |
| 2.4.3. Выявление и отчетность, оценка и принятие решений и ответное реагирование на инциденты ИБ согласно серии стандартов ISO/IEC 27035 ..... | 87        |
| 2.4.4. Улучшение процесса управления инцидентами ИБ ....   | 91        |

|  |            |
|--|------------|
| 2.5. Высокоуровневое представление процесса управления инцидентами ИБ .....                | 93         |
| 2.6. Обнаружение событий ИБ и оповещение (информирование) о них .....                      | 99         |
| 2.7. Обработка сообщений о событиях ИБ и инцидентах ИБ                                     | 109        |
| 2.7.1. Первичная оценка и предварительное решение по событию ИБ .....                      | 114        |
| 2.7.2. Вторичная оценка и подтверждение инцидента ИБ ...                                   | 117        |
| 2.8. Реагирование на инциденты ИБ .....  | 129        |
| 2.8.1. Немедленное реагирование на инцидент ИБ .....                                       | 143        |
| 2.8.2. Контролируемость инцидента ИБ .....   | 146        |
| 2.8.3. Последующее реагирование на инцидент ИБ .....                                       | 146        |
| 2.8.4. Антикризисное управление .....  | 147        |
| 2.8.5. Расследование инцидентов ИБ .....   | 148        |
| 2.8.6. Передача информации (информирование) в процессе управления инцидентами ИБ .....     | 167        |
| 2.8.7. Мониторинг возможностей реагирования на инциденты ИБ .....                          | 171        |
| 2.9. Извлечение опыта из управления инцидентами ИБ .....                                   | 172        |
| Выводы .....   | 176        |
| Вопросы для самоконтроля .....   | 178        |
| <b>3. Обеспечение управления инцидентами информационной безопасности .....</b>             | <b>180</b> |
| 3.1. Кадровое обеспечение управления инцидентами ИБ .....                                  | 180        |
| 3.1.1. Группа реагирования на инциденты ИБ .....   | 180        |
| 3.1.2. Обеспечение осведомленности и обучение в области реагирования на инциденты ИБ ..... | 193        |
| 3.2. Документация системы управления инцидентами ИБ ..                                     | 197        |
| 3.2.1. Политика управления инцидентами ИБ .....  | 200        |
| 3.2.2. План реагирования на инциденты ИБ .....   | 204        |
| 3.3. Техническая поддержка управления инцидентами ИБ ..                                    | 217        |
| 3.4. SIEM-системы для автоматизации управления информацией и событиями ИБ .....            | 228        |
| Выводы .....   | 246        |
| Вопросы для самоконтроля .....   | 247        |
| Заключение .....   | 249        |
| Приложения. Примеры систем управления событиями .....                                      | 251        |
| Принятые сокращения .....  | 254        |
| Глоссарий .....  | 255        |
| Литература .....   | 266        |