

# ОГЛАВЛЕНИЕ

<b>ПРЕДИСЛОВИЕ</b> .....	3
<b>ВВЕДЕНИЕ</b> .....	7
<b>1. НОРМАТИВНАЯ БАЗА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ</b> .....	10
1.1. ГОСТ Р ИСО/МЭК 18044-2007 — инфраструктура управления инцидентами ИБ в рамках циклической модели PDCA .....	13
1.2. NIST SP Rev 2 800-61 — обработка инцидентов компьютерной безопасности .....	15
1.3. РС ВР ИБВС-2.5-2014 — управление инцидентами ИБ .....	16
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 .....	35
1.6. Серия стандартов ISO/IEC 27035 об управлении инцидентами ИБ .....	37
1.7. ГОСТы, посвященные управлению компьютерными инцидентами .....	47
Вопросы для самоконтроля .....	51
<b>2. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ</b> .....	52
2.1. Событие и инцидент ИБ .....	53
2.2. Цели и задачи управления инцидентами ИБ .....	70
2.3. Система управления инцидентами ИБ .....	80
2.4. Этапы процесса управления инцидентами ИБ .....	90
2.4.1. «Планирование и подготовка» (1) этап процесса управления инцидентами ИБ .....	96
2.4.2. «Использование» (2), «Анализ» (3) и «Улучшение» (4) этапы процесса управления инцидентами ИБ согласно ГОСТ Р ИСО/МЭК ТО 18044-2007 .....	99
2.4.3. «Обнаружение и регистрация инцидентов» (2), «Реагирование на инциденты» (3) и «Анализ результатов деятельности по управлению инцидентами» (4) этапы согласно ГОСТ Р 59710-2022 .....	105
2.4.4. «Выявление и отчетность» (2), «Оценка и принятие решений» (3), «Ответное реагирование на инциденты ИБ» (4) и «Извлечение опыта» (5) этапы согласно серии стандартов ISO/IEC 27035 .....	110

2.5. Высокоуровневое представление процесса управления инцидентами ИБ .....	119
2.6. Обнаружение событий ИБ и оповещение (информирование) о них .....	127
2.7. Обработка сообщений о событиях ИБ и инцидентах ИБ .....	140
2.7.1. Первичная оценка и предварительное решение по событию ИБ .....	145
2.7.2. Вторичная оценка и подтверждение инцидента ИБ ..	154
2.8. Реагирование на инциденты ИБ .....	169
2.8.1. Немедленное реагирование на инцидент ИБ .....	191
2.8.2. Контролируемость инцидента ИБ .....	194
2.8.3. Последующее реагирование на инцидент ИБ .....	194
2.8.4. Антикризисное управление .....	196
2.8.5. Расследование инцидентов ИБ .....	198
2.8.6. Передача информации (информирование) в процессе управления инцидентами ИБ .....	218
2.8.7. Мониторинг возможностей реагирования на инциденты ИБ .....	223
2.9. Извлечение опыта из управления инцидентами ИБ ..	225
Вопросы для самоконтроля .....	232
<b>3. ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИБ .....</b>	<b>234</b>
3.1. Кадровое обеспечение управления инцидентами ИБ ..	235
3.1.1. Группа управления инцидентами ИБ .....	237
3.1.2. Группа реагирования на инциденты ИБ .....	246
3.2. Обеспечение осведомленности и обучение в области реагирования на инциденты ИБ .....	258
3.3. Документация системы управления инцидентами ИБ	263
3.3.1. Политика и план управления инцидентами ИБ .....	266
3.3.2. План реагирования на инциденты ИБ .....	272
3.4. Материально-техническая поддержка управления инцидентами ИБ .....	287
3.5. SIEM-системы для автоматизации управления информацией и событиями ИБ .....	300
Вопросы для самоконтроля .....	324
<b>ПРИНЯТЫЕ СОКРАЩЕНИЯ .....</b>	<b>325</b>
<b>ГЛОССАРИЙ .....</b>	<b>327</b>
<b>ЛИТЕРАТУРА .....</b>	<b>337</b>