

# Оглавление

|  |           |
|--|-----------|
| Предисловие .....  | 3         |
| Введение .....   | 6         |
| <b>1. Нормативное обеспечение проверки управления информационной безопасностью .....</b>                                   | <b>10</b> |
| 1.1. ISO 19011:2018 и ГОСТ Р ИСО 19011–2021 — руководящие указания по аудиту систем менеджмента .....                      | 12        |
| 1.2. ISO/IEC 27006:2015 и ГОСТ Р ИСО/МЭК 27006–2020 — требования к органам, осуществляющим аудит и сертификацию СУИБ ..... | 15        |
| 1.3. ISO/IEC 27007:2020 и ГОСТ Р ИСО/МЭК 27007–2014 — руководство по аудиту СУИБ .....                                     | 18        |
| 1.4. ISO/IEC 27008:2019 и ГОСТ Р 56045–2021 — руководство по аудиту средств управления ИБ, реализованных в СУИБ .....      | 20        |
| Выводы .....   | 23        |
| Вопросы для самоконтроля .....   | 23        |
| <b>2. Процессы проверки управления информационной безопасностью .....</b>  | <b>25</b> |
| 2.1. Виды проверок ИБ .....  | 25        |
| 2.2. Мониторинг ИБ .....   | 33        |
| 2.3. Самооценка ИБ .....   | 48        |
| 2.4. Внутренний аудит ИБ .....   | 55        |
| 2.5. Внешний аудит ИБ .....  | 61        |
| 2.5.1. Принципы проведения внешнего аудита ИБ .....  | 65        |
| 2.5.2. Управление программой внешнего аудита ИБ .....  | 68        |
| 2.5.3. Этапы проведения внешнего аудита ИБ .....   | 79        |
| 2.5.4. Компетентность аудиторов ИБ .....   | 109       |
| 2.5.5. Взаимоотношения представителей аудиторской группы и проверяемых организаций .....                                   | 120       |
| 2.6. Анализ СУИБ со стороны высшего руководства организации .....  | 124       |
| 2.7. Методы и инструментальные средства проверки ИБ .....  | 128       |

---

|  |     |
|--|-----|
| Выводы .....   | 142 |
| Вопросы для самоконтроля .....   | 143 |
| Заключение .....   | 145 |
| Приложения .....   | 147 |
| П1. Выдержка из примерной программы аудита вопросов<br>управления непрерывностью бизнеса ..... | 147 |
| П2. Примеры систем анализа защищенности .....  | 152 |
| П3. Примеры систем обнаружения и предотвращения втор-<br>жений .....                           | 153 |
| Принятые сокращения .....  | 154 |
| Глоссарий .....  | 155 |
| Литература .....   | 168 |