**Практика**

Предлагаю теперь под другим углом взглянуть на нашу схему, с которой мы начали данный урок.

1. Обеспечение и управление ИБ.
2. Управление рисками.
3. Обработка инцидентов ИБ.
4. Аудит IT и ИБ.
5. Управление IT.
6. Оценка, сертификация IT-систем.
7. Непрерывность бизнеса.
8. Рекомендации по защите.
9. Повышение осведомленности пользователей.
10. Рекомендации по безопасности для персонального использования.

Исходя из вашей методички и тех знаний, которые вы получили на сегодняшнем уроке, я предлагаю вам сделать 10 минутный тест и направить его мне почтовым сообщением.

Формат теста:

|  |  |  |
| --- | --- | --- |
|  | **ФИО студента: Лешков Игорь Александрович** | |
| **№** | **Область «best practice»** | **Применение методологии\стандартов + возможный пример процесса ИБ** |
| 1 | Обеспечение и управление ИБ | ISO 27002:2013/ Например – Безопасность связи (Управление сетевой безопасностью) |
| 2 | Управление рисками | ISO 27005:2018/Например – Установление контекста управления рисками (объем, обязательства, политики и критерии) |
| 3 | Обработка инцидентов ИБ | ISO 27035:2016/Например – Поиск уязвимостей, тестирование на проникновение (пентест), SIEM-системы. |
| 4 | Аудит IT и ИБ | ISO 27007&27008/Например – проведения аудита СМИБ + внедрение технических средств контроля. |
| 5 | Управление IT | OWASP/Например – разработка руководств по безопасности приложений для CISO. |
| 6 | Оценка, сертификация IT-систем | ISO 27001:2013/Например – мониторинг, оценка и анализ СУИБ. |
| 7 | Непрерывность бизнеса | ISO 27031:2011/Например – Внедрение технологий реагирования на стихийные бедствия и ЧС(аварийное восстановление итд.). |
| 8 | Рекомендации по защите | ISO 27033-1:2009/Например – разработка концепций защиты сетей в организации. |
| 9 | Повышение осведомленности пользователей | SANS/CIS Controls/Например – рекомендации по защите паролей, понимания антивирусного ПО, итд. |
| 10 | Рекомендации по безопасности для персонального использования | NSA/Например – безопасность в соц.сетях |