**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: Глинник Дмитрий Вячеславович** | |
| **№** | **Область «best practice»** | **Применение методологии\стандартов + возможный пример процесса ИБ** |
| 1 | Обеспечение и управление ИБ | ISO/IEC 27002:2013  Политики информационной безопасности (создание верхнеуровневой общей политики информационной безопасности) |
| 2 | Управление рисками | ISO/IEC 27005:2018  Управление рисками информационной безопасности (процесс выявления, оценки и обработки информационных рисков [безопасности], включающий как стратегические/долгосрочные, так и операционные/среднесрочные и краткосрочные циклы.) |
| 3 | Обработка инцидентов ИБ | ISO/IEC 27035:2016  Установка политики управления инцидентами информационной безопасности, формирование группы реагирования на инциденты |
| 4 | Аудит IT и ИБ | ISO/IEC 27007:2020  Управление программой аудита СМИБ (определение того, что, когда и как проверять; назначение соответствующих аудиторов; управление рисками аудита; ведение записей аудита; постоянное улучшение процесса); |
| 5 | Управление IT | ITIL.  Внедрение CMDB (база данных управления конфигурацией) |
| 6 | Оценка, сертификация IT-систем | ISO/IEC TS 27008:2019  Проверках средств управления информационной безопасностью, включая проверку технического соответствия, на соответствие стандарту реализации информационной безопасности, установленному организацией |
| 7 | Непрерывность бизнеса | ISO/IEC 27031:2011  Практики обработки инцидентов информационной безопасности и управления ими |
| 8 | Рекомендации по защите | NSA. Блокировка USB-накопителей для предотвращения утечки корпоративной информации. |
| 9 | Повышение осведомленности пользователей | SANS Использование двухфакторной аутентификации |
| 10 | Рекомендации по безопасности для персонального использования | NSA Безопасность в социальных сетях |