

## Практическая работа

### «Построение концепции информационной безопасности предприятия»

#### 1. Цель работы

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

#### 2. Краткие теоретические сведения

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – **Концепции и Политики информационной безопасности**. Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит **КАК**, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности.

#### 3. Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

## **1. Общие положения**

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

## **2. Проблемная ситуация в сфере информационной безопасности**

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

## **3. Механизмы обеспечения информационной безопасности Предприятия**

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

## **4. Мероприятия по реализации мер информационной безопасности Предприятия**

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.

- Подразделения, занятые в обеспечении информационной безопасности.

- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

#### 4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

#### 4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия.
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

### **5. Программа создания системы информационной безопасности Предприятия**

#### **4. Содержание отчета**

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании

## 5. Варианты

Вариант – номер по списку в журнале.

| Номер варианта | Организация   | Метод оценки риска (см. Приложение Е ГОСТа) |
|----------------|---|---|
| 1              | Отделение коммерческого банка                       | 1   |
| 2              | Поликлиника   | 2   |
| 3              | Колледж   | 3   |
| 4              | Офис страховой компании                             | 4   |
| 5              | Рекрутинговое агентство                             | 1   |
| 6              | Интернет-магазин                                    | 2   |
| 7              | Центр оказания государственных услуг                | 3   |
| 8              | Отделение полиции                                   | 4   |
| 9              | Аудиторская компания                                | 1   |
| 10             | Дизайнерская фирма                                  | 2   |
| 11             | Офис интернет-провайдера                            | 3   |
| 12             | Офис адвоката                                       | 4   |
| 13             | Компания по разработке ПО для сторонних организаций | 1   |
| 14             | Агентство недвижимости                              | 2   |
| 15             | Туристическое агентство                             | 3   |
| 16             | Офис благотворительного фонда                       | 4   |
| 17             | Издательство  | 1   |
| 18             | Консалтинговая фирма                                | 2   |
| 19             | Рекламное агентство                                 | 3   |
| 20             | Отделение налоговой службы                          | 4   |
| 21             | Офис нотариуса                                      | 1   |
| 22             | Бюро перевода (документов)                          | 2   |
| 23             | Научно проектное предприятие                        | 3   |

|           |                            |   |
|-----------|----------------------------|---|
| <b>24</b> | Брачное агентство          | 4 |
| <b>25</b> | Редакция газеты            | 1 |
| <b>26</b> | Гостиница                  | 2 |
| <b>27</b> | Праздничное агентство      | 3 |
| <b>28</b> | Городской архив            | 4 |
| <b>29</b> | Диспетчерская служба такси | 1 |
| <b>30</b> | Железнодорожная касса      | 2 |

ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий»