**Содержание**

1. Область применения . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .1
2. Термины и определения
3. Политика безопасности
   1. Политика информационной безопасности
4. Организационные вопросы безопасности
   1. Организационная инфраструктура информационной безопасности
   2. Обеспечение безопасности при наличии доступа к информационным системам сторонних организаций
   3. Привлечение сторонних организаций к обработке информации (аутсорсинг)
5. Классификация и управление активами  
   5.1. Учет активов

5.2. Классификация информации

6. Вопросы безопасности, связанные с персоналом  
 6.1. Учет вопросов безопасности в должностных обязанностях и при найме персонала.

6.2. Обучение пользователей.

6.3. Реагирование на инциденты нарушения информационной безопасности и сбои.

7. Физическая защита и защита от воздействий окружающей среды.

7.1. Охраняемые зоны.

7.2. Безопасность оборудования.

7.3. Общие мероприятия по управлению информационной безопасностью.

8. Управление передачей данных и операционной деятельностью.

8.1. Операционные процедуры и обязанности.

8.2. Планирование нагрузки и приемка систем.

8.3. Защита от вредоносного программного обеспечения.

8.4. Вспомогательные операции  
 8.5. Управление сетевыми ресурсами.

8.6. Безопасность носителей информации.

8.7. Обмен информацией и программным обеспечением.

9. Контроль доступа.

9.1. Требование бизнеса по обеспечению контроля в отношении логического доступа.

9.2. Контроль в отношении доступа пользователей.

9.3. Обязанности пользователей.

9.4. Контроль сетевого доступа.

9.5. Контроль доступа к операционной системе.

9.6. Контроль доступа к приложениям.

9.7. Мониторинг доступа и использования системы.

9.8. Работа с переносными устройствами и работа в дистанционном режиме.

10. Разработка и обслуживание систем

10.1. Требования к безопасности системы.

10.2. Безопасность в прикладных системах.

10.3. Меры защиты информации, связанные с использованием криптографии.

10.4. Безопасность системных файлов.

10.5. Безопасность в процессах разработки и поддержки.

11. Управление непрерывностью бизнеса.

12. Соответствие требованиям.

12.1. Соответствие требованиям законодательства.  
 12.2. Пересмотр политики безопасности и техническое соответствие требованиям безопасности

12.3. Меры безопасности при проведении аудита

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Информационная технология

ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Information technology. Code of practice for information  
security management

**Дата введения – 2007 – 01- 01**

1. **Область применения.**

Настоящий стандарт устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управление безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями. Рекомендации настоящего стандарта следует выбирать и использовать в соответствии с действующим законодательством.

1. **Термины и определения**

В настоящем стандарте применены следующие термины с соответствующими определениями:

* 1. **информационная безопасность**: Защита конфиденциальности, целостности и доступности информации.

Примечания   
 1 **конфиденциальность**: Обеспечение доступа к информации только авторизованным пользователям.   
 2 **целостность**: Обеспечение достоверности и полноты информации и методов ее обработки.   
 3 **доступность**: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

2.2 **оценка рисков**: Оценка угроз, их последствий, уязвимости информации и средств ее обработки, а также вероятности их возникновения.

2.3 **управление рисками**: Процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на информационные системы, в рамках допустимых затрат.

1. **Политики безопасности**
   1. **Политика информационной безопасности**

Цель: обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс.

Разработка и реализация политики информационной безопасности организации осуществляется высшим руководством путем выработки четкой позиции в решении вопросов информационной безопасности.

* + 1. **Документальное оформление**

Политика информационной безопасности должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность

Издание официальное

руководства, а также излагать подход организации к управлению информационной безопасностью. Как минимум, политика должна включать следующее:

а) определение информационной безопасности, ее общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

б) изложение целей и принципов информационной безопасности, сформулированных руководством;

в) краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например:

1) соответствие законодательным требованиям и договорным обязательствам;

2) требования в отношении обучения вопросам безопасности;

3) предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

4) управление непрерывностью бизнеса;

5) ответственность за нарушения политики безопасности;

г) определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

д) ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Такая политика должна быть доведена до сведения всех сотрудников организации в доступной и понятной форме.