МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиал) СКФУ

ОП. 05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ЛАБОРАТОРНЫХ РАБОТ

Специальности СПО

СПО 09.02.11 Разработка и управление программным обеспечением

Квалификация: программист

Пятигорск 2026

Методические указания для лабораторных работ по дисциплине «Основы информационной безопасности» составлены в соответствии с ФГОС СПО. Предназначены для студентов, обучающихся по специальности 09.02.11 Разработка и управление программным обеспечением

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа дисциплины «Основы информационной безопасности» предусматривает изучение базовых понятий, угроз, методов и средств защиты информации в современных информационных системах. При изучении предмета следует соблюдать единство терминологии в соответствии с действующими стандартами (ГОСТ, ISO/IEC 27000) и законодательством РФ в области защиты информации.

В результате освоения учебной дисциплины обучающийся должен **уметь:**

1. Классифицировать угрозы информационной безопасности и оценивать ущерб от их реализации.
2. Применять программно-аппаратные средства защиты информации (антивирусы, межсетевые экраны).
3. Обеспечивать защиту информации при работе в локальной сети и сети Интернет.
4. Выполнять базовую настройку политик безопасности операционных систем.
5. Применять методы шифрования и резервного копирования для обеспечения конфиденциальности и целостности данных.

В результате освоения учебной дисциплины обучающийся должен **знать:**

1. Основные понятия, цели и задачи информационной безопасности.
2. Классификацию угроз, уязвимостей и атак на информацию.
3. Принципы и методы защиты информации от несанкционированного доступа.
4. Правовые и нормативные основы обеспечения информационной безопасности в РФ.
5. Назначение и принципы работы антивирусных средств, межсетевых экранов, средств криптографической защиты.
6. Основные задачи администрирования безопасности в операционных системах семейств Windows и Linux.

Лабораторная работа № 1

Информационная безопасность. Моделирование угроз.

Цель: выработать практические навыки идентификации угроз информационной безопасности и построения модели угроз для условного объекта информатизации.

Подготовка к работе: изучить теоретический материал и конспект лекций по теме.

Краткие теоретические сведения

Информационная безопасность (ИБ) — это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Основными составляющими ИБ являются три категории: конфиденциальность, целостность и доступность информации.

Угроза информационной безопасности — это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности и/или доступности информации.

Угрозы можно классифицировать по различным признакам:

По природе возникновения: естественные (стихийные бедствия) и искусственные (антропогенные, техногенные).

По степени преднамеренности: случайные (ошибки пользователей, сбои) и преднамеренные (атаки хакеров, промышленный шпионаж).

По источнику: внутренние (от сотрудников) и внешние (от злоумышленников вне организации).

Уязвимость — это слабое место в системе, которое может быть использовано для реализации угрозы. **Атака** — это действие, направленное на реализацию угрозы путем использования уязвимости.

Модель угроз — это формализованное описание наиболее вероятных угроз безопасности информации, действующих на конкретном объекте информатизации. Она включает в себя описание источников угроз, способов их реализации, используемых уязвимостей и возможных последствий.

Для оценки критичности угроз часто используют шкалу, состоящую из трёх уровней:

Низкий уровень: угроза может привести к незначительным нарушениям, которые легко устраняются.

Средний уровень: угроза может привести к временным сбоям в работе системы или к утечке информации ограниченного распространения.

Высокий уровень: угроза может привести к критическим последствиям, остановке бизнес-процессов, утечке конфиденциальных данных, финансовым или репутационным потерям.

Задания для самостоятельного выполнения:

Задание 1. На основе предложенной ситуации идентифицируйте основные активы, подлежащие защите, и заполните таблицу.

№	Актив	Тип информации	Критичность для работы
1.	Сервер с базами данных студентов	ФИО, оценки, личные дела	Высокая

Задание 2. Составьте модель угроз. Идентифицируйте не менее 10 угроз, классифицируйте их (внешняя/внутренняя, преднамеренная/случайная) и оцените уровень риска (Высокий/Средний/Низкий).

№	Описание угрозы	Источник угрозы	Уязвимость	Тип (Конф./Цел./Дост.)	Уровень риска
1	Заражение вирусом-шифровальщиком	Внешний злоумышленник (фишинг)	Отсутствие антивируса, невнимательность пользователя	Целостность, Доступность	Высокий
2					
...					

Задание 3. Для трёх угроз с наивысшим уровнем риска предложите организационные и технические меры защиты.

1. Для угрозы №1 (Заражение вирусом): **Меры защиты:** Установка и регулярное обновление антивирусного ПО, проведение инструктажа для студентов и преподавателей, ограничение прав на установку ПО.
2. ...
3. ...

Контрольные вопросы:

1. Дайте определение понятиям «информационная безопасность», «угроза», «уязвимость».
2. В чем разница между случайными и преднамеренными угрозами? Приведите примеры.
3. Для чего нужна модель угроз?

Лабораторная работа № 2

Правовые и нормативные основы информационной безопасности.

Цель: изучить структуру законодательной базы РФ в области ИБ и научиться применять нормативные документы для решения практических задач.

Подготовка к работе: изучить теоретический материал и конспект лекций по теме.

Краткие теоретические сведения

Правовое обеспечение информационной безопасности базируется на Конституции РФ, федеральных законах, указах Президента, постановлениях Правительства и ведомственных нормативных актах (ФСТЭК, ФСБ).

Ключевые законы РФ:

Конституция РФ: Статья 23 (право на неприкосновенность частной жизни, личную и семейную тайну), Статья 24 (запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия), Статья 29 (право свободно искать, получать, передавать, производить и распространять информацию любым законным способом).

Гражданский кодекс РФ: Регулирует вопросы авторского права, интеллектуальной собственности, ответственности за причинение вреда.

Уголовный кодекс РФ: Глава 28 «Преступления в сфере компьютерной информации» (ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»).

ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006. Базовый закон, определяющий основные понятия, правовой режим информации, обязанности обладателя информации по ее защите.

ФЗ № 152-ФЗ «О персональных данных» от 27.07.2006. Регулирует сбор, обработку, хранение и защиту персональных данных граждан РФ. Вводит понятие оператора ПДн, обязанности по обеспечению конфиденциальности и безопасности ПДн.

ФЗ № 63-ФЗ «Об электронной подписи» от 06.04.2011. Устанавливает правовые условия использования электронной подписи, приравнивая ее к собственноручной.

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646). Стратегический документ, определяющий национальные интересы, угрозы и приоритеты государственной политики в информационной сфере.

Задания для самостоятельного выполнения:

Задание 1. Ознакомьтесь с содержанием Доктрины информационной безопасности РФ и заполните таблицу, выделив ключевые положения.

Раздел Доктрины	Основные положения, интересующие специалиста по ИБ
Национальные интересы	1. ... 2. ...
Основные угрозы	1. ... 2. ...
Стратегические цели	1. ... 2. ...

Задание 2. Кейс «Утечка персональных данных». В одной из коммерческих компаний произошла утечка базы данных клиентов, содержащей ФИО, паспортные данные и номера телефонов. Используя текст ФЗ-152, ответьте на вопросы:

1. Какие требования по защите ПДн были, предположительно, нарушены?
2. Какие санкции (штрафы, предписания) грозят компании согласно КоАП РФ?
3. Кто несет ответственность за данное нарушение?

Задание 3. Соотнесите статью УК РФ и возможное наказание (соедините линиями или заполните таблицу соответствия).

Статья УК РФ	Пример деяния	Максимальное наказание (по выбору студента)
Ст. 272	Создание и распространение вируса-шифровальщика	Лишение свободы до 7 лет
Ст. 273	Взлом почтового ящика преподавателя	Лишение свободы до 5 лет
Ст. 274	Вывод из строя сервера колледжа из-за нарушения правил эксплуатации	Лишение свободы до 5 лет

Контрольные вопросы:

1. Какой закон регулирует порядок обработки персональных данных?
2. Какие виды ответственности предусмотрены за преступления в сфере компьютерной информации?
3. В чем разница между ФЗ-149 и ФЗ-152?

Лабораторная работа № 3

Криптографические методы защиты. Шифрование данных.

Цель занятия: изучить принципы симметричного и асимметричного шифрования, научиться применять простейшие шифры и программные средства для шифрования данных.

Подготовка к работе: изучить теоретический материал и конспект лекций по теме.

Краткие теоретические сведения

Криптография — наука о методах обеспечения конфиденциальности, целостности и аутентичности информации путем преобразования данных.

Основные понятия:

Шифрование — процесс преобразования открытого текста в шифротекст (зашифрованный) с помощью ключа и алгоритма шифрования.

Дешифрование — обратный процесс преобразования шифротекста в открытый текст.

Ключ — секретная информация, используемая алгоритмом шифрования для преобразования данных.

Типы алгоритмов шифрования:

Симметричное шифрование: Для шифрования и дешифрования используется один и тот же ключ.

Плюсы: Высокая скорость работы.

Минусы: Сложность передачи ключа (нужно передать ключ получателю по надежному каналу).

Примеры: AES, ГОСТ 28147-89, 3DES.

Асимметричное шифрование: используется пара ключей: открытый (публичный) для шифрования и закрытый (приватный) для дешифрования. Открытый ключ можно передавать по открытым каналам, закрытый хранится в секрете.

Плюсы: решает проблему передачи ключа.

Минусы: работает значительно медленнее симметричного.

Примеры: RSA, ElGamal.

Хэширование — необратимое преобразование данных в строку фиксированной длины (хэш). Используется для контроля целостности и хранения паролей. Примеры: MD5 (устарел), SHA-1 (устарел), SHA-256.

Задания для самостоятельного выполнения:

Задание 1. Реализуйте шифр Цезаря (сдвиг алфавита). Зашифруйте свою фамилию, используя сдвиг вправо на 3 позиции (например, А→Г, Б→Д). Проверьте результат дешифрованием.

- *Исходный текст:* Иванов
- *Шифротекст: ...*

Задание 2. Используя, онлайн-калькулятор хэш-функций или встроенные средства ОС (CertUtil -hashfile в Windows), вычислите хэш SHA-256 для небольшого текстового файла. Внесите в файл одно любое изменение (например, точку в конце) и снова вычислите хэш. Сравните результаты.

- *Хэш исходного файла: ...*
- *Хэш измененного файла: ...*
- *Вывод: ...*

Задание 3. Создайте зашифрованный контейнер (архив) с помощью программы 7-Zip (или WinRAR) с использованием пароля. Задание выполняется под наблюдением преподавателя, чтобы не забыть пароль.

1. Создайте на рабочем столе папку «Секретные_данные» и поместите туда 2-3 любых текстовых файла.
2. Выделите папку, нажмите правую кнопку мыши -> 7-Zip -> «Добавить к архиву...».
3. В окне настроек укажите имя архива, формат (zip/7z), введите пароль в поле «Шифрование» и выберите метод шифрования (AES-256).
4. Создайте архив. Удалите исходную папку.
5. Попробуйте открыть архив и извлечь файлы без ввода пароля, а затем с вводом пароля.

Контрольные вопросы:

1. В чем принципиальное различие между симметричным и асимметричным шифрованием?
2. Для каких целей используется хэширование?
3. Что такое электронная подпись и для чего она нужна?

Лабораторная работа № 4

Управление учетными записями и политиками безопасности в Windows

Цель работы: изучить механизмы управления учетными записями, разграничения прав доступа и настройки локальных политик безопасности в ОС Windows.

Подготовка к работе: изучить теоретический материал и конспект лекций по теме.

Краткие теоретические сведения

Безопасность ОС Windows во многом базируется на корректном управлении учетными записями пользователей и применении политик безопасности.

Учетная запись — это запись, содержащая сведения о пользователе, необходимые для его опознавания (аутентификации) и предоставления доступа к ресурсам (авторизации). Учетные записи могут быть:

Встроенные: Администратор (полный контроль), Гость (минимальные права).

Созданные пользователем.

Группы используются для объединения учетных записей с одинаковыми правами, что упрощает администрирование. Примеры групп: Администраторы, Пользователи, Опытные пользователи.

UAC (User Account Control) — компонент Windows, который запрашивает подтверждение на выполнение действий, требующих прав администратора, даже если пользователь работает из-под учетной записи администратора. Это защищает систему от несанкционированных изменений.

Локальные политики безопасности — набор правил, определяющих параметры безопасности на локальном компьютере. Управляются через оснастку secpol.msc. Включают политики:

Политики учетных записей: Требования к паролям (длина, сложность, срок действия), блокировка учетных записей.

Локальные политики: Назначение прав пользователя, настройка аудита.

Задания для выполнения:

Задание 1. Проанализируйте существующие учетные записи.

1. Откройте оснастку «Локальные пользователи и группы» (lusrmgr.msc).
2. Просмотрите список пользователей и групп.
3. Выпишите в тетрадь названия 5 встроенных групп и кратко опишите их права.

Задание 2. Создание и настройка пользователей.

1. Создайте двух новых пользователей: "User1" и "User2" с паролями.
2. Настройте для пользователя "User1" запрет на смену пароля.
3. Включите пользователя "User2" в группу "Пользователи", а затем добавьте его в группу "Администраторы". Что изменилось в правах пользователя?

Задание 3. Настройка политики паролей.

1. Откройте редактор локальной политики безопасности (secpol.msc).
2. Перейдите в раздел «Политики учетных записей» -> «Политика паролей».
3. Измените следующие параметры и запишите их назначение:

Параметр	Установленное значение	Назначение
Минимальная длина пароля	8 символов	
Пароль должен отвечать	Включена	

требованиям сложности		
Максимальный срок действия пароля	30 дней	

Задание 4. Настройка прав доступа к папке.

1. Создайте на диске C: папку "Студент_ИБ".
2. В свойствах папки перейдите на вкладку «Безопасность».
3. Нажмите «Изменить» и для пользователя "User1" установите разрешение только на «Чтение», а для "User2" — «Полный доступ».
4. Войдите в систему под каждым из пользователей и проверьте, какие действия (создание, удаление, изменение файлов) им доступны в этой папке. Опишите результаты.

Контрольные вопросы:

1. Для чего нужна система групп пользователей?
2. Какую роль играет UAC в обеспечении безопасности?
3. Что произойдет с учетными записями пользователей, если в политике безопасности установить срок действия пароля 0 дней?

Лабораторная работа № 5

Защита от вредоносного программного обеспечения. Антивирусы

Цель работы: изучить классификацию вредоносного ПО, принципы работы антивирусов и научиться проводить базовую проверку системы и лечение от вирусов.

Подготовка к работе: изучить теоретический материал и конспект лекций по теме.

Краткие теоретические сведения

Вредоносная программа (ВПО) — это программа, предназначенная для осуществления несанкционированного доступа к информации и/или воздействия на информацию или ресурсы информационной системы.

Классификация ВПО:

Вирусы: Способны к саморазмножению и внедрению своего кода в другие программы.

Черви: Самостоятельные программы, распространяющиеся в основном через сеть, не изменяя другие файлы.

Троянские программы (Трояны): Маскируются под полезные программы, но выполняют вредоносные действия (кража данных, установка бэкдоров).

Шифровальщики (Ransomware): Шифруют данные пользователя и требуют выкуп за их расшифровку.

Шпионское ПО (Spyware): Собирает информацию о пользователе и его действиях без его ведома.

Руткиты (Rootkits): Предназначены для скрытия следов присутствия злоумышленника в системе, маскируют другие вредоносные программы.

Рекламное ПО (Adware): Навязчиво отображает рекламу.

Логические бомбы: Запускаются при наступлении определенного события (дата, действие).

Принципы работы антивирусов:

Сигнатурный анализ: Поиск совпадений фрагментов кода с базой известных вирусов. Минус: не видит новые вирусы.

Эвристический анализ: Анализ поведения программы и подозрительных действий. Позволяет обнаруживать неизвестные угрозы, но может давать ложные срабатывания.

Проактивная защита: Мониторинг поведения всех программ в реальном времени и блокировка подозрительной активности.

Облачные технологии: Проверка файлов происходит на серверах антивирусной компании, что снижает нагрузку на ПК.

Задания для выполнения:

Задание 1. Исследование запущенных процессов.

1. Запустите диспетчер задач (Ctrl+Shift+Esc).
2. На вкладке «Процессы» изучите список. Найдите процесс, потребляющий больше всего ресурсов ЦП и памяти.

3. С помощью поиска в интернете определите, является ли этот процесс системным или прикладным, безопасен ли он.
4. Запустите оснастку «Просмотр событий» (eventvwr.msc) и найдите в журналах Windows любые предупреждения или ошибки, связанные с безопасностью.
5. Запишите названия 3 процессов, которые показались вам подозрительными, и результаты их проверки.

Задание 2. Работа с антивирусом (на примере Kaspersky Free / Windows Defender).

1. Запустите центр защиты Защитника Windows (или установленный антивирус).
2. Изучите основные разделы: «Защита от вирусов и угроз», «Брандмауэр и безопасность сети», «Управление приложениями и браузером».
3. Запустите полную проверку компьютера (только с разрешения преподавателя, т.к. это длительный процесс). Зафиксируйте время начала проверки и количество просканированных объектов.
4. Изучите «Журнал угроз» или «Карантин». Есть ли там какие-либо объекты? Если да, опишите их.

Задание 3. Проверка подозрительного файла онлайн-сканером.

1. Создайте простой текстовый файл и поместите в него условно-вредоносную строку (например, тестовый сигнатурный код X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*, известный как тестовый файл EICAR). *Внимание: это стандартный тестовый файл, безопасный для системы, но детектируемый антивирусами.*
2. Загрузите этот файл на сайт онлайн-сканера **VirusTotal.com**.
3. Проанализируйте отчет. Сколько антивирусных движков определили файл как вредоносный?
4. Сделайте скриншот отчета.

Контрольные вопросы:

1. В чем отличие вируса от червя?
2. Как работает эвристический анализ?
3. Почему антивирус может блокировать работу легальной, но "подозрительно" ведущей себя программы?

Лабораторная работа № 6

Сетевая безопасность. Межсетевые экраны

Цель работы: изучить принципы функционирования межсетевых экранов (брандмауэров) и научиться создавать правила фильтрации трафика для обеспечения безопасности сети.

Подготовка к работе: изучить теоретический материал и конспект лекций по теме.

Краткие теоретические сведения

Межсетевой экран (МЭ), брандмауэр, фаервол — это программный или программно-аппаратный комплекс, который контролирует и фильтрует сетевой трафик, проходящий через него, в соответствии с заданными правилами. Основная цель — защита сети или отдельного компьютера от несанкционированного доступа.

Принципы работы:

МЭ анализирует заголовки сетевых пакетов (IP-адреса, порты, протоколы) и, реже, их содержимое.

На основе набора правил принимается решение: пропустить пакет (ALLOW), заблокировать (DENY) или выполнить другое действие.

Типы межсетевых экранов:

Пакетные фильтры: Анализируют каждый пакет изолированно, на основе статических правил.

Stateful-фильтры (с отслеживанием состояния): Отслеживают состояние соединений (TCP-сессий). Они помнят, какой компьютер инициировал соединение, и пропускают только те пакеты, которые являются ответами на разрешенные запросы. Это более безопасный и интеллектуальный подход.

Прокси-серверы (шлюзы прикладного уровня): Выступают посредниками между клиентом и сервером, анализируя трафик на уровне приложений (HTTP, FTP). Могут проверять содержимое пакетов, блокировать опасные команды, но работают медленнее.

Правила фильтрации обычно строятся на основе критериев:

- Направление (входящее/исходящее соединение).
- IP-адрес источника и назначения.
- Порт источника и назначения (например, порт 80 для web-трафика, 25 для почты).
- Протокол (TCP, UDP, ICMP).

Задания для выполнения:

Задание 1. Изучение настроек встроенного брандмауэра Windows Defender.

1. Откройте «Панель управления» -> «Брандмауэр Защитника Windows».
2. Посмотрите состояние брандмауэра для частных и гостевых/общественных сетей. Включен ли он?
3. Перейдите в «Дополнительные параметры». Откроется оснастка «Брандмауэр в режиме повышенной безопасности».
4. Изучите структуру: «Правила для входящих подключений», «Правила для исходящих подключений».

Задание 2. Анализ существующих правил.

1. В оснастке откройте «Правила для входящих подключений».

2. Найдите в списке правила для служб «Удаленный помощник» и «Общий доступ к файлам и принтерам».
3. Дважды щелкните по любому правилу и изучите его свойства на вкладках «Общие», «Протоколы и порты», «Область действия». Определите, какие порты и протоколы оно разрешает.
4. Запишите в тетрадь параметры одного из правил.

Задание 3. Создание блокирующего правила.

1. Создайте правило, блокирующее весь исходящий трафик для программы браузера (например, chrome.exe или firefox.exe).

Действие: Нажмите правой кнопкой на «Правила для исходящих подключений» -> «Создать правило...».

Тип правила: «Для программы».

Путь: Укажите путь к исполняемому файлу браузера (например, C:\Program Files\Mozilla Firefox\firefox.exe).

Действие: «Блокировать подключение».

Профиль: Оставьте все (Доменный, Частный, Публичный).

Имя: Дайте правилу имя, например "Блокировка Firefox".

2. Проверьте работу правила. Попробуйте открыть браузер и зайти на любой сайт. Удается ли это сделать?
3. Удалите созданное правило или отключите его.

Задание 4. Создание разрешающего правила для порта.

1. Создайте правило, разрешающее входящие подключения на TCP-порт 3389 (порт службы удаленного рабочего стола RDP). *Внимание: Оставлять это правило включенным без необходимости опасно.*

Тип правила: «Для порта».

Протокол: TCP.

Порт: 3389.

Действие: «Разрешить подключение».

Имя: "Разрешить RDP".

Контрольные вопросы:

1. В чем разница между блокировкой программы и блокировкой порта?
2. Что такое Stateful-фильтрация?
3. Почему не рекомендуется без необходимости открывать порты в брандмауэре?

Основная литература:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 30.01.2024) // Собрание законодательства Российской Федерации. — 2006. — № 52 (1 ч.). — Ст. 5496. — Гл. 70.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.10.2024) // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954. — Гл. 28.

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изм. и доп.).

6. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

7. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

8. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

10. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст). — М.: Стандартинформ, 2008. — 12 с.