

Практическая работа №1 (ПАЗИ)

Тема: Ознакомление и работа с основными нормативно-правовыми документами, связанными с программно-аппаратной защитой информации

Цель: Познакомиться с основными НПА по ПАЗИ, получить опыт поиска и анализа нормативных документов.

Теоретическая часть

Нормативно-правовая база Российской Федерации содержит ряд законодательных и нормативно-правовых актов, национальных стандартов и методических документов, которые связаны с требованиями к программным и программно-техническим средствам защиты информации, а также средствам обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Перечень некоторых основных документов:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Федеральный закон № 152-ФЗ от 27 июля 2006 г «О персональных данных»
4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
5. Приказ ФСТЭК России от 02.06.2020 № 76 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»
6. Приказ ФСТЭК России от 18.02.2022 № 21 «Об утверждении Требований к обеспечению безопасности информации в автоматизированных системах управления производственными и технологическими процессами»
7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
8. Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»
9. Приказ ФСТЭК России от 07.03.2023 г. № 44 об утверждении «Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети»
10. Требования к средствам обнаружения и реагирования на уровне узла. Утвержден приказом ФСТЭК России от 26 февраля 2025 г. № 58
11. Требования по безопасности информации к средствам контейнеризации. Утверждены приказом ФСТЭК России от 4 июля 2022 г. № 118
12. Приказ ФСБ России № 378 от 9 февраля 2005 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»
13. Приказ ФСБ России от 11 мая 2023 г. N 213 "Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими"

14. Приказ ФСТЭК России от 31 августа 2010 г. N 489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»
15. Приказ ФСТЭК России от 14 марта 2014 года №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
16. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
17. ГОСТ Р 51624-2000 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности».
18. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная безопасность. Системы менеджмента информационной безопасности. Требования
19. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3»
20. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
21. ГОСТ Р 56939-2024. «Защита информации. Разработка безопасного программного обеспечения. Общие требования»
22. ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»
23. ГОСТ Р 53115-2008. «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства»
24. ГОСТ Р 56546-2015. «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»
25. ГОСТ Р 58412-2019. «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»
26. ГОСТ Р 58142-2018. «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей»
27. ГОСТ Р 58143-2018. «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения»
28. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»
29. Методика построения модели угроз (ФСТЭК России) утверждена 5 февраля 2021 года. Документ называется «Методический документ. Методика оценки угроз безопасности информации»
30. Методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств». ФСТЭК 30.06.2025

Практическая часть

1. В соответствии с вариантом найдите в справочно-правовой системе (КонсультантПлюс, Гарант или официальный сайт ведомства, сделайте скриншоты работы с системой) и изучите нормативно-правовой документ из списка, представленного в теории и ответьте на вопросы:
 - Что данный нормативный документ регламентирует (устанавливает, разъясняет)
 - Как данный документ связан с программно-аппаратными или программными средствами защиты информации (опишите кратко)
 - Если в документе имеется информация по ПАСЗИ, сделайте несколько скриншотов, подтверждающих это

- Когда в данный документ последний раз вносились изменения (скриншот для подтверждения)
2. <https://regulation.gov.ru/> - Официальный сайт для размещения информации о подготовке федеральными органами исполнительной власти проектов нормативных правовых актов и результатах их общественного обсуждения.
На данном сайте вам необходимо найти 2-3 документа связанных с защитой информации, желательно с ПАЗИ. По каждому документу (проекту НПА) кратко напишите о чём он, как связан с ПАЗИ. (желательно проекты от разных ведомств и получаемые разными поисковыми запросами)
 3. На примере межсетевых экранов попробуйте найдите существующие МЭ разных классов защиты (всего их 6). Проверьте имеются ли у них сертификаты. Отметьте какой класс встречается чаще, почему?
 4. Ответьте на контрольные вопросы (несколько вопросов устно – на выбор преподавателя)

Контрольные вопросы:

1. Какие имеются 2 основных подхода к классификации объектов защиты информации, в чём разница?
2. 3 группы АС – классификация РД АС
3. Какие выделяют основные типы информационных систем, требующих защиты информации, которая в них имеется?
4. Для чего используются уровни доверия средств защиты информации, сколько их?
5. Зачем следить за проектами нормативно-правовых документов, которые ещё не приняты?