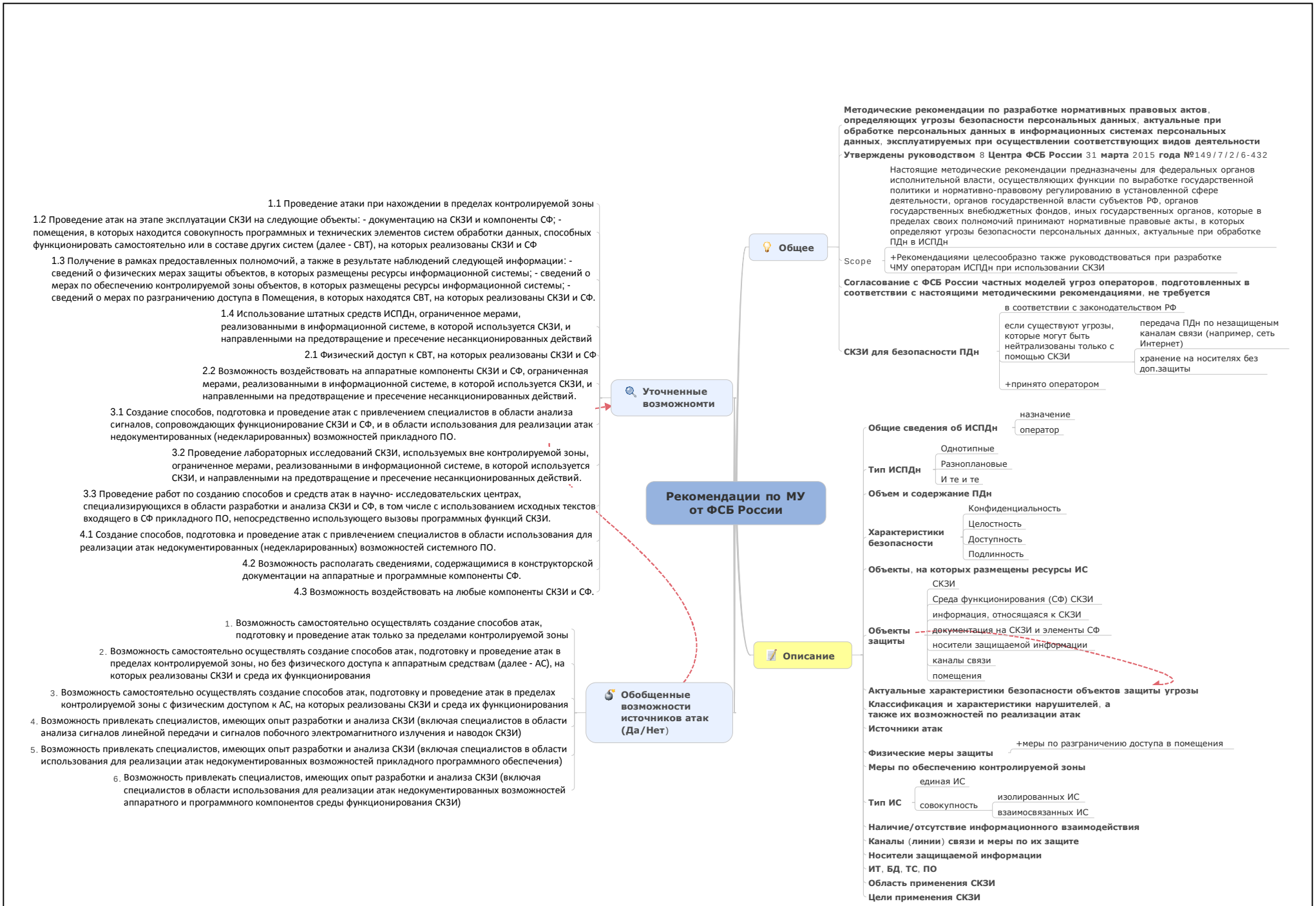
Рекомендации по МУ от ФСБ России
Общее
Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности
Утверждены руководством 8 Центра ФСБ России 31 марта 2015 года №149/7/2/6-432
Настоящие методические рекомендации предназначены для федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органов государственной власти субъектов РФ, органов государственных внебюджетных фондов, иных государственных органов, которые в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке ПДн в ИСПДн
Scope
+Рекомендациями целесообразно также руководствоваться при разработке ЧМУ операторам ИСПДн при использовании СКЗИ
Согласование с ФСБ России частных моделей угроз операторов, подготовленных в соответствии с настоящими методическими рекомендациями, не требуется
СКЗИ для безопасности ПДн
в соответствии с законодательством РФ
если существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ
передача ПДн по незащищеным каналам связи (например, сеть Интернет)
хранение на носителях без доп.защиты
+принято оператором
Уточненные возможнмти
1.1 Проведение атаки при нахождении в пределах контролируемой зоны
1.2 Проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ
1.3 Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.
1.4 Использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий
2.1 Физический доступ к СВТ, на которых реализованы СКЗИ и СФ
2.2 Возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.
3.1 Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.
3.2 Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.
3.3 Проведение работ по созданию способов и средств атак в научно- исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.
4.1 Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.
4.2 Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.
4.3 Возможность воздействовать на любые компоненты СКЗИ и СФ.
Обобщенные возможности источников атак (Да/Нет)
1. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны
2. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования
3. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования
4. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)
5. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)
6. Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)
Описание
Общие сведения об ИСПДн
назначение
оператор
Тип ИСПДн
Однотипные
Разноплановые
И те и те
Объем и содержание ПДн
Характеристики безопасности
Конфиденциальность
Целостность
Доступность
Подлинность
Объекты, на которых размещены ресурсы ИС
Объекты защиты
СКЗИ
Среда функционирования (СФ) СКЗИ
информация, относящаяся к СКЗИ
документация на СКЗИ и элементы СФ
носители защищаемой информации
каналы связи
помещения
Актуальные характеристики безопасности объектов защиты угрозы
Классификация и характеристики нарушителей, а также их возможностей по реализации атак
Источники атак
Физические меры защиты
+меры по разграничению доступа в помещения
Меры по обеспечению контролируемой зоны
Тип ИС
единая ИС
совокупность
изолированных ИС
взаимосвязанных ИС
Наличие/отсутствие информационного взаимодействия
Каналы (линии) связи и меры по их защите
Носители защищаемой информации
ИТ, БД, ТС, ПО
Область применения СКЗИ
Цели применения СКЗИ