СБЕР
КИБЕР
БЕЗОПАСНОСТЬ

DATA
PROTECTION
OFFICE

Создание системы защиты персональных данных в компании

Дата разработки: «06» апреля 2023 г.

DATA PROTECTION OFFICE

СОДЕРЖАНИЕ

1 ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АРМ
Автоматизированное рабочее место

БДУ
Банк данных угроз безопасности информации

ВИ
Виртуальная инфраструктура

ЗПДн
Защита персональных данных

ИС
Информационная система

ИСПДн
Информационная система ПДн

МУБИ
Модель угроз безопасности информации

НДВ
Недокументированные (недекларированные) возможности

НПА
Нормативные правовые акты

НСД
Несанкционированный доступ

ПДн
Персональные данные

ПО
Программное обеспечение

СЗИ
Средство защиты информации

СКЗИ
Средства криптографической защиты информации

СЗПДн
Система защиты персональных данных

СП
Структурное подразделение

УЗ
Уровень защищенности

ЧТЗ
Частное техническое задание

К ОГЛАВЛЕНИЮ

2 НПА, РЕГЛАМЕНТИРУЮЩИЕ ЗАЩИТУ ПДн

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 №149-ФЗ
«Об информации, информационных технологиях и о защите информации»

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 №152-ФЗ
«О персональных данных»

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 03.02.2012 №79
«Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации»

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 01.11.2012 №1119
«Об утверждении требований к защите персональных данных при их обработке в ИСПДн»

ПРИКАЗ ФСТЭК РОССИИ ОТ 18.02.2013 №21
«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»

ПРИКАЗ ФСТЭК РОССИИ ОТ 29.04.2021 №77
«Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
(утверждена ФСТЭК России 05.02.2021)

ПРИКАЗ ФСБ РОССИИ ОТ 10.07.2014 №378
«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из уровней защищенности»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ФСБ РОССИИ
По разработке нормативных правовых актов, определяющих угрозы безопасности ПДн, актуальные при обработке ПДн в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности
(утв. 31.03.2015 №149/7/2/6-432)

ГОСТ Р 51583
«Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

ГОСТ Р 51624
«Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»

ГОСТ 34.ххх серии
Стандарты на автоматизированные системы

К ОГЛАВЛЕНИЮ

3 ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПДн

В соответствии со статьей 19 152-ФЗ компании, обрабатывающей ПДн (в том числе по поручению оператора), обязана принять организационные и технические меры для ЗПДн, то есть **создать СЗПДн**

ЦЕЛЬ СОЗДАНИЯ СЗПДн

Обеспечение ЗПДн от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн, а также соблюдение конфиденциальности ПДн, реализация права субъекта на доступ к его ПДн

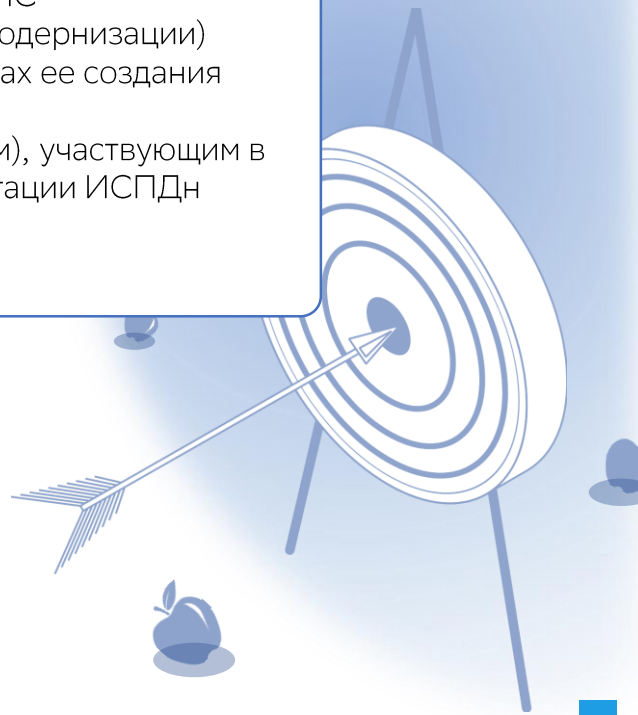
СОСТАВ ЗАДАЧ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ОПРЕДЕЛЯЕТСЯ:

- применяемыми программными и аппаратными средствами
- требованиями, предъявляемыми к обрабатываемой информации
- угрозами безопасности информации

ТРЕБОВАНИЯ К СИСТЕМЕ ЗПДн

В рамках создания СЗПДн необходимо сформировать требования к ЗПДн, а именно:

- к процессу хранения, передачи и обработки ПДн в ИСПДн
- к обеспечению соответствия СЗПДн требованиям применимых НПА
- к взаимодействию ИСПДн с иными ИС
- к содержанию работ по созданию (модернизации) ИСПДн на различных стадиях и этапах ее создания (модернизации)
- к организациям (должностным лицам), участвующим в создании (модернизации) и эксплуатации ИСПДн
- к документации на ИСПДн



К ОГЛАВЛЕНИЮ

4 КЛЮЧЕВЫЕ ЭЛЕМЕНТЫ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПДн

ДОРОЖНАЯ КАРТА СОЗДАНИЯ СЗПДн

1. **Инициация создания системы защиты ПДн**
   Концепция проекта, бизнес-обоснование
2. **Обследование ИС,**
   в которых осуществляется обработка ПДн
3. **Определение нарушителей, оценка актуальных угроз**
   безопасности ПДн
4. **Определение уровня защищенности**
5. **Определение базового набора мер и определение типов и классов СЗИ / СКЗИ**
   для нейтрализации актуальных угроз безопасности ПДн
6. **Внедрение (доработка) мер и средств защиты ПДн**
7. **Оценка эффективности принимаемых мер по защите ПДн**

ПОЧЕМУ ЭТО ВАЖНО?

Приведенная последовательность действий позволяет обеспечить структурированный и методичный подход к созданию СЗПДн

ЧТО НУЖНО УЧЕСТЬ?

Специфику бизнес-процессов и особенности требований отраслевых регуляторов, которые могут предъявлять дополнительные требования к ЗПДн (например, применение конкретных СЗИ, СКЗИ, соответствие определенному УЗ ПДн и т.п.).

КАК ЭТО СДЕЛАТЬ?

Самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации

К ОГЛАВЛЕНИЮ

5 ИНИЦИАЦИЯ СОЗДАНИЯ СИСТЕМЫ ЗАЩИТЫ ПДн

С ЧЕГО НАЧАТЬ?

Подготовить комплект документов с обоснованием необходимости создания СЗПДн

КТО РАССМАТРИВАЕТ ДОКУМЕНТЫ?

Лица, уполномоченные принимать решения о запуске проекта

РЕЗУЛЬТАТЫ РАССМОТРЕНИЯ ДОКУМЕНТОВ

Решение уполномоченных лиц о запуске проекта по созданию СЗПДн

ТАКИМ ОБРАЗОМ, ЗАПУСК ПРОЕКТА (ИЛИ ЕГО ОТКРЫТИЕ) ПРОХОДИТ В НЕСКОЛЬКО ЭТАПОВ:

1 Определение потенциальных участников проекта

2 Подготовка для руководства комплекта документов, обосновывающих необходимость создания СЗПДн, в частности:

- концепции и дорожной карты проекта
- технико-экономического обоснования (бизнес-плана)
- бюджета проекта (предварительный расчет, который корректируется при формировании технических мер ЗПДн)
- плана мероприятий проекта

3 Принятие решения о запуске проекта по созданию СЗПДн и назначении руководителя проекта (приказ, распоряжение)

Прежде чем инициировать проект, необходимо оценить целесообразность его реализации

Наиболее распространенные ошибки, которые приводят к провалу проекта:

1. нечетко определенные цели
2. отсутствие понимания применимых требований НПА
3. занижение/завышение масштаба проекта
4. отсутствие количественных критериев проекта
5. отсутствие анализа возможных рисков при реализации проекта
6. неопределенные методы и средства реализации проекта

К ОГЛАВЛЕНИЮ

6 ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ О ЗАПУСКЕ ПРОЕКТА ПРОВОДИТСЯ ОБСЛЕДОВАНИЕ ИС:

СБОР (ИССЛЕДОВАНИЕ) ИНФОРМАЦИИ О КОМПАНИИ

- организационная структура компании
- наличие внутренних документов, регламентирующих порядок обработки и ЗПДн
- территориальные площадки, схемы помещений, расположение технических средств и меры физической безопасности

ОБСЛЕДОВАНИЕ ИСПДН

- сбор и анализ данных о назначении, функциях, условиях функционирования ИС и характере обрабатываемой информации
- определение технологических процессов обработки информации
- сбор данных о структуре и составе программного и аппаратного обеспечения ИС
- сбор данных об архитектуре ИС;
- определение перечня информации, подлежащей защите;
- определение используемых средств обеспечения безопасности информации;
- интервьюирование должностных лиц, отвечающих за процессы обработки информации и эксплуатацию ИС

ПО ИТОГАМ РАБОТ ФОРМИРУЕТСЯ ОТЧЕТ (АКТ) ОБ ОБСЛЕДОВАНИИ ИСПДН

СОДЕРЖАЩИЙ СЛЕДУЮЩУЮ ИНФОРМАЦИЮ:

- общие сведения о компании
- сведенья о процессах, в рамках которых осуществляется обработка ПДн
- сводный перечень и описание ИС, задействованных в обработке ПДн
- перечень подразделений и должностных лиц, участвующих в обработке ПДн и администрировании ИСПДн
- описание архитектуры ИСПДн (состав информационных подсистем, обрабатывающих ПДн, включая, программные средства, ресурсы ИСПДн, технологии управления, перечень технических подсистем (информация о каналах связи между площадками, схемы размещения оборудования (АРМ, сервера, сетевое оборудование, СЗИ и т.п.)
- описание информационных потоков ПДн между ИС, технологическими площадками и третьими лицами
- размещение технических средств ИСПДн на площадках и с учетом мест расположения объектов компании
- состав и описание организационных и технических мер, в т.ч. СЗИ и СКЗИ, используемых для защиты ИСПДн
- описание принимаемых мер по обеспечению физической безопасности и технических средств охраны

К ОГЛАВЛЕНИЮ

7 ОЦЕНКА АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПДн

РЕЗУЛЬТАТ ОБСЛЕДОВАНИЯ

По результатам обследования ИС необходимо сформировать требования к ЗПДн

УСЛОВИЯ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ

При создании (доработке) СЗПДн необходимым условием формирования обоснованных требований к ЗПДн является оценка актуальных угроз безопасности ПДн. По результатам оценки актуальных угроз безопасности формируется МУБИ. Формирование МУБИ проводится по методическим документам ФСБ России и ФСТЭК России

ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПДН ВКЛЮЧАЕТ СЛЕДУЮЩИЕ ЭТАПЫ:

Перечень этапов	Наименование этапа	Задачи
Первый этап	Определение негативных последствий	✓ Анализ документации систем и сетей и иных исходных данных ✓ Определение негативных последствий от реализации угроз
Второй этап	Определение объектов воздействия	✓ Анализ документации систем и сетей и иных исходных данных ✓ Инвентаризация систем и сетей ✓ Определение групп информационных ресурсов и компонентов систем и сетей
Третий этап	Оценка возможности реализации угроз и их актуальности	✓ Определение источников угроз ✓ Оценка способов реализации угроз ✓ Оценка актуальности угроз

Оценка актуальных угроз безопасности проводится экспертным методом. Для объективности получаемой оценки рекомендуется создавать экспертную группу

В рабочую группу должны привлекаться:
- ✓ специалисты по информационной безопасности
- ✓ специалисты ИТ
- ✓ владельцы АС
- ✓ представители владельцев бизнес процессов

Привлекаемые эксперты должны обладать независимостью, отсутствием коммерческого и финансового интереса который может оказать влияние на принимаемые решения.

Порядок формирования экспертной группы по проведению оценки определен в Приложении 2 Методического документа ФСТЭК

МУБИ ДОЛЖНА СОДЕРЖАТЬ:

- общее описание ИСПДн;
- перечень негативных последствий, которые могут наступить при реализации (возникновения) угроз безопасности ПДн;
- перечень ИС и возможных объектов воздействия;
- перечень источников угроз безопасности ПДн и определение возможностей нарушителей;
- способы реализации угроз безопасности ПДн и оценка возможности возникновения угроз безопасности ПДн и их актуальность;
- тип актуальных угроз, в том числе НДВ и сценарии их реализации.

ИСХОДНЫЕ ДАННЫЕ ДЛЯ ФОРМИРОВАНИЯ МУБИ:

- Банк данных угроз ФСТЭК (https://bdu.fstec.ru/)
- Описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.)

К ОГЛАВЛЕНИЮ

7 ОПРЕДЕЛЕНИЕ НАРУШИТЕЛЕЙ

ЧТО НУЖНО СДЕЛАТЬ?

Определить потенциальных нарушителей безопасности, изучить возможности нарушителей по способам подготовки и проведения атак

КТО ПРИЗНАЕТСЯ НАРУШИТЕЛЕМ?

Лицо, проводящее атаку на объекты компании

Нарушители признаются **актуальными**, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для компании негативным последствиям и соответствующим рискам (видам ущерба) нарушения безопасности.

Уровень возможностей нарушителя	Описание возможностей нарушителя	Вид (тип) нарушителя	Категория нарушителя
Нарушитель, обладающий базовыми возможностями	Нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	✓ Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) ✓ Авторизованные пользователи систем и сетей	Внутренний
		✓ Физическое лицо (хакер) ✓ Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем ✓ Бывшие работники	Внешний
Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.	✓ Поставщики вычислительных услуг, услуг связи ✓ Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ ✓ Системные администраторы и администраторы безопасности	Внутренний
		✓ Преступные группы (два лица и более, действующие по единому плану) ✓ Конкурирующие организации	Внешний
Нарушитель, обладающий средними возможностями	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.	✓ Разработчики программных, программно-аппаратных средств	Внутренний
		✓ Террористические, экстремистские группировки	Внешний
Нарушитель, обладающий высокими возможностями	Обладают всеми возможностями нарушителей со средними возможностями. Нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием НДВ, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.	✓ Специальные службы иностранных государств	Внешний

Специальные службы иностранных государств и террористические, экстремистские группировки могут привлекать внутренних нарушителей, в том числе обладающих привилегированными правами доступа, а также входить с ними в сговор

В этом случае уровень возможностей актуальных нарушителей будет определяться совокупностью возможностей нарушителей, входящих в сговор

К ОГЛАВЛЕНИЮ

7 ОПРЕДЕЛЕНИЕ ТИПА АКТУАЛЬНЫХ УГРОЗ

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 01.11.2012 №1119
«Об утверждении требований к защите персональных данных при их обработке в ИСПДн»

Установлено **три типа актуальных угроз безопасности ПДн** - совокупности условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в ИС, копирование, предоставление, распространение ПДн результатом которого могут стать уничтожение, изменение, блокирование

АКТУАЛЬНОСТЬ УГРОЗ, СВЯЗАННЫХ С НДВ, ЗАВИСИТ ОТ ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЯ, ЕГО МОТИВАЦИИ И ЦЕННОСТИ ДАННЫХ В ИС

Реализация угроз 1-го и 2-го типа возможна за счет наличия **уязвимостей** в используемом системном и прикладном ПО соответственно

При этом под уязвимостью понимаются НДВ ПО, которые могут быть использованы для реализации угрозы безопасности ПДн

Угрозы 1-го и 2-го типа актуальны в случае:
- ✓ ошибок при проектировании и разработке ПО;
- ✓ возможности преднамеренных действия по внесению уязвимостей в ходе проектирования и разработки ПО

При определении типов угроз, необходимо учитывать следующие условия:
- ✓ реализация технических мер защиты, направленных на обеспечение безопасности ПДн;
- ✓ возможность негативных последствий для субъектов ПДн от возможной реализации угроз 1-го и 2-го типа.

УГРОЗЫ 1-ГО ТИПА

Актуальны для информационной системы, если для нее актуальны угрозы, связанные с наличием **недокументированных возможностей в системном ПО**, используемом в информационной системе

УГРОЗЫ 2-ГО ТИПА

Актуальны для информационной системы, если для нее актуальны угрозы, связанные с наличием **недокументированных возможностей в прикладном ПО**, используемом в информационной системе

УГРОЗЫ 3-ГО ТИПА

Актуальны для информационной системы, если для нее актуальны угрозы, **не связанные** с наличием **недокументированных возможностей в системном и прикладном ПО**, используемом в информационной системе

К ОГЛАВЛЕНИЮ

8 ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ

ЧТО НУЖНО СДЕЛАТЬ?

Определить набор организационных и технических мер по обеспечению безопасности ПДн и установить УЗ ПДн, влияющий на перечень мер установленных НПА

ЧТО НУЖНО СДЕЛАТЬ ДЛЯ ОПРЕДЕНИЯ УЗ ПДн?

Составом комиссии определить и утвердить приказом (распоряжением) руководителя компании УЗ ПДн

В комиссию должны входить владельцы процессов и ИС, а так же эксперты, которые участвовали в определении актуальных угроз безопасности ПДн

Уровень защищенности определяется для каждой ИСПДн по результатам сбора и анализа исходных данных, представленных в Отчете (акте) об обследовании ИС и МУБИ. Допустимо определять уровень защищенности по группе ИСПДн, имеющих схожие характеристики и категории обрабатываемой информации

Результаты определения УЗ оформляются актом, содержащим характеристики ИСПДн:

- ✓категории обрабатываемых ПДн
- ✓количество субъектов ПДн, обрабатываемых в ИСПДн
- ✓тип угроз безопасности ПДн, актуальных для ИСПД.

Акт утверждается руководителем компании и хранится у владельца ИСПДн

На основе результатов определения УЗ формируется набор мер ЗПДн в соответствии с Приказом 21 ФСТЭК, ПП 1119 и, в случае применения СКЗИ, Приказом 378 ФСБ

Детализированная таблица определения УЗ отражена на следующем слайде

Пример Акта определения УЗ

Утверждаю
Директор_____
«__» _____2023 г.

АКТ № __
определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных _____

В соответствии с п.8 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 №1119, комиссия в составе:

	Должность / ФИО
Председатель	
Члены комиссии	

рассмотрев «Модель угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных «_____», а также учитывая исходные данные на информационную систему персональных данных «_____»:

Тип актуальных угроз: Угрозы ___ типа

Категории персональных данных, обрабатываемых в информационной системе персональных данных _____

Субъекты, персональные данные которых обрабатываются в информационной системе _____

Объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) _____

РЕШИЛА:

В соответствии с п.___ «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 №1119, установить для информационной системы персональных данных «_____» необходимость обеспечения **_____-го уровня защищенности персональных данных.**

	Подпись	**Должность / ФИО**
Председатель		
Члены комиссии		

К ОГЛАВЛЕНИЮ

8 ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 01.11.2012 №1119
«Об утверждении требований к защите персональных данных при их обработке в ИСПДн»

ПРИ ОБРАБОТКЕ ПДН В ИСПДН УСТАНАВЛИВАЮТСЯ 4 УЗ ПДН:

УЗ 1 – максимальные требования к уровню защищенности,
УЗ 4 – минимальные требования к уровню защищенности.

Чем выше УЗ, тем больше мер, определенных Приказом 21 ФСТЭК необходимо реализовать. Описание реализовываемых мер включается в ЧТЗ

Уровень защищенности ПДн при их обработке в ИСПДн определяется в зависимости от следующих параметров:

- категория ПДн (специальные, биометрические, общедоступные, иные)
- категория субъектов ПДн (сотрудников, не сотрудников)
- количество обрабатываемых ПДн (более 100 000, менее чем 100 000)
- тип актуальных угроз (1-й, 2-й, 3-й)

КРИТЕРИИ ОПРЕДЕЛЕНИЯ УЗ ПДН УКАЗАНЫ В ТАБЛИЦЕ:

Категория ПДн и количество субъектов	1 тип актуальных угроз	2 тип актуальных угроз	3 тип актуальных угроз
Специальные категории ПДн более чем 100 000 субъектов ПДн, не сотрудников оператора	1	1	2
Специальные категории ПДн менее чем 100 000 субъектов ПДн, не сотрудников оператора	1	2	3
Специальная категории ПДн сотрудников оператора	1	2	3
Биометрические ПДн	1	2	3
Иные категории ПДн более чем 100 000 субъектов ПДн, не сотрудников оператора	1	2	3
Иные категории ПДн сотрудников оператора	1	3	4
Иные категории ПДн менее чем 100 000 субъектов ПДн, не сотрудников оператора	1	3	4
Общедоступные ПДн более чем 100 000 субъектов ПДн, не сотрудников оператора	2	2	4
Общедоступные ПДн сотрудников оператора	2	3	4
Общедоступные ПДн менее чем 100 000 субъектов ПДн, не сотрудников оператора	2	3	4

К ОГЛАВЛЕНИЮ

9 ОПРЕДЕЛЕНИЕ БАЗОВОГО НАБОРА МЕР

По результатам оценки угроз безопасности ПДн и определения УЗ ПДн формируются организационные и технические меры, которые компания должна внедрить (модернизировать) для СЗПДн, **при этом необходимо учитывать требования указанные в различных НПА**

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 №152-ФЗ

«О персональных данных»

- применение прошедших процедуру оценки соответствия СЗИ (определение типов и классов СЗИ) **приведены на следующем слайде**
- оценка эффективности принимаемых мер обеспечения безопасности ПДн до ввода ИС в эксплуатацию
- учет носителей ПДн
- обнаружение фактов несанкционированного доступа (далее - НСД), обнаружение, предупреждение и ликвидация последствий компьютерных атак
- восстановление ПДн, модифицированных или уничтоженных при НСД
- установление правил доступа к ПДн
- контроль за применяемыми мерами по обеспечению безопасности ПДн и УЗ
- организация информирования о фактах компьютерных инцидентов с ПДн

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ ОТ 01.11.2012 №1119

«Об утверждении требований к защите персональных данных при их обработке в ИСПДн»

- организация режима безопасности помещений и контроля доступа
- обеспечение сохранности носителей ПДн
- определение перечня лиц, допущенных к ПДн
- назначение должностного лица (подразделения), ответственного за обеспечение безопасности ПДн
- ограничение доступа к ведению электронных журналов

ПРИКАЗ ФСБ РОССИИ ОТ 10.07.2014 №378

«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн…»

- организация режима обеспечения безопасности помещений
- обеспечение сохранности ПДн
- утверждение перечня лиц, допущенных к ПДн
- использование СКЗИ, прошедших процедуру оценки соответствия требованиям законодательства, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

ПРИКАЗ ФСТЭК РОССИИ ОТ 18.02.2013 №21

«Об утверждении Состава и содержания организационных и технических мер…»

- идентификация и аутентификация субъектов доступа и объектов доступа
- управление доступом субъектов доступа к объектам доступа
- ограничение программной среды
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн
- регистрация событий безопасности
- антивирусная защита
- обнаружение (предотвращение) вторжений
- контроль (анализ) защищенности ПДн
- обеспечение целостности ИС и ПДн
- обеспечение доступности ПДн
- защита среды виртуализации
- защита технических средств
- защита ИС, ее средств, систем связи и передачи данных
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ПДн, и реагирование на них
- управление конфигурацией ИС и СЗПДн

К ОГЛАВЛЕНИЮ

10 ОПРЕДЕЛЕНИЕ ТИПОВ И КЛАССОВ СЗИ / СКЗИ

ЧТО ТРЕБУЕТСЯ ДЛЯ НЕЙТРАЛИЗАЦИИ АКТУАЛЬНЫХ УГРОЗ?

Использовать СЗИ/СКЗИ прошедшие процедуру оценки соответствия в соответствии с законодательством по обеспечению безопасности информации в форме обязательной или добровольной сертификации (декларирования соответствия)

ТРЕБОВАНИЯ К СЗИ/СКЗИ

При использовании сертифицированных по требованиям безопасности информации СЗИ и СКЗИ для обеспечения необходимого УЗ ПДн, а также с учетом типа актуальных угроз, указанные средства должны соответствовать **следующим классам защиты**

КЛАССЫ СЗИ В СООТВЕТСТВИИ С ПРИКАЗОМ 21 ФСТЭК

УЗ ПДн	Средства вычислительной техники	Средства защиты информации	Уровень доверия
1 уровень	5+	4+	4
2 уровень	5+	5+	5
3 уровень	5+	6	6
4 уровень	6+	6	6

КЛАССЫ СЗИ В СООТВЕТСТВИИ С ПРИКАЗОМ 378 ФСБ

УЗ ПДн	1 тип актуальных угроз	2 тип актуальных угроз	3 тип актуальных угроз
1 уровень	КА	КВ2+	-
2 уровень	КА	КВ2+	КС1+
3 уровень	-	КВ2+	КС1+
4 уровень	-	-	КС1+

ПЕРЕЧНИ СЕРТИФИЦИРОВАННЫХ СЗИ/СКЗИ РАЗМЕЩЕНЫ В СООТВЕТСТВУЮЩИХ РЕЕСТРАХ:

РЕЕСТР СЕРТИФИЦИРОВАННЫХ СЗИ

ПЕРЕЧЕНЬ СЕРТИФИЦИРОВАННЫХ СКЗИ

К ОГЛАВЛЕНИЮ

11 РАЗРАБОТКА ЧАСТНОГО ТЕХНИЧЕСКОГО ЗАДАНИЯ

ЧТО ТРЕБУЕТСЯ ДЛЯ ФИКСАЦИИ ИТОГОВЫХ ТРЕБОВАНИЙ?

Разработать ЧТЗ и включить в него итоговые требования по ЗПДн

ЧТЗ РАЗРАБАТЫВАЕТСЯ НА ОСНОВЕ МУБИ И ВКЛЮЧАЕТ В СЕБЯ:

- описание характеристик защищаемой ИСПДн
- требования к СЗПДн в целом и ее подсистемам
- требования к видам обеспечения ИТ/СЗИ (поддержки, поставщикам)
- требования, направленные на оптимизацию устройств, обрабатывающих ПДн в ИСПДн (минимизация АРМ и серверов, обрабатывающих ПДн, ограничение внешних подключений т.п.)
- состав и содержание выполняемых работ по созданию СЗПДн
- порядок контроля проектирования и внедрения СЗПДн;
- требования к составу и содержанию работ по подготовке СЗПДн к вводу в эксплуатацию

РЕКОМЕНДУЕМАЯ СТРУКТУРА ЧТЗ:

1. **Общие положения**
   - Назначение проектируемой СЗПДн
   - Перечень организаций, участвующих в разработке СЗПДн (в случае привлечения)
   - Этапы и сроки выполнения работ
   - Перечень нормативных и технических документов, на основании которых осуществляется проектирование СЗПДн
2. **Описание ИСПДн**
3. **Требования СЗПДн**
   - Результаты моделирования угроз безопасности
   - Требования к структуре СЗПДн, подсистемам СЗПДн, средствам и способам защиты ПДн
   - Требования к численности, квалификации и функциям обслуживающего персонала СЗПДн, режимам его работы, порядку взаимодействия
   - Требования к режимам функционирования, диагностированию работы СЗПДн
4. **Порядок контроля и приемки СЗПДн**
   - Требования к проведению приёмочных испытаний СЗПДн
5. **Требования к подготовке ИСПДн к вводу СЗПДн в действие**
   - Требования по обучению и проверке квалификации персонала
   - Требования по созданию необходимых подразделений и рабочих мест (при необходимости)
6. **Требования к документированию**
   - Требования к составу внутренней документации на СЗПДн

ЧТЗ должно быть согласовано с СП, участвующими в обработке ПДн (владельцами бизнес-процессов, подразделениями ИТ, разработки ПО и т.п.)

К ОГЛАВЛЕНИЮ

12 ВНЕДРЕНИЕ (ДОРАБОТКА) МЕР И СРЕДСТВ ЗАЩИТЫ ПДН

НА ОСНОВАНИИ РАЗРАБОТАННОГО ЧТЗ НЕОБХОДИМО ОСУЩЕСТВИТЬ ВНЕДРЕНИЕ МЕР ЗАЩИТЫ И СЗИ/СКЗИ

На данном этапе происходит внедрение технических мер защиты, а также уточнение и разработка (доработка) необходимых документов определяющих порядок эксплуатации СЗПДн

НА ЭТАПЕ ВНЕДРЕНИЯ СЗИ/СКЗИ

- осуществляется поставка (закупка) СЗИ/СКЗИ;
- создается пилотная зона ИСПДн (выбор групп АРМ, сетевого оборудования и т.п. для первичной тестовой установки) с целью тестирования функций СЗИ/СКЗИ;
- осуществляется установка, настройка СЗИ/СКЗИ;
- проводятся стендовые испытания на пилотной зоне;
- осуществляется тиражирование решений на всю ИТ ИСПДн;
- проводятся приемо-сдаточные испытания СЗПДн;
- оформляется документация по результатам установки и настройки СЗИ/СКЗИ (актов установки (внедрения) СЗИ, журналов учета СЗИ/ СКЗИ, формуляров на поставленные СЗИ/СКЗИ (при наличии));
- осуществляется корректировка (при необходимости) ЧТЗ и выработка дополнительных мер, если по результатам приемочных испытаний будут выявлены отклонения (ошибки, неточности) в выработанных ранее мерах ЗПДн.

НА ЭТАПЕ РАЗРАБОТКИ (ДОРАБОТКИ) И УТВЕРЖДЕНИЯ ДОКУМЕНТОВ

- определяются обязанности и описываются процедуры, выполняемые администратором безопасности по управлению (администрированию), аварийному восстановлению СЗПДн и управлению изменениями в ней;
- определяются обязанности и описываются процедуры, выполняемые пользователями в рамках созданной СЗПДн, а также правила и процедуры использования СЗИ/ СКЗИ;
- требования к ЗПДн, реализуемые СЗПДн, включаются в политику/ положение об обеспечении безопасности ПДн, обрабатываемых в ИСПДн;
- формируются (актуализируются) перечни лиц, допущенных к обработке ПДн в ИСПДн, а также имеющих право доступа в помещения, где размещены СКЗИ;
- руководителем компании подписывается приказ (распоряжение) о вводе системы СЗПДн в эксплуатацию.

К ОГЛАВЛЕНИЮ

13 ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИНИМАЕМЫХ МЕР ПО ЗАЩИТЕ ПДН

По завершении этапа внедрения (доработки) мер и средств ЗПДн, до ввода в эксплуатацию ИСПДн проводится **оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн**

В последующем указанная оценка проводится не реже одного раза в 3 года

ОСНОВНЫЕ МЕРОПРИЯТИЯ, ПРОВОДИМЫЕ В РАМКАХ ЭТАПА:

1. анализ структуры ИСПДн и технологического процесса обработки ПДн;
2. оценка достаточности разработанных внутренних документов и соответствия их содержания требованиям по безопасности ПДн;
3. оценка корректности определения уровней защищенности ПДн и мер защиты;
4. оценка соответствия состава и структуры программно-технических средств ИСПДн представленной документации;
5. оценка состояния организации работ и выполнения организационно-технических требований по ЗПДн;
6. оценка достаточности мер физической охраны технических средств ИСПДн и СЗИ/ СКЗИ;
7. оценка уровня подготовки кадров и распределения ответственности персонала

В случае выявления несоответствия ИСПДн установленным требованиям по ЗПДн необходимо разработать план по устранению выявленных несоответствий

При этом могут применяться следующие меры:

- доработка внутренней документации, регламентирующей обработку и ЗПДн
- изменение архитектуры ИСПДн, конфигурации оборудования и сети
- внесение дополнительных настроек в СЗПДн и изменение рабочей и эксплуатационной документации
- применение дополнительных организационно-технических мер ЗПДн
- применение дополнительных СЗИ

По результатам оценки оформляется заключение (акт), которое(ый) хранится у владельца ИСПДн

К заключению прилагаются протоколы оценки по конкретным зонам (участкам) ИСПДн, подтверждающие полученные результаты и обосновывающие приведенный в заключении вывод

Протоколы подписываются экспертами – членами комиссии, проводившими оценку ИСПДн

ОЦЕНКА МОЖЕТ ПРОВОДИТЬСЯ:

- **самостоятельно или с привлечением на договорной основе** юридического лица или индивидуального предпринимателя, имеющего лицензию на осуществление деятельности по технической защите конфиденциальной информации;
- **в виде добровольной аттестации** ИСПДн в соответствии с Приказом ФСТЭК России от 29.02.2021 № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

К ОГЛАВЛЕНИЮ

SBER PRIVACY JOURNAL

Первое издание в России, посвящённого персональным данным и приватности, которое выпускают специалисты Сбербанка

SBER BANK PRIVACY

Узнайте больше о том, как Банк обрабатывает и защищает персональные данные

КИБРАРИЙ. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Что нужно для того, чтобы минимизировать риски, связанные с обработкой персональных данных?