

Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Тема 1.2. Стандарты безопасности

— Я хочу знать всё,
что нужно знать про
компьютерную
безопасность



— Готово.



— Оу...



— О, Боже!



@SKELETON-CLAW

План занятия

1. Введение
2. ФЗ 149, ГОСТ Р 50922-2006
3. СТР-К и РД АС
4. Приказы ФСТЭК и ФСБ РФ
5. Общие требования законодательства по ПАСЗИ
6. Общие требования к безопасности СЗИ

Введение

Существуют два основных подхода для обеспечения информационной безопасности.

1. Фрагментарный подход.

Характеризуется высокой избирательностью и высокой скоростью внедрения.

Основной недостаток: медленная актуализация защиты, потому что любое изменение структуры систем или актуальных угроз приводит к снижению эффективности системы защиты информации.

Введение

Существуют два основных подхода для обеспечения информационной безопасности.

2. Комплексный подход.

Характеризуется охватом всей инфраструктуры компании и низкой скоростью внедрения. Этот подход объединяет разнородные методы и средства защиты и предполагает внедрение менеджмента информационной безопасности.

Соответственно для поддержания информационной безопасности в надлежащем состоянии рекомендуется применять комплексный подход к построению системы защиты.

Введение

Основной и самой важной базой для построения информационной безопасности является надлежащее организационно-правовое обеспечение.

На его основе происходит построение программных, программно-аппаратных и аппаратных систем защиты информации.



Введение

В последнее время становится популярной тенденция применения комплексного подхода к защите информации и использования многоуровневой модели защиты. Успешная реализация комплексного подхода и многоуровневой модели защиты информации базируется на эффективной политике информационной безопасности, которая обеспечивает непротиворечивость и взаимосвязанность всех элементов и систем защиты информационных и автоматизированных систем.

Политика информационной безопасности компаний в своем построении должна опираться на требования нормативно-правовых актов государства и регуляторов в сфере информационной безопасности, а также учитывать положительный мировой опыт в данной области.

Введение

Государственные организации публикуют документы, которые определяют вопросы регулирования использования информационных систем и распространения информации с целью недопущения противоправных действий, наносящих ущерб другим участникам информационного обмена, обществу и государственным органам. Этот уровень документации является обязательным.

Глобальные ИТ-компании разрабатывают методологическое обеспечение с целью эффективного использования своих популярных продуктов, в том числе с учетом вопросов информационной безопасности.

1. ФЗ 149, ГОСТ Р 50922-2006

Основные нормативно-правовые акты Российской Федерации, которые вводят понятия «защита информации» и «виды защиты информации», а также определяют цели защиты информации:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»

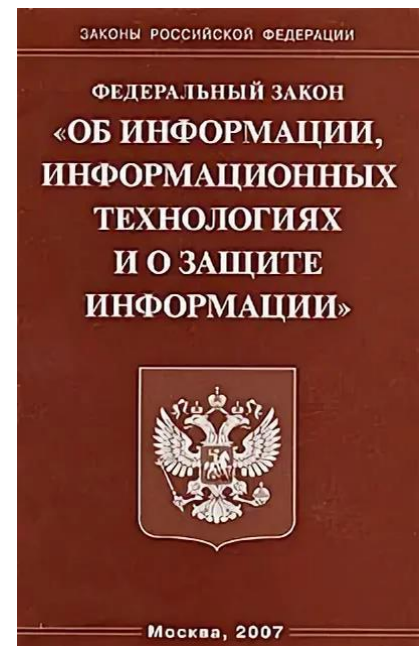
1. ФЗ 149, ГОСТ Р 50922-2006

Федеральный закон № 149-ФЗ гласит, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

- 1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- 2) соблюдение конфиденциальности информации ограниченного доступа;
- 3) реализацию права на доступ к информации.

1. ФЗ 149, ГОСТ Р 50922-2006

Таким образом, 149-ФЗ устанавливает, что процесс защиты информации направлен на защиту конфиденциальности, целостности и доступности информации путем применения правовых, организационных и далее технических мер.



1. ФЗ 149, ГОСТ Р 50922-2006

В соответствии с ГОСТ Р 50922–2006 существует четыре вида защиты информации: правовая, техническая, криптографическая и физическая.

- Правовая защита информации включает в себя разработку законодательных и нормативных документов, которые регулируют отношения субъектов в области информационной безопасности, а также обязательность применения этих документов и контроль их исполнения.
- Техническая защита информации направлена на применение технических, программных и программно-технических средств для защиты информации без криптографических преобразований в соответствии с действующим законодательством

2. Подходы к классификации объектов защиты

Выбор мер защиты информационных и автоматизированных систем (ИС, АС) регламентируется в зависимости от категории объекта защиты, при этом в настоящее время в РФ существует два подхода к классификации объектов защиты.



2. Подходы к классификации объектов защиты

Первый подход основан на документах:

«Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее – СТР-К)

РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования о защите информации» (далее – РД АС),

где установлены классы защищенности АС и выбор мер защиты опирается на класс защищенности АС.

Этот подход не учитывает структурно-функциональные особенности объектов защиты

2. Подходы к классификации объектов защиты

Второй подход основан на приказах Федеральной службы по техническому и экспортному контролю (ФСТЭК России) № 17, 21, 31, 239, 489 и приказе Федеральной службы безопасности (ФСБ России) № 378. **Приказ ФСТЭК 117**.

В соответствии с приказами ФСТЭК России ИС и АС подразделяются на:

1. информационные системы персональных данных (ИСПДн),
2. автоматизированные системы управления технологическими процессами (АСУ ТП),
3. государственные и муниципальные информационные системы (ГИС и МИС),
4. значимые объекты критической информационной инфраструктуры (ЗО КИИ),
5. информационные системы общего пользования (ИС ОП).

2. Подходы к классификации объектов защиты

Каждый из типов систем имеет свою классификацию по классам защищенности или категории значимости, которые влияют на выбор мер защиты. Приказ ФСБ России также устанавливает требования к мерам защиты, использующим криптографические преобразования.

3. СТР-К и РД АС

Классификация объекта информатизации осуществляется на основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утвержден решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.) [8].

Определяющие признаки при классификации объекта информатизации:

- наличие в объекте информатизации сведений различной степени конфиденциальности;
- режим обработки данных (коллективный, индивидуальный);
- различие полномочий доступа субъектов к защищаемой информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала. Всего имеется три группы АС: первая, вторая и третья.

3. СТР-К и РД АС

Третья группа АС – это АС, где работает единственный пользователь. Этот пользователь имеет доступ ко всей информации, которая имеет один уровень конфиденциальности. Группа содержит два класса: 3А и 3Б. Класс 3А – это класс АС, обрабатывающих информацию, составляющую государственную тайну; 3Б – класс АС, обрабатывающих информацию, не составляющую государственную тайну.

Вторая группа АС – это АС, в которых работает несколько пользователей, имеющих одинаковый доступ ко всей информации с одним уровнем конфиденциальности. Группа содержит два класса: 2А и 2Б. Класс 2А – это класс АС, обрабатывающих информацию, составляющую государственную тайну; 2Б – класс АС, обрабатывающих информацию, не составляющую государственную тайну.

3. СТР-К и РД АС

Первая группа АС – это АС, в которых работает несколько пользователей. Информация, обрабатываемая такой АС, имеет разные уровни конфиденциальности, и каждый пользователь имеет доступ не ко всей информации. Группа содержит пять классов:

1А – класс АС, обрабатывающих информацию, составляющую государственную тайну с грифом «Особая важность»;

1Б – класс АС, обрабатывающих информацию, составляющую государственную тайну с грифом не выше «Совершенно секретно»;

1В – класс АС, обрабатывающих информацию, составляющую государственную тайну с грифом не выше «Секретно»;

1Г – класс АС, обрабатывающих информацию, не составляющую государственную тайну и относящуюся к группе служебной тайны;

1Д – класс АС, обрабатывающих информацию, не составляющую государственную тайну и относящуюся к группе персональных данных.

3. СТР-К и РД АС

В целях повышения уровня защищенности информации рекомендуется использовать средства вычислительной техники (СВТ), сертифицированные по требованиям безопасности информации.

При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ согласно руководящему документу [28]:

- не ниже четвертого класса – для класса защищенности АС 1В;
- не ниже третьего класса – для класса защищенности АС 1Б;
- не ниже второго класса – для класса защищенности АС 1А.

СТР-К [7] устанавливает меры защиты, которые необходимо применять для каждого из классов защищенности АС.

Третья группа

АС, в которых работает *один пользователь*, допущенный *ко всей информации* АС, размещенной на носителях одного уровня конфиденциальности

3 А

информация,
составляющая гостайну

3 Б

служебная тайна
или персональные данные

Вторая группа

АС, в которых *пользователи имеют одинаковые права доступа* (полномочия) *ко всей информации* АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности

2 А

информация,
составляющая гостайну

2 Б

служебная тайна
или персональные данные

Первая группа

многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация *разных уровней конфиденциальности* и *не все пользователи имеют право доступа ко всей информации* АС

1 А

1 Б

1 В

1 Г

1 Д

АС, в которых циркулирует информация, составляющая гостайну:
1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»

1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»

1 А - в случае обработки секретной информации с грифом «особая важность»

1 Г - АС, в которых циркулирует служебная тайна

1 Д - АС, в которых циркулируют персональные данные

3. СТР-К и РД АС

Ознакомление с документом
«Автоматизированные системы. Защита от
несанкционированного доступа к информации.
Классификация автоматизированных систем и
требования о защите информации»

<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3>

4. Приказы ФСТЭК и ФСБ РФ

В рассматриваемом подходе два регулятора (ФСТЭК России и ФСБ России) устанавливают требования к обеспечению информационной безопасности ИСПДн, АСУ ТП, ГИС и МИС, ЗО КИИ, а также ИС ОП.

При этом ФСБ России регулирует сферу применения средств крипто-графической защиты информации (СКЗИ), а ФСТЭК России регулирует все остальное, в том числе классы защищенности и категории значимости.

Перечислим приказы ФСТЭК России, регламентирующие меры защиты различных систем.

4. Приказы ФСТЭК и ФСБ РФ

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

2. 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» [10].

3. Приказ ФСТЭК России от 14 марта 2014 г. № 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» [11].

4. Приказы ФСТЭК и ФСБ РФ

4. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [12].

5. Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» [13].

Перечисленные приказы содержат набор технических и организационных мер для защиты, а также порядок выбора необходимых мер для различных систем в зависимости от категории значимости ИС или требуемого класса защищенности.

<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117>

4. Приказы ФСТЭК и ФСБ РФ

Приказ ФСБ России № 378 устанавливает классы СКЗИ. В зависимости от степени обеспечиваемой защиты СКЗИ разделяют на классы КС1, КС2, КС3, КВ1, КВ2, КА1.

Принцип разделения зависит от следующих факторов:

- комплекса инструментов нарушителя, таких как удаленный или физический доступ, привлечение специалистов в области реализации атак и наличие актуальных угроз недокументированных возможностей;
- защищаемых объектов, таких как информация, документация, компоненты информационной системы (серверы, рабочие станции, базы данных и др.);
- места проведения потенциальных атак (внутри или вне контролируемых зон).

Модели возможностей нарушителя с классами СКЗИ прописаны в Приложении к приказу ФСБ России РФ № 378 от 10.07.2014

4. Приказы ФСТЭК и ФСБ РФ

<https://www.ec-rs.ru/blog/sredstva-zashhity-informacii/kak-proveryaet-fsb-ili-pravila-pravilnoy-ekspluatatsii-skzi-dlya-zashchity-personalnykh-dannykh/>

Уровень защищенности ПДн	4 УЗ	3 УЗ		2 УЗ			1 УЗ	
Тип актуальных угроз	3	2	3	1	2	3	1	2
Минимальный класс СКЗИ	КС1	КВ	КС1	КА	КВ	КС1	КА	КВ

Уровни специальной защиты от утечки по каналам ПЭМИН	КС			КВ		КА
Уровни криптографической защиты	КС1	КС2	КС3	КВ1	КВ2	КА1
Встраивание криптосредств осуществляется	без контроля		только под контролем со стороны ФСБ России			
Встраивание криптосредства класса осуществляется организацией, имеющей соответствующую лицензию ФСБ России	не обязательно (самим пользователем при наличии лицензии ФСБ)			обязательно		
Уровни защиты от несанкционированного доступа к ПДн (классы автоматизированных систем)	АК1	АК2	АК3	АК4	АК5	АК6
Тип нарушителя (Н _і)	Н1	Н2	Н3	Н4	Н5	Н6
Н1						
Н2						
Н3						
Н4						
Н5						
Н6						

5. Общие требования законодательства по ПАСЗИ

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.

5. Общие требования законодательства по ПАСЗИ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [5].
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [15].
3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [12].
4. 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» [16].
5. Требования безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 № 119 [17].

5. Общие требования законодательства по ПАСЗИ

6. ГОСТ Р ИСО/МЭК 15408-3 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» [18].

7. ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» [19].

8. ГОСТ Р 56939–2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» [20].

9. ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» [21].

10. ГОСТ Р 53115–2008 «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства» [22].

5. Общие требования законодательства по ПАСЗИ

11. ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» [23].

12. ГОСТ Р 58412–2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения» [24].

13. ГОСТ Р ИСО/МЭК ТО 19791 «Информационные технологии. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» [25].

14. ГОСТ Р 58142–2018 «Информационные технологии. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей ПО в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей. Частичное применение MS-EQV/NEQ ISO/IEC TR 20004-1» [26].

5. Общие требования законодательства по ПАСЗИ

15. ГОСТ Р 58143–2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/ОСК 15408 и ГОСТ Р ИСО/ОСК 18045. Часть 2. Тестирование проникновения. Частичное применение MS-EQV/NEQ ISO/IEC TR 20004-2» [27].

16. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [28].

17. Методика выявления уязвимостей и недекларированных возможностей (новая редакция). Утверждена ФСТЭК России 25 декабря 2020 г. [29].

6. Общие требования к безопасности СЗИ

Для дифференциации требований по безопасности информации к средствам устанавливается шесть уровней доверия. Самый низкий – 6-й уровень, самый высокий – 1-й уровень [16].

Средства, соответствующие 6-му уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 3-й категории, в государственных информационных системах 3-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 3-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го и 4-го уровня защищенности персональных данных.

6. Общие требования к безопасности СЗИ

Уровни доверия – для средств защиты (6 уровней)

Класс защиты – для средств защиты (6 уровней)

Классы защиты СВТ – средств вычислительной техники

6. Общие требования к безопасности СЗИ

Средства, соответствующие 5-му уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 2-й категории, в государственных информационных системах 2-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2-го уровня защищенности персональных данных.

Средства, соответствующие 4-му уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 1-й категории, в государственных информационных системах 1-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1-го уровня защищенности персональных данных, в информационных системах общего пользования II класса [13].

6. Общие требования к безопасности СЗИ

При проведении сертификации средства защиты информации должно быть подтверждено соответствие средства указанным требованиям.

Устанавливается следующее соответствие классов средств защиты информации и средств вычислительной техники уровням доверия:

- средства защиты информации 6-го класса должны соответствовать 6-му уровню доверия;
- средства защиты информации 5-го класса должны соответствовать 5-му уровню доверия;
- средства защиты информации 4-го класса и средства вычислительной техники 5-го класса должны соответствовать 4-му уровню доверия.

Средство соответствует уровню доверия, если оно удовлетворяет требованиям к разработке и производству средства, проведению испытаний и поддержке безопасности средства, приведенным в табл. 1.

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
1. Требования к разработке и производству средства				
1.1	Требования к разработке модели безопасности средства	–	–	+
1.2	Требования к проектированию архитектуры безопасности средства	+	=	=
1.3	Требования к разработке функциональной спецификации средства	+	+	+
1.4	Требования к проектированию средства	+	=	=
1.5	Требования к разработке проектной (программной) документации	+	+	+
1.6	Требования к средствам разработки, применяемым для создания средства	+	=	=
1.7	Требования к управлению конфигурацией средства	+	+	+
1.8	Требования к разработке документации по безопасной разработке средства	+	=	+
1.9	Требования к разработке эксплуатационной документации	+	=	=

2. Требования к проведению испытаний средства

2.1	Требования к тестированию средства	+	+	+
2.2	Требования к испытаниям по выявлению уязвимостей и недеklarированных возможностей средства	+	+	+
2.3	Требования к проведению анализа скрытых каналов в средстве	-	-	+

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4

3. Требования к поддержке безопасности средства

3.1	Требования к устранению недостатков средства	+	+	+
3.2	Требования к обновлению средства	+	+	+
3.3	Требования к документированию процедур устранения недостатков и обновления средства	+	=	=
3.4	Требования к информированию об окончании производства и (или) поддержки безопасности средства	+	=	=

6. Общие требования к безопасности СЗИ

Знак «+» в строке требования к уровню доверия указывает на наличие требований, предъявляемых к соответствующему уровню доверия.

Знак «=» означает, что требования к уровню доверия совпадают с требованиями, предъявляемыми к предыдущему уровню доверия.

Знак «-» означает, что требования к уровню доверия не предъявляются.

6. Общие требования к безопасности СЗИ

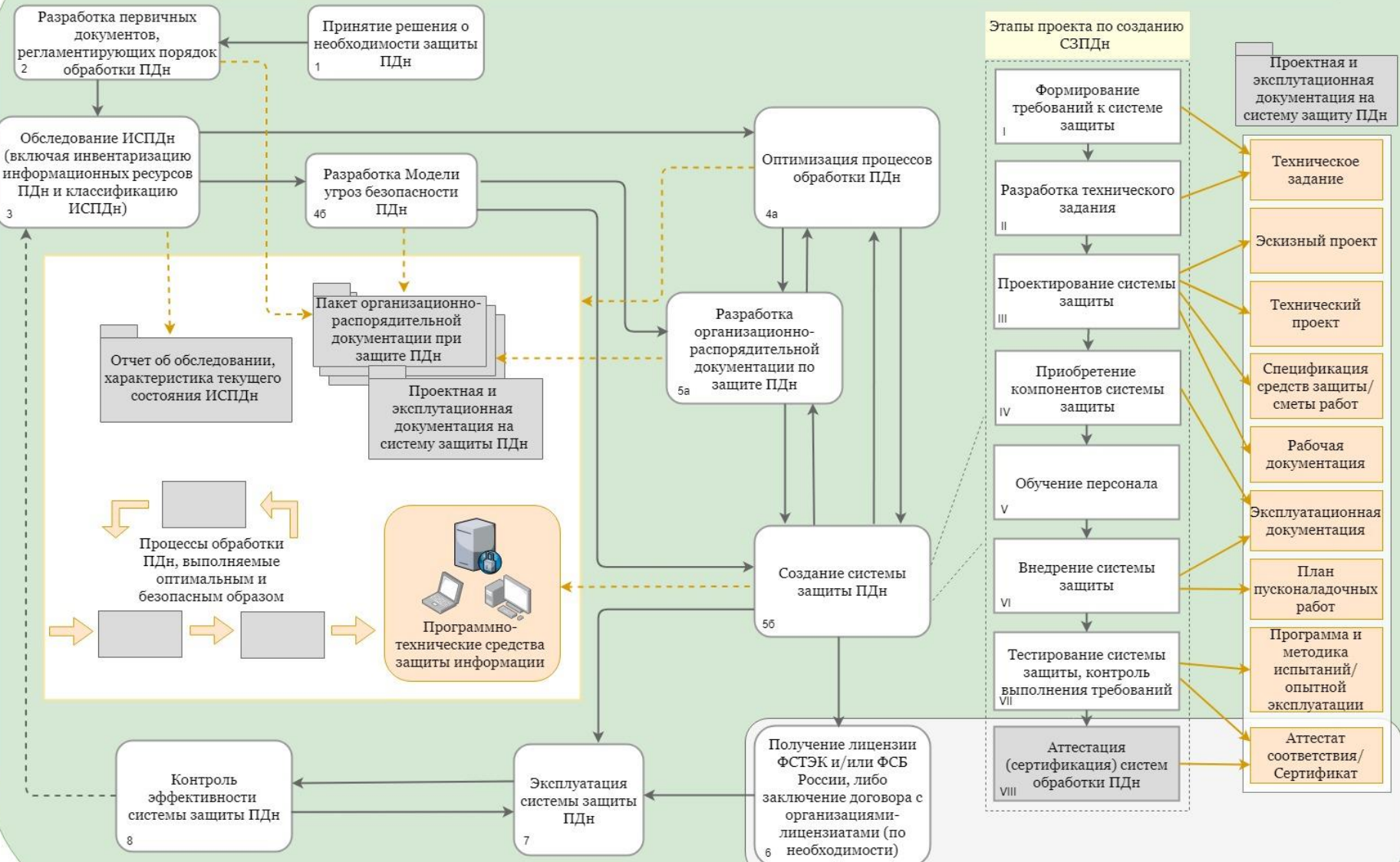
Класс защиты межсетевого экрана	Класс защищенности ГИС	Уровень защищенности ИСПДн	Класс защищенности АСУ ТП
6	3, 4	3, 4	3
5	2	2	2
4	1	1	1
3	Информационные системы, осуществляющие обработку информации, содержащей сведения, составляющие государственную тайну		
2			
1			

	УЗ1		УЗ2		УЗ3			УЗ4
	АУ1, АУ2 или АУЗ с ССОП	АУЗ без подключения к ССОП	АУ1, АУ2 или АУЗ с ССОП	АУЗ без подключения к ССОП	АУ2 или ССОП	АУЗ с подключением к ССОП	АУЗ без подключения к ССОП	-
СВТ	5 класс СВТ		5 класс СВТ		5 класс СВТ			6 класс СВТ
СОВ	4 класс СОВ и 4 НДС		4 класс СОВ и 4 НДС		4 класс СОВ и 4 НДС	4 класс СОВ	5 класс СОВ	5 класс СОВ
САЗ	4 класс САЗ и 4 НДС		4 класс САЗ и 4 НДС		4 класс САЗ и 4 НДС	4 класс САЗ	5 класс САЗ	5 класс САЗ
МЭ	3 класс МЭ и 4 НДС	4 класс МЭ и 4 НДС	3 класс МЭ и 4 НДС	4 класс МЭ и 4 НДС	3 класс МЭ и 4 НДС	3 класс МЭ	4 класс МЭ	5 класс МЭ
Другие СИ	любое ТУ или ЗБ и 4 НДС		любое ТУ или ЗБ и 4 НДС		любое ТУ или ЗБ и 4 НДС	любое ТУ или ЗБ		любое ТУ или ЗБ

7. Изучение основных НПА

Разбираем приказ ФСТЭК № 21

Последовательность шагов по выполнению требований 152-ФЗ "О персональных данных"



Решение о необходимости проведения данных работ принимается Оператором