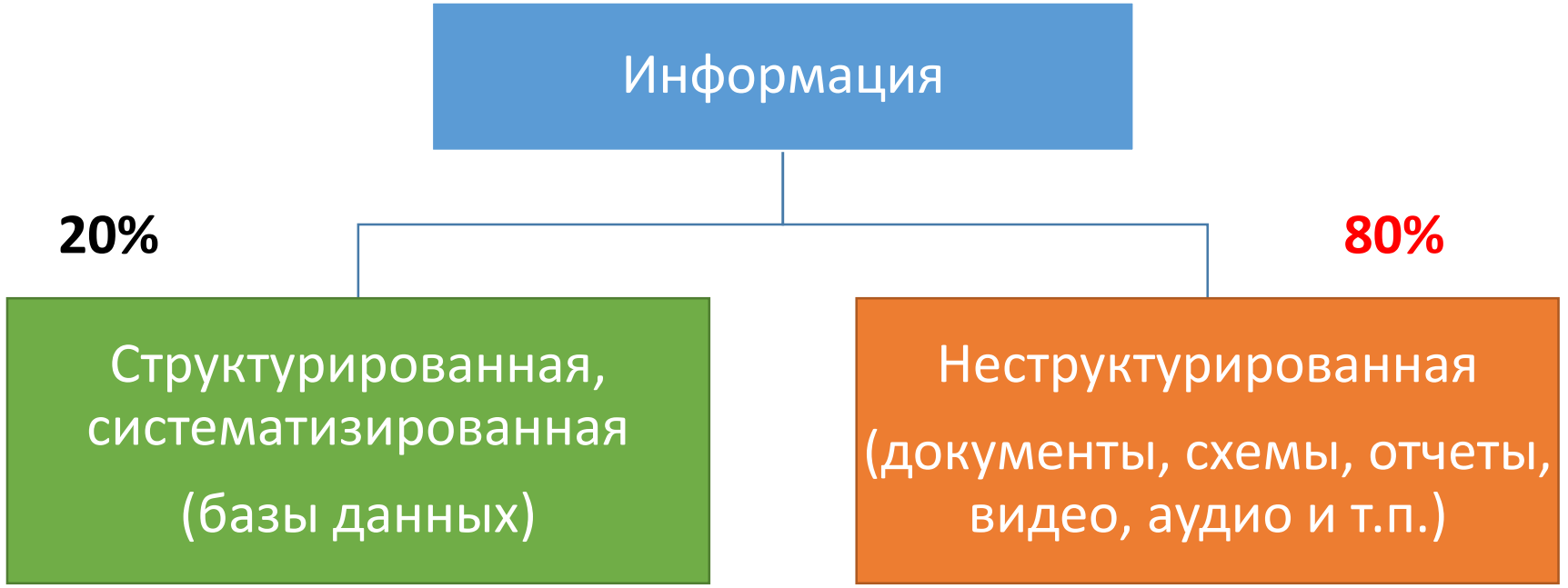
Министерство образования Кировской области

Техническая защита информации в образовательных организациях

- Сергей Городилов
- Руководитель направления ИБ, АСПЕКТ СПб

Объекты защиты

Что организации обрабатывают?



Что обычно есть

ИСПДн:

- 1С:Бухгалтерия (бухгалтерия) – *часто ЦБ*
- Партнер-персонал (з/п, кадры)
- Аверс «Директор»
- Аверс «Электронный журнал»
- Сайт (часто – Ucoz)

У некоторых:

- Сайт подразделения/направления (школа развития и др.)
- Система управления обучением (Moodle, BBB)

Подключения к внешним ИС

- СБИС Электронная отчетность
- Электронный бюджет (не ИСПДн?)
- Отчетность в Минобразования Кировской области (обезличенные данные?)
- Клиент-банк (Сбербанк, ВТБ, Хлынов и др)
- Электронные Торги/закупки

- АРМ защищенной сети ЕИОС КО
- ФИС ФРДО (некоторые)
- ИС зачисления в ОО
- ИС Контингент ДОО, ДОУ

Внешние сервисы

- Электронная почта (Yandex.Почта, mail.ru)
- Сириус.Курсы (Всерос олимпиада школьный этап)
- Office 365
- Площадки типа Учи.ру, Яндекс.Учебник

Проблемы отнесения к ИСПДн

152-ФЗ, ст.3. **Информационная система персональных данных** - совокупность содержащихся **в базах данных** ПДн и обеспечивающих их обработку информационных технологий и технических средств

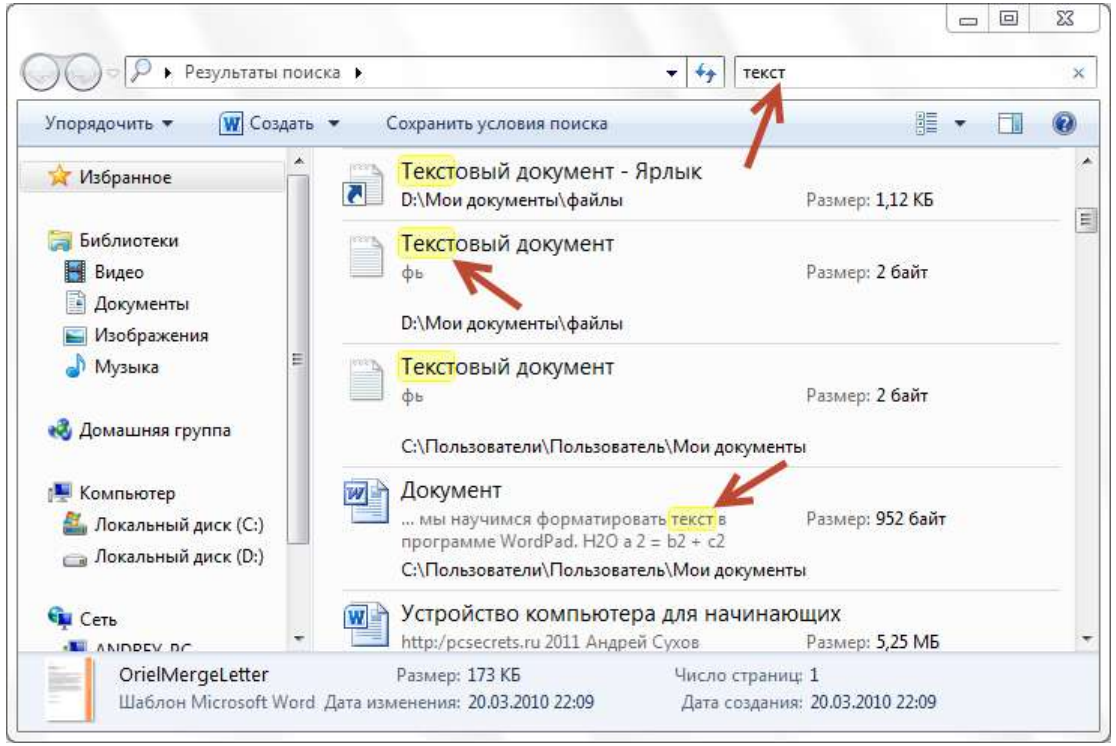
ГК РФ, ст.1260. **Базой данных** является представленная в объективной форме **совокупность самостоятельных материалов** (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), **систематизированных** таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

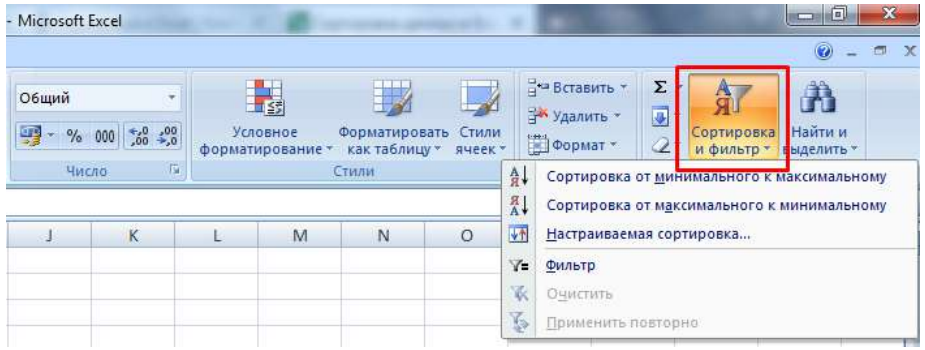
РКН: **БД** - **упорядоченный массив данных**, независимый от вида материального носителя информации и используемых средств обработки (архивы, картотеки, электронные базы данных)*.

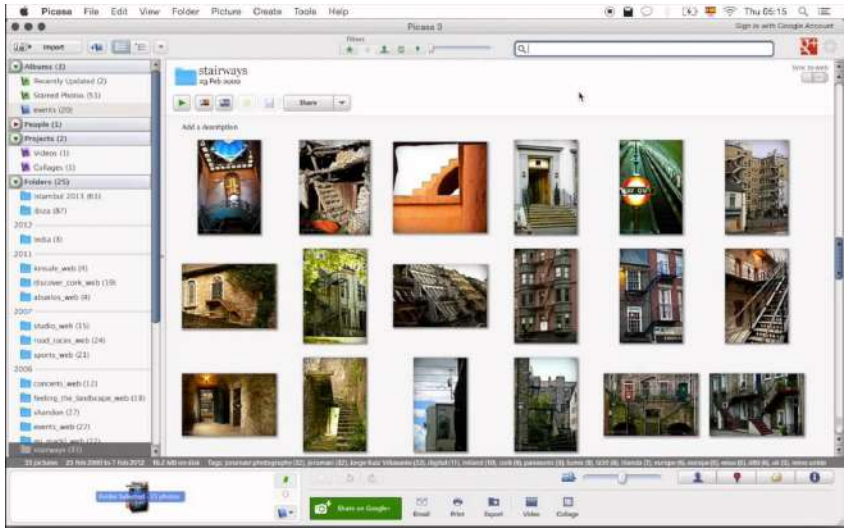
*Комментарий к ФЗ от 21 июля 2014 г. №242-ФЗ.

Примеры БД?

- Поиск по документам в проводнике (службы индексирования Windows)
- Сортировка в Excel
- Подборки фотографий в ACDSee, Picasa







Рекомендуется определять в качестве объектов защиты

ИСПДн (БД)

Включать в состав ИСПДн:

- Информационные ресурсы (неструктурированные)
- ПК (тоже с ресурсами)
- Другое оборудование (если есть)

Цель:

- *держать под вниманием;*
- *знать, всё ли мы защищаем*.

Требования НПА

НПА

- Статья 18.1 закона 152-ФЗ
- Статья 19 закона 152-ФЗ
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК №21
- Приказ ФСБ №378

Статья 18.1 закона 152-ФЗ

Меры по обеспечению безопасности персональных данных при их обработке

Статья 18.1 Часть 1

1) назначение **оператором, являющимся юридическим лицом**, ответственного за организацию обработки персональных данных (ЛОООПДн);

2) издание **оператором, являющимся юридическим лицом**, документов, определяющих

политику оператора в отношении обработки персональных данных,

локальных актов по вопросам обработки персональных данных,

а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

3) применение **правовых, организационных и технических мер** по обеспечению безопасности персональных данных в соответствии со статьей 19;

4) осуществление **внутреннего контроля и (или) аудита** соответствия обработки персональных данных

152-ФЗ и принятым в соответствии с ним нормативным правовым актам,

требованиям к защите персональных данных,

политике оператора в отношении обработки персональных данных,

локальным актам оператора;

5) **оценка вреда**, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, **соотношение указанного вреда и принимаемых оператором мер**…;

6) **ознакомление работников оператора**, непосредственно осуществляющих обработку персональных данных, с

положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных,

документами, определяющими политику оператора в отношении обработки персональных данных,

локальными актами по вопросам обработки персональных данных,

и (или) **обучение указанных** работников.

Статья 19 закона 152-ФЗ

Меры по обеспечению безопасности персональных данных при их обработке

Статья 19
Часть 1

1. **Оператор** при обработке ПДн **обязан принимать необходимые правовые, организационные и технические меры** или **обеспечивать их принятие** для защиты ПДн от
   неправомерного или случайного доступа к ним,
   уничтожения,
   изменения,
   блокирования,
   копирования,
   предоставления,
   распространения персональных данных,
   а также от иных неправомерных действий в отношении ПДн.

*«**Обеспечивать**» значит:*

1) *Поручить обработку и предусмотреть требования*
2) *Вести контроль, мониторинг, аудиты ИБ.*

Статья 19 Часть 2

- 2. Обеспечение безопасности ПДн достигается, в частности:
- 1) **определением угроз безопасности ПДн** при их обработке **в ИСПДн**;
- 2) применением **организационных и технических мер** по обеспечению безопасности ПДн при их обработке **в ИСПДн**, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- 3) **применением прошедших в установленном порядке процедуру оценки соответствия** средств защиты информации;
- 4) **оценкой эффективности принимаемых мер** по обеспечению безопасности ПДн до ввода в эксплуатацию **ИСПДн**;
- 5) **учетом машинных носителей ПДн**;
- 6) **обнаружением фактов несанкционированного доступа к ПДн** и **принятием мер**, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак **на ИСПДн** и по **реагированию на компьютерные инциденты в них**; (30.12.2020)
- 7) **восстановлением ПДн**, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) **установлением правил доступа к персональным данным**, обрабатываемым **в ИСПДн**, а также обеспечением **регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн**;
- 9) **контролем за принимаемыми мерами** по обеспечению безопасности ПДн и уровня защищенности **ИСПДн**.

Статья 19 Часть 3

3. Правительство РФ с учетом возможного вреда субъекту ПДн, объема и содержания обрабатываемых ПДн, вида деятельности, при осуществлении которого обрабатываются ПДн, актуальности угроз безопасности ПДн устанавливает:

1) **уровни защищенности ПДн** при их обработке **в ИСПДн** в зависимости от угроз безопасности этих данных;

2) **требования к защите ПДн** при их обработке **в ИСПДн**, исполнение которых обеспечивает установленные уровни защищенности ПДн;

3) **требования к материальным носителям биометрических ПДн** и технологиям хранения таких данных **вне ИСПДн**.

1,2) -> ПП РФ № 1119

3) -> ПП РФ № 512

Статья 19
Часть 4

- 4. Состав и содержание необходимых … требований к защите ПДн для каждого из УЗ, организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн устанавливаются ФСБ, и ФСТЭК, в пределах их полномочий

->Приказ ФСТЭК от 18.02.2013 № 21

->Приказ ФСБ от 10.07.2014 № 378

Статья 10
Часть 11

11. Для целей настоящей статьи **под угрозами безопасности ПДн** понимается совокупность **условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн**, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия при их обработке **в ИСПДн**.

Под уровнем защищенности ПДн понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке **в ИСПДн**.

Постановление Правительства РФ от 1.11.2012 №1119

Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

Тип актуальных угроз

Виды ИСПДн

- ИСПДн-С – обработка специальных категорий
- ИСПДн-Б – обработка биометрических ПДн
- ИСПДн-И – иные ПДн
- ИСПДн-О – общедоступные ПДн (полученные из общедоступных источников по 8 ст. 152-ФЗ)

ПП 1119 Уровни защищенности ПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
ИСПДн-С		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4

99%

4 уровень защищенности - требования

13. **Для обеспечения 4-го уровня защищенности ПДн** при их обработке в информационных системах необходимо выполнение следующих требований:

а) **организация режима обеспечения безопасности помещений, в которых размещена информационная система**, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) **обеспечение сохранности носителей персональных данных**;

в) утверждение руководителем оператора **документа, определяющего перечень лиц**, **доступ которых** к персональным данным, обрабатываемым в информационной системе, **необходим** для выполнения ими служебных (трудовых) обязанностей;

г) **использование средств защиты информации, прошедших процедуру оценки соответствия требованиям** законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

3 уровень защищенности - требования

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было **назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе**.

21 приказ ФСТЭК

Меры по 21 приказу

- идентификация и аутентификация (6);
- управление доступом (17);
- ограничение программной среды (4);
- защита машинных носителей информации (8);
- регистрация событий безопасности (7);
- антивирусная защита (2);
- обнаружение (предотвращение) вторжений (2);
- контроль (анализ) защищенности (5);
- обеспечение целостности (8);
- обеспечение доступности (5);
- защита среды виртуализации (10);
- защита технических средств (5);
- защита информационной системы, ее средств, систем связи и передачи данных (20);
- выявление инцидентов (6);
- управление конфигурацией ИС (4).

Итого: 109 мер.

По уровням защищенности

- Всего мер - 109
- Базовых мер для УЗ 4 - 27
- Базовых мер для УЗ 3 - 41
- Базовых мер для УЗ 2 - 63
- Базовых мер для УЗ 1 - 69
- Всего дополнительных (компенсирующих) мер - 40

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

Мера	Содержание	Уровни защищенности			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+

II. Управление доступом субъектов доступа к объектам доступа (УПД)

II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				

II. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+

III. Ограничение программной среды (ОПС)

III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				

IV. Защита машинных носителей персональных данных (ЗНИ)

IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+

V. Регистрация событий безопасности (РСБ)

V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+

VI. Антивирусная защита (АВЗ)

VII. Обнаружение вторжений (СОВ)

VIII. Контроль (анализ) защищенности персональных данных (АНЗ)

VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.I	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+

IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)

IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				

X. Обеспечение доступности персональных данных (ОДТ)

X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+

XI. Защита среды виртуализации (ЗСВ)

XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+

XII. Защита технических средств (ЗТС)

XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				

ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+

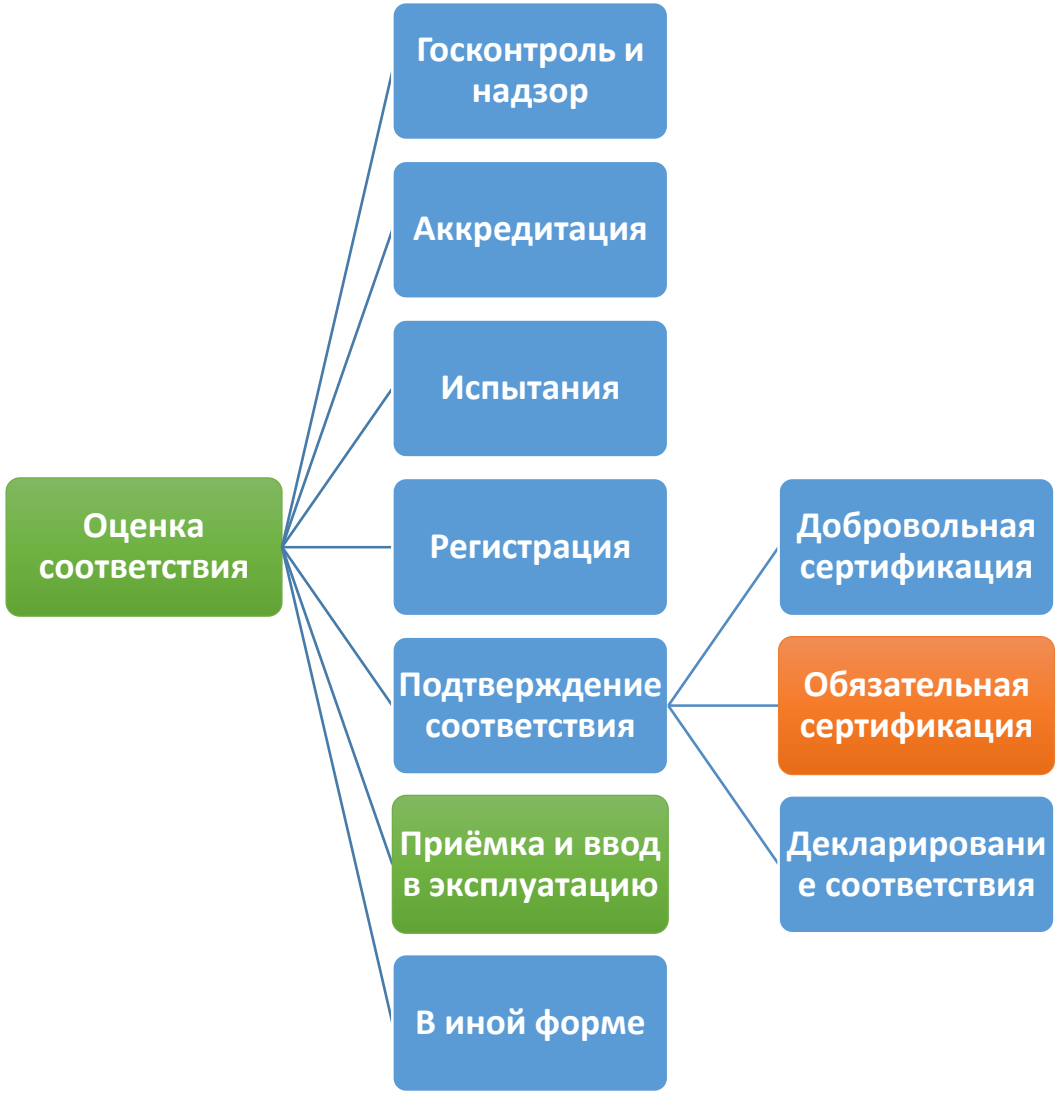
XIV. Выявление инцидентов и реагирование на них (ИНЦ)

XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+

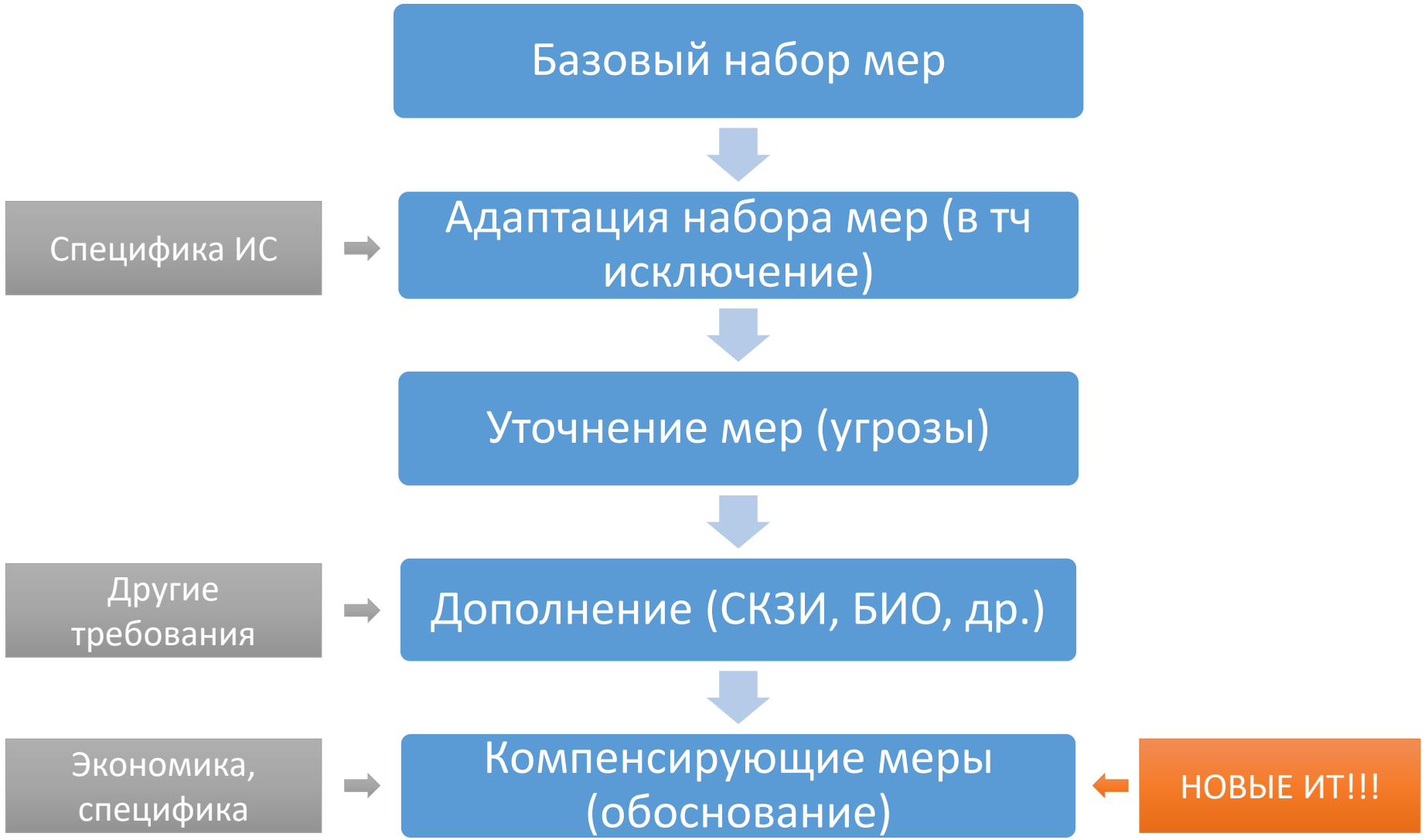
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)

XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

184-ФЗ - Оценка соответствия средств защиты



Приказ ФСТЭК 21 Процедура выбора мер



Основные процессы ИБ

Основные процессы ИБ

1. Обеспечение жизненного цикла ИСПДН и ИР
2. Предоставление доступа
3. Управление конфигурацией
4. Управление инцидентами (выявление и реагирование)
5. Контроль (аудиты)
6. Резервирование и восстановление
7. Уничтожение данных

1. Жизненный цикл ИСПДн и ИР

- Решение о создании (об использовании) ИСПДн и ИР
- Решение об уровне защищенности ПДн в ИСПДн
- Моделирование угроз
- Выбор мер защиты
- Внедрение мер защиты
- Оценка эффективности перед началом обработки ПДн
- Ввод в эксплуатацию
- Эксплуатация
- Вывод из эксплуатации

Важно! Только в этих ИСПДн и ИР допускается обрабатывать персональные данные.

2. Предоставление доступа

- Должностные обязанности или договор
- Доступ в помещения с ИСПДн, ПК
- Включение в перечни:
  - должностей, допущенных к автоматизированной и неавтоматизированной обработке
  - допуска к работе с СКЗИ
  - разрешающие работу со съемными носителями
- Ознакомление, инструктаж, обучение
- Предоставление доступа
  - Регистрация учетных записей, паролей
  - Назначение прав доступа
- Контроль предоставленного доступа

3. Управление конфигурацией

Цель управления конфигурацией

- знать, что все средства обработки под контролем, в том числе в части их состава, ПО, структуры;
- распределять ответственность.

- Перечень ИСПДн и уровней защищенности ПДн
- Перечни оборудования по видам и конфигурации
- Учет установленного ПО
- Проверка обновлений, установка обновлений
- Учет изменений в структуре, в конфигурации

Выполняется на этапах жизненного цикла.

4. Управление инцидентами

Источники информации об инцидентах:

- Регистрация событий безопасности
  - ОС (вход, выход, доступ, запуск, останов, изменение конфигурации, др)
  - антивирусы
  - межсетевые экраны
  - прикладное ПО
- Оповещения от ПО, средств обнаружения атак
- Аудиты/проверки/контроль
- Ежедневная работа системного администратора, администратора безопасности
- Сообщения сотрудников

Что относится к инцидентам

- Заражение вирусом
- Шифрование данных
- Утечка данных
- Многократный неправильный ввод пароля
- Компрометация пароля
- Компрометация ключа электронной подписи
- Сканирование ИТ-инфраструктуры и сервисов
- Попытки проникновения
- Неразрешенное использование ПО, оборудования, носителей
- Частое обнаружение вирусов у пользователя
- Массовое копирование/воздействие на файлы и папки или записи в ИС
- Множественный сбой ПК
- Сбой сервера

Что можно не относить к инцидентам

- Неправильный ввод пароля
- Обнаруженный вирус в почте (удаленный)
- Нежелательные письма (спам)
- Обнаруженный вирус однократно
- Однократная попытка доступа к папке (вероятно ошибка)
- Однократный сбой ПК

Порядок реагирования на инциденты

Администратор ИБ (Ответственный ИБ)

1. Получение сведений о предположительном инциденте.
2. Определение «инцидент» – «не инцидент».
3. Если «инцидент» то определяется критичность.
4. Собирается рабочая группа по реагированию (при необходимости).
5. Реагирование (расследование):
   - локализация/изоляция
   - сбор необходимой информации, фактов
   - Документирование инцидента (журнал учета, факты)
   - Формирование заключения об инциденте (акт)
6. Принятие решений
   - Восстановление работоспособности
   - Усиление безопасности (корректирующие и превентивные действия)

6. Резервное копирование и восстановление

Резервному копированию подлежит информация следующих основных категорий:

- информация пользователей
- информация, обрабатываемая пользователями в ИСПДн и ИР;
- базы данных (БД);
- конфигурация и дистрибутивы системного ПО для развертывания на серверы;
- образы систем и информация сервисов инфраструктуры;
- образы систем и информация сервисов и средств ИБ;
- конфигурация сетевого оборудования;
- другая информация, являющаяся критичной.

Регламент резервного копирования

№	Типа резервируемого объекта	Периодичность и тип резервного копирования	Срок хранения копий	Допустимый период, за который данные могут быть потеряны
1.	База данных	24 часа - полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	24 часа
2.	Общие сетевые ресурсы	24 часа - полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	24 часа
3.	Серверы (системные разделы)	При изменении конфигурации - полное	3 последних копии	-
4.	Контроллеры домена, серверы безопасности	24 часа – полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца4 часа	
5.	Виртуальные машины	24 часа – полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	24 часа
6.	Рабочие станции	При изменении конфигурации - полное	1 последняя копия	Не установлен
7.	Журналы безопасности, журналы резервных копий	24 часа	1 год	4 часа

Требования к резервному копированию и восстановлению

- На отдельные машинные носители
- Конфиденциальность резервных копий
- Резервное копирование по регламенту
- Контроль состояния резервирования
- Ротация носителей
- Проверка резервных копий восстановлением

7. Уничтожение ПДн

Когда:

- **при достижении целей** обработки ПДн (в том числе по **истечении установленных сроков** хранения) – рекомендуется ежегодно;
- в случае **отзыва субъектом согласия** на обработку своих ПДн (если обработка ведется на его основании) – не более 30 дней;
- при **невозможности устранения нарушений**, допущенных при обработке ПДн – не более 10 рабочих дней или 6 месяцев при условии блокирования;
- при **выводе из эксплуатации машинных носителей информации** – в момент вывода;
- в случае получения **предписания** от Роскомнадзора не более 10 рабочих дней.

Порядок уничтожения

- Материальные носители
  - шредирование, сжигание
- Машинные носители информации
  - Надежное стирание (WIPE, Sdelete, DallasLock)
- Базы данных и информационные ресурсы
  - удаление соответствующих записей или значений полей таблиц в основной базе данных;
  - удаление записей или значений полей таблиц в резервных (тестовых) копиях базы данных;
  - удаление снапшотов виртуальных машин, дисковых томов.

Оформление уничтожения

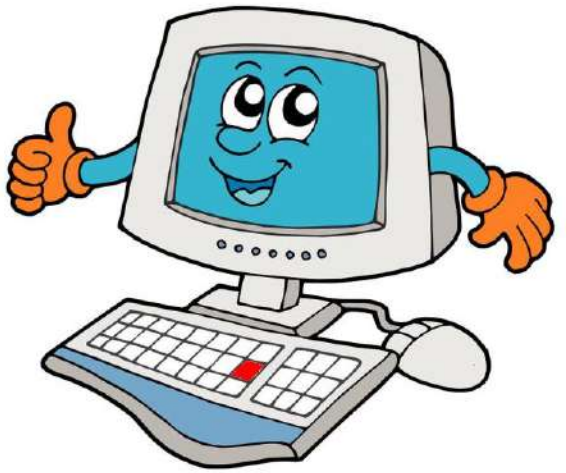
- *Акт об уничтожении документов с истекшим сроком хранения (форма приведена в Приложении 3 к Порядку)*
- *Акт уничтожения машинных носителей информации (Приложение 1 к Порядку)*;
- *Акт об уничтожении персональных данных, хранящихся в информационной системе персональных данных (Приложение 2 к Порядку)*

Документы должны появляться регулярно!

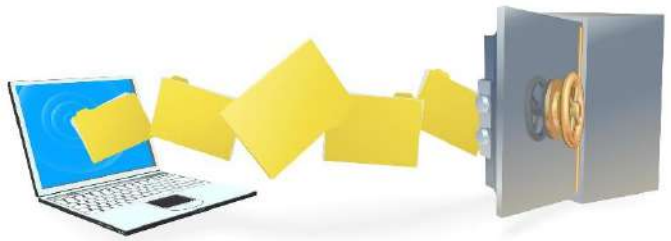
Хранятся постоянно в отдельном деле.

Документы

3.	**Автоматизированная обработка**
3.2.	**Ответственные лица**
-	Образец приказа «О безопасности персональных данных, обрабатываемых в информационных системах персональных данных и информационных ресурсах» (с приложениями)
3.3.	**Жизненный цикл информационных систем персональных данных и средств вычислительной техники**
-	Перечень информационных систем и информационных ресурсов
-	Форма акта определения уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных
-	Образец определения уровней защищенности персональных данных во внутренних ИСПДн (в соответствии с ПП РФ от 01.11.2012 №1119)



3.6	**Базовые технические меры обеспечения ИБ в ИСПДн и ИР**
	Политика назначения смены паролей
	Инструкция по антивирусной защите
	Инструкция по обращению с машинными носителями информации
	Правила безопасной работы в сети Интернет и входящей электронной корреспонденцией
	Положение о работе с корпоративной электронной почтой
	Регламент реагирования на инциденты ИБ
	Порядок уничтожения персональных данных (с приложениями)



- Сергей Городилов
- Руководитель направления ИБ, АСПЕКТ СПб