Частное образовательное учреждение
дополнительного профессионального образования
«Учебно-методический центр Газ-Нефть-Сервис»

ЧОУ ДПО " УМЦ ГНС"

Подписан: ЧОУ ДПО "УМЦ ГНС"
DN: ИНН ЮЛ=0273990100, СНИЛС=12192325528, ОГРН=1100200003485, ИНН=027613909351, C=RU, S=02 Республика Башкортостан, L=УФА ГОРОД, STREET="ТРАМВАЙНАЯ УЛИЦА, ДОМ 4А", O="ЧОУ ДПО "" УМЦ ГНС"""", CN="ЧОУ ДПО ""УМЦ ГНС"""", T=ДИРЕКТОР, G=ТАТЬЯНА МИХАЙЛОВНА, SN=ВАСИЛЬЕВА
Основание: Я являюсь автором этого документа
Местоположение:
Дата: 2026-06-18 12:56:22
Foxit Reader Версия: 9.3.0

УТВЕРЖДАЮ
Директор
ЧОУ ДПО «УМЦ ГНС»
_____Т.М. Васильева
17.10.2025г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Рассмотрено на заседании
Учебно-методического совета
ЧОУ ДПО «УМЦ ГНС»
Протокол №31
От «17» октября 2025г.

Уфа-2025

Содержание

1. Общая характеристика образовательной программы

Программа повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» разработана в соответствии с требованиями:

-Федерального Закона от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации»,

-Приказ Минобрнауки России от 24.03.2025 N 266 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" (Зарегистрировано в Минюсте России 22.04.2025 N 81928) Приказ Министерства просвещения Российской Федерации от 14.07.2023 № 534 "Об утверждении Перечня профессий рабочих, должностей служащих, по которым осуществляется профессиональное обучение".

- Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ (в действующей редакции)

-Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

- Федеральным законом от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» введена ответственность для компаний за утечку персональных данных.»

Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025)

- Федеральный закон № 421 «О внесении изменений в Уголовный кодекс Российской Федерации» , который вступает в силу 11 декабря 2024 г. Изменения в ст. 13.11 КоАП.

К освоению программы допускаются: лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование.

Форма обучения – очная с использованием дистанционных технологий.

Цель программы: теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой персональных данных (ПДн), обучением принципам и методам защиты информации в информационных системах персональных данных (ИСПДн), совершенствование и актуализация компетенций, необходимых для профессиональной деятельности по защите персональных данных, содержащихся в информационных системах.

Задачи обучения:

- изучение типовых угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
- овладение средствами и методами проектирования и построения защищенных ИСПДн; - овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности ИСПДн.

Содержание программы представлено пояснительной запиской, рабочим учебно-тематическим планом, содержанием рабочей программы, планируемыми результатами освоения программы, условиями реализации программы, системой оценки результатов освоения программы, учебно-методическими материалами,

обеспечивающими реализацию программы. Учебно-тематический план содержит перечень учебных тем, с указанием времени, отводимого на освоение учебных тем, включая время, отводимое на теоретические и практические занятия. Программа раскрывает рекомендуемую последовательность изучения тем, а также распределение учебных часов по разделам и темам. Условия реализации программы содержат организационно-педагогические, кадровые, информационно-методические и материально-технические требования. Учебно-методические материалы обеспечивают реализацию программы. Образовательная программа рассчитана на 72 акд.часов.

Требования к результатам освоения рабочей программы сформированы на основе требований, предъявляемым к специалистам, деятельность которых, связанна с защитой персональных данных. В требованиях к результатам освоения программы описываются требования к умениям, приобретаемым в ходе освоения рабочей программы, указываются усваиваемые знания, на базе которых формируются умения и приобретаются практические навыки защиты персональных данных. Структура и содержание программы представлены требованиями к подготовке обучающихся, учебно-тематическим планом и программой, требованиями к минимальному материально-техническому обеспечению реализации программы, информационным обеспечением обучения, критериями оценивания знаний и умений обучающихся. Освоение программы завершается обязательной итоговой аттестацией в форме зачета. Проведение итоговой аттестации обучающихся осуществляется с аттестационной комиссией ЧОУ ДПО «УМЦ ГНС» Результаты итоговой аттестации оформляются протоколом. По результатам итоговой аттестации выдается удостоверение о повышении квалификации установленного образца. Индивидуальный учет результатов освоения обучающимися образовательных программ, а также хранение в архивах информации об этих результатах осуществляются ЧОУ ДПО «УМЦ ГНС» на бумажных и (или) электронных носителях.

2. Планируемые результаты
Требования к профессиональной подготовленности (компетентности) обучающегося, прошедшего обучение по программе повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

В результате изучения программы «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» обучающиеся **должны знать**:

- содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах персональных данных;
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
- процедуры задания и реализации требований по защите информации в информационных системах персональных данных;
- меры обеспечения безопасности персональных данных;
- требования по обеспечению безопасности персональных данных;

- порядок применения организационных мер и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

В результате изучения программы повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» обучающиеся должны **уметь**:

- разрабатывать модели угроз для информационных систем с учетом их назначения, условий и особенностей функционирования;
- разрабатывать необходимую организационно-распорядительную и нормативно-техническую документацию в интересах системы защиты информационных систем;
- оценивать эффективность системы защиты информационных систем;
- составлять перечень сведений, отнесенных к персональным данным, и проводить их классификацию;
- проводить классификацию информационных систем персональных данных с составлением соответствующего акта;
- выявлять актуальные угрозы безопасности информации в информационных системах персональных данных;
- планировать, организовывать и контролировать выполнение работ и мероприятий по защите персональных данных.

В результате изучения программы повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» обучающиеся **должны владеть навыками**:

- навыками применения программно-аппаратных средств защиты персональных данных;
- навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных.

В результате освоения программы обучающийся **должен обладать следующими компетенциями:**

- общекультурными
- способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма ;
- способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности в целях обеспечения полноценной социальной и профессиональной деятельности

. профессиональными :

- способностью проводить обоснование и выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований ;
- способностью прогнозировать, ранжировать, моделировать информационные угрозы телекоммуникационных систем и оценивать уровни риска ;
- способностью осуществлять аудит уровня защищенности и аттестацию телекоммуникационных систем ;
- способностью проводить анализ и формализацию поставленных задач в области компьютерной безопасности ;
- способностью применять технические средства защиты информации в сетях специальной связи и на объектах информатизации.

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

1. Продолжительность учебного года

Начало учебных занятий – **по формированию учебной группы.**

Начало учебного года – 09 января

Конец учебного года **–** 31 декабря

Продолжительность учебного года совпадает с календарным.

2. Регламент образовательного процесса:

Продолжительность учебной недели – 5 дней.

Не более 8 часов в день**.**

3. Продолжительность занятий:

Занятия проводятся по расписанию, утвержденному директором

Продолжительность занятий в группах:

- 45 минут;

- перерыв между занятиями составляет - 10 минут

4. Регламент административных совещаний:

Собрания трудового коллектива – по мере необходимости, но не реже 1 раза в год

4. Учебный план дополнительной профессиональной образовательной программы «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

№ п/п	Наименование тем	Всего, час	В том числе	
			теоретические занятия	практические занятия
1	Правовое, нормативное и методическое обеспечение безопасности персональных данных	8	8	-
2	Угрозы безопасности персональных данных, уязвимости информационных систем персональных данных	16	16	-
3	Организация обработки персональных данных	8	8	-
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных	16	16	-

	системах персональных данных			
5	Особенности обработки персональных данных без использования средств автоматизации	8	8	-
6	Виды правонарушений, административная ответственность, штрафы	8	8	
	Консультация Зачет	**8**	**8**	
	ИТОГО	**72**	**8**	

5. Содержание дополнительной профессиональной программы повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Тема 1. Правовое, нормативное и методическое обеспечение безопасности персональных данных Основные понятия термины и определения в области обеспечения безопасности персональных данных. Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. Основные понятия и определения. Персональные данные. Федеральный закон РФ от 27 июля 2006 г.№ 152-ФЗ «О персональных данных». Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. Категории персональных данных. Права субъекта персональных данных. Техническая защита информации ограниченного доступа и обеспечение безопасности персональных данных. Использование средств криптографической защиты информации.

Тема 2. Угрозы безопасности персональных данных, уязвимости информационных систем персональных данных Общие положения и классификация угроз безопасности персональных данных Общая характеристика уязвимостей информационной системы персональных данных. Классификация угроз. Наиболее часто реализуемые угрозы. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов.

Тема 3. Организация обработки персональных данных Общий порядок организации обработки персональных данных. Разработка уведомления об обработке (о намерении осуществлять обработку) персональных данных. Разработка документации (приказы, должностные инструкции, положения, уведомления) по обработке персональных данных.
Тема 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Определение уровня защищенности персональных данных. Состав и содержание мер по обеспечению безопасности персональных данных. Особенности использования средств криптографической защиты информации в рамках

построения системы защиты персональных данных в организации Оценка обстановки и формирование замысла защиты персональных данных. Основные этапы при построении системы защиты персональных данных. Комплекс организационных и технических мероприятий в рамках СЗПД. Классификация ИСПД. Подсистемы криптографической защиты информации в составе СЗПД. Функции подсистемы криптографической защиты информации.

Тема 5. Методы защиты информационных систем персональных данных Особенности обработки персональных данных без использования средств автоматизации. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных. Основные обязанности операторов информационных систем, обрабатывающих персональные данные.

Тема 6. Основные изменения в законе 152-ФЗ «О персональных данных» с декабря 2024-2025 года. Федеральный закон № 420 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» , который вступит в силу **30 мая 2025 г.**, и Федеральный закон № 421 «О внесении изменений в Уголовный кодекс Российской Федерации» , который вступает в силу 11 декабря 2024 г. Изменения в ст. 13.11 КоАП.

6. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Организационно-педагогические условия реализации программы должны обеспечивать реализацию программы в полном объеме, соответствие качества подготовки обучающихся установленным требованиям, соответствие применяемых форм, средств, методов обучения и воспитания возрастным, психофизическим особенностям, склонностям, способностям, интересам и потребностям обучающихся.

Для определения соответствия применяемых форм, средств, методов обучения и воспитания возрастным, психофизическим особенностям и способностям обучающихся организация, осуществляющая образовательную деятельность, проводит тестирование обучающихся с помощью соответствующих специалистов.

Теоретическое обучение проводится в оборудованных учебных кабинетах с использованием учебно-материальной базы, соответствующей установленным требованиям.

Наполняемость учебной группы не должна превышать 30 человек.

Продолжительность учебного часа теоретических и практических занятий должна составлять 1 академический час (45 минут). Продолжительность учебного часа практического обучения должна составлять 1 астрономический час (60 минут).

Расчетная формула для определения общего числа учебных кабинетов для теоретического обучения:

$$П = \frac{Р\,гр * n}{0,75 * Ф\,пом};$$

где П - число необходимых помещений;

$P_{гр}$ - расчетное учебное время полного курса теоретического обучения на одну группу, в часах;

n - общее число групп;

0,75 - постоянный коэффициент (загрузка учебного кабинета принимается равной 75%);

$Ф_{пом}$ _ фонд времени использования помещения в часах.

Обучение состоит из лекций и практических занятий в лицензируемой организации

Для проведения теоретических и практических занятий привлекать преподавателей с опытом работ

Педагогические работники, реализующие данную образовательную программу, должны удовлетворять квалификационным требованиям, указанным в квалификационных справочниках по соответствующим должностям и (или) профессиональных стандартах.

Информационно-методические условия реализации программы:

учебный план;

календарный учебный график;

рабочие программы учебных предметов;

методические материалы и разработки;

расписание занятий.

Перечень учебного оборудования

Наименование учебного оборудования	Единица измерения	Количество
Оборудование и технические средства обучения		
Компьютер с соответствующим программным обеспечением	комплект	1
Мультимедийный проектор	комплект	1
Экран (монитор, электронная доска)	комплект	1

Организация-разработчик: Частное образовательное учреждение дополнительного профессионального образования «Учебно-методический центр Газ-Нефть-Сервис»

7. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

Многолетний опыт работы ЧОУ ДПО «УМЦ ГНС» в сфере дополнительного профессионального образования.

Обучение по данной программе ведется специалистом, имеющим опыт работы в данной сфере и в учебном центре.

Оборудованные учебные классы, компьютерная техника, наглядные пособия. Учебный план и программа, лекции по теоретическому обучению, методические рекомендации по организации образовательного процесса, утвержденными руководителем организации. Билеты для проведения экзаменов у обучающихся, утвержденными руководителем организации.

Корпоративная культура.

Оперативное реагирование на запросы заказчиков.

7. Информационное обеспечение обучения

1. Конституция РФ.

2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

3. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

6. Федеральный закон №63-ФЗ от 06.04.2011 «Об электронной подписи».

7. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

8. Постановление Правительства Российской Федерации, 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

9. Постановление Правительства Российской Федерации, 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

10. Постановление Правительства Российской Федерации, 15 сентября 2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

11. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

12. Приказ Роскомнадзора от 19.06.2025 N 140 "Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Зарегистрировано в Минюсте России 31.07.2025 N 83110)

13. Приказ Федеральной службы безопасности России, 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).
14. Приказ Федеральной службы по техническому и экспортному контролю России, 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

15. Приказ Федеральной службы по техническому и экспортному контролю России, 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.

16. Приказ Роскомнадзора от 19.06.2025 N 140 "Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Зарегистрировано в Минюсте России 31.07.2025 N 83110)

17. Федеральный закон № 420 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» ,

18.Федеральный закон № 421 «О внесении изменений в Уголовный кодекс Российской Федерации»

19. Воробьев Е.Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: Учебное пособие / Е.Г. Воробьев - СПб.: Издательский центр «Интермедия», 2016.

20. Вихорев С. В. Диалоги о безопасности информации, или введение в основы построения систем обеспечения информации: пособие // С. В. Вихорев, А. М. Сычев. - Москва: Медиа Группа «Авангард», 2015.

21. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024.
22. Змеев С. А. Методы и средства повышения защищенности автоматизированных систем на основе задания требований к механизмам защиты: учеб. пособие / С. А. Змеев [и др.]. - Воронеж: Воронежский институт МВД РФ, 2013.

23. Мещеряков В. А. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления: научно-

методическое пособие //В. А. Мещеряков [и др.] – Воронеж: ВИ МВД России, 2014. 24. Назаров, Д. М. Основы персональных данных обеспечения безопасности в организации: учеб. пособие / Д. М. Назаров, К. М. Саматов; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019.

25. Петренко В.И. Защита персональных данных в информационных системах. Издательство: Лань, 2024.

24. Прохорова О.В, Информационная безопасность и защита информации. Издательство: Лань, 2024.

25. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. Интернет-ресурсы:

1. Информационно-правовой портал Гарант – URL: http://www.garant.ru

2. Официальный сайт компании – КонсультантПлюс».URL: http://www.consultant.ru

3. Электронно-библиотечная система «КнигаФонд – URL: http://www.knigafundt.ru

4. Электронно-библиотечная система – URL: http://www.iprbookshop.ru «IPRbooks».

5. Официальный сайт Федеральной службы по техническому и экспортному контролю – URL: http://fstec.ru

6. Официальный сайт Федеральной службы безопасности – URL: http://www.fsb.ru
7. Официальный сайт Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций – URL: http://rkn.gov.ru

8. Критерии оценивания знаний и умений по дисциплине

8.1. Критерии оценки полученных знаний и эффективности учебной программы по устным ответам на контрольные вопросы (текущая успеваемость)

Оценка 5 («отлично») выставляется при условии точного и полного ответа на вопрос и ответа на дополнительные вопросы. При этом учитывается не только объем ответа, но и умение обучающегося профессионально аргументировано излагать материал, иллюстрировать теоретические выводы примерами на практике. При изложении материала также оценивается умение строить логическое умозаключение.

Оценка 4 («хорошо») выставляется при условии правильного ответа на вопрос, но при незначительных неточностях ответа, которые обучающийся восполняет, отвечая на дополнительные вопросы преподавателя, что позволяет восстановить целостную картину ответа.

Оценка 3 («удовлетворительно») выставляется при условии в основном правильного ответа на поставленные вопросы, но неспособности обучающегося ответить на дополнительные вопросы, нечеткости ответа.

Оценка 2 («неудовлетворительно») выставляется при условии неправильного ответа на поставленный вопрос, за несамостоятельную подготовку к ответу.

Оценка 1 («плохо») выставляется за отказ от ответа по причине незнания вопроса.

8.2. Критерии оценки полученных знаний и эффективности учебной программы по ответам на контрольные вопросы в форме зачета Зачетный билет состоит из 20 тестовых заданий. Вопросы, включенные в зачетный билет, позволяют оценить знания обучающихся в следующей области: - требования законодательной и нормативной правовой базы, регламентирующей защиту персональных данных; - классификация угроз безопасности персональных данных и каналы утечки информации; - основные этапы организации обработки и защиты персональных данных; - основные методы, способы, программно-аппаратные и технические средства защиты персональных данных. Положительное оценивание по системе «зачтено»-«не зачтено» осуществляется при наличии не менее 80 % правильных ответов.

9. Контрольно-оценочные материалы

Вопросы для самоконтроля

1. Определение персональных данных (ПДн) и информационной системы персональных данных.

2. Нормативно-правовая база в сфере защиты и обработки ПДн (№ 149-ФЗ, № 152ФЗ).
3. Категории персональных данных.

4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Уровни защищённости информационных систем персональных данных.

6. Процесс подготовки пакета документов к аккредитации ИСПДн: обязательство о неразглашении информации, содержащей ПДн; согласие на обработку ПДн; перечень ИСПДн.

7. Процесс подготовки пакета документов к аккредитации ИСПДн: перечень ПДн, обрабатываемых и хранящихся в ИСПДн; положение об обработки ПДн работников; акт определения уровня защищённости ИСПДн.

8. Принципы обеспечения безопасности ПДн.

9. Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.

10. Нормативно-правовая база в области обезличивания ПДн (Приказ Роскомнадзора от 19.06.2025 N 140 "Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Зарегистрировано в Минюсте России 31.07.2025 N 83110)

11. Свойства обезличенных данных.

12. Свойства методов обезличивания.

13. Методы обезличивания персональных данных. Сравнительный анализ методов обезличивания.

14. Алгоритм перемешивания данных в общем виде.

15. Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок.

16. Анализ эффективности алгоритма перемешивания ПДн с помощью циклических перестановок.

17. Определение политик безопасности (ПБ). Представление ПБ.

18. Закрытые, открытые, гибридные политики информационной безопасности.

19. Методы описания ПБ. Сравнительный анализ методов описания ПБ.

20. Аналитический метод описания ПБ.

21. Графовый метод описания ПБ.

22. Объектный метод описания ПБ.

23. Логический метод описания ПБ.

24. Пример графового метода описания ПБ: визуальный язык объектных ограничений «Language on Objects for Security Constraints» (LaSCO).

25. Определение графа атак. Формальное описание построения модели графа атак.

26. Анализ графа атак. Модель злоумышленника.

27. Определение гарантированной (верифицируемой) защиты.

28. Методы обеспечения гарантированности защиты.

29. Каналы несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду (НСДУВ).

30. Вероятностная оценка реализации канала НСДУВ.

31. Правовое и нормативное обеспечение защиты ПДн.

32. Назначение и средства антивирусной защиты.

33. Категории ПДн.

34. Назначение и средства идентификации и аутентификации субъектов.

35. Контролирующие органы в области ПДн, их функции.

36. Назначение и способы ограничения программной среды.

37. Мероприятия по обеспечению защиты ПДн при их обработке в информационных системах ПДн.

8. Согласие субъекта на обработку ПДн.

39. Назначение и способы физической защиты технических средств компьютерной системы.

40. Документы, предусмотренные постановлением Правительства 211, вид и краткое содержание.

41. Назначение и способы обеспечения доступности персональных данных.

42. Назначение выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и

(или) к возникновению угроз безопасности персональных данных, и реагирование на них.
43. Условия обработки персональных данных.

44. Назначение средств обнаружения (предотвращения) вторжений.

45. Модель угроз ИСПДн. Методика разработки.

46. Назначение и способы управление доступом субъектов доступа к объектам доступа.

47. Классификация информационных систем.

48. Назначение и способы обеспечение целостности информационной системы и персональных данных.

49. Определение уровня защищенности ПДн.

50. Назначение средств контроля (анализа) защищенности персональных данных.

51. Аттестация ОИ, имеющего в своем составе ИСПДн.

52. Назначение и средства регистрация событий безопасности (аудит).

53. Контроль и надзор за выполнением требований по обеспечению безопасности ПДн.

54. Назначение и способы защиты машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные.

55. Особенности гарантированного уничтожения информации на магнитных носителях с использованием магнитных воздействий.

56. Особенности гарантированного уничтожения информации на оптических носителях с использованием редуцирующего механического воздействия.

57. Особенности гарантированного уничтожения информации на полупроводниковых носителях с использованием термических воздействий.

Тестовые задания для зачета

1. Угрозы безопасности ПДн:

а) совокупность условий факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн;

б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности персональных данных;

в) только стихийное или бедствие техногенного характера.

2. Несанкционированный доступ (НСД) к информации:

а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС);

б) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств;

в) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа.

3. Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

а) несанкционированный доступ к информации, вредительские программы;

б) электромагнитные излучения и наводки, несанкционированная модификация структур;
в) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала.

4. Для защиты от случайных угроз компьютерной информации используют:

а) обучение пользователей правилам работы с КС, разрешительную систему доступа в помещение;

б) межсетевые экраны, идентификацию и аутентификацию пользователей;

в) дублирование информации, создание отказоустойчивых КС, блокировка ошибочных операций.

5. Системы анализа уязвимостей позволяют:

а) выявить злоумышленника работающего в компьютерной сети;

б) выявить уязвимости проектируемой системы защиты информации;

в) выявить уязвимости действующей системы защиты информации.

6. Персональные данные:

а) информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу;

б) данные, касающиеся состояния здоровья и религиозных взглядов человека;

в) информация о месте работы, паспортные данные, сведения о доходе.

7. Обработка персональных данных:

а) действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

б) накопление, хранение и передача персональных данных;

в) размещение персональных данных в информационных системах.

8. Оператор:

а) государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие

обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

б) юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных;

в) юридическое или физическое лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к персональным данным.

9. Контроль над выполнением требований в сфере защиты персональных данных выполняют: а) ФСБ РФ;

б) ФСТЭК России и Роскомнадзор;

в) все перечисленные организации.

10. За несоблюдение положений закона 152-ФЗ «О персональных данных» предусматривается:

а) гражданская, уголовная, административная ответственность;

б) дисциплинарная и другие виды ответственности;

в) все перечисленные виды ответственности. 1

1. Блокирование персональных данных:

а) временное прекращение обработки персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

в) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

12. Обезличивание персональных данных:

а) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных;

в) все перечисленные действия.

13. Срок хранения персональных данных в форме, позволяющей определить субъекта персональных данных:

а) 1 год;

б) 5 лет;

в) не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором.

14. Какую роль играют центры сертификации ключей:

а) они играют роль доверенной третьей стороны для доказывания факта передачи информации;

б) они служат для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов;

в) они выдают сертификат соответствия длины сгенерированных ключей требованиям нормативных документов.

15. Использование электронной подписи позволяет не допустить (лишнее исключить):

а) отказ от авторства;

б) приписывание авторства;

в) несанкционированное ознакомление с подписанным документов.

16. Обязано ли лицо, осуществляющее обработку персональных данных по поручению оператора, получать согласие субъекта персональных данных на обработку его персональных данных:

а) не обязано;

б) обязано;

в) не обязано только в случаях, предусмотренных законом.

17. В общедоступные источники персональных данных (в том числе справочники, адресные книги) персональные данные включаются:

а) с письменного согласия субъекта персональных данных;

б) согласия субъекта персональных данных не требуется;

в) согласия субъекта персональных данных не требуется, но по требованию субъекта данные в любое время должны быть исключены из общедоступных источников персональных данных.

18. В общем случае, согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в:

а) только письменной форме;

б) любой, позволяющей подтвердить факт его получения форме;

в) устной форме.

19. При проведении контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах персональных данных регуляторы:

а) вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных;

б) не вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных;

в) вправе знакомиться с персональными данными, обрабатываемыми в информационных системах персональных данных, только в установленных законом случаях.

20. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение:

а) тридцати дней с даты получения такого запроса;

б) десяти дней с даты получения такого запроса;

в) трех дней с даты получения такого запроса.