ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «БИС»

ОГРН 1181690023460, ИНН/КПП 1656102110/165601001;
Юридический адрес: 420032, РТ, г. Казань, ул. Гладилова, д. 27 пом. 1Н
Почтовый адрес: 420032, РТ, г. Казань, а/я №645, Тел. 8(843)203-40-40
БАНКОВСКИЕ РЕКВИЗИТЫ: БИК: 049205603, Наименование банка: ОТДЕЛЕНИЕ «БАНК ТАТАРСТАН» N8610 ПАО СБЕРБАНК,
Отделение Банка: 420094, г. Казань, ул. Чуйкова, 2, В,
К/С: 30101810600000000603 Р/С: 40702810562000033499

УТВЕРЖДАЮ
Директор
А.Ф. Скачкова
Приказ № ХБИС от 02.11.2022
«02» 11 2022 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

повышения квалификации по направлению:
«Цифровая компетенция педагога в области защиты персональных данных в образовательной среде,
включая обеспечение безопасности детей в интернет-пространстве»

(Срок освоения – 16 академ. часа
Форма обучения – Дистанционно, с применением исключительно электронного обучения, дистанционных образовательных технологий
Категория обучающихся – лица, имеющие среднее профессиональное и (или) высшее образование)

Казань – 2022

Содержание

1.	**Пояснительная записка**	3
2.	**Требования к результатам освоения программы**	3
2.	**Цели и задачи программы**	4
3.	**Требования к итоговой аттестации**	4
4.	**Календарный учебный график**	5
5.	**Содержание дополнительной профессиональной программы повышения квалификации**	5
6.	Раздел 1. Основы информационной безопасности	5
7.	Раздел 2. Персональные данные	6
8.	Раздел 3. Разработка организационно - распорядительной документации	8
9.	Раздел 4. Нормативно-правовые основы обеспечения информационной безопасности детей	9
10.	Раздел 5. Обеспечение безопасности детей в киберпространстве	10
11.	Раздел 6. Разработка организационно - распорядительной документации	10
12.	Раздел 7. Нормативно-правовые основы обеспечения информационной безопасности детей	11
13.	**Учебный план**	12
14.	**Перечень учебно-методической литературы и информационное обеспечение программы**	12
15.	**Материально-техническое обеспечение программы**	14
16.	**Кадровое обеспечение образовательного процесса**	14
17.	**Оценочные материалы**	15

1. Пояснительная записка.

Программа рассмотрена и одобрена на заседании Методического совета ООО «БИС» Протокол №4 от 02 ноября 2022 года.

Программа разработана в соответствии с нормами:

- Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, N 53, ст.7598; ст.4134,пунктом 1 и подпунктом 4.2.5. пункта 4 Положения о Министерстве Просвещения Российской Федерации от 28.07.2018 №884);
- с учетом требований приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрирован Минюстом России 20 августа 2013 г., регистрационный № 29444), с изменением внесенным приказом Минобрнауки России от 15 ноября 2013 г. № 1244 «О внесении изменений в Порядок организации и осуществлении образовательной деятельности по дополнительным профессиональным программам, утвержденный приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499» (зарегистрирован Минюстом России 14 января 2014 г., регистрационный номер № 31014);
- приказа Минобрнауки России от 23.08.2017 N 816 "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ" (Зарегистрировано в Минюсте России 18.09.2017 регистрационный № 48226).

1.1. **Категория обучающихся** – лица, имеющие среднее профессиональное и (или) высшее образование.

1.2. **Документ, выдаваемый после завершения обучения** – удостоверение о повышении квалификации установленного образца.

1.3. **Форма обучения** - Дистанционно, с применением исключительно электронного обучения, дистанционных образовательных технологий

1.4. **Длительность обучения** - 16 академ. часа.

2. Требования к результатам освоения программы.

2.1. **В результате освоения Программы**, слушатели:

Должны уметь:

составлять перечень сведений, отнесенных к персональным данным и проводить их классификацию;

выбирать современные методы, средства и технологии обеспечения информационной безопасности, с учетом характера защищаемой информации;

оперативно актуализировать внутренние локально-нормативные акты в области информационной безопасности в организации

готовить уведомления в уполномоченный орган по защите прав субъектов персональных данных;

применять полученные навыки по информационной безопасности в трудовой деятельности;

внедрять полученные знание при проведении профилактических мероприятиях на тему безопасности детей в интернет-пространстве;

определять виды угроз в Интернете;

Должны владеть:

основами информационной безопасности;

базовыми знаниями нормативно-правовых основ обеспечения информационной безопасности детей;

навыками использования позитивными социокультурными онлайн-практиками.

3. Цели и задачи дополнительной профессиональной программы повышения квалификации.

Цель: формирование знаний и применение на практике необходимых навыков для организации сбора, обработки, хранения и защиты персональных данных в соответствии с требованиями законодательства и органов государственного контроля и надзора

Задачи:

1. Познакомить с основами информационной безопасности;
2. Расширить знания о действующих правовых нормах и законодательных актах, регулирующих отношения в сфере персональных данных.
3. Обучить навыкам обработки персональных данных в соответствии с законодательством;
4. Сформировать навыки по составлению и разработке организационно-распорядительной документации;
5. Дать информацию об особенностях работы с электронными подписями.
6. Актуализировать знания по темам интернет безопасности.

4. Требования к итоговой аттестации.

4.1. **Промежуточный контроль** знаний осуществляется через экспертную оценку преподавателем курса успеваемости слушателей в процессе выполнения практических заданий и других видов работ по разделам программы Дополнительная профессиональная программа повышения квалификации «Цифровая компетенция педагога в области защиты персональных данных в образовательной среде, включая обеспечение безопасности детей в интернет-пространстве» заканчивается итоговым тестированием. В случае успешного прохождения итогового тестирования по образовательному курсу Программы, слушатель получает удостоверение о повышении квалификации. Слушателю, не прошедшему итоговое тестирование или получившему на итоговом тестировании неудовлетворительную оценку, выдается справка об обучении.

4.2. **Практические занятия** проходят в формате учебных дискуссий, решение проблемных кейсов, деловые игры, обучающий тренинг.

5. Календарный учебный график.

График обучения / Форма обучения	Кол-во часов/дней	Кол-во дней	Общая труд. час.
Дистанционно, с применением исключительного электронного обучения, дистанционных образовательных технологий	6-8	2	16
Всего часов	16	2	16

6. Содержание дополнительной профессиональной программы повышения квалификации.

6.1. Рабочие программы учебных разделов

Раздел 1. Основы информационной безопасности

Тема 1. Основные понятия, термины, структура.

Предметная область теории информационной безопасности. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Концепция информационной безопасности организации. Организационная структура системы обеспечения информационной безопасности. Систематизация понятий в области защиты информации.

Тема 2. Информация: что это такое, виды информации, понятия. Основные свойства информации: целостность, доступность, конфиденциальность.

Понятие об информации как объекте защиты. Виды защищаемой информации. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Основные термины: информация, информационные технологии, информационная система, обладатель информации, оператор информационной системы, конфиденциальность информации.

Тема 3. Информационная безопасность. Понятие и практическое применение в ежедневной работе.

История становления теории информационной безопасности. Проблемы информационной безопасности. Основные понятия и анализ угроз информационной безопасности. Стандарты информационной безопасности. Методологические подходы к защите информации и принципы ее организации. Угрозы информационной безопасности. Основные меры противодействия угрозам информационной безопасности.

Тема 4. Основные группы конфиденциальной информации, порядок защиты.

Виды конфиденциальной информации. Виды информационных угроз. Классификация методов защиты информации. Нормативная база конфиденциальной информации. Категории информации по степени конфиденциальности. Государственная тайна. Коммерческая тайна. Профессиональная тайна. Меры защиты конфиденциальной информации: правовые, организационные, технические.

Раздел 2. Персональные данные

Тема 5. Основные понятия, связанные с персональными данными. Виды и группы персональных данных. Субъекты персональных данных.

Основные термины и понятия (персональные данные, информационные системы персональных данных, обработка персональных данных и т.п.). Классификация персональных данных: общие, биометрические, специальные, иные. Способы защиты персональных данных в зависимости от их класса. Нормативные правовые акты, устанавливающие требования по защите персональных данных.

Тема 6. Способы обработки персональных данных: автоматизированный, неавтоматизированный, смешанный.

Принципы обработки персональных данных. Способы обработки персональных данных государственными и муниципальными органами. Условия обработки. Цели обработки персональных данных. Особенности обеспечения безопасности персональных данных в автоматизированных системах. Обеспечение безопасности данных, обрабатываемых неавтоматизированными способами.

Тема 7. Виды действий и операций, связанных с обработкой персональных данных. Особенности взаимодействия с персональными данными в государственных учреждениях.

Информационная система персональных данных. Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Организация работ и назначение ответственных лиц. Основные виды действий при обработке персональных данных: распространение персональных данных, предоставление персональных данных, блокирование персональных данных, уничтожение персональных данных, обезличивание персональных данных, трансграничная передача персональных данных.

Тема 8. Безопасная работа при осуществлении организацией информационного взаимодействия, с использованием сервисов Государственной интегрированной системы телекоммуникаций Республики Татарстан.

Информационная безопасность организации - правовые основы. Способы обработки персональных данных государственными и муниципальными органами. Обеспечение безопасности персональных данных при их обработке в государственных информационных системах. Общая характеристика уязвимостей информационной системы персональных данных

Тема 9. Законодательство, регулирующее отношения в сфере информационной безопасности и защиты персональных данных. Нормативно-правовое регулирование в сфере защиты персональных данных.

Нормативно- правовые акты, устанавливающих требования по защите персональных данных. Система нормативного правового регулирования организации обработки и обеспечения безопасности персональных данных в Российской Федерации. Основные положения Закона «О персональных данных». Актуальные изменения государственной политики России в сфере информационной безопасности.

Тема 10. Регуляторы (государственные органы), осуществляющие функции контроля и проверок в сфере защиты конфиденциальной информации. Санкции и ответственность.

Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность. Система государственного контроля и надзора за обеспечением безопасности персональных данных. Ответственность за нарушение требований по обращению с персональными данными. Практика правоприменения. Рекомендации по подготовке к проведению контроля и надзора за выполнением требований нормативных правовых актов Российской Федерации по защите персональных данных.

Тема 11. Согласие на обработку персональных данных: правильность составления, необходимые условия.

Согласие на обработку персональных данных: основание, назначение, вид документа, содержание документа, ответственный за составление. Требования к согласию на обработку персональных данных. Разработка типового согласия на обработку персональных данных сотрудников организации и иных субъектов персональных данных. Основные ошибки в составлении согласия на обработку персональных данных.

Тема 12. Отказ от предоставления информации. Правовые аспекты и законность действий, правильное оформление отказа в юридическом аспекте.

Случаи, предусмотренные законодательством, в которых предоставление согласия не является обязательным. Прием и обработка обращений и запросов субъектов персональных данных или их представителей. Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

Раздел 3. Разработка организационно-распорядительной документации.

Тема 13. Основы правильности составления и разработки организационно-распорядительной документации, структура документов.

Состав организационно-распорядительной документации в области персональных данных: приказы, инструкции, техническая документация, модели угроз. Корректное определение целей и способов обработки персональных данных. Правовые основания обработки персональных данных. Составление согласий в различных ситуациях. Локальные акты по вопросам обработки

персональных данных: их содержание, порядок разработки и ввода в действие. Политика в отношении обработки персональных данных в организации.

Тема 14. Требования к интернет-сайту организации в части информационной безопасности.

Политика конфиденциальности: основные составляющие. Текст согласия на обработку персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган. Определение правового основания обработки персональных данных и прочих сведений, необходимых для регистрации организации в реестре Роскомнадзора.

Тема 15. Порядок изготовления, получения, установки и безопасного использования электронной подписи. Особенности работы с электронными подписями.

История криптографии. Модели шифров. Виды электронной подписи: простая электронная подпись, неквалифицированная электронная подпись, квалифицированная электронная подпись. Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи". Требования к хранению электронной подписи в организации. Состав электронной подписи. Риски использования электронной подписи. Требования и рекомендации по обеспечению информационной безопасности на рабочем месте пользователя.

Раздел 4. Нормативно-правовые основы обеспечения информационной безопасности детей

Тема 16. Нормативно-правовая база в области обеспечения информационной безопасности детей

Федеральный закон от 29.12.2012N273-ФЗ «Об образовании в Российской Федерации»; Федеральный закон от 29.12.2010 N436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; Указ Президента Российской Федерации от 01.06.2012 г. N761 «О национальной стратегии действий в интересах детей на 2012-2017 годы»; Распоряжение Правительства Российской Федерации от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей»

Тема 17. Ответственность за правонарушения в области информационной безопасности.

Понятие и характеристика информационного правонарушения. Виды ответственности за информационные правонарушения: уголовная ответственность, административная ответственность, дисциплинарная ответственность, гражданско-правовая (имущественная) ответственность.

Раздел 5. Обеспечение безопасности детей в киберпространстве

Тема 18. Виды информации, запрещенной к распространению посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей.

Перечень видов информации, запрещенной к распространению посредством сети "интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования. Описание видов информации, запрещенной для распространения среди детей, согласно ч. 2 ст. 5 Федерального закона № 436-ФЗ. Описание видов информации, распространение которой среди детей определенных возрастных категорий ограничено, согласно ч. 3 ст. 5 Федерального закона № 436-ФЗ. Описание видов информации, не соответствующей задачам образования.

Тема 19. Виды угроз в интернете.

Терминология и подходы к классификации. Классификация Интернет-угроз: технологические угрозы, социальные угрозы. Типология угроз и рисков безопасности

Тема 20. Технологические угрозы.

Вредоносное ПО. Фишинг. Бесплатный WI-FI. Надежный пароль. Интернет - шопинг (платежные карты в интернете). Компьютерное пиратство.

Тема 21. Социальные угрозы.

Овершеринг/Шерентинг (+цифровая репутация). Киберагрессия. Цифровой этикет. Вербовка: Интернет, как современный источник распространения террористической и экстремистской идеологии. Фейковые новости/когнитивные искажения. Социальные сети, сообщества, быстрые заработки: лудомания, кладмены, нормализация насилия, аморальных ценностей. Влияние гаджетов на здоровье: психическое/ментальное.

Раздел 6. Позитивные социокультурные онлайн-практики

Тема 22. Анализ зарубежных и российских работ и результаты собственного мониторинга позитивных онлайн-практик.

Разбор понятий социокультурные и социальные практики. Виды социокультурных практик. Функции социокультурных практик. Виды онлайн практик. Сравнение зарубежных и российских онлайн практик: выявление особенностей.

Тема 23. Онлайн-практики взаимодействия с информацией: критичность и безопасность.

Особенности понятия «Информация» в цифровую эпоху. Практики медиапотребления в Сети. Понятие новые и традиционные медиа. Информационные онлайн-риски: виды и способы преодоления. Практики противодействия деструктивному онлайн-контенту. Практики создания позитивного онлайн-контента

Тема 24. Коммуникативные онлайн-практики: особенности и функции.

Особенности коммуникации в сети Интернет. Социальные сети: понятие и функции. Невербальные средства онлайн-коммуникации. Анализ позитивных практик онлайн-коммуникации. Деструктивные коммуникативные практики. Исследование практик онлайн-коммуникации.

Тема 25. Основные виды современных онлайн - практик

Флешмоб. Челлендж. Блогинг. Краудсорсинг. Онлайн-волонтерство. Онлайн-благотворительность. Цифровой активизм как практика цифрового гражданина.

Раздел 7. Формирование медиаграмотности среди учеников

Тема 26. Понятие медиаграмотности;

Медиаграмотность: сущность, основные понятия, проблемы формирования. Функции медиаграмотности. Методы формирования медиаграмотности.

Тема 27. Диагностика медиаграмотности у учеников;

Теоретические основы формирования элементов медиаграмотности в процессе обучения. Методика повышения уровня медиаграмотности учащихся средствами медиаобразования в процессе обучения.

Тема 28. Практические занятия.

Медиаобразовательные упражнения и игры для учеников: «Хорошо и плохо», «Разговор на тему…», «Выпуск новостей». Применение на практики.

7.Учебный план.

№ п/п	Наименование учебных разделов	Всего час.	в том числе	
			Лекции	Практика
1.	Основы информационной безопасности	2	2	-
2.	Персональные данные	2	2	-
3.	Разработка организационно - распорядительной документации	2	1	1
4.	Нормативно-правовые основы обеспечения информационной безопасности детей	2	2	-
5.	Обеспечение безопасности детей в киберпространстве	2	2	-
6.	Позитивные социокультурные онлайн – практики	2	2	-
7.	Формирование медиаграмотности среди учеников	2	1	1
8.	Итоговая аттестация	2		2
	Итого:	16	12	4

8. Перечень учебно-методической литературы и информационное обеспечение программы.

8.1 Федеральные законы и нормативные документы:

Федеральный закон «О персональных данных» от 27.07.2006 N152-ФЗ.

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

Федеральный закон от 29.12.2012N273-ФЗ «Об образовании в Российской Федерации»;

Федеральный закон от 29.12.2010 N436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

Указ Президента Российской Федерации от 01.06.2012 г. N761 «О национальной стратегии действий в интересах детей на 2012-2017 годы»;

Распоряжение Правительства Российской Федерации от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей».

8.2 Основная литература:

1. Информационная безопасность и защита информации: учеб. пособие / В. П. Мельников и др.; под ред. С. А. Клейменова.- М. : Академия , 2009.-330 с.
2. Галатенко, В. А. Основы информационной безопасности: Курс лекций: Учеб. пособие для вузов по специальностям в обл. информ. технологий / В. А. Галатенко; Под ред. В. Б. Бетелина; Интернет-ун-т информ. технологий.- Интернет-Университет Информационных Технологий, 2006.-205 с.
3. Информационная безопасность: нормативно-правовые аспекты: учеб. пособие по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информ. безопасности автоматиз. систем" / Ю. А. Родичев.- СПб. и др. : Питер , 2008.-271 с.
4. Абаев Ф.А. Понятие, правовая природа персональных данных // Право и государство: теория и практика. 2014. № 3 (111). С. 126-131.
5. Бондарь А.О., Железняк В.П., Мещеряков В.А. Организация работы по обеспечению защиты государственных информационных систем персональных данных // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции. Воронеж: ИПЦ «Научная книга», 2013. С. 174-175.
6. Г. У. Солдатова, С. В. Чигарькова, С. Н. Илюхина
Социокультурные онлайн-практики в молодежной среде: МЫ В ОТВЕТЕ ЗА ЦИФРОВОЙ МИР, Учебное пособие, Москва 2021г.

8.3 Дополнительная литература:

1. Защита конфиденциальной информации: учеб. пособие для вузов по спец. 090103 "Орг. и технология защиты информации" и 090104 "Комплекс. защита объектов информатизации" / В. Я. Ищейнов, М. В. Мецатунян.- М. : Форум , 2009.-254 с.
2. Терещенко, Л.К. Правовой режим персональных данных и безопасность личности /Л. К. Терещенко //Закон. -2018.- №6.- С. 37 -43.
Трофимова, И.А. Обработка и хранение персональных данных/ И.А. Трофимова // Делопроизводство.- 2015. — № 3. — С. 107 — 110.
3. Алексеева Е. Гарантии защиты персональных данных работника в современном российском законодательстве // К познанию права. Сборник студенческих научных работ. - Брянск: Изд-во Группа компаний "Десяточка", 2008, Вып. 3. - С. 42-48
Вельдер И.А. Принципы защиты персональных данных в законодательстве ЕС // Сборник аспирантских научных работ юридического факультета КГУ. - Казань: Изд-во Казан. ун-та, 2005, Вып. 6. - С. 99-104.
4. Волчинская Е.К., Дятленко В.В. Законодательство о защите персональных данных: проблемы и решения // Информационное право. - М.: Юрист, 2006, № 1 (4). - С. 11-16.

8.4 Электронные источники

1.Защита персональных данных https://www.open-vision.ru/solutions/information-security/zashhityi-personalnyix-dannyix/

8.5 Базы данных, информационно-справочные и поисковые систем:

1.Информационно-справочные системы «Гарант», «Консультант +»;

9. Материально-техническое обеспечение программы.

	Наименование программы в соответствии с учебным планом	Наименование объектов для проведения практических занятий с перечнем основного оборудования	Фактический адрес учебных кабинетов и объектов
	«Цифровая компетенция педагога в области защиты персональных данных в образовательной среде, включая обеспечение безопасности детей в интернет-пространстве»	Ноутбуки– 5 шт. Принтер – 1 шт. Мультимедиа устройство (проектор) – 1 шт. Наушники проводные – 5 шт. Высокоскоростной Интернет	420032, Республика Татарстан г. Казань, ул. Гладилова зд. 27, помещение 1н. (17,2 кв.м.)

Обучение проходит дистанционно (онлайн), с применением исключительного электронного обучения, дистанционных образовательных технологий, по ссылке https://distant.bis-comp.ru

10. Кадровое обеспечение образовательного процесса.

Квалификация руководящих и педагогических работников соответствует квалификационным характеристикам, установленным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих, разделе "Квалификационные характеристики должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования", утвержденном приказом Министерства здравоохранения и социального развития Российской Федерации от 11.01.2011 №1н.

11. Оценочные материалы.

11.1 Система оценки достижений

Тестовые вопросы для итоговой аттестации

Тестирование проводится в модульной объектно-ориентированной динамической учебной среде на базе платформы «Moodle».

Для определения уровня знаний слушателей принята следующая шкала оценки знаний:

«отлично» – 85–100% правильных ответов;

«хорошо» – 70–84,99 % правильных ответов;

«удовлетворительно» – 55–69,99% правильных ответов;

«неудовлетворительно» – 54,99% и меньше правильных ответов.

11.2 Конторольное тестирование:

1. Определите термин и впишите его

Информация _____ — это...

2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц называется:

a)защита информации

b)распространение информации

c)доступ к информации

3. Термин означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение

a)доступность информации

b)целостность информации

c)открытость информации

4. Что из нижеперечисленного является информацией?

a)разговор с коллегой

b)дипломная работа

c)переписка со знакомым

e)все вышеперечисленное

5. К какому методу защиты информации относятся антивирусы

организационному

a)физическому

b)программному

6. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения требований по защите персональных данных?

a)Нет, только к административной ответственности

b)Нет, если это государственное предприятие

c)Да

7. Что такое биометрические персональные данные?

a)отпечатки пальцев, слепок голоса, код ДНК;

b)данные о моей активности в Интернете;

c)сведения о вкусовых пристрастиях и привычках.

8. Являются ли фотографии персональными данными?

a)Да, если это портретная съемка, и лицо изображено крупным планом

b)Нет. Персональными данными может быть только текстовая информация

c)Да, если рядом с фото есть указание имени и фамилии человека, и эти сведения позволяют его идентифицировать.

9. К основным регуляторам в сфере обработки персональных данных относятся:

a)Роскомнадзор

b)ФСТЭК

c)ФСБ

e)Все вышеперечисленное

10. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?

a)Биометрические

b)Общие персональные данные

c)Специальные

e)Дополнительные

11. Обработка персональных данных с помощью средств вычислительной техники называется:

a)Автоматизированная обработка

b)Без использования средств автоматизации

c)Смешанный способ

12. Какой федеральный закон является базовым в Российском законодательстве в области информационных отношений и информационной безопасности?

a)о техническом регулировании

b)об информации, информационных технологиях и о защите информации

c)о лицензировании отдельных видов деятельности

13. В какой орган нужно отправить Уведомление об обработке персональных данных?

a)Администрация района;

b)Департамент информационных технологий;

c)Управление Роскомнадзора

14. Оператор до начала обработки персональных данных обязан уведомить территориальный орган Роскомнадзора о своем намерении осуществлять обработку персональных данных. Верно ли данное утверждение?

a)Да

b)Нет

15 Разрешается ли редактирование файла, подписанного электронной подписью:

a)нет;

b)да;

c)разрешается только владельцу с полными правами.

16. На вашем рабочем компьютере закончилась лицензия антивируса (средство защиты информации), Ваши действия.

a)продолжу пользоваться как обычно

b)обращусь к системному администратору за помощью

c)самостоятельно скачаю антивирус из интернета

17. Сопоставьте персональные данные с их видами

1)	Специальные	a)	национальная принадлежность
2)	Биометрические	b)	фамилия, имя, отчеств
3)	Общие	c)	рост и вес

18. Что такое кибербуллинг?

a) вид цифровой агрессии

b) кража логинов и паролей

c) вид компьютерного вируса

19. Выберите признак фейковой новости. Это…

a) Правдивое содержание

b) Информация без настоящих фактов

c) Короткий заголовок

Ответы:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
совокупность каких-либо сведений, данных, передаваемых устно (в форме речи), письменно (в виде текста, таблиц, рисунков, чертежей, схем, условных обозначений), либо другим способом	b	b	e	b	c	a	c	e	c	a	b	c	a	a	b	1-a; 2-c; 3-b	a	b

Заместитель директора ООО «БИС» _____ Е.В. Александрова

Методист _____ А.Н. Галеева