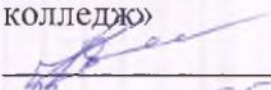


Министерство образования и науки Тамбовской области
Тамбовское областное государственное бюджетное
профессиональное образовательное учреждение
«Мичуринский агросоциальный техникум»
(ТОГБПОУ «Мичуринский агросоциальный техникум»)

УТВЕРЖДАЮ
Директор ТОГБПОУ
«Мичуринский агросоциальный
колледж»

О.В. Котельникова
«32» 05 2023 г.

**Фонд оценочных средств
учебной дисциплины**

**ОП.04 Законодательство Российской Федерации в области хранения и
распространения персональных данных, интеллектуальной собственности,
правил использования информационных материалов в информационно-
телекоммуникационной сети «Интернет»**

программы подготовки квалифицированных рабочих, должности служащих
по профессии

09.01.03 Оператор информационных систем и ресурсов

РАССМОТРЕНО

На заседании методического совета

Протокол № 10 от 22.05. 2023г.

Председатель  А.В. Свиридов

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по профессии 09.01.03 Оператор информационных систем и ресурсов

Разработчик:

Данилова Наталия Владимировна,

мастер п/о ТОГБПОУ «Мичуринский агросоциальный техникум»

Рассмотрена на заседании предметно-цикловой комиссии гуманитарного, математического, естественно-научного и информационного цикла.

Протокол № 8 от 19 мая 2023 г.

Председатель Лошаков /Лошаков С.Ю./

Согласовано:

Зам. директора по УПР

С.Ю. Гусельникова

« 22 » 05 2023 г.

I. Паспорт фонда оценочных средств

1. Область применения фонда оценочных средств

Фонд оценочных средств предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП.04 Законодательство Российской Федерации в области хранения и распространения персональных данных, интеллектуальной собственности, правил использования информационных материалов в информационно-телекоммуникационной сети «Интернет».

В рамках оценочных материалов результатов освоения рабочей программы осуществляется оценка результатов практической подготовки обучающихся.

Оценка результатов практической подготовки осуществляется в образовательной организации (в техникуме) и(или) на предприятии, в организации.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме зачета.

Фонд оценочных средств разработан на основании: основной профессиональной образовательной программы по профессии 09.01.03 Оператор информационных систем и ресурсов;

программы учебной дисциплины ОП.04 Законодательство Российской Федерации в области хранения и распространения персональных данных, интеллектуальной собственности, правил использования информационных материалов в информационно-телекоммуникационной сети «Интернет».

Таблица 1

Наименование объектов контроля и оценки (объекты оценивания) ¹	Основные показатели оценки результата и их критерии	Тип задания; № задания	Форма аттестации (в соответствии с учебным планом)
У1 принимать юридические решения в соответствии с действующим законодательством в области информационного права, защиты любой информации	демонстрирует умение принимать юридические решения в соответствии с действующим законодательством в области информационного права, защиты любой информации	Тестирование Индивидуальные задания Презентации	Защита презентации
У2 применять нормативно-правовые акты, регулирующие информационные общественные отношения	демонстрирует знание нормативно-правовых актов, регулирующих информационные общественные отношения участвовать в разработке	Тестирование Индивидуальные задания Презентации	
У3 обеспечить в рамках правового поля защиту информации о различных субъектах, объектах, фактах; организовать работу с документами на базе	-обеспечить в рамках правового поля защиту информации о различных субъектах, объектах, фактах; организовать работу с документами на	Тестирование Индивидуальные задания Презентации	

¹ Личностные результаты обучающихся в соответствии с Рабочей программой воспитания по профессии 09.01.03 Оператор информационных систем и ресурсов учитываются в ходе оценки результатов освоения учебной дисциплины.

современных информационных технологий;	базе современных информационных технологий.	
31 знать основные субъекты информационного права, объекты информационного права, информационные технологии и средства их обеспечения	демонстрирует знание основных субъектов информационного права, объектов информационного права, информационных технологий и средств их обеспечения	Тестирование Индивидуальные задания Презентации
32 различные нормативные акты, регулирующие информационные отношения	-демонстрирует знание различных нормативных актов, регулирующих информационные отношения	Тестирование Индивидуальные задания Презентации
-основу техники создания, обработки и хранения документов; современные технические средства автоматизированного управления офисного делопроизводства, средства составления и изготовления текстовых документов, средства обработки документов, средства поиска, хранения и транспортирования документов, средства административно-управленческой связи;	- демонстрирует основу техники создания, обработки и хранения документов; современные технические средства автоматизированного управления офисного делопроизводства, средства составления и изготовления текстовых документов, средства обработки документов, средства поиска, хранения и транспортирования документов, средства административно-управленческой связи;	Тестирование Индивидуальные задания Презентации
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Участие во внеурочной деятельности (олимпиадах, конкурсах, неделях ЦМК, празднике «Студенческая весна»); систематическая подготовка к практическим занятиям; оформление портфолио;	Тестирование Индивидуальные задания Презентации
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Извлечение и анализ информации из различных источников; использование различных способов поиска информации; применение найденной информации для решения профессиональных задач;	Тестирование Индивидуальные задания Презентации
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	Точное выполнение требований преподавателя; рациональное планирование этапов	Тестирование Индивидуальные задания Презентации

	деятельности; оптимальный выбор методов и способов выполнения практических и самостоятельных работ;		
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Способность работать в команде, толерантно воспринимать социальные, этнические, конфессиональные и культурные различия;	Тестирование Индивидуальные задания Презентации	
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Целесообразное использование разнообразных источников информации, включая Интернет, при подготовке к практическим занятиям, написании докладов, сообщений и т.д. Обладание навыками работы с различными видами информации; результативное использование технологии ИКТ и их применение в соответствии с конкретным характером профессиональной деятельности;	Тестирование Индивидуальные задания Презентации	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Посещает культурные и исторические памятники, дает толкование понятий «гражданин», «гражданство», «патриотизм», «социальная ответственность», «социальный конфликт», анализирует программные документы различных партий и общественных объединений по заданным критериям, объясняет значение семьи в современном обществе, приводя примеры, участвует в социально-ориентированных акциях и т.д.	Тестирование Индивидуальные задания Презентации	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Разработка и защита докладов, сообщений, презентаций в соответствии с изменяющимися технологиями; участие в фестивалях творческих	Тестирование Индивидуальные задания Презентации	

	проектов; участие в конкурсах, олимпиадах; участие в месячнике специальности		
<i>ВПД 2. техническая обработка и размещение информационных ресурсов на сайте (по выбору)</i> ПК 2.1. Использовать систему электронного документооборота	владеть способностью использовать информационно-коммуникационные технологии, управлять информацией с использованием прикладных программ деловой сферы деятельности использовать компьютерные технологии и базы данных;	Тестирование Индивидуальные задания Презентации	
<i>ВПД 3. Подготовка интерфейсной графики (по выбору)</i> ПК 2.2. Сопровождать документы с электронно-цифровой подписью	подготовка, техническая обработка и размещение контента электронного документооборота (по выбору)	Тестирование Индивидуальные задания Презентации	<i>Защита презентации</i>
<i>ВПД 4. Подготовка, техническая обработка и размещение контента электронного документооборота (по выбору)</i> ПК 2.3. Устанавливать и разграничивать права доступа к разделам веб-ресурса		Тестирование Индивидуальные задания Презентации	<i>Защита презентации</i>

2. Комплект оценочных средств

2.1. Задания для текущего контроля

Задания практического характера

Тема 1.1. Вопросы для обсуждения:

1. Информационные отношения как предмет информационного права: - правоотношения, связанные с созданием и преобразованием информации; - правоотношения, связанные с хранением информации; - правоотношения, связанные с передачей и распространением информации; - правоотношения, связанные с потреблением информации.
2. Методы регулирования информационных правоотношений.
3. Субъекты информационных правоотношений.
4. Соотношение системы информационного законодательства и системы информационного права. Дискуссия о месте информационного права в системе российского права.

Тема 2.1. Вопросы для обсуждения:

1. Роль информации в жизни личности, общества, государства, Информационное общество. Стадии становления.
2. Понятие информационного общества. Правовое обеспечение формирования информационного общества в Российской Федерации.
3. Окинавская хартия глобального информационного общества. Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии».

Тема 3.1. Вопросы для обсуждения:

1. Понятие источников информационного права.
2. Подготовка перечней нормативных правовых актов, регулирующих информационные правоотношения: законодательные акты, нормативные правовые акты Президента РФ и Правительства РФ, федеральных органов исполнительной власти.

Тема 4.1. Вопросы для обсуждения:

1. Понятие документирования информации. Юридическая сила документов на электронных носителях.
2. Электронная подпись как институт информационного права.
3. Понятие и структура государственных информационных ресурсов РФ.
4. Правовой режим информационных ресурсов.

Тема 5.1. Вопросы для обсуждения:

1. Электронный документооборот. Система межведомственного электронного документооборота.
2. Государственные и муниципальные услуги в электронной форме.
3. Система межведомственного электронного взаимодействия.

Тема 6.1. Доклады и презентации:

1. Соотношение понятий «право на информацию» и «право на доступ к информации».
2. Общедоступные информационные ресурсы.
3. Право на доступ к информации. Законодательное регулирование права на информацию.
4. Понятие и структура информации с ограниченным доступом. Классификация видов тайн.
5. Понятие доступа к информации. Правовое обеспечение доступа к информации о деятельности органов государственной власти, местного самоуправления и судов РФ.
6. Проблемы допуска к информации, составляющей государственную, служебную, коммерческую и иные виды тайн.
7. Доступ к информации как обеспечение мер борьбы с коррупцией.

Тема 7. Доклады и презентации:

1. Принципы обеспечения права на доступ к информации.
2. Предоставление информации. Распространение информации.
3. Защита права на доступ к информации. Институт тайны как правовой режим защиты информации ограниченного доступа.
4. Понятие и структура информации с ограниченным доступом. Классификация видов тайн.
5. Проблемы допуска к информации, составляющей государственную, служебную, коммерческую и иные виды тайн.

Тема 8. Доклады и презентации:

1. Понятие персональных данных.
2. Понятие и структура права на неприкосновенность частной жизни.
3. Персональные данные как особый институт охраны права на неприкосновенность частной жизни.
4. Особенности защиты персональных данных и частной жизни в сети Интернет.

Тема 9. Доклады и презентации:

1. Правовые формы организации деятельности СМИ. Роль государства в деятельности СМИ.
2. Рекламная информация в СМИ. Понятие рекламы и основные требования к рекламной деятельности. Цели законодательного регулирования рекламы.
3. Особенности отдельных способов распространения рекламы.
4. Реклама с использованием новых информационных технологий.

5. Проблемы рекламы товаров и услуг, а также политической рекламы в информационно-телекоммуникационных сетях.

Тема 10. Доклады и презентации:

1. Принципы деятельности библиотек, гарантирующие права человека, общественных объединений, народов и этнических общностей на свободный доступ к информации.
2. Основные виды библиотек. Электронные библиотеки.
3. Архивный фонд РФ.
4. Понятие архивного документа. Виды архивных документов.
5. Электронные архивные документы. Проблемы, связанные с определением подлинника и копии электронного документа.
6. Правовой режим архивных документов. Защита права собственности на архивные документы.

Тема 11. Доклады и презентации:

1. Сайт и доменное имя как объект информационного права.
2. Проблемы обеспечения авторского права и использование объектов авторского права и смежных прав в информационно-телекоммуникационной сети Интернет.
3. Основы международной информационной безопасности.
4. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.
5. Правонарушения в информационно-телекоммуникационной сети Интернет.

Тема 12. Доклады и презентации:

1. Понятие информационной безопасности. Положения Доктрины информационной безопасности РФ.
2. Государственная политика РФ в области организационно-правового обеспечения информационной безопасности.
3. Юридическая ответственность за правонарушения в информационной сфере.
4. Актуальные вопросы охраны персональных данных в социальных сетях.

Шкала оценки образовательных достижений

Процент результативности (правильных ответов)	Оценка уровня подготовки	
	балл (отметка)	вербальный аналог
90 - 100	5	отлично
70 - 89	4	хорошо
55 - 79	3	удовлетворительно
менее 55	2	неудовлетворительно

Тема 1.1. Информационная безопасность.

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- + Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

- + Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

- + Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

- + Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

- + Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- + органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

- + Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компания
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

- + Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

- + Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

- + Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

- + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
- + Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- + Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
- + Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
- + Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- + Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
- + Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

- + Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- + Целостность
- Доступность
- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

- + Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
- + Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

- + Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- + Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

- + Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- + Аудит, анализ уязвимостей, риск-ситуаций

Тема 2.1. Этика сетевого общения

Вопрос № 1

Как по-другому называются нормативные акты, регулирующие частные аспекты функционирования сети?

- незаконные
- подзаконные
- законные

Вопрос № 2

Присутствует ли регулирование правовых отношений в Интернете на международном (межгосударственном) уровне?

- присутствует
- практически отсутствует
- полностью исключено

Вопрос № 3

В чём заключается основная проблема Интернета?

- Интернет не имеет территориальных границ своего распространения
- Интернет имеет территориальные границы своего распространения
- У Интернета нет проблем

Вопрос № 4

Где наиболее очевидна связь с территорией при размещении информации?

- на определённом сервере
- на любом сервере
- затрудняюсь ответить

Вопрос № 5

В чём достоинство Интернета?

- расширяет среду общения до размеров земного шара
- можно общаться только в отведённых зонах
- расширяет среду общения до размеров вселенной

Вопрос № 6

С чем возникло понятие «сетевой этикет»?

- с появлением социальных сетей
- с появлением электронной почты
- с появлением различных браузеров

Вопрос № 7

На что похожи правила сетевого этикета?

- похожи на правила в метро
- похожи на правила в игре
- похожи на правила поведения в реальной жизни

Вопрос № 8

Что такое спам?

- обязательная реклама
- навязчивая реклама
- затрудняюсь ответить

Вопрос № 9

Что принято вписывать в поле темы, отвечая на чьё-либо письмо?

- Re: Исходная_тема
- Re: Любимая_тема
- Re: Научная_тема

Вопрос № 10

Что означает фраза, написанная БОЛЬШИМИ БУКВАМИ?

- автор смеётся
- автор громко кричит
- затрудняюсь ответить

Вопрос № 11

Что такое смайлики?

- комбинация текстовых символов
- комбинация чисел
- затрудняюсь ответить

Вопрос № 12

Где становится доступным для лиц любой материал, размещённый в Интернете?

- в определённой точке земного шара
- только в столице
- в любой точке земного шара

Тема 3.1. Информационная безопасность сетевой технологии работы

Тест с ответами: «Информационная безопасность»

1. Основная масса угроз информационной безопасности приходится на:
 - а) Троянские программы +
 - б) Шпионские программы
 - в) Черви

2. Какой вид идентификации и аутентификации получил наибольшее распространение:
 - а) системы PKI
 - б) постоянные пароли +
 - в) одноразовые пароли

3. Под какие системы распространение вирусов происходит наиболее динамично:
 - а) Windows
 - б) Mac OS
 - в) Android +

4. Заключительным этапом построения системы защиты является:
 - а) сопровождение +
 - б) планирование
 - в) анализ уязвимых мест

5. Какие угрозы безопасности информации являются преднамеренными:
 - а) ошибки персонала
 - б) открытие электронного письма, содержащего вирус
 - в) не авторизованный доступ +

6. Какой подход к обеспечению безопасности имеет место:
 - а) теоретический
 - б) комплексный +
 - в) логический

7. Системой криптографической защиты информации является:
 - а) VFox Pro
 - б) CAudit Pro
 - в) Крипто Про +

8. Какие вирусы активизируются в самом начале работы с операционной системой:
 - а) загрузочные вирусы +
 - б) троянцы
 - в) черви

9. Stuxnet — это:
 - а) троянская программа
 - б) макровирус
 - в) промышленный вирус +

10. Таргетированная атака — это:
 - а) атака на сетевое оборудование
 - б) атака на компьютерную систему крупного предприятия +
 - в) атака на конкретный компьютер пользователя

11. Под информационной безопасностью понимается:

- а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре +
- б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
- в) нет верного ответа

12. Защита информации:

- а) небольшая программа для выполнения определенной задачи
- б) комплекс мероприятий, направленных на обеспечение информационной безопасности +
- в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

13. Информационная безопасность зависит от:

- а) компьютеров, поддерживающей инфраструктуры +
- б) пользователей
- в) информации

14. Конфиденциальностью называется:

- а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
- б) описание процедур
- в) защита от несанкционированного доступа к информации +

15. Для чего создаются информационные системы:

- а) получения определенных информационных услуг +
- б) обработки информации
- в) оба варианта верны

16. Кто является основным ответственным за определение уровня классификации информации:

- а) руководитель среднего звена
- б) владелец +
- в) высшее руководство

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:

- а) хакеры
- б) контрагенты
- в) сотрудники +

18. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:

- а) снизить уровень классификации этой информации
- б) улучшить контроль за безопасностью этой информации +
- в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

19. Что самое главное должно продумать руководство при классификации данных:

- а) управление доступом, которое должно защищать данные
- б) оценить уровень риска и отменить контрмеры
- в) необходимый уровень доступности, целостности и конфиденциальности +

20. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:

- а) владельцы данных
- б) руководство +
- в) администраторы

21. Процедурой называется:

- а) пошаговая инструкция по выполнению задачи +
- б) обязательные действия
- в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

22. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:

- а) проведение тренингов по безопасности для всех сотрудников
- б) поддержка высшего руководства +
- в) эффективные защитные меры и методы их внедрения

23. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:

- а) когда риски не могут быть приняты во внимание по политическим соображениям
- б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- в) когда стоимость контрмер превышает ценность актива и потенциальные потери +

24. Что такое политика безопасности:

- а) детализированные документы по обработке инцидентов безопасности
- б) широкие, высокоуровневые заявления руководства +
- в) общие руководящие требования по достижению определенного уровня безопасности

25. Какая из приведенных техник является самой важной при выборе конкретных защитных мер:

- а) анализ рисков
- б) результаты ALE
- в) анализ затрат / выгоды +

26. Что лучше всего описывает цель расчета ALE:

- а) количественно оценить уровень безопасности среды
- б) оценить потенциальные потери от угрозы в год +
- в) количественно оценить уровень безопасности среды

27. Тактическое планирование:

- а) среднесрочное планирование +
- б) ежедневное планирование
- в) долгосрочное планирование

28. Эффективная программа безопасности требует сбалансированного применения:

- а) контрмер и защитных механизмов
- б) процедур безопасности и шифрования
- в) технических и нетехнических методов +

29. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

- а) уровень доверия, обеспечиваемый механизмом безопасности +
- б) внедрение управления механизмами безопасности
- в) классификацию данных после внедрения механизмов безопасности

30. Что из перечисленного не является целью проведения анализа рисков:

- а) выявление рисков
- б) делегирование полномочий +
- в) количественная оценка воздействия потенциальных угроз

4.1. Информационная безопасность России

1. Какую юридическую силу имеет Доктрина информационной безопасности?

Возможные варианты ответов:

- А) Силу постановления Правительства РФ
- Б) Силу указа Президента РФ
- В) Представляет собой систему официальных взглядов на проблемы информационной безопасности
- Г) Имеет силу закона

2. При каких условиях можно отнести технические средства и системы, обрабатывающие открытую информацию, к объектам, подверженным внешним угрозам и нуждающимся в защите наряду с объектами ограниченного доступа?

Возможные варианты ответов:

- А) При условии, что эти системы или их компоненты импортного производства
- Б) При условии, что к этим системам имеется свободный доступ граждан
- В) При условии, что эти системы размещены в помещениях, в которых обрабатывается информация ограниченного доступа

3. Какие угрозы объектам информации не приведены в Доктрине информационной безопасности?

Возможные варианты ответов:

- А) Утечка информации по техническим каналам
- Б) Нарушение свободы слова
- В) Несанкционированный доступ к информации, находящейся в базах и банках данных
- Г) Нарушение прав собственности на средства защиты информации

4. Какие наиболее важные мероприятия должны реализовываться в направлении организационно-технического противодействия информационным угрозам?

Возможные варианты ответов:

- А) Контроль за выполнением специальных требований по защите информации
- Б) Контроль за средствами массовой информации
- В) Контроль за действиями персонала.

Тема 5.1. Передача и публикация цифровой информации

Тест с ответами: «Передача информации»

1. Приемников информации несколько в случае:
 - а) демонстрации проекта в классе с последующим обсуждением +
 - б) получения электронного письма
 - в) индивидуальной работы над проектом
2. Приемников информации несколько в случае:
 - а) получения электронного письма
 - б) школьной экскурсии в картинную галерею на выставку современного искусства +
 - в) индивидуальной работы над заданием
3. Адрес электронной почты состоит из ... корреспондента и ... сервера, на котором зарегистрирован почтовый ящик:
 - а) имени, принадлежности
 - б) адреса, имени
 - в) имени, адреса +
4. Человек получает информацию из одного источника во время:
 - а) чтения книги +
 - б) прогулки по городу
 - в) просмотра иллюстраций
5. Человек получает информацию из нескольких источников во время:
 - а) чтения журнала
 - б) просмотра фильма
 - в) посещения картинной галереи +
6. Человек получает информацию из нескольких источников во время:
 - а) просмотра фильма
 - б) прогулки по городу +
 - в) чтения газеты
7. Источник информации, с помощью которого человек не может сообщить об опасности:
 - а) звук музыкального инструмента
 - б) сигнальный костер
 - в) радиопьеса +
8. Источник информации, с помощью которого человек может сообщить об опасности:
 - а) электронное письмо +
 - б) радиопьеса
 - в) оба варианта верны
9. Пример двухстороннего информационного обмена:
 - а) человек переходит дорогу по сигналу светофора
 - б) девочка размышляет, как выполнить домашнее задание
 - в) друзья делятся планами на лето и договариваются о совместной поездке +

10. Не является примером двухстороннего информационного обмена:
а) друзья делятся планами на лето и договариваются о совместной поездке
б) мальчик смотрит фильм «Каникулы Петрова и Васечкина» +
в) оба варианта верны
11. Биологический информационный канал:
а) глаза +
б) телефон
в) компьютер
12. Приемник информации один в случае:
а) школьной экскурсии в картинную галерею на выставку современного искусства
б) самостоятельного решения задачи +
в) работы в группе над проектом
13. Приемник информации один в случае:
а) рисования с использованием компьютерной программы +
б) работы в группе над проектом
в) школьной экскурсии в картинную галерею на выставку современного искусства
14. Пересылка корреспонденции с помощью компьютерных сетей:
а) электронная телеграмма
б) электрическая почта
в) электронная почта +
15. Человек получает информацию из нескольких источников одновременно во время:
а) прогулки по городу +
б) чтения газеты
в) просмотра фильма
16. Человек получает информацию из нескольких источников одновременно во время:
а) просмотра иллюстрации
б) просмотра иллюстраций +
в) чтения газеты
17. Человек получает информацию из одного источника во время:
а) посещения фотовыставки
б) посещения музея
в) чтения журнала +
18. Человек получает информацию из одного источника во время:
а) посещения художественной галереи
б) просмотра мультфильма +
в) посещения фотовыставки
19. Источник информации, с помощью которого человек не может сообщить об опасности:
а) рисунок на песке
б) азбука Морзе
в) велосипедная прогулка +

20. Источник информации, с помощью которого человек не может сообщить об опасности:

- а) азбука Морзе
- б) пешая прогулка +
- в) электронное письмо

21. Пример одностороннего информационного обмена:

- а) младшая сестра смотрит мультфильм «Трое из Простоквашино» +
- б) друзья делятся планами на лето и решают отправиться в поход
- в) школьники обсуждают проект

22. Не является примером одностороннего информационного обмена:

- а) младшая сестра смотрит мультфильм «Трое из Простоквашино»
- б) школьники обсуждают проект +
- в) оба варианта верны

23. Технический информационный канал:

- а) глаза
- б) записка
- в) телефон +

24. Приемников информации несколько в случае:

- а) индивидуальной работы над домашним заданием
- б) показ презентации в классе +
- в) получения письма

25. Приемников информации несколько в случае:

- а) индивидуальной работы над домашним заданием
- б) получения письма
- в) экскурсии классом в картинную галерею +

26. Сторона принимающая информацию-приемник, так ли это:

- а) нет
- б) да +
- в) отчасти

27. Если передаваемая информация потеряна или искажена, то в информационном канале были(а):

- а) помехи +
- б) плохая связь
- в) утечка информации

28. Укажите соответствие: «Аня смотрит мультфильм по телевизору, а Иван слушает музыку через аудиоплеер»:

источник информации:

- а) Аня
- б) Иван
- в) аудиоплеер +

29. Укажите соответствие: «Аня смотрит мультфильм по телевизору, а Иван слушает музыку через аудиоплеер»:

источник информации:

- а) телевизор +
- б) Иван
- в) Аня

30. Укажите соответствие: «Аня смотрит мультфильм по телевизору, а Иван слушает музыку через аудиоплеер»:

приемник(и) информации:

- а) телевизор
- б) Иван, Аня +
- в) аудиоплеер

Тема 6.1.

Стандарты Антикоррупционного поведения

Тест с ответами по теме: «Коррупция»

1. Что из перечисленного относится к запретам, предусмотренным нормами ФЗ №79:

- а) совместная работа близких родственников +
- б) публичные высказывания
- в) участие в управлении некоммерческой организацией

2. Правовая основа противодействия коррупции в Российской Федерации:

- а) включает нормативные правовые акты только федерального уровня управления
- б) включает как общепризнанные принципы и нормы международного права и международные договоры Российской Федерации, так и различные виды нормативных правовых актов Российской Федерации +
- в) включает только Федеральный закон «О противодействии коррупции»

3. Выберите пример коррупционных действий:

- а) преподавательскую деятельность за вознаграждение в качестве совместителя
- б) получение любого подарка
- в) использование служебного положения для получения выгоды в отношении родственников +

4. К числу основных принципов противодействия коррупции в Российской Федерации не относится принцип:

- а) конфиденциальности при решении вопроса о привлечении к ответственности за совершение коррупционных правонарушений +
- б) сотрудничества государства с институтами гражданского общества, международными организациями и физическими лицами
- в) приоритетного применения мер по предупреждению коррупции

5. В каком случае возможна утрата доверия государственного лица за совершенные коррупционные действия:

- а) за получение взятки в крупных размерах
- б) наличие личной заинтересованности
- в) во всех случаях предусмотренных ФЗ №273 без учета размера причиненного ущерба +

6. В сфере противодействия коррупции утрата доверия подразумевает:

- а) утрату доверия государственного гражданского служащего по отношению к представителю нанимателя

б) утрату доверия представителя нанимателя по отношению к государственному гражданскому служащему +

в) утрату доверия комиссии по соблюдению требований к служебному поведению и урегулированию интересов по отношению к руководителю государственного органа

7. Отметьте, в какой ситуации госслужащий может принять подарок в ходе выполнения своих должностных обязанностей:

а) если стоимость подарка не превышает 3 тысяч рублей

б) если подарок выражается в оказании услуг, оплате транспортных расходов, к примеру

в) если подарок вручен на официальном мероприятии +

8. Граждане Российской Федерации, иностранные граждане и лица без гражданства за совершение коррупционных правонарушений не несут:

а) материальную ответственность +

б) уголовную ответственность

в) дисциплинарную ответственность

9. Определите ситуации, при которых госслужащий имеет право участвовать в управлении некоммерческой организации:

а) при избрании единоличным исполнительным органом

б) в качестве представителя учредителя, коим выступает субъект Российской Федерации, имеющий долю в уставном капитале +

в) при вхождении в коллегиальный орган управления

10. Основные направления государственной политики в области противодействия коррупции определяются:

а) Правительством Российской Федерации

б) Президентом Российской Федерации +

в) Федеральным Собранием Российской Федерации

11. Какая форма предусмотрена для уведомления госслужащим о возникшем конфликте интересов или о возможности его возникновения:

а) письменная +

б) устная

в) не имеет значения

12. Выберите верное утверждение:

а) Основные полномочия по координации и контролю в сфере противодействия коррупции возложены на Федеральное антикоррупционное агентство

б) Координация деятельности правоохранительных органов в сфере противодействия коррупции возложена на Генерального прокурора Российской Федерации и подчиненных ему прокуроров +

в) Проверку сведений о доходах, расходах, об имуществе и обязательствах имущественного характера любых лиц, которые обязаны представлять такие сведения, может проводить Счетная палата Российской Федерации

13. Кто должен знать о возникшем конфликте интересов или о возможности его возникновения, кроме госслужащего:

а) представитель наниматель +

б) лицо, ответственное за работу по профилактике коррупционных и иных правонарушений в

государственном органе
в) правоохранительные органы

14. В соответствии с Федеральным законом «О противодействии коррупции» коррупция:
а) возможна только в государственном секторе экономики
б) не включает случаи, когда незаконная выгода должностного лица незначительна (не превышает одной тысячи рублей)
в) связана с незаконным использованием должностного положения в целях приобретения имущественной выгоды +

15. Кем был утверждён Национальный план противодействия коррупции:
а) Федеральным законом
б) Указом Президента РФ+
в) Постановлением Правительства РФ

16. Принятие Федерального закона № 273-ФЗ «О противодействии коррупции»:
а) имело ограниченный эффект, поскольку данный закон регулировал противодействие коррупции только на федеральном уровне управления
б) позволило установить единые правовые и организационные основы противодействия коррупции в Российской Федерации +
в) позволило ввести законодательно установленное определение коррупции

17. В какой ситуации лицо, которое дало взятку освобождается от уголовной ответственности:
а) при возмещении причиненного вреда
б) в случае деятельного раскаяния
в) если имело место вымогательство взятки со стороны должностного лица +

18. К специальным мерам противодействия коррупции относится:
а) применение к государственным гражданским служащим мер дисциплинарной ответственности за нарушение служебного распорядка государственного органа
б) введение на государственной гражданской службе института увольнения в связи с утратой доверия +
в) регулярная оценка результативности деятельности государственных гражданских служащих

19. В какой ситуации лицо, которое дало взятку освобождается от уголовной ответственности:
а) в случае деятельного раскаяния
б) при возмещении причиненного вреда
в) если лицо добровольно сообщило органу, имеющему право возбудить уголовное дело, о даче взятки +

20. К специальным мерам противодействия коррупции относится:
а) регулярная оценка результативности деятельности государственных гражданских служащих
б) установление для государственных гражданских служащих запрета заниматься предпринимательской деятельностью +
в) применение к государственным гражданским служащим мер дисциплинарной ответственности за нарушение служебного распорядка государственного органа

21. При трудоустройстве на новую должность после увольнения с государственной службы гражданин обязан уведомить:
а) подразделение кадровой службы государственного органа по профилактике коррупционных

и иных правонарушений +

б) комиссию по соблюдению требований к служебному поведению

в) представителя нанимателя о намерении заключить трудовой договор

22. К последствиям коррупции относится:

а) рост численности государственных служащих

б) ущерб репутации государственных органов +

в) оба варианта верны

г) нет верного ответа

23. Государственному служащему не запрещено:

а) быть представителем по делам третьих лиц в государственном органе

б) занимать оплачиваемую должность в Профсоюзной организации при государственном аппарате

в) быть членом ревизионной комиссии в организации, при условии, что часть уставного капитала принадлежит РФ +

24. Выявление коррупционных преступлений и уголовное преследование виновных лиц является основным способом профилактики коррупции, так ли это:

а) да

б) нет +

в) отчасти

25. Государственный служащий обязан предоставлять сведения о доходах следующих членов семьи:

а) на всех родственников

б) на всех близких родственников, включая родителей, а также сестер и братьев

в) на супругу(а) и детей +

26. Коррупция существует как в государственном, так и частном секторе экономики, так ли это:

а) нет

б) да +

в) неизвестно

27. К взысканиям, которые предусмотрены за совершение коррупционных действий, независимо от их тяжести относятся:

а) дисциплинарные взыскания в виде выговора, строго выговора либо же увольнения +

б) отмена выплаты премии

в) понижение в должности либо же снижении чина, классности

28. Антикоррупционный стандарт устанавливает:

а) перечень возможных действий гражданского служащего в рамках своей служебной деятельности, считающихся коррупционными

б) нравственные основы служебного поведения гражданских служащих

в) единую систему запретов, ограничений и дозволений, обеспечивающих предупреждение коррупции в соответствующей области деятельности +

29. Государственный служащий обязан уведомить представителя нанимателя:

а) обо всех случаях совершенных коррупционных действий +

б) о коррупционных действиях, сведения о которых были получены в ходе исполнения

должностных обязанностей

в) только о склонении к коррупционным действиям лично государственного служащего

30. В каких случаях государственный служащий имеет право участвовать в управлении некоммерческой организации:

а) при вхождении в коллегиальный орган управления

б) в качестве представителя учредителя, коим выступает субъект Российской Федерации, имеющий долю в уставном капитале +

в) при избрании единоличным исполнительным органом

Тема 6.2. Ответственность в информационной сфере

Упражнение 1:

Номер 1

Какие методы обеспечения информационной безопасности существуют?

Ответ:

(1) общие и частные

(2) правовые, организационно-технические и экономические

(3) правовые и экономические

(4) внешние и внутренние

Номер 2

Что является основной задачей по обеспечению информационной безопасности?

Ответ:

(1) разработка основных направлений государственной политики в области обеспечения информационной безопасности России, а также мероприятий и механизмов, связанных с реализацией этой программы

(2) разработка федеральных целевых программ обеспечения информационной безопасности России

(3) разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности, а также сертификации этих систем и средств

(4) совершенствование нормативно-правовой базы обеспечения информационной безопасности России, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации

Номер 3

Что является совокупностью официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности государства?

Ответ:

(1) Доктрина политической безопасности Российской Федерации

(2) Конституция Российской Федерации

(3) Доктрина информационной безопасности Российской Федерации

(4) Доктрина экономической безопасности Российской Федерации

Упражнение 2:

Номер 1

На каком принципе базируется ответственность в информационной сфере?

Ответ:

(1) законность

(2) обоснованность

(3) справедливость

(4) все перечисленное верно

Номер 2

Ответственность за правонарушения в информационной сфере реализуется в рамках

Ответ:

(1) регулятивных правоотношений

(2) правоохранительных правоотношений

(3) карательных правоотношений

(4) социальных правоотношений

Номер 3

Правонарушения можно рассматривать в качестве информационно-правовых, если их связь с информацией является

Ответ:

(1) непосредственной или опосредованной наличием ее материального носителя

(2) опосредованной наличием ее подтверждения

(3) закономерной

(4) все перечисленное верно

Упражнение 3:

Номер 1

Что относится к важнейшим функциям системы обеспечения информационной безопасности?

Ответ:

(1) разработка нормативной правовой базы в сфере обеспечения информационной безопасности

(2) создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере

(3) оценка состояния информационной безопасности РФ, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз

(4) все перечисленное верно

Номер 2

Кто выступает основным элементом организационной основы системы обеспечения информационной безопасности?

Ответ:

(1) Президент РФ

(2) Совет Федерации

(3) Государственная Дума

(4) Правительство РФ

Номер 3

Чем является система обеспечения информационной безопасности РФ?

Ответ:

(1) частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере

(2) системой обеспечения национальной безопасности страны, призванной к реализации государственной политики в информационной сфере

(3) частью системы обеспечения национальной безопасности страны, призванной к реализации государственной политики в экономической сфере

(4) системой обеспечения национальной безопасности страны, призванной к реализации государственной политики в экономической сфере

Упражнение 4:

Номер 1

Какой закон, регламентирующий отношения в области науки и техники, занимает главенствующее место среди специально разработанных для этих целей нормативных правовых

актов?

Ответ:

(1) ФЗ «О науке и государственной научно-технической политике»

(2) ФЗ «О государственной тайне»

(3) ФЗ «О средствах массовой информации»

(4) ФЗ «О связи»

Номер 2

Какие из внешних угроз информационной безопасности РФ в сфере внешней политики представляют наибольшую опасность?

Ответ:

(1) информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики России

(2) нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом

(3) попытка несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях

(4) все варианты верные

Номер 3

Кем согласно Конституции РФ определяются основные направления внутренней политики государства

Ответ:

(1) Федеральным собранием

(2) Правительством РФ

(3) Президентом РФ

(4) Государственной Думой РФ

Упражнение 5:

Номер 1

Государственное властное принуждение является

Ответ:

(1) содержанием юридической ответственности

(2) сущностью юридической ответственности

(3) функцией юридической ответственности

(4) целью юридической ответственности

Номер 2

Если распространение определенной информации ограничивается или запрещается федеральными законами, лицо, оказывающее услуги по передаче информации, предоставленной другим лицом, передавшее ее без изменений и исправлений

Ответ:

(1) несет полную гражданско-правовую ответственность

(2) несет ограниченную гражданско-правовую ответственность

(3) не несет гражданско-правовой ответственности

(4) несет уголовную ответственность

Номер 3

Может ли быть удовлетворено требование о возмещении убытков в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством РФ требования защиты информации, если

принятие этих мер и соблюдение таких требований являлось обязанностями данного лица?

Ответ:

- (1) да, на общих основаниях
- (2) да, но только по усмотрению суда

(3) нет

- (4) да, но только по усмотрению правоохранительных органов

Упражнение 6:

Номер 1

Административно-правовая ответственность за правонарушения в информационной сфере носит

Ответ:

(1) публичный характер

- (2) частный характер
- (3) публично-частный характер
- (4) частно-публичный характер

Номер 2

В какой главе Особенной части УК РФ не содержится норма об ответственности за преступления в информационной сфере?

Ответ:

- (1) в главе о преступлениях против свободы, чести и достоинства личности
- (2) в главе о преступлениях против конституционных прав и свобод человека и гражданина

(3) в главе о преступлениях против интересов службы в коммерческих и иных организациях

- (4) все перечисленное верно

Номер 3

Какой характер носит уголовная ответственность за правонарушения в информационной сфере?

Ответ:

(1) личный характер

- (2) коллективный характер
- (3) групповой характер
- (4) может носить и личный и коллективный характер

Критерии оценивания по тестовым заданиям:

Оценка за контроль ключевых компетенций учащихся производится по пятибалльной системе.

При выполнении заданий ставится отметка:

- «3» - за 50-70% правильно выполненных заданий,
- «4» - за 70-85% правильно выполненных заданий,
- «5» - за правильное выполнение более 85% заданий.

2.2. Задания для промежуточной аттестации

Защита презентации

Темы для подготовки презентаций

Тема 1 . ПРАВОВЫЕ РЕЖИМЫ ИНФОРМАЦИИ

1. Понятие правового режима информации и его разновидности
2. Режим свободного доступа
3. Режим ограниченного доступа
4. Режим документированной информации

Тема 2. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ ФОРМИРОВАНИЯ ОБЯЗАТЕЛЬНОГО ЭКЗЕМПЛЯРА ДОКУМЕНТОВ, АРХИВНОГО ДЕЛА.

1. Правовое регулирование отношений
2. Правовое регулирование отношений в области формирования обязательного экземпляра документов
3. Правовое регулирование отношений в сфере формирования, хранения, учета и использования архивов и архивных фондов

Тема 3. РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ ОРГАНИЗАЦИИ И ДЕЯТЕЛЬНОСТИ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ

1. Средства массовой информации и организация
2. Распространение массовой информации
3. Отношения средств массовой информации с гражданами и организациями
4. Профессиональный статус журналиста

Тема 4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

1. Понятие рекламы и требования, предъявляемые к ней.
2. Особенности отдельных способов распространения рекламы
3. Особенности рекламы отдельных видов товаров
4. Субъекты рекламной деятельности
5. Государственный контроль в сфере рекламной деятельности

Тема 5. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В ОБЛАСТИ СВЯЗИ

1. Общие сведения о связи и структуре ее функционирования
2. Государственное регулирование деятельности в области связи

Тема 6. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В СФЕРЕ ОХРАНЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ

1. Понятие государственной тайны, состав и принципы формирования сведений, подлежащих засекречиванию
2. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание
3. Распоряжение сведениями, составляющими государственную тайну
4. Допуск к государственной тайне
5. Сертификация средств защиты информации

Тема 7. ПРАВОВЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Понятие информационной безопасности, основные задачи и методы ее обеспечения
2. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни
3. Государственная политика информационной безопасности и организационная основа системы ее обеспечения

Тема 8 . ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

1. Общие сведения о юридической ответственности за нарушение законодательства в информационной сфере
2. Гражданско-правовая ответственность за правонарушения в информационной сфере
3. Административно-правовая ответственность за правонарушения в информационной сфере
4. Уголовная ответственность за преступления в информационной сфере

Инструкция по выполнению презентации

Общие требования к презентации.

1. Презентация не должна быть меньше 15 слайдов.
2. Первый лист – это титульный лист, на котором обязательно должны быть представлены: название; название выпускающей организации; фамилия, имя, отчество автора; МБОУ, где работает автор проекта и его должность.
3. Следующим слайдом должно быть содержание, где представлены основные этапы (моменты) презентации. Желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание.
4. Дизайн - эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста.

5. Последними слайдами презентации должен быть список литературы.

Требования к оформлению презентаций.

В оформлении презентаций выделяют два блока: оформление слайдов и представление информации на них. Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

Оформление слайдов. Стиль.

Соблюдайте единый стиль оформления

Избегайте стилей, которые будут отвлекать от самой презентации.

Вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текстом, иллюстрациями).

Фон. Для фона предпочтительны холодные тона. Использование цвета.

На одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовка, один для текста.

Для фона и текста используйте контрастные цвета.

Обратите внимание на цвет гиперссылок (до и после использования).

Анимационные эффекты

Используйте возможности компьютерной анимации для представления информации на слайде.

Не стоит злоупотреблять различными анимационными эффектами, они не должны отвлекать внимание от содержания информации на слайде.

Представление информации

Содержание информации

Используйте короткие слова и предложения.

Минимизируйте количество предлогов, наречий, прилагательных.

Заголовки должны привлекать внимание аудитории.

Расположение информации на странице

Предпочтительно горизонтальное расположение информации.

Наиболее важная информация должна располагаться в центре экрана.

Если на слайде располагается картинка, надпись должна располагаться под ней.

Шрифты

Для заголовков – не менее 24.

Для информации не менее 18.

Шрифты без засечек легче читать с большого расстояния.

Нельзя смешивать разные типы шрифтов в одной презентации.

Для выделения информации следует использовать жирный шрифт, курсив или подчеркивание.

Нельзя злоупотреблять прописными буквами (они читаются хуже строчных).

Способы выделения информации

Следует использовать:

-рамки; границы, заливку;

-штриховку, стрелки;

- рисунки, диаграммы, схемы для иллюстрации наиболее важных фактов.

Объем информации

Не стоит заполнять один слайд слишком большим объемом информации.

Виды слайдов

Для обеспечения разнообразия следует использовать разные виды слайдов: с текстом; с таблицами; с диаграммами.

- На последнем слайде презентации размещение ссылок на использованные источники и иллюстрации является обязательным.

- Все иллюстрации и фотографии, используемые в презентации, должны быть оптимизированы (сжаты).

- Для файла мультимедийной презентации необходимо предоставить имя, он должен иметь расширение ppt. Например: Петренко-petrenko.ppt.

- Желательно добавлять в мультимедийную презентацию звуковые фрагменты, мультипликацию, фрагменты фильмов для обеспечения эмоционального воздействия.

Критерии оценивания презентаций:

Оформление слайдов	Параметры
Стиль	Соблюдать единого стиля оформления.
Фон	Фон должен соответствовать теме презентации
Использование цвета	<ul style="list-style-type: none"> o Слайд не должен содержать более трех цветов o Фон и текст должны быть оформлены контрастными цветами
Анимационные эффекты	<ul style="list-style-type: none"> o При оформлении слайда использовать возможности анимации o Анимационные эффекты не должны отвлекать внимание от содержания слайдов
Представление информации	Параметры
Содержание информации	<ul style="list-style-type: none"> o Слайд должен содержать минимум информации o Информация должна быть изложена профессиональным языком o Содержание текста должно точно отражать этапы <u>выполненной работы</u> o Текст должен быть расположен на слайде так, чтобы его удобно было читать o В содержании текста должны быть ответы на проблемные вопросы o Текст должен соответствовать теме презентации
Расположение информации на странице	<ul style="list-style-type: none"> o Предпочтительно горизонтальное расположение информации o Наиболее важная информация должна располагаться в центре o Надпись должна располагаться под картинкой
Шрифты	<ul style="list-style-type: none"> o Для заголовка – не менее 24 o Для информации не менее – 18 o Лучше использовать один тип шрифта o Важную информацию лучше выделять жирным шрифтом, курсивом. Подчеркиванием o На слайде не должно быть много текста, оформленного прописными буквами
Выделения информации	На слайде не должно быть много выделенного текста (заголовки, важная информация)
Объем информации	<ul style="list-style-type: none"> o Слайд не должен содержать большого количества информации o Лучше ключевые пункты располагать по одному на слайде
Виды слайдов	<p>Для обеспечения разнообразия следует использовать разные виды слайдов:</p> <ul style="list-style-type: none"> o с таблицами o с текстом o с диаграммами

Если студенческая работа отвечает всем требованиям критериев, то ей дается оценка *отлично*. При незначительном нарушении или отсутствии каких-либо параметров в работе, она оценивается *хорошо*. Если при оценивании половина критериев отсутствует, то работа оценивается *удовлетворительно*.