Министерство науки и высшего образования Российской Федерации
Лысьвенский филиал
федерального государственного автономного образовательного учреждения
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
**для проведения промежуточной аттестации обучающихся по дисциплине**
**«Информатика в приложении к отрасли»**
***Приложение к рабочей программе дисциплины***

| | |
|---|---|
| **Направление подготовки:** | 20.03.01 Техносферная безопасность |
| **Направленность (профиль) образовательной программы:** | Безопасность технологических процессов и производств |
| **Квалификация выпускника:** | «Бакалавр» |
| **Выпускающая кафедра:** | Технических дисциплин |
| **Форма обучения:** | Очная, заочная |

**Курс:** 2 (3) **Семестр**: 3 (5)

**Трудоёмкость:**
Кредитов по рабочему учебному плану: 3 ЗЕ
Часов по рабочему учебному плану: 108 ч.

**Форма промежуточной аттестации:**
Зачёт: 3 (5) семестр

Лысьва 2024

**Фонд оценочных средств** для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

## 1.Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД освоение учебного материала дисциплины запланировано в течение одного семестра (3-го семестра учебного плана очной формы обучения; 5-го семестра учебного плана заочной формы обучения). Предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим занятиям и зачета. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

| **Контролируемые результаты обучения по дисциплине (ЗУВы)** | **Вид контроля** | | | | | |
|---|---|---|---|---|---|---|
| | **Текущий** | | **Рубежный** | | **Итоговый** | |
| | **С** | **ТО** | **ОПЗ** | **Т/КР** | | **Зачёт** |
| **Усвоенные знания** | | | | | | |
| **З.1** Знать математические, физические, химические и прочие определения, формулы и соотношения необходимые для использования в современных информационных технологиях, обеспечивающих безопасность человека | С | ТО | | Т | | ТВ |
| **З.2** Знать проблемы и общие подходы к обеспечению техносферной безопасности | | ТО | | Т | | ТВ |
| **Освоенные умения** | | | | | | |
| **У.1** Уметь осуществлять деятельность в области обеспечения безопасности посредством использования современных информационных технологий | | | ОПЗ 1 ОПЗ 2 ОПЗ 3 | Т | | ПЗ |
| **У.2** Уметь обобщать, анализировать и систематизировать информацию по вопросам обеспечения безопасности; | | | ОПЗ 4 ОПЗ 5 ОПЗ 6 | Т | | ПЗ |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | ОПЗ 7 | | | |
| **У.3** Уметь формировать отчеты по практическим заданиям | | | ОПЗ 1-7 | | | ПЗ |
| **Приобретенные владения** | | | | | | |
| **В.1** Владеть навыками навыками использования информационных технологий для решения проблем в области обеспечения безопасности человека. | | | ОПЗ 1-7 | | | ПЗ |
| **В.2** Владеть навыками самостоятельного изучения, критического осмысления и систематизации, а также планирования и проведения исследований, направленных на обеспечение техносферной безопасности | | | ОПЗ 1-7 | | | ПЗ |

*С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОПЗ – отчет по практическим занятиям; Т/КР – рубежное тестирование (контрольная работа); ТВ – теоретический вопрос; ПЗ – практическое задание*

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в форме зачета, проводимая с учётом результатов текущего и рубежного контроля.

## 2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

- контроль остаточных знаний.

**2.1. Текущий контроль усвоения материала**

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

**2.2. Рубежный контроль**

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты отчета по практическим занятиям и рубежного тестирования.

**2.2.1. Защита практических занятий**

Всего запланировано 7 практических занятий. Типовые темы практических занятий приведены в РПД.

Защита отчета по практическим занятиям проводится индивидуально каждым студентом или группой студентов. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

**2.2.2. Рубежная контрольная работа**

Запланировано 2 рубежных тестирования. Первое Т по темам: классификация информационных технологий и безопасность человека; глобальная сеть INTERNET и управление безопасностью; системы мониторинга управления безопасностью, «Основы информатики в транспортной отрасли», второе Т – по темам: прикладные информационные технологии безопасности человека; системы поддержки принятия решений в управлении безопасностью; методо-ориентированные пакеты прикладных программ в управлении безопасностью, «Общие принципы построения и анализ проектов развития интеллектуальных транспортных систем».

**Типовые задания первого Т:**

**1. Что такое информация?**

а. сообщения, находящиеся в памяти компьютера

б. сообщения, находящиеся в хранилищах данных

в. предварительно обработанные данные, годные для принятия управленческих решений

г. сообщения, зафиксированные на машинных носителях

**2. Сколько революций было в развитии информационных технологий?**

а. 2

б. 3

в. 4

г. 5

**3. Что понимается под даннмыми об объектах, событиях и процессах?**
а. содержимое баз знаний
б. необработанные сообщения, отражающие отдельные факты, процессы, события
в. предварительно обработанная информация
г. сообщения, находящиеся в хранилищах данных

**4. Какой процесс подвержен заражению компьютерными вирусами?**
а. работы с файлами
б. форматирования дискеты
в. выключения компьютера
г. печати на принтере

**5. Что нужно для проверки на вирус жесткого диска?**
а. защищенную программу
б. загрузочную программу
в. файл с антивирусной программой
г. дискету с антивирусной программой, защищенную от записи

**6. Основная масса угроз информационной безопасности приходится на:**
……

**7. Какой вид идентификации и аутентификации получил наибольшее**
……

**8. Под какие системы распространение вирусов происходит наиболее**
**…….**

**9. Заключительным этапом построения системы защиты является:**
**……**

**10. Какие угрозы безопасности информации являются преднамеренными:**
**…….**

**11. Какой из способов подключения к Интернет обеспечивает наибольшие возможности для доступа к информационным ресурсам:**
……

**12. Модем — это: ……**

**13. Модем, передающий информацию со скоростью 28 800 бит/с, может передать две страницы текста (3 600 байт) в течение:**
**……**

**14. Электронная почта (e-mail) позволяет передавать:**
**…….**

**15. Какой протокол является базовым в Интернет:**
**……**

**16. Компьютер, подключенный к Интернет, обязательно имеет:**
**……**

**17. Гиперссылки на web — странице могут обеспечить переход:**
**……**

**18. Аналоговый сигнал это……**

**19. Какая из навигационных систем надёжней к преднамеренным помехам?**
**……**

**20. Что преобразует сигнал управления на физическое воздействие на объект управления? ……**

Ответы к тесту 1:

| № вопр | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| ответ | в | б | б | г | г |

| | |
|---|---|
| 6 | Троянские программы |
| 7 | постоянные пароли |
| 8 | Android |
| 9 | сопровождение |
| 10 | не авторизованный доступ |
| 11 | постоянное соединение по оптоволоконному каналу |
| 12 | техническое устройство |
| 13 | 1 секунды |
| 14 | сообщения и приложенные файлы |
| 15 | TCP/IP |
| 16 | IP-адрес |
| 17 | на любую web — страницу любого сервера Интернет |
| 18 | электромагнитные волны, характеризующиеся частотой колебания |
| 19 | ГЛОНАСС |
| 20 | Исполняющее устройство |

**Типовые задания второго Т:**

1. **Кто является основным ответственным за определение уровня классификации информации?**
   а) Руководитель среднего звена
   б) Высшее руководство
   в) Владелец
   г) Пользователь

**2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?**
   а) Сотрудники
   б) Хакеры
   в) Атакующие
   г) Контрагенты (лица, работающие по договору)

**3. 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 безопасности этой информации для обеспечения ее доступности и удобства использовании
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

**4. Что самое главное должно продумать руководство при классификации данных?**
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

**5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?**
а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство

**6. Что такое процедура?**.....

**7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?** .....

**8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?**.....

**9. Что такое политики безопасности?**.....

**10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?**.....

**11. Цель интеграции для разработчиков интеллектуальных систем:**
**……**

**12. Физическая модель —……**

**13. Модель — ……**

**14. Цель интеграции для администраторов БЗ:**
**…….**

**15. Естественные угрозы безопасности информации вызваны:**
.....

**16. К посторонним лицам нарушителям информационной безопасности относится:**
.....
.....

**17. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:**
.....

**18. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:** .....

**19. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:** .....

**20. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?** .....

Ответы к тесту 2:

| № вопр | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| ответ | в | а | в | б | г |

| | |
|---|---|
| 6 | Пошаговая инструкция по выполнению задачи |
| 7 | Поддержка высшего руководства |
| 8 | Когда стоимость контрмер превышает ценность актива и потенциальные потери |
| 9 | Широкие, высокоуровневые заявления руководства |
| 10 | Анализ затрат / выгоды |
| 11 | обеспечить создание единых инструментальных (языковых средств, успешно и эффективно реализующих методы доступа к информации и обработки ее, типичные и для искусственного интеллекта, и для технологии баз данных, и не зависящие от того, где эта информация размещается |
| 12 | наименее абстрактная модель — является физической копией системы, обычно в отличном от оригинала масштабе. |
| 13 | упрощенное представление или абстракция действительности. |
| 14 | обеспечить ряд средств, представленных в основном в технологии баз данных, но приспособленных к требованиям СУБЗ. |
| 15 | воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; |
| 16 | представители конкурирующих организаций. |
| 17 | черный пиар; |
| 18 | детектор; |
| 19 | ревизор; |
| 20 | OECD |

### 2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех практических занятий и положительная интегральная оценка по результатам текущего и рубежного контроля.

#### 2.3.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания

Промежуточная аттестация проводится в форме зачета. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде зачета приведены в общей части ФОС образовательной программы.

**2.3.2. Процедура промежуточной аттестации с проведением аттестационного испытания**

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций.

**2.3.2.1. Типовые вопросы и задания для зачета по дисциплине**

**Типовые вопросы для контроля усвоенных знаний:**

1. **К негативным последствиям развития современных информационных и коммуникационных технологий можно отнести:**

а. формирование единого информационного пространства
б. работа с информацией становится главным содержанием профессиональной деятельности
в. организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации
г. широкое использование информационных технологий во всех сферах человеческой деятельности
д. доступность личной информации для общества и государства, вторжение информационных технологий в частную жизнь людей

2. **Термин «информатизация общества» обозначает:**

а. целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий
б. увеличение избыточной информации, циркулирующей в обществе
в. увеличение роли средств массовой информации
г. введение изучения информатики во все учебные заведения страны
д. организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации

3. **Развитый рынок информационных продуктов и услуг, изменение в структуре экономики, массовое использование информационных и коммуникационных технологий являются признаками:**

а. информационной культуры
б. высшей степени развития цивилизации

в. информационного кризиса
г. информационного общества
д. информационной зависимости

**4.** Отличительными особенностями компьютерного вируса являются:

а. значительный объем программного кода
б. способность к самостоятельному запуску и многократному копированию кода
в. способность к созданию помех корректной работе компьютера
г. легкость распознавания
д. Пункты Б) и В)

**5. Обеспечение защиты информации проводится конструкторами и разработчиками программного обеспечения в следующих направлениях (указать неправильный ответ):**

а. защита от сбоев работы оборудования
б. защита от случайной потери информации
в. защита от преднамеренного искажения
г. разработка правовой базы для борьбы с преступлениями в сфере информационных технологий
д. защита от несанкционированного доступа к информации

**6. Компьютерные вирусы – это: …….**

**7. Методы обеспечения информационной безопасности делятся (указать неправильные ответ):**
**…….**

**8. Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?.....**
**…….**

**9. Что не относится к объектам информационной безопасности Российской Федерации?.....**
**…….**

**10. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?**
**…….**

**11. Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?**
**……**

**12. Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?**

**……..**

**13. Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:**

**…….**

**14.Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?.....**

**15. Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?**

**……**

**16. Что необходимо указать при цитировании статьи, размещенной на чьем-то сайте?**

**…….**

**17. Можно ли использовать статьи из разных журналов и газет на политические, экономические, религиозные или социальные темы для подготовки с их использованием учебного материала?**

**……**

**18. Считается ли статья, обнародованная в Интернет, объектом авторского права?**

**……..**

**19. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:**

**…….**

**20. Активный перехват информации — это перехват, который:**

Ответы к тесту:

| № вопр | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| ответ | д | а | г | д | г |

| | |
|---|---|
| 6 | программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК |
| 7 | политические |
| 8 | Доктрина информационной безопасности РФ |
| 9 | природные и энергетические ресурсы |
| 10 | Все перечисленное выше |
| 11 | Закон «О правовой охране программ для ЭВМ и баз данных» |
| 12 | Закон «Об информации, информатизации и защите информации» |
| 13 | Закон «Об информации, информатизации и защите информации» |
| 14 | нет, так как нормативно-правовые акты не являются объектом авторского |

| | |
|---|---|
| | права |
| 15 | можно, с разрешения издателя, издавшего данную статью, или автора статьи |
| 16 | имя автора, название статьи, адрес сайта, с которого заимствована статья |
| 17 | да, не спрашивая согласия правообладателей, но с обязательным указанием источника заимствования и имен авторов |
| 18 | да, так как любая статья является объектом авторского права как произведение науки или литературы |
| 19 | аудиоперехват; |
| 20 | осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера. |

**Типовые вопросы и практические задания для контроля освоенных умений:**

1. Произвести моделирование в среде табличного процессора MS Excel.
2. Повести регистрацию компании – клиента с использованием информационных сервисных центров в сети Интернет.
3. Определить базовые принципы построения информационных систем предприятий на базе АРМов.
4. Расчет и выбор программные продукты для конечных пользователей предприятий сервиса

**Типовые комплексные задания для контроля приобретенных владений:**

1.Произвести подбор программного обеспечения для АРМов в автосервисе на основе исходных данных деятельности предприятия.

2. Провести оценку организации систем обработки данных на предприятии автосервиса.

3. Составить план организации локальной вычислительной сети на предприятии автосервиса и выбрать сетевое программное обеспечение.

**2.3.2.2. Шкалы оценивания результатов обучения на зачете**

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь и владеть* заявленных дисциплинарных компетенций проводится в режиме «зачтено» и «не зачтено».

Типовые шкала и критерии оценки результатов обучения при сдаче зачёта для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

**3. Критерии оценивания уровня сформированности компонентов и компетенций**

**3.1. Оценка уровня сформированности компонентов компетенций**

При оценке уровня сформированности компетенций в рамках выборочного контроля при зачете считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля

в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в форме зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.