



Министерство образования Иркутской области
Областное государственное образовательное
учреждение среднего профессионального образования
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ОГБОУ СПО "ИАТ"

_____/Семёнов В.Г.
«29» мая 2015 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.12 Безопасность информационных систем


специальности

09.02.03 Программирование в компьютерных системах

Иркутск, 2015

Рассмотрена
цикловой комиссией

Председатель ЦК

 /М.А. Кудрявцева /

№	Разработчик ФИО
1	Филимонова Ольга Николаевна

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения фонда оценочных средств (ФОС)

ФОС по дисциплине является частью программы подготовки специалистов среднего звена по специальности 09.02.03 Программирование в компьютерных системах

1.2. Место дисциплины в структуре ППССЗ:

ОП.00 Общепрофессиональный цикл.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

В результате освоения дисциплины обучающийся должен	№ дидактической единицы	Формируемая дидактическая единица
Знать	1.1	Сущность и понятие информационной безопасности, характеристику ее составляющих
	1.2	Место информационной безопасности в системе национальной безопасности страны
	1.3	Источники угроз информационной безопасности и меры по их предотвращению
	1.4	Современные средства и способы обеспечения информационной безопасности
	1.5	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи
Уметь	2.1	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
	2.2	Классифицировать основные угрозы безопасности информации
	2.3	Применять основные правила и документы сертификации Российской Федерации

1.4. Формируемые компетенции:

ОК.1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

- ОК.2 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК.3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК.4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК.5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК.6 Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
- ОК.7 Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
- ОК.8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
- ОК.9 Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

- ПК.1.1 Выполнять разработку спецификаций отдельных компонент.
- ПК.1.2 Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.
- ПК.1.3 Выполнять отладку программных модулей с использованием специализированных программных средств.
- ПК.1.4 Выполнять тестирование программных модулей.
- ПК.1.5 Осуществлять оптимизацию программного кода модуля.
- ПК.1.6 Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.
- ПК.2.1 Разрабатывать объекты базы данных.
- ПК.2.2 Реализовывать базу данных в конкретной системе управления базами данных (далее - СУБД).
- ПК.2.3 Решать вопросы администрирования базы данных.
- ПК.2.4 Реализовывать методы и технологии защиты информации в базах данных.
- ПК.3.1 Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.
- ПК.3.2 Выполнять интеграцию модулей в программную систему.
- ПК.3.3 Выполнять отладку программного продукта с использованием специализированных программных средств.
- ПК.3.4 Осуществлять разработку тестовых наборов и тестовых сценариев.
- ПК.3.5 Производить инспектирование компонент программного продукта на

предмет соответствия стандартам кодирования.

ПК.3.6 Разрабатывать технологическую документацию.

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

2.1 Текущий контроль (ТК) № 1

Тема занятия: 1.2.3. Информационная безопасность как состояние защищенности национальных интересов в информационной сфере

Метод и форма контроля: Письменный опрос (Опрос)

Вид контроля: Проверочная работа

Дидактическая единица: 1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих

Занятие(-я):

1.1.1. Введение в проблему информационной безопасности, ее актуальность

1.1.2. Цели и задачи обеспечения информационной безопасности для различных объектов

1.1.3. Основные составляющие информационной безопасности

Задание №1

Вставьте пропущенные слова:

Основные понятия защиты информации и информационной безопасности

Современные методы обработки, передачи и накопления информации способствовали появлению _____, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям.

Поэтому обеспечение _____ компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Защита информации – это _____ по предотвращению _____ защищаемой информации, _____ и _____ воздействий на защищаемую информацию.

Под информационной безопасностью понимают _____ от незаконного ознакомления, преобразования и уничтожения.

Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Компоненты АС можно разбить на следующие группы:

- _____;
- _____;
- _____;
- _____.

С допуском к информации и ресурсам системы связана группа таких понятий, как _____, _____, _____.

<i>Оценка</i>	<i>Показатели оценки</i>
3	Вставлено 7 пропущенных слов и выражений

4	Вставлено 10 пропущенных слов и выражений
5	Вставлено 10 пропущенных слов и выражений

Дидактическая единица: 1.2 Место информационной безопасности в системе национальной безопасности страны

Занятие(-я):

1.2.1. Понятие национальной безопасности

1.2.2. Обеспечение национальной безопасности Российской Федерации

Задание №1

Вставьте пропущенные слова и выражения:

Место информационной безопасности в системе национальной безопасности России

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на _____ как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем _____ информационных потребностей _____, _____ и самого _____, обеспечение их ИБ.

Информационная безопасность определяется *способностью государства (общества, личности):*

- _____ с определенной вероятностью достаточные и защищенные _____ для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;
- _____ информационным _____, на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники _____;
- _____ личностные и групповые навыки и умения безопасного поведения;
- _____ постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Оценка	Показатели оценки
3	Вставлено 6 пропущенных слов и выражений
4	Вставлено 9 пропущенных слов и выражений
5	Вставлено 12 пропущенных слов и выражений

Дидактическая единица: 2.3 Применять основные правила и документы

сертификации Российской Федерации

Занятие(-я):

1.2.2.Обеспечение национальной безопасности Российской Федерации

Задание №1

1. Ознакомьтесь с документом Политика информационной безопасности ([Политика_ИБ](#));
2. Определите неправильные данные в этом документе;
3. Внесите изменения в документ и сохраните на своем сетевом ресурсе.

<i>Оценка</i>	<i>Показатели оценки</i>
3	Внесено 13 изменений в документ
4	Внесено 19 изменений в документ
5	Внесено 25 изменений в документ

2.2 Текущий контроль (ТК) № 2

Тема занятия: 2.1.6.Проектирование системы защиты информации с использованием модели с полным перекрытием множества угроз

Метод и форма контроля: Письменный опрос (Опрос)

Вид контроля: Проверочная работа

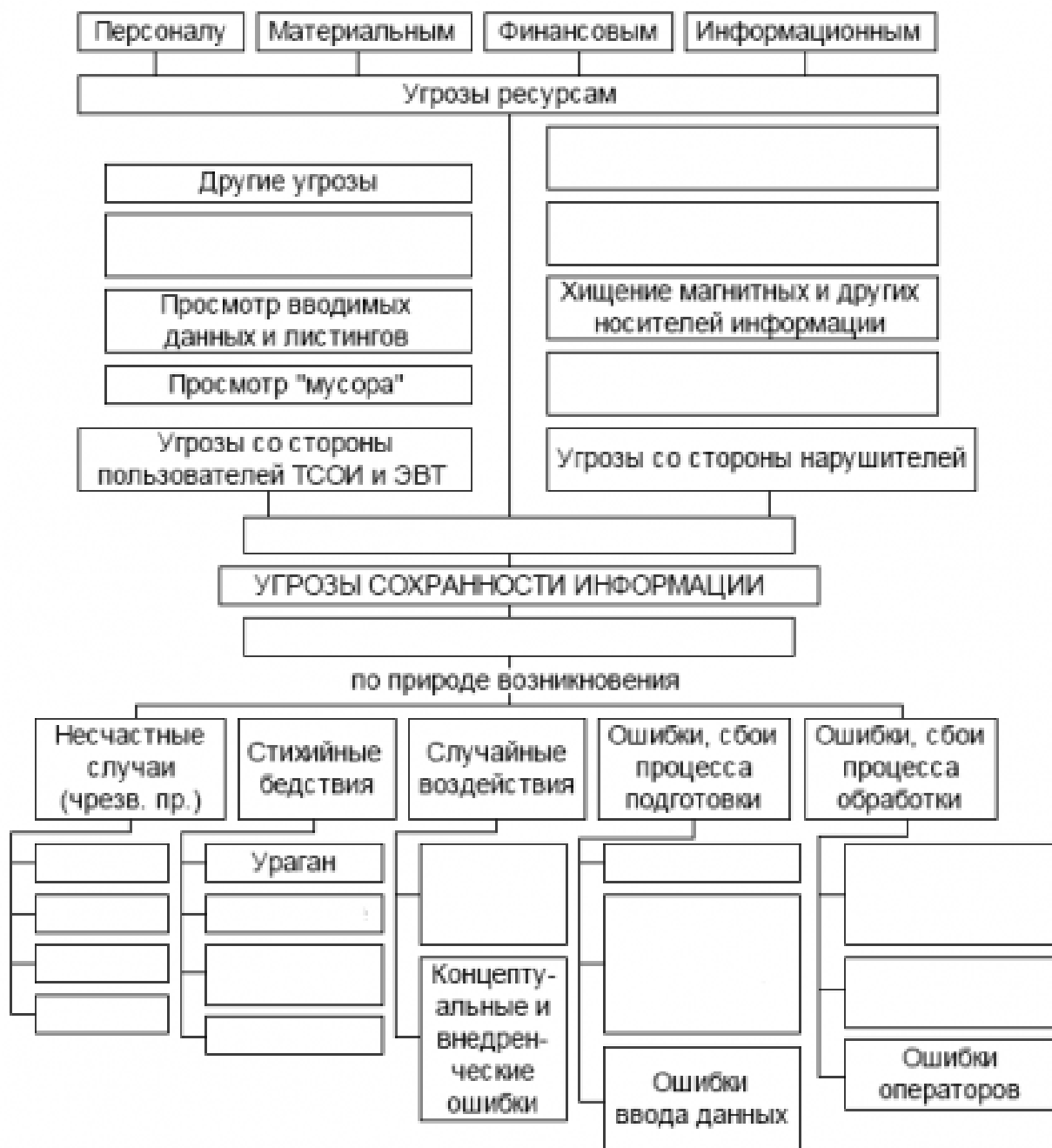
Дидактическая единица: 1.3 Источники угроз информационной безопасности и меры по их предотвращению

Занятие(-я):

- 2.1.1.Угрозы информационной безопасности Российской Федерации
- 2.1.2.Принципы и приоритетные направления государственной политики обеспечения информационной безопасности
- 2.1.3.Угрозы безопасности автоматизированных систем
- 2.1.4.Меры и основные принципы обеспечения безопасности автоматизированных систем
- 2.1.5.Анализ и оценка информационных рисков, угроз и уязвимостей системы

Задание №1

Заполните схему "Классификация Угроз безопасности" недостающими данными



<i>Оценка</i>	<i>Показатели оценки</i>
3	Правильно заполнены 10 элементов
4	Правильно заполнены 14 элементов
5	Правильно заполнены 18 элементов

2.3 Текущий контроль (ТК) № 3

Тема занятия: 2.1.13. Анализ и оценка рисков информационной безопасности с использованием нечеткой логики

Метод и форма контроля: Письменный опрос (Опрос)

Вид контроля: Проверочная работа

Дидактическая единица: 2.2 Классифицировать основные угрозы безопасности информации

Занятие(-я):

2.1.5. Анализ и оценка информационных рисков, угроз и уязвимостей системы

2.1.6. Проектирование системы защиты информации с использованием модели с полным перекрытием множества угроз

2.1.7. Анализ рисков информационной безопасности с использованием методики COBIT

2.1.8. Анализ рисков информационной безопасности с использованием программного комплекса ГРИФ

2.1.9. Разработка сценариев действий нарушителя информационной безопасности с использованием сети ПЕТРИ

2.1.10. Определение показателей защищенности информации при несанкционированном доступе

2.1.11. Использование методологии и стандартов IDEF для моделирования процессов в защищенных системах

2.1.12. Анализ рисков информационной безопасности для малого и среднего бизнеса

Задание №1

1. Укажите виды угроз соответствующие следующим признакам:

- По природе возникновения;
- По источнику угроз;
- По положению источника угроз;
- По степени воздействия на автоматизированную систему;
- По степени преднамеренности проявления;
- По текущему месту расположения информации.

2. Для каждого вида угроз приведите пример.

<i>Оценка</i>	<i>Показатели оценки</i>
3	Частично указаны угрозы, частично приведены примеры
4	Указаны все угрозы, частично приведены примеры
5	Указаны все угрозы, для каждой угрозы приведены примеры

2.4 Текущий контроль (ТК) № 4

Тема занятия: 3.2.2. Категорирование и документирование защищаемых ресурсов

Метод и форма контроля: Творческая работа (доклад, презентация) (Опрос)

Вид контроля: Задание с применением ИКТ

Дидактическая единица: 1.4 Современные средства и способы обеспечения

информационной безопасности

Занятие(-я):

3.1.1.Обеспечение информационной безопасности Российской Федерации

3.1.2.Обеспечение безопасности автоматизированных систем

3.1.3.Обеспечение безопасности компьютерных сетей

3.1.4.Отечественные и зарубежные программно-технические средства защиты информации в интегрированных информационных системах управления предприятием

3.1.5.Вредоносные программы и защита от них

Задание №1

Создайте презентацию, по программно-техническим средствам, предназначенным для защиты информации в ПК, в которой необходимо отразить следующие вопросы:

- Программно-техническое средство;
- Функции/ общий вид изделия;
- Принципы функционирования и характеристики.

Рекомендуемые сайты для подготовки презентации:

<https://ancud.ru/index.html>

<https://ru.neospy.net/>

<https://www.adaware.com/>

<http://zbackup.org/>

<http://zdisk.cz/en/>

<http://www.zecurion.ru/products/>

<http://printmanager.com/>

<http://www.deleteit.ru/01.html>

Общие требования к презентации:

- Презентация не должна быть меньше 15 слайдов.
- Первый лист – это титульный лист, на котором обязательно должны быть представлены: название работы; название выпускающей организации; фамилия, имя, отчество автора;
- Следующим слайдом должно быть содержание. Желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание.
- Дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста.

<i>Оценка</i>	<i>Показатели оценки</i>
---------------	--------------------------

3	Презентация оформлена в соответствии с требованиями, освещены менее 5 программно-технических средств защиты
4	Презентация оформлена в соответствии с требованиями, освещены 7 программно-технических средств защиты
5	Презентация оформлена в соответствии с требованиями, освещены 10 программно-технических средств защиты

Дидактическая единица: 1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи

Занятие(-я):

1.2.2. Обеспечение национальной безопасности Российской Федерации

3.2.1. Концепция управления жизненным циклом конфиденциальной информации

Задание №1

Используя электронные материалы, ответьте на предложенные вопросы и сделайте вывод о жизненном цикле конфиденциальной информации

- 1) Выяснить, что понимается под конфиденциальной информацией.
- 2) Выяснить, что понимается под носителями, источниками, каналами утечки конфиденциальной информации.
- 3) Выяснить, что понимается под грифом конфиденциального документа, виды грифов.
- 4) Каковы правила засекречивания?
- 5) Каковы правила рассекречивания?
- 6) Кто имеет право работать с конфиденциальными документами?
- 7) Какие бывают виды нарушений при работе с конфиденциальной информацией и наказания в соответствии с УК (шпионаж, утрата, разглашение)?

<i>Оценка</i>	<i>Показатели оценки</i>
3	Ответы на пять вопросов полные, правильные
4	Ответы на шесть вопросов полные, правильные
5	Ответы на семь вопросов полные, правильные

Дидактическая единица: 2.1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Занятие(-я):

3.2.1. Концепция управления жизненным циклом конфиденциальной информации

Задание №1

1. Для выбранного объекта защиты описать

- 1) Название и характеристика объекта информатизации
- 2) Критичные ресурсы, которые нуждаются в защите (ПО, оборудование,

информация)

- 3) Степень конфиденциальности информации
- 4) Виды угроз, которые могут быть признаны реальными.
- 5) Характер происхождения
- 6) Классы каналов
- 7) Источники появления угроз
- 8) Причины нарушения целостности
- 9) Потенциально возможные злоумышленные действия
- 10) Предложить средства защиты для каждого вида угроз.
- 11) Определить класс защиты информации. (см. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»).

2. Оформите отчет о проделанной работе.

Объекты информатизации (варианты)

- 1 Одиночно стоящий компьютер в бухгалтерии.
- 2 Сервер в бухгалтерии.
- 3 Почтовый сервер.
- 4 Веб-сервер.
- 5 Компьютерная сеть материальной группы.
- 6 Одноранговая локальная сеть без выхода в Интернет.
- 7 Одноранговая локальная сеть с выходом в Интернет.
- 8 Сеть с выделенным сервером без выхода в Интернет.
- 9 Сеть с выделенным сервером с выходом в Интернет.
- 10 Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
- 11 Телефонная сеть.
- 12 Средства телекоммуникации (радиотелефон, мобильный телефон, пейджер).
- 13 Банковские операции (внесение денег на счет и снятие со счета).
- 14 Операции с банковскими пластиковыми карточками.
- 15 Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
- 16 Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
- 17 Материалы для служебного пользования на твердых носителях в производстве.
- 18 Материалы для служебного пользования на твердых носителях на закрытом предприятии.
- 19 Материалы для служебного пользования на твердых носителях в архиве.
- 20 Материалы для служебного пользования на твердых носителях в налоговой инспекции.

- 21 Комната для переговоров по сделкам на охраняемой территории.
- 22 Комната для переговоров по сделкам на неохраняемой территории.
- 23 Сведения для СМИ, цензура на различных носителях информации (твердая копия, фотография, электронный носитель и др.).
- 24 Судебные материалы (твердая копия).
- 25 Паспортный стол РОВД.
- 26 Материалы по владельцам автомобилей (твердая копия, фотография, электронный носитель и др.).
- 27 Материалы по недвижимости (твердая копия, фотография, электронный носитель и др.).
- 28 Сведения по тоталитарным сектам и другим общественно вредным организациям.
- 29 Сведения по общественно полезным организациям (Красный Крест и др.).
- 30 Партийные списки и руководящие документы.

<i>Оценка</i>	<i>Показатели оценки</i>
3	В отчете полно отражены 6 пунктов задания
4	В отчете полно отражены 8 пунктов задания
5	В отчете полно отражены 11 пунктов задания

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

№ семестра	Вид промежуточной аттестации
7	Дифференцированный зачет

Дифференцированный зачет может быть выставлен автоматически по результатам текущих контролей
Текущий контроль №1
Текущий контроль №2
Текущий контроль №3
Текущий контроль №4

Метод и форма контроля: Контрольная работа (Опрос)

Вид контроля: по выбору выполнить три задания

Дидактическая единица для контроля:

1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих

Задание №1 (из текущего контроля)

Вставьте пропущенные слова:

Основные понятия защиты информации и информационной безопасности

Современные методы обработки, передачи и накопления информации способствовали появлению _____, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям. Поэтому обеспечение _____ компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Защита информации – это _____ по предотвращению _____ защищаемой информации, _____ и _____ воздействий на защищаемую информацию.

Под информационной безопасностью понимают _____ от незаконного ознакомления, преобразования и уничтожения.

Современная автоматизированная система (АС) обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Компоненты АС можно разбить на следующие группы:

- _____ ;
- _____ ;
- _____ ;
- _____ .

С допуском к информации и ресурсам системы связана группа таких понятий, как

Оценка	Показатели оценки
3	Вставлено 7 пропущенных слов и выражений
4	Вставлено 10 пропущенных слов и выражений
5	Вставлено 10 пропущенных слов и выражений

Дидактическая единица для контроля:

1.2 Место информационной безопасности в системе национальной безопасности страны

Задание №1 (из текущего контроля)

Вставьте пропущенные слова и выражения:

Место информационной безопасности в системе национальной безопасности России

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на _____ как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней. Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем _____ информационных потребностей _____, _____ и самого _____, обеспечение их ИБ.

Информационная безопасность определяется *способностью государства (общества, личности):*

- _____ с определенной вероятностью достаточные и защищенные _____ для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;
- _____ информационным _____, на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники _____;
- _____ личностные и групповые навыки и умения безопасного поведения;
- _____ постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

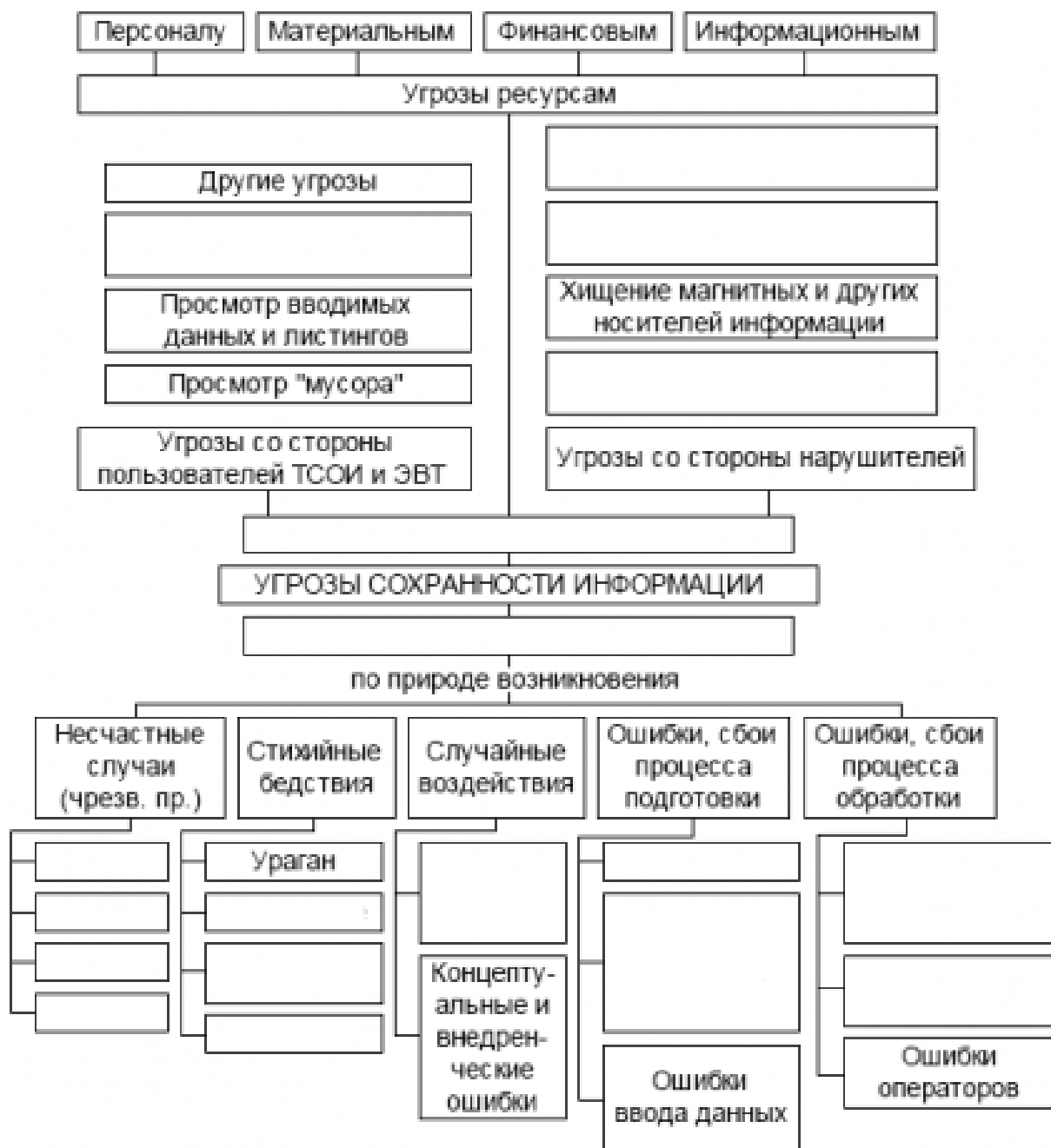
Оценка	Показатели оценки
3	Вставлено 6 пропущенных слов и выражений
4	Вставлено 9 пропущенных слов и выражений

Дидактическая единица для контроля:

1.3 Источники угроз информационной безопасности и меры по их предотвращению

Задание №1 (из текущего контроля)

Заполните схему "Классификация Угроз безопасности" недостающими данными



<i>Оценка</i>	<i>Показатели оценки</i>
3	Правильно заполнены 10 элементов
4	Правильно заполнены 14 элементов

Дидактическая единица для контроля:

1.4 Современные средства и способы обеспечения информационной безопасности

Задание №1 (из текущего контроля)

Создайте презентацию, по программно-техническим средствам, предназначенным для защиты информации в ПК, в которой необходимо отразить следующие вопросы:

- Программно-техническое средство;
- Функции/ общий вид изделия;
- Принципы функционирования и характеристики.

Рекомендуемые сайты для подготовки презентации:

<https://ancud.ru/index.html>

<https://ru.neospy.net/>

<https://www.adaware.com/>

<http://zbackup.org/>

<http://zdisk.cz/en/>

<http://www.zecurion.ru/products/>

<http://printmanager.com/>

<http://www.deleteit.ru/01.html>

Общие требования к презентации:

- Презентация не должна быть меньше 15 слайдов.
- Первый лист – это титульный лист, на котором обязательно должны быть представлены: название работы; название выпускающей организации; фамилия, имя, отчество автора;
- Следующим слайдом должно быть содержание. Желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание.
- Дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста.

<i>Оценка</i>	<i>Показатели оценки</i>
3	Презентация оформлена в соответствии с требованиями, освещены менее 5 программно-технических средств защиты
4	Презентация оформлена в соответствии с требованиями, освещены 7 программно-технических средств защиты

5	Презентация оформлена в соответствии с требованиями, освещены 10 программно-технических средств защиты
---	--

Дидактическая единица для контроля:

1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи

Задание №1 (из текущего контроля)

Используя электронные материалы, ответьте на предложенные вопросы и сделайте вывод о жизненном цикле конфиденциальной информации

- 1) Выяснить, что понимается под конфиденциальной информацией.
- 2) Выяснить, что понимается под носителями, источниками, каналами утечки конфиденциальной информации.
- 3) Выяснить, что понимается под грифом конфиденциального документа, виды грифов.
- 4) Каковы правила засекречивания?
- 5) Каковы правила рассекречивания?
- 6) Кто имеет право работать с конфиденциальными документами?
- 7) Какие бывают виды нарушений при работе с конфиденциальной информацией и наказания в соответствии с УК (шпионаж, утрата, разглашение)?

<i>Оценка</i>	<i>Показатели оценки</i>
3	Ответы на пять вопросов полные, правильные
4	Ответы на шесть вопросов полные, правильные
5	Ответы на семь вопросов полные, правильные

Дидактическая единица для контроля:

2.1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Задание №1 (из текущего контроля)

1. Для выбранного объекта защиты описать

- 1) Название и характеристика объекта информатизации
- 2) Критичные ресурсы, которые нуждаются в защите (ПО, оборудование, информация)
- 3) Степень конфиденциальности информации
- 4) Виды угроз, которые могут быть признаны реальными.
- 5) Характер происхождения
- 6) Классы каналов
- 7) Источники появления угроз
- 8) Причины нарушения целостности
- 9) Потенциально возможные злоумышленные действия

- 10) Предложить средства защиты для каждого вида угроз.
- 11) Определить класс защиты информации. (см. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»).

2. Оформите отчет о проделанной работе.

Объекты информатизации (варианты)

- 1 Одиночно стоящий компьютер в бухгалтерии.
- 2 Сервер в бухгалтерии.
- 3 Почтовый сервер.
- 4 Веб-сервер.
- 5 Компьютерная сеть материальной группы.
- 6 Одноранговая локальная сеть без выхода в Интернет.
- 7 Одноранговая локальная сеть с выходом в Интернет.
- 8 Сеть с выделенным сервером без выхода в Интернет.
- 9 Сеть с выделенным сервером с выходом в Интернет.
- 10 Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
- 11 Телефонная сеть.
- 12 Средства телекоммуникации (радиотелефон, мобильный телефон, пейджер).
- 13 Банковские операции (внесение денег на счет и снятие со счета).
- 14 Операции с банковскими пластиковыми карточками.
- 15 Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
- 16 Компьютер, хранящий конфиденциальную информацию о разработках предприятия.
- 17 Материалы для служебного пользования на твердых носителях в производстве.
- 18 Материалы для служебного пользования на твердых носителях на закрытом предприятии.
- 19 Материалы для служебного пользования на твердых носителях в архиве.
- 20 Материалы для служебного пользования на твердых носителях в налоговой инспекции.
- 21 Комната для переговоров по сделкам на охраняемой территории.
- 22 Комната для переговоров по сделкам на неохраняемой территории.
- 23 Сведения для СМИ, цензура на различных носителях информации (твердая копия, фотография, электронный носитель и др.).
- 24 Судебные материалы (твердая копия).
- 25 Паспортный стол РОВД.
- 26 Материалы по владельцам автомобилей (твердая копия, фотография, электронный носитель и др.).

27 Материалы по недвижимости (твердая копия, фотография, электронный носитель и др.).

28 Сведения по тоталитарным сектам и другим общественно вредным организациям.

29 Сведения по общественно полезным организациям (Красный Крест и др.).

30 Партийные списки и руководящие документы.

<i>Оценка</i>	<i>Показатели оценки</i>
3	В отчете полно отражены 6 пунктов задания
4	В отчете полно отражены 8 пунктов задания
5	В отчете полно отражены 11 пунктов задания

Дидактическая единица для контроля:

2.2 Классифицировать основные угрозы безопасности информации

Задание №1 (из текущего контроля)

1. Укажите виды угроз соответствующие следующим признакам:

- По природе возникновения;
- По источнику угроз;
- По положению источника угроз;
- По степени воздействия на автоматизированную систему;
- По степени преднамеренности проявления;
- По текущему месту расположения информации.

2. Для каждого вида угроз приведите пример.

<i>Оценка</i>	<i>Показатели оценки</i>
3	Частично указаны угрозы, частично приведены примеры
4	Указаны все угрозы, частично приведены примеры
5	Указаны все угрозы, для каждой угрозы приведены примеры

Дидактическая единица для контроля:

2.3 Применять основные правила и документы сертификации Российской Федерации

Задание №1 (из текущего контроля)

1. Ознакомьтесь с документом Политика информационной безопасности ([Политика_ИБ](#));
2. Определите неправильные данные в этом документе;
3. Внесите изменения в документ и сохраните на своем сетевом ресурсе.

<i>Оценка</i>	<i>Показатели оценки</i>
---------------	--------------------------

3	Внесено 13 изменений в документ
4	Внесено 19 изменений в документ
5	Внесено 25 изменений в документ