Министерство образования Иркутской области
Государственное бюджетное профессиональное образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»

_____/Семёнов В.Г.
«31» мая 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

ОП.16 Безопасность информационных систем

специальности

09.02.03 Программирование в компьютерных системах

Иркутск, 2016

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.

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 _____, _____, _____.

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: 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.

Оценка	***Показатели оценки***
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: 2.1.8.Анализ рисков информационной безопасности для малого и среднего бизнеса
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
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
Задание №1
1. Заполните схему "Классификация угроз безопасности" недостающими данными, схема расположена по адресу:
https://learningapps.org/display?v=pqf0ff5q518
2. Сделайте скриншот заполненной схемы, сохраните на свой сетевой ресурс.

Оценка	***Показатели оценки***

3	Правильно заполнены 10 элементов
4	Правильно заполнены 14 элементов
5	Правильно заполнены 18 элементов

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

Задание №1

1. Укажите виды угроз соответстующие 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.

Оценка	*Показатели оценки*
3	Частично указаны угрозы, частично приведены примеры
4	Указаны все угрозы, частично приведены примеры
5	Указаны все угрозы, для каждоу угрозы приведены примеры

2.3 Текущий контроль (ТК) № 3

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.

Оценка	***Показатели оценки***
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)?

Оценка	***Показатели оценки***
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.

Оценка	***Показатели оценки***
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

Метод и форма контроля: Тестирование (Опрос)
Вид контроля: Ответьте на 24 вопроса теста
Дидактическая единица для контроля:
1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих
Задание №1
Вопрос 1. Выберите правильное определение термина «информационная безопасность» - это

- защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений
- актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
- это совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности: экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других

Вопрос 2. Выберите правильное определение термина «защита информации»

- комплекс мероприятий, направленных на обеспечение информационной безопасности.
- спектр интересов субъектов, связанных с использованием информационных систем, которые можно разделить на категории

- возможность за приемлемое время получить требуемую информационную услугу
- спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и *поддерживающей инфраструктуры*.

Вопрос 3. Соотнесите определения и термины категорий

Целостность	возможность за приемлемое время получить требуемую информационную услугу
Конфиденциальность	актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
Доступность	защита от несанкционированного доступа к информации

Вопрос 4. О каком базовом структурном элементе информационной безопасности идет речь:

достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомленности (англ. *need-to-know*). Иными словами, авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей.

- Конфиденциальность
- Целостность
- Доступность

Вопрос 5. О каком базовом структурном элементе информационной безопасности идет речь:

Четкое осуществление операций или принятие верных решений в организации возможно лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, либо транслируемых по компьютерным сетям. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки

- Конфиденциальность

- Целостность
- Доступность

Оценка	*Показатели оценки*
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

Дидактическая единица для контроля:

1.2 Место информационной безопасности в системе национальной безопасности страны

Задание №1

Вопрос 1. Система национальных интересов России определяется совокупностью основных интересов.

Соотнесите термины и определения основных интересов:

общества	состоят в обеспечении конституционных прав и свобод, личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии;
государства	включают в себя упрочение демократии, достижение и поддержание общественного согласия, повышение созидательной активности населения и духовное возрождение России
личности	состоят в защите конституционного строя, суверенитета и территориальной целостности России, в установлении политической, экономической и социальной стабильности, в безусловном исполнении законов и поддержании правопорядка, в развитии международного сотрудничества на основе партнерства

Вопрос 2. Какой принцип деятельности по обеспечению информационной безопасности заключается в обеспечении прав и свобод человека и гражданина при осуществлении противодействия угрозам информационной безопасности, недопущении противоправных посягательств на его личность, унижения чести и достоинства человека, произвольного вмешательства в его частную жизнь, личную и семейную тайны, ограничения свободы его информационной

деятельности, а также в минимизации ущерба этим правам и свободам в случаях, когда их ограничение осуществляется на законных основаниях.

- Принцип гуманизма
- Принцип законности
- Принцип конкретности

Вопрос 3. Какой принцип деятельности по обеспечению информационной безопасности состоит в обеспечении безопасности применительно к конкретным жизненным обстоятельствам с учетом разнообразных форм проявления объективных законов на основе достоверной информации как о внутренних и внешних угрозах, так и о возможностях противодействия им. Достоверная информация позволяет установить конкретные формы проявления угроз, определить в соответствии с этим цели и действия по обеспечению безопасности, конкретизировать методы противодействия угрозам, а также необходимые для их реализации силы и средства.

- Принцип гуманизма
- Принцип законности
- Принцип конкретности

Вопрос 4. Какой принцип деятельности по обеспечению информационной безопасности состоит в нахождении и поддержании необходимого баланса между открытостью деятельности по противодействию угрозам информационной безопасности, позволяющей добиться доверия и поддержки общества, и защитой определенной информации, разглашение которой может снизить эффективность противодействия угрозам безопасности.

- Принцип гуманизма
- Принцип законности и конституционности
- Принцип сочетания гласности и профессиональной тайны

Вопрос 5. Какой принцип деятельности по обеспечению информационной безопасности означает осуществление всех свойственных государственным организациям и должностным лицам функций в строгом соответствии с действующей конституцией, законами и подзаконными актами, согласно установленной в законодательном порядке компетенции. Строгое и неуклонное соблюдение законности и конституционности должно быть непременным

требованием, принципом деятельности не только государственных, но и негосударственных органов, учреждений и организаций.

- Принцип гуманизма
- Принцип законности и конституционности
- Принцип сочетания гласности и профессиональной тайны

Оценка	***Показатели оценки***
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

Дидактическая единица для контроля:

1.3 Источники угроз информационной безопасности и меры по их предотвращению

Задание №1

Вопрос 1. Выберите источники внутренних угроз

- Сотрудники
- Аппаратные средства
- Организации
- Вредоносное программное обеспечение

Вопрос 2. Выберите источники внешних угроз

- Аппаратные средства
- Программное обеспечение
- Стихийные бедствия
- Вредосносное программное обеспечение
- Организации

Вопрос 3. По способам воздействия все меры по минимизации угроз подразделяют на:

- правовые (законодательные);
- психологические;
- административные;

- физические;
- аппаратно-программные.

Вопрос 4. Административные меры по предотвращению угроз информационной безопасности включают:

- разработку правил обработки информации в компьютерных информационных системах
- организацию надежного пропускного режима
- обеспечение конфиденциальности данных
- регистрацию и анализ событий, происходящих в компьютерных информационных системах

Вопрос 5. Аппаратно-программные средства защиты, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

- разграничение доступа к ресурсам компьютерных информационных систем
- контроль целостности данных
- обеспечение конфиденциальности данных
- распределение реквизитов разграничения доступа (паролей, полномочий и т.п.)
- организацию скрытого контроля над работой пользователей и персонала

Оценка	***Показатели оценки***
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

Дидактическая единица для контроля:
1.4 Современные средства и способы обеспечения информационной безопасности
Задание №1
Вопрос 1. Выберите примеры которые относятся к методу обеспечения безопасности информации - ОГРАНИЧЕНИЕ ДОСТУПА

- Физическая преграда

- Система охранной сигнализации
- Контрольно-пропускная преграда
- Установка специальных фильтров
- Применение волоконно-оптических кабелей

Вопрос 2. Выберите угрозы который относятся к методу обеспечения безопасности информации - КОНТРОЛЬ ДОСТУПА К АППАРАТУРЕ

- Изменение и разрушение принципиальной схемы компьютерной системы и аппаратуры
- Подключения постороннего устройства
- Изменения алгоритма работы КС путем использования технологических пультов
- Применение волоконно-оптических кабелей
- Размещение технических средств в отдельных помещениях

Вопрос 3. Выберите действия которые относятся к методу обеспечения безопасности информации - РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ В СИСТЕМЕ

- Организация доступа пользователей к устройствам памяти
- Размещение технических средств в отдельных помещениях
- Разделение информации по виду, характеру, назначению
- Разработка должностных инструкций по обеспечению режима секретности
- Изменения алгоритма работы КС путем использования технологических пультов

Вопрос 4. Выберите пример который относятся к методу обеспечения безопасности информации - РАЗДЕЛЕНИЕ ПРИВИЛЕГИЙ НА ДОСТУП

- Сейф с несколькими ключами
- Установка специальных фильтров
- Разделение информации по виду, характеру, назначению

Вопрос 5. Выберите пример который относятся к методу обеспечения безопасности информации - ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ЛИЧНОСТИ

- Системы распознавания образа
- Присвоение лицу уникального имени или числа – пароля
- Метод «запрос-ответ»
- Символы исходного текста записанные в одном алфавите, заменяются символами другого алфавита
- Установка специальных экранов

Оценка	*Показатели оценки*
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

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

Задание №1

Вопрос 1. Какое правило конфиденциального документооборота означает, что все операции по приему, отправке, обработке, хранению в организации осуществляются в подразделении (отделе, группе) конфиденциального делопроизводства или специально выделенным сотрудником подразделения общего делопроизводства.

- Централизация всех стадий, процедур и операций по обработке и хранению конфиденциальных документов
- Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа
- Проверка комплектности, целостности документа при любом перемещении

Вопрос 2. Соблюдение какого правила конфиденциального документооборота необходимо для формирования такого массива данных о документах, который в любой момент времени может дать информацию о месте нахождения каждого документа, операциях, совершенных или совершаемых с ним.

- Централизация всех стадий, процедур и операций по обработке и хранению конфиденциальных документов
- Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа

- Проверка комплектности, целостности документа при любом перемещении

Вопрос 3. Для выполнения этого правила, конфиденциального документооборота, работник подразделения конфиденциального делопроизводства должен
при каждом получении или передаче конфиденциального документа пересчитывать количество листов основного документа, количество приложений и
количество листов приложений для подтверждения целостности и комплектности конфиденциального документа. При этом в учетной форме и на самом
документе отмечается количество листов основного документа и количество приложений и листов приложений. На документе эти сведения проставляются в составе отметки о поступлении (входящем штампе), где наряду с датой и номером поступления указываются перечисленные данные, например:
16.04.2008 вх. № 58к
5 л. + 3 прил. 6 л.

- Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа
- Проверка комплектности, целостности документа при любом перемещении
- Письменная фиксация всех обращений персонала к документу

Вопрос 4. Соблюдение этого правила конфиденциального документооборота требует фиксировать в учетных формах не только те действия, которые санкционированы и совершаются в соответствии с нормативными актами организации, но и несанкционированные действия, совершаемые с конфиденциальным документом

- Пооперационный учет всех действий, совершаемых с конфиденциальными документами, учет каждого факта "жизненного цикла" документа
- Проверка комплектности, целостности документа при любом перемещении
- Письменная фиксация всех обращений персонала к документу

Вопрос 5. Это правило конфиденциального документооборота требует, чтобы в процедуре уничтожения проектов, черновиков, конфиденциальных документов участвовало не менее двух работников. Данная процедура производится только по акту.

- Коллегиальность процедуры уничтожения документов, дел и баз данных
- Проверка комплектности, целостности документа при любом перемещении
- Письменная фиксация всех обращений персонала к документу

Оценка	*Показатели оценки*
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

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

Задание №1

Вопрос 1. Соотнесите категории конфиденциальности защищаемой информации с определениями:

Строго конфиденциальная	информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства, а также информация, ограничение на распространение которой введены решениями руководства организации
Конфиденциальная	информация, ограничения на распространение которой вводятся решением руководства организации в соответствии с предоставленными ему как собственнику информации действующим законодательством правами
Открытая	информация, обеспечения конфиденциальности (введения ограничений на распространение) которой не требуется

Вопрос 2. Соотнесите категории целостности защищаемой информации с определениями:

Высокая	к данной категории относят информацию, несанкционированная модификация или фальсификация которой может привести к нанесению значительного прямого ущерба организации
Низкая	данная категория включает в себя информацию, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, ее клиентам, партнерам или сотрудникам
Нет требований	к данной категории относится информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется

Вопрос 3. Соотнесите категории доступности защищаемой информации с определениями:

Беспрепятственная доступность	доступ к задаче должен обеспечиваться в любое время
Высокая доступность	доступ к задаче осуществляется без существенных временных задержек
Средняя доступность	доступ к задаче может обеспечиваться с существенными временными задержками

Низкая доступность	временные задержки при доступе к задаче практически не лимитированы

Оценка	*Показатели оценки*
3	Дан правильный ответ на 1 вопрос
4	Даны правильные ответы на 2 вопроса
5	Даны правильные ответы на 3 вопроса

Дидактическая единица для контроля:

2.2 Классифицировать основные угрозы безопасности информации

Задание №1

Вопрос 1. Выберите угрозы, которые относятся к классификации по природе возникновения:

- Независимо от активности автоматизированной системы
- Естественные угрозы
- Искусственные угрозы
- Программно-аппаратные средства

Вопрос 2. Выберите угрозы, которые относятся к классификации по источнику угроз

- Природная среда
- Человек
- Программно-аппаратные средства
- На внешних запоминающих угрозах
- Угрозы доступа к информации, циркулирующей в линиях связи

Вопрос 3. Выберите угрозы, которые относятся к классификации по положению источника угроз

- Вне контролируемой зоны
- Искусственные угрозы
- Халатность персонала
- Непосредственно в автоматизированной системе

Вопрос 4. Выберите угрозы, которые относятся к классификации по степени воздействия на автоматизированную систему

- Пассивные угрозы
- Активные угрозы
- Халатность персонала
- Искусственные угрозы

Вопрос 5. Выберите угрозы, которые относятся к классификации по текущему месту расположения информации

- На внешних запоминающих устройствах
- Угрозы доступа к информации, циркулирующей в линиях связи
- Человек
- Природная среда

Оценка	***Показатели оценки***
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов

Дидактическая единица для контроля:
2.3 Применять основные правила и документы сертификации Российской Федерации

Задание №1

Вопрос 1. Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации.

- Указанные средства подлежат обязательной сертификации
- Указанные средства подлежат обязательной проверки федеральных органов
- Указанные средства подлежат обязательной проверки службой безопасности

Вопрос 2. Соотнесите основные схемы проведения сертификации средств защиты информации:

для единичных образцов средств защиты информации	проведение испытаний этих образцов на соответствие требованиям по защите информации
для серийного производства средств защиты информации	проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований

Вопрос 3. В каких случаях Федеральный орган по сертификации и органы по сертификации средств защиты информации имеют право приостанавливать или аннулировать действие сертификата:

- изменение нормативных и методических документов по защите информации в части требований к средствам защиты информации, методам испытаний и контроля;
- изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;
- отказ изготовителя обеспечить беспрепятственное выполнение своих полномочий лицами, осуществляющими государственные контроль и надзор, инспекционный контроль за сертификацией и сертифицированными средствами защиты информации.
- проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований
- проведение испытаний этих образцов на соответствие требованиям по защите информации

Вопрос 4. Выберите участников сертификации средств защиты информации:

- федеральный орган по сертификации;
- органы по сертификации средств защиты информации;
- испытательные лаборатории;
- изготовители-продавцы, исполнители продукции.

- конструкторы-испытатели
- правоохранительные органы

Вопрос 5. Срок действия сертификата средств защиты информации не может превышать:

- пяти лет
- десяти лет
- трех лет

Оценка	***Показатели оценки***
3	Даны правильные ответы на 3 вопроса
4	Даны правильные ответы на 4 вопроса
5	Даны правильные ответы на 5 вопросов