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.16 Безопасность информационных систем

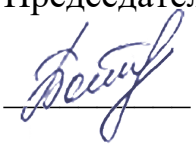
специальности

09.02.01 Компьютерные системы и комплексы

Иркутск, 2015

Рассмотрена
цикловой комиссией

Председатель ЦК


/М.А. Богачева /

№	Разработчик ФИО
1	Белова Алена Александровна

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения фонда оценочных средств (ФОС)

ФОС по дисциплине является частью программы подготовки специалистов среднего звена по специальности 09.02.01 Компьютерные системы и комплексы

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: 1.3.4.Итоговое занятие по теме "Введение в информационную безопасность"

Метод и форма контроля: Тестирование (Опрос)

Вид контроля: Письменное тестирование

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

Занятие(-я):

1.1.1.Основные понятия информационной безопасности.

1.1.2.Анализ угроз информационной безопасности

1.3.3.Семинар «Информация как объект защиты»

Задание №1

Ответить на вопросы теста.

1. Вставьте пропущенное слово.

«Под информационной безопасностью будем понимать защищенность информации и … от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»

а) поддерживающей инфраструктуры

б) человека

в) конфиденциальных данных

2. Защита информации – это …

а) комплекс мероприятий, направленных на обеспечение информационной безопасности

б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

г) все определения корректны

3. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:

а) доступностью информации

б) целостностью информации

в) предоставлением информации

г) конфиденциальностью информации
4. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:
а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
г) учетными записями пользователей
5. Некоторая уникальная информация, позволяющая различать пользователей называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ
6. Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ
6. Совокупность идентификатора и пароля пользователя называется:
а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя
7. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) опознанием пользователя
г) созданием учетной записи пользователя
8. Проверка принадлежности пользователю предъявленного им идентификатора является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя
г) созданием учетной записи пользователя
9. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:
а) утечкой
б) разглашением
в) взломом

9. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:
а) утечкой
б) разглашением
в) взломом
10. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называется:
а) утечкой
б) разглашением
в) взломом

Оценка	***Показатели оценки***
3	3 - 6 правильно выполненных заданий
4	7 - 8 правильно выполненных заданий
5	9 - 10 правильно выполненных заданий

Дидактическая единица: 1.2 Место информационной безопасности в системе национальной безопасности страны
Занятие(-я):
1.2.1.Информационная безопасность в системе национальной безопасности Российской Федерации
1.2.2.Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.
1.2.3.Основные положения государственной информационной политики России
1.2.4.Доктрина информационной безопасности Российской Федерации
Задание №1
Ответить на вопросы теста.
1. Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации?
а) доступность информации
б) целостность информации
в) предоставление информации
г) конфиденциальность информации
2. Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:
а) законодательного уровня
б) административного уровня
в) процедурного уровня
г) программно-технического уровня

д) программно-аппаратного уровня
3. Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?
а) ISO
б) ITU
в) ANSI
г) NIST
д) NASA
е) SWIFT
ж) GISA
4. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:
а) утечкой
б) разглашением
в) взломом
5. Возможность за приемлемое время получить требуемую информационную услугу называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
6. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:
а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации
7. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:
а) утечкой
б) разглашением
в) взломом

Оценка	***Показатели оценки***
3	Выполнено 2 - 3 задания
4	Выполнено 4 -5 заданий
5	Выполнено 6 - 7 заданий

Дидактическая единица: 1.3 Источники угроз информационной безопасности и

меры по их предотвращению

Занятие(-я):

1.3.1.Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации

1.3.2.Методы оценки уязвимости информации. Виды утечки информации.

1.3.3.Семинар «Информация как объект защиты»

Задание №1

Ответить на вопросы теста.

1. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:

а) обнаружение угроз

б) пресечения и локализация угроз

в) ликвидация угроз

2. Потенциальная возможность определенным образом нарушить информационную безопасность – это ….

а) угроза

б) атака

в) взлом

3. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …

а) окном безопасности

б) окном опасности

в) скользящим окном

г) окном угрозы

4. Источниками угрозы называют …

а) потенциальных злоумышленников

б) компьютерные вирусы

в) глобальную сеть Интернет

5. Ошибки программного обеспечения с точки зрения информационной безопасности являются:

а) уязвимым местом

б) окном опасности

в) окном безопасности

г) источником угрозы

6. Ошибки администрирования системы с точки зрения информационной безопасности являются:

а) уязвимым местом

б) окном опасности

в) окном безопасности

г) источником угрозы

7. Ошибка в программе, вызвавшая крах системы с точки зрения информационной

безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы
8. Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) перехват передаваемой по сети информации (Sniffing)
д) спуфинг
е) сканирование портов
9. Атака, целью которой является трафик локальной сети, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов
10. Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов
11. Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

Оценка	*Показатели оценки*
3	Выполнено 5 - 6 заданий
4	Выполнено 7 - 9 заданий
5	Выполнено 10 - 11 заданий

2.2 Текущий контроль (ТК) № 2

Тема занятия: 3.1.8.Контрольная работа № 2 "Средства и способы обеспечения информационной безопасности"
Метод и форма контроля: Письменный опрос (Опрос)
Вид контроля: Проверочная работа
Дидактическая единица: 1.4 Современные средства и способы обеспечения информационной безопасности
Занятие(-я):
3.1.1.Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД)
3.1.2.Стандарты в области информационной безопасности АСОД
3.1.3.Показатели защищенности СВТ. Защита информации в АСОД
3.1.4.Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа
3.1.5.Автоматизированная система, как объект информационной защиты.
3.1.6.Основные методы и приемы защиты от несанкционированного доступа
3.1.7.Семинар «Методы и средства защиты информации»
Задание №1

Приведите основные методы защиты информационной безопасности в разных информационных пространствах.

Оценка	*Показатели оценки*

3	Перечислено не менее двух методов защиты информационной безопасности в разных информационных пространствах: 1. Организационно-распорядительная защита информации. 2. Инженерная защита и техническая охрана объектов информатизации. 3. Защита информации от утечки по техническим каналам. 4. Обнаружение и нейтрализация средств технической разведки. 5. Защита компьютерной информации и компьютерных систем от вредоносных программ. 6. Семантическое сокрытие информации.
4	Перечислено не менее четырех методов защиты информационной безопасности в разных нформационных пространствах: 1. Организационно-распорядительная защита информации. 2. Инженерная защита и техническая охрана объектов информатизации. 3. Защита информации от утечки по техническим каналам. 4. Обнаружение и нейтрализация средств технической разведки. 5. Защита компьютерной информации и компьютерных систем от вредоносных программ. 6. Семантическое сокрытие информации.
5	Перечислено не менее пяти методов защиты информационной безопасности в разных информационных пространствах: 1. Организационно-распорядительная защита информации. 2. Инженерная защита и техническая охрана объектов информатизации. 3. Защита информации от утечки по техническим каналам. 4. Обнаружение и нейтрализация средств технической разведки. 5. Защита компьютерной информации и компьютерных систем от вредоносных программ. 6. Семантическое сокрытие информации.

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

Занятие(-я):

2.1.1.Понятие конфиденциальной информации.

2.1.2.Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.

2.1.3.Жизненные циклы конфиденциальной информации

2.1.4.Защита информации составляющей государственную тайну

2.1.5.Защита информации, охраняемая авторским и патентным правом.

3.1.7.Семинар «Методы и средства защиты информации»

Задание №1

Дайте определение следующим терминам:

1) собственник информации;
2) владелец информации;
3) пользователь;
4) гриф секретности;
5) дезинформация;
6) легендирование;
7) клевета.

Оценка	***Показатели оценки***

5	Даны не менее шести определений. 1) Собственник информации - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами. 2) Владелец информации - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации. 3) Пользователь - лицо или организация, которое использует действующую систему для выполнения конкретной функции. 4) гриф секретности - показатель степени секретности документов, изданий, специзделий и работ. Степень секретности определяется грифами "особой важности", "совершенносекретно", "секретно", "для служебного пользования". 5) Дезинформация - заведомо ложная информация, предоставляемая противнику или деловому партнеру для более эффективного ведения боевых действий, сотрудничества, проверки на утечку информации и направление ее утечки, выявление потенциальных клиентов черного рынка. 6) Легендирование - способ защиты информации от технических разведок, предусматривающий преднамеренное распространение и поддержание ложной информации о функциональном предназначении объекта защиты. 7) Клевета - то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. УК РФ, Статья 128.1. Клевета (введена Федеральным законом от 28.07.2012 N 141-ФЗ).
4	Даны не менее пяти определений.
3	Даны не менее трех определений.

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

Занятие(-я):

1.2.5.Практическая работа №1 «Анализ Доктрины информационной безопасности Российской Федерации»

Задание №1

Дайте определение следующим видам тайн:

1. государственная тайна;
2. коммерческая тайна;
3. банковская тайна;
4. профессиональная тайна;
5. служебная тайна;
6. персональные данные.

Оценка	***Показатели оценки***

5	Даны не менее пяти определений. 1. государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. 2. коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. 3. банковская тайна - юридический принцип в законодательствах некоторых государств мира, в соответствии с которым банки и иные кредитные организации защищают сведения о вкладах и счетах своих клиентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни. 4. профессиональная тайна - общее название группыохраняемых законом тайн, необходимость соблюдения которых вытекает из доверительного характераотдельных профессий. 5. служебная тайна - это охраняемые законом конфиденциальные сведения о деятельности государственных органов, доступ к которым ограничен федеральным законом или в силу служебной необходимости. 6. персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу.
4	Даны не менее четырех определений.
3	Даны не менее двух определений.

2.3 Текущий контроль (ТК) № 3

Тема занятия: 3.3.10.Практическая работа №2 «Анализ защищенности объекта

защиты информации»
Метод и форма контроля: Индивидуальные задания (Опрос)
Вид контроля: Письменное индивидуальное задание
Дидактическая единица: 2.2 Классифицировать основные угрозы безопасности информации
Занятие(-я):
1.2.5.Практическая работа №1 «Анализ Доктрины информационной безопасности Российской Федерации»
1.3.1.Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации
3.3.8.Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности обнаружения атак на сетевом и операционном уровне. Реагирование на атаку.
Задание №1
Для выбранного объекта защиты информации провести анализ защищенности по следующим разделам:
1) виды угроз;
2) характер происхождения угроз;
3) классы каналов несанкционированного получения информации;
4) источники появления угроз;
5) причины нарушения целостности информации.

Объект защиты информации:
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 выхода в Интернет;
10) телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях;
11) телефонная сеть;
12) средства телекоммуникации (радиотелефоны, мобильные телефоны);
13) банковские операции (внесение денег на счет и снятие);
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 и на электронных носителях в производстве;
18) материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии;
19) материалы для служебного пользования на твердых носителях в архиве;
20) материалы для служебного пользования на твердых носителях и на электронных 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 средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.);
24) судебные материалы (твердая копия и на электронных носителях);
25) паспортный стол РОВД (твердая копия и на электронных носителях).

Оценка	***Показатели оценки***
5	Проведен анализ защищености не менее чем по четырем разделам.
4	Проведен анализ защищенности не менее чем по трем разделам.
3	Проведен анализ защищенности не менее чем по двум разделам.

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

Занятие(-я):

3.3.9.Обзор современных средств обнаружения атак

Задание №1

Ответить на вопросы теста.

1. К какой разновидности моделей управления доступом относится модель Белла-ЛаПадулы?
а) модель дискреционного доступа;
б) модель мандатного доступа;
в) ролевая модель.
2. К каким мерам защиты относится политика безопасности?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.
3. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
а) ACL;

б) списки полномочий субъектов;
в) атрибутные схемы.
4. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.
5. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;
д) простота.
6. Какие из следующих высказываний о модели управления доступом RBAC справедливы?
а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей;
б) роли упорядочены в иерархию;
в) с каждым объектом доступа ассоциировано несколько ролей ;
г) для каждой пары «субъект-объект» назначен набор возможных разрешений.
7. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;
8. Какие предположения включает неформальная модель нарушителя?
а) о возможностях нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о привычках нарушителя;
г) о предыдущих атаках, осуществленных нарушителем;
д) об уровне знаний нарушителя.
9. Что представляет собой доктрина информационной безопасности РФ?
а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
б) федеральный закон, регулирующий правоотношения в области информационной безопасности;
в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.
10. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?
а) политика безопасности верхнего уровня;
б) политика безопасности среднего уровня;
в) политика безопасности нижнего уровня;
г) принцип минимизации привилегий;
д) защита поддерживающей инфраструктуры.
11. Какие из перечисленных ниже угроз относятся к классу преднамеренных?
а) заражение компьютера вирусами;
б) физическое разрушение системы в результате пожара;
в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
е) вскрытие шифров криптозащиты информации.

Оценка	***Показатели оценки***
3	Выполнено 3-6 заданий.
4	Выполнено 7-9 заданий.
5	Выполнено 10-11 заданий.

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: Письменный опрос (Опрос)
Вид контроля: по выбору выполнить одно теоретическое задание и одно практическое задание
Дидактическая единица для контроля:
1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих
Задание №1 (из текущего контроля)
Ответить на вопросы теста.
1. Вставьте пропущенное слово.
«Под информационной безопасностью будем понимать защищенность информации и … от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»
а) поддерживающей инфраструктуры
б) человека
в) конфиденциальных данных
2. Защита информации – это …
а) комплекс мероприятий, направленных на обеспечение информационной безопасности
б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов
в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

г) все определения корректны
3. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
г) конфиденциальностью информации
4. Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:
а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
г) учетными записями пользователей
5. Некоторая уникальная информация, позволяющая различать пользователей называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ
6. Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:
а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ
6. Совокупность идентификатора и пароля пользователя называется:
а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя
7. Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) опознанием пользователя
г) созданием учетной записи пользователя
8. Проверка принадлежности пользователю предъявленного им идентификатора является:
а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя

г) созданием учетной записи пользователя
9. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:
а) утечкой
б) разглашением
в) взломом
9. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:
а) утечкой
б) разглашением
в) взломом
10. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена, называется:
а) утечкой
б) разглашением
в) взломом

Оценка	***Показатели оценки***
3	3 - 6 правильно выполненных заданий
4	7 - 8 правильно выполненных заданий
5	9 - 10 правильно выполненных заданий

Дидактическая единица для контроля:
1.2 Место информационной безопасности в системе национальной безопасности страны
Задание №1 (из текущего контроля)
Ответить на вопросы теста.
1. Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации?
а) доступность информации
б) целостность информации
в) предоставление информации
г) конфиденциальность информации
2. Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:
а) законодательного уровня
б) административного уровня
в) процедурного уровня
г) программно-технического уровня

д) программно-аппаратного уровня
3. Многообразие нормативных документов представлено международными, национальными, отраслевыми нормативными документами. Какая организация НЕ занимается вопросами формирования законодательства в сфере информационных ресурсов?
а) ISO
б) ITU
в) ANSI
г) NIST
д) NASA
е) SWIFT
ж) GISA
4. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним, называется:
а) утечкой
б) разглашением
в) взломом
5. Возможность за приемлемое время получить требуемую информационную услугу называется:
а) доступностью информации
б) целостностью информации
в) предоставлением информации
6. Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:
а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации
7. Факт получения охраняемых сведений злоумышленниками или конкурентами называется:
а) утечкой
б) разглашением
в) взломом

Оценка	***Показатели оценки***
3	Выполнено 2 - 3 задания
4	Выполнено 4 -5 заданий
5	Выполнено 6 - 7 заданий

Дидактическая единица для контроля:

1.3 Источники угроз информационной безопасности и меры по их предотвращению

Задание №1 (из текущего контроля)

Ответить на вопросы теста.

1. Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:
а) обнаружение угроз
б) пресечения и локализация угроз
в) ликвидация угроз
2. Потенциальная возможность определенным образом нарушить информационную безопасность – это ….
а) угроза
б) атака
в) взлом
3. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется …
а) окном безопасности
б) окном опасности
в) скользящим окном
г) окном угрозы
4. Источниками угрозы называют …
а) потенциальных злоумышленников
б) компьютерные вирусы
в) глобальную сеть Интернет
5. Ошибки программного обеспечения с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы
6. Ошибки администрирования системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы
7. Ошибка в программе, вызвавшая крах системы с точки зрения информационной безопасности являются:
а) уязвимым местом
б) окном опасности
в) окном безопасности
г) источником угрозы

8. Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) перехват передаваемой по сети информации (Sniffing)
д) спуфинг
е) сканирование портов
9. Атака, целью которой является трафик локальной сети, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов
10. Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов
11. Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:
а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

Оценка	***Показатели оценки***
3	Выполнено 5 - 6 заданий
4	Выполнено 7 - 9 заданий
5	Выполнено 10 - 11 заданий

Дидактическая единица для контроля:

1.4 Современные средства и способы обеспечения информационной безопасности

Задание №1 (из текущего контроля)

Приведите основные методы защиты информационной безопасности в разных информационных пространствах.

Оценка	***Показатели оценки***
3	Перечислено не менее двух методов защиты информационной безопасности в разных информационных пространствах: 1. Организационно-распорядительная защита информации. 2. Инженерная защита и техническая охрана объектов информатизации. 3. Защита информации от утечки по техническим каналам. 4. Обнаружение и нейтрализация средств технической разведки. 5. Защита компьютерной информации и компьютерных систем от вредоносных программ. 6. Семантическое сокрытие информации.
4	Перечислено не менее четырех методов защиты информационной безопасности в разных нформационных пространствах: 1. Организационно-распорядительная защита информации. 2. Инженерная защита и техническая охрана объектов информатизации. 3. Защита информации от утечки по техническим каналам. 4. Обнаружение и нейтрализация средств технической разведки. 5. Защита компьютерной информации и компьютерных систем от вредоносных программ. 6. Семантическое сокрытие информации.

5	Перечислено не менее пяти методов защиты информационной безопасности в разных информационных пространствах: 1. Организационно-распорядительная защита информации. 2. Инженерная защита и техническая охрана объектов информатизации. 3. Защита информации от утечки по техническим каналам. 4. Обнаружение и нейтрализация средств технической разведки. 5. Защита компьютерной информации и компьютерных систем от вредоносных программ. 6. Семантическое сокрытие информации.

Дидактическая единица для контроля:

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

Задание №1 (из текущего контроля)

Дайте определение следующим терминам:

1) собственник информации;
2) владелец информации;
3) пользователь;
4) гриф секретности;
5) дезинформация;
6) легендирование;
7) клевета.

Оценка	***Показатели оценки***

5	Даны не менее шести определений. 1) Собственник информации - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами. 2) Владелец информации - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации. 3) Пользователь - лицо или организация, которое использует действующую систему для выполнения конкретной функции. 4) гриф секретности - показатель степени секретности документов, изданий, специзделий и работ. Степень секретности определяется грифами "особой важности", "совершенносекретно", "секретно", "для служебного пользования". 5) Дезинформация - заведомо ложная информация, предоставляемая противнику или деловому партнеру для более эффективного ведения боевых действий, сотрудничества, проверки на утечку информации и направление ее утечки, выявление потенциальных клиентов черного рынка. 6) Легендирование - способ защиты информации от технических разведок, предусматривающий преднамеренное распространение и поддержание ложной информации о функциональном предназначении объекта защиты. 7) Клевета - то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. УК РФ, Статья 128.1. Клевета (введена Федеральным законом от 28.07.2012 N 141-ФЗ).
4	Даны не менее пяти определений.
3	Даны не менее трех определений.

Дидактическая единица для контроля:

2.1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Задание №1 (из текущего контроля)

Дайте определение следующим видам тайн:

1. государственная тайна;
2. коммерческая тайна;

3. банковская тайна;
4. профессиональная тайна;
5. служебная тайна;
6. персональные данные.

Оценка	***Показатели оценки***
5	Даны не менее пяти определений. 1. государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. 2. коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. 3. банковская тайна - юридический принцип в законодательствах некоторых государств мира, в соответствии с которым банки и иные кредитные организации защищают сведения о вкладах и счетах своих клиентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни. 4. профессиональная тайна - общее название группыохраняемых законом тайн, необходимость соблюдения которых вытекает из доверительного характераотдельных профессий. 5. служебная тайна - это охраняемые законом конфиденциальные сведения о деятельности государственных органов, доступ к которым ограничен федеральным законом или в силу служебной необходимости. 6. персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу.

4	Даны не менее четырех определений.
3	Даны не менее двух определений.

Дидактическая единица для контроля:

2.2 Классифицировать основные угрозы безопасности информации

Задание №1 (из текущего контроля)

Для выбранного объекта защиты информации провести анализ защищенности по следующим разделам:

1) виды угроз;
2) характер происхождения угроз;
3) классы каналов несанкционированного получения информации;
4) источники появления угроз;
5) причины нарушения целостности информации.

Объект защиты информации:

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 выхода в Интернет;
10) телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях;
11) телефонная сеть;
12) средства телекоммуникации (радиотелефоны, мобильные телефоны);
13) банковские операции (внесение денег на счет и снятие);
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 и на электронных носителях в производстве;
18) материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии;
19) материалы для служебного пользования на твердых носителях в архиве;
20) материалы для служебного пользования на твердых носителях и на электронных

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 средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.);
24) судебные материалы (твердая копия и на электронных носителях);
25) паспортный стол РОВД (твердая копия и на электронных носителях).

Оценка	***Показатели оценки***
5	Проведен анализ защищености не менее чем по четырем разделам.
4	Проведен анализ защищенности не менее чем по трем разделам.
3	Проведен анализ защищенности не менее чем по двум разделам.

Дидактическая единица для контроля:
2.3 Применять основные правила и документы сертификации Российской Федерации
Задание №1 (из текущего контроля)
Ответить на вопросы теста.
1. К какой разновидности моделей управления доступом относится модель Белла-ЛаПадулы?
а) модель дискреционного доступа;
б) модель мандатного доступа;
в) ролевая модель.
2. К каким мерам защиты относится политика безопасности?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.
3. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.
4. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;

д) аутентичность.
5. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;
д) простота.
6. Какие из следующих высказываний о модели управления доступом RBAC справедливы?
а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей;
б) роли упорядочены в иерархию;
в) с каждым объектом доступа ассоциировано несколько ролей ;
г) для каждой пары «субъект-объект» назначен набор возможных разрешений.
7. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;
8. Какие предположения включает неформальная модель нарушителя?
а) о возможностях нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о привычках нарушителя;
г) о предыдущих атаках, осуществленных нарушителем;
д) об уровне знаний нарушителя.
9. Что представляет собой доктрина информационной безопасности РФ?
а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
б) федеральный закон, регулирующий правоотношения в области информационной безопасности;
в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;
г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.
10. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?
а) политика безопасности верхнего уровня;
б) политика безопасности среднего уровня;
в) политика безопасности нижнего уровня;
г) принцип минимизации привилегий;

д) защита поддерживающей инфраструктуры.
11. Какие из перечисленных ниже угроз относятся к классу преднамеренных?
а) заражение компьютера вирусами;
б) физическое разрушение системы в результате пожара;
в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
е) вскрытие шифров криптозащиты информации.

Оценка	***Показатели оценки***
3	Выполнено 3-6 заданий.
4	Выполнено 7-9 заданий.
5	Выполнено 10-11 заданий.