МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ) ДГТУ в г. Азове

УТВЕРЖДАЮ:
Директор
_____ Д.Н. Кривошеев
«26» ноября 2019 г.
М.П.

ПРОГРАММА

профессиональной переподготовки
«Информационная безопасность»

форма обучения – очно-заочная

ОБЪЁМ УЧЕБНОЙ НАГРУЗКИ И ВИДЫ ОТЧЁТНОСТИ

Вид занятий	Объём (часов)
Лекции	20
Практические занятия	10
Стажировка	-
(другие виды занятий)	
Самостоятельная работа	230
Подготовка к итоговой аттестации	-
Итоговая аттестация	4
ВСЕГО:	260

г. Азов
2019 г.

СОДЕРЖАНИЕ

1. Аннотация

1.1. Краткая характеристика программы

Данная программа профессиональной переподготовки представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий, форм аттестации, необходимых для реализации качественного образовательного процесса по данной программе переподготовки. Программа профессиональной переподготовки разработана с учетом развития науки, культуры, экономики, техники, технологий и социальной сферы, а также с учетом потребностей регионального рынка труда и требований профессиональных стандартов.

Данная программа профессиональной переподготовки призвана дать слушателям необходимый объем знаний, умений, навыков и компетенций в области профессиональной деятельности, которая включает изучение нормативно-правовой базы информационной безопасности, методологии обеспечения информационной безопасности, исследование методов и средств обеспечения безопасности информационных технологий.

Программа включает в себя учебный план, календарный учебный график, рабочие программы модулей, формы аттестации, оценочные материалы, обеспечивающие качество подготовки слушателей. Срок освоения программы – 4 месяца. Трудоемкость – 260 часов. Форма обучения – очно-заочная.

1.2. Цель реализации программы

Целью реализации программы является получение компетенций в информационной безопасности, необходимых для выполнения нового вида профессиональной деятельности, приобретение новой квалификации.

1.3 Требования к поступающему для обучения на программу слушателю

К освоению программы допускаются лица, имеющие высшее профессиональное образование по всем направлениям и специальностям подготовки, либо среднее профессиональное образование.

1.4. Формализованные результаты обучения и связь с образовательными стандартами ФГОС ВО и ФГОС СПО

Программа обеспечивает:

Формирование компетенций, обеспечивающих готовность к следующим видам деятельности:

– научно-исследовательская деятельность;
– научно-педагогическая;
– организационно-управленческая.

Область профессиональной деятельности слушателей:

– сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Объектами профессиональной деятельности слушателей являются:

– Фундаментальные проблемы информационной безопасности в условиях становления современного информационного общества.
– Информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-

аналитические системы. Технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта).

– Процессы управления информационной безопасностью (ИБ) защищаемых объектов, методы и средства оптимизации процессов управления.

Слушатель, освоивший программу «Информационная безопасность » должен обладать следующими компетенциями:

научно-исследовательская деятельность:

– способен анализировать фундаментальные и прикладные проблемы ИБ в условиях становления современного информационного общества (ПК.БИТ-1);

– способен анализировать угрозы ИБ объектов и разрабатывать методы противодействия им (ПК.БИТ-2);

научно-педагогическая деятельность:

– способен выполнять педагогическую работу в средних специальных и высших учебных заведениях по дисциплинам направления «Информационная безопасность» (ПК.БИТ-3);

– способен разрабатывать методические материалы, используемые студентами в учебном процессе (ПК.БИТ-4);

организационно-управленческая деятельность:

– способен организовать работу по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения ИБ в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России (ПК.БИТ-5);

– способен разрабатывать проекты методических и нормативных документов, технической документации, а также предложения и мероприятия по реализации разработанных проектов и программ (ПК.БИТ-6);

– способностью произвести и детально обосновать выбор структуры, принципов организации, комплекса средств и технологий обеспечения ИБ объектов защиты (ПК.БИТ-7);

– способностью самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения ИБ, вновь вводимые отечественные и международные стандарты (ПК.БИТ-8).

После успешного освоения программы слушатель должен:

знать:

- фундаментальные и прикладные проблемы ИБ в условиях становления современного информационного общества;

- Информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы;

- Процессы управления информационной безопасностью (ИБ) защищаемых объектов, методы и средства оптимизации процессов управления.

уметь:

- организовать работу по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения ИБ в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

- разрабатывать проекты методических и нормативных документов, технической документации, а также предложения и мероприятия по реализации разработанных проектов и программ.

владеть:

- методами выбора структуры, принципов организации, комплекса средств и технологий обеспечения ИБ объектов защиты;

- способами освоения и адаптации к защищаемым объектам современные методы обеспечения ИБ, вновь вводимые отечественные и международные стандарты.

По модулям программы профессиональной переподготовки «Информационная безопасность» проводится промежуточная аттестация в форме зачета (экзамена). Промежуточная аттестация проходит в устной форме и включает в себя подготовку и ответ на 2 вопроса из билета.

По результатам экзамена обучающемуся выставляется оценка «отлично», «хорошо», «удовлетворительно», или «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, если:

- обучающийся знает, понимает основные положения модуля, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения;
- обучающийся анализирует элементы, устанавливает связи между ними, сводит их в единую систему, способен выдвинуть идею, спроектировать и презентовать свой проект (решение);
- ответ обучающегося по теоретическому и практическому материалу, содержащемуся в задании для промежуточного контроля, является полным, и удовлетворяет требованиям программы модуля;
- обучающийся продемонстрировал свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующего модуля;
- на дополнительные вопросы преподавателя обучающийся дал правильные ответы.

Компетенция (и) или ее часть (и) сформированы на высоком уровне.

Оценка «хорошо» выставляется обучающемуся, если:

- обучающийся знает, понимает основные положения модуля, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения; анализирует элементы, устанавливает связи между ними;
- ответ по теоретическому материалу, содержащемуся в задании для промежуточного контроля, является полным, или частично полным и удовлетворяет требованиям программы, но не всегда дается точное, уверенное и аргументированное изложение материала;
- на дополнительные вопросы преподавателя обучающийся дал правильные ответы;
- обучающийся продемонстрировал владение терминологией соответствующего модуля.

Компетенция (и) или ее часть (и) сформированы на среднем уровне.

Оценка «удовлетворительно» выставляется обучающемуся, если:

- обучающийся знает и воспроизводит основные положения модуля в соответствии с заданием, применяет их для выполнения типового задания в котором очевиден способ решения;
- обучающийся продемонстрировал базовые знания важнейших разделов модуля и содержания лекционного курса;
- у обучающегося имеются затруднения в использовании научно-понятийного аппарата в терминологии курса;
- несмотря на недостаточность знаний, обучающийся имеется стремление логически четко построить ответ, что свидетельствует о возможности последующего обучения.

Компетенция (и) или ее часть (и) сформированы на базовом уровне.

Оценка «неудовлетворительно» выставляется обучающемуся, если:

- обучающийся имеет представление о содержании модуля, но не знает основные положения (темы, раздела, закона и т.д.), к которому относится задание, не способен выполнить задание с очевидным решением,

- у обучающегося имеются существенные пробелы в знании основного материала по модулю;

- в процессе ответа по теоретическому материалу, содержащемуся в вопросах экзаменационного билета, допущены принципиальные ошибки при изложении материала.

Компетенция(и) или ее часть (и) не сформированы.

По результатам зачета обучающемуся выставляется оценка «зачтено» или «незачтено».

Оценка «зачтено» выставляется на зачете обучающимся*, если:*

- обучающийся знает и воспроизводит основные положения модуля в соответствии с заданием, применяет их для выполнения типового задания в котором очевиден способ решения;

- обучающийся продемонстрировал базовые знания, умения и навыки важнейших разделов модуля;

- у обучающегося не имеется затруднений в использовании научно-понятийного аппарата в терминологии курса, а если затруднения имеются, то они незначительные;

- на дополнительные вопросы преподавателя обучающийся дал правильные или частично правильные ответы;

Компетенция (и) или ее часть (и) сформированы на базовом уровне.

Оценка «не зачтено» ставится на зачете обучающийся, если:

- обучающийся имеет представление о содержании модуля, но не знает основные положения (темы, раздела, закона и т.д.), к которому относится задание, не способен выполнить задание с очевидным решением, не владеет навыками и приемами решения типовых заданий в данной предметной области;

- имеются существенные пробелы в знании основного материала по программе курса;

- в процессе ответа по теоретическому и практическому материалу, содержащемуся в вопросах зачетного билета, допущены принципиальные ошибки при изложении материала;

- имеются систематические пропуски обучающийся лекционных и практических занятий по неуважительным причинам;

- вовремя не подготовил отчет по практическим работам, предусмотренным программой.

Компетенция(и) или ее часть (и) не сформированы.

2. Содержание программы

2.1. Учебный план

В учебном плане отображается логическая последовательность освоения циклов и разделов ДПП (дисциплин, модулей, практик), обеспечивающих формирование компетенций. Указывается общая трудоемкость дисциплин, модулей, стажировок, практик и т.д.

Учебный план
программы профессиональной переподготовки
«Информационная безопасность»

№ п/п	Название разделов и дисциплин	Всего, часов	в том числе:			Форма контроля
			лекции	практические занятия	самостоятельная работа	
Общепрофессиональные дисциплины						

1.	**Нормативно-правовая база обеспечения безопасности информационных технологий**	**60**	**6**	-	54	зачет
Специальные дисциплины						
2.	**Методология обеспечения информационной безопасности**	**60**	**4**	-	**56**	зачет
3.	**Управление обеспечением безопасности информационных технологий**	**60**	**4**	-	**56**	зачет
Дисциплины специализации						
4.	**Методы и средства обеспечения безопасности информационных технологий**	**76**	**6**	**6**	**64**	зачет
5.	**Итоговая аттестация**	**4**	-	**4**	-	экзамен
	ИТОГО:	**260**	20	10	**230**	

2.2. Учебно-тематический план

Учебно-тематический план
программы профессиональной переподготовки
«Информационная безопасность»

№ п/п	Наименование разделов (дисциплин, модулей) и тем	Всего, час.	в том числе:			Форма промежуточной аттестации
			лекции	практич. занятия	самост. работа	
1	2	3	4	5	6	7
1	**Модуль 1 «Нормативно-правовая база обеспечения безопасности информационных технологий»**	**60**	**6**	-	54	**зачет**
1.1	Законодательная база обеспечения ИБ	10	1	-	9	
1.2	Роль технического регулирования в области обеспечения ИБ	10	1	-	9	
1.3	Стандартизация обеспечения ИБ на международном уровне	10	1	-	9	
1.4	Национальные стандарты в области обеспечения ИБ	10	1	-	9	
1.5	Документальное обеспечение ИБ на уровне организации	10	1	-	9	
1.6	Роль стандартизации в формировании учебно-методической базы подготовки профессионалов в области обеспечения ИБ	10	1	-	9	
2	**Модуль 2 «Методология обеспечения информационной безопасности»**	**60**	**4**	-	**56**	**зачет**
2.1	Современная парадигма в области обеспечения ИБ	7	1	-	6	
2.2	Концептуальные подходы к обеспечению ИБ.	6	-	-	6	

2.3	Использование процессных моделей в области обеспечения ИБ	6	-	-	6	
2.4	Риск-ориентированный подход к обеспечению ИБ	7	1	-	6	
2.5	Обеспечение непрерывности функционирования информационных технологий в условия существования угроз в информационной сфере	6	-	-	6	
2.6	Наступательная безопасность: Анализ защищенности устройств	6	-	-	6	
2.7	Экспертные оценки в информационной безопасности	7	1	-	6	
2.8	Метод аналитических сетей Саати	6	-	-	6	
2.9	Принятие решений в условиях неопределенности и рисков	9	1	-	8	
3	**Модуль 3 «Управление обеспечением безопасности информационных технологий»**	**60**	**4**	-	**56**	**зачет**
3.1	Роль управления в обеспечении ИБ..	9	1	-	8	
3.2	Процессы управления обеспечением ИБ	8		-	8	
3.3	Система управления ИБ (ЭОК)	13	1	-	12	
3.4	Основы управления рисками обеспечения ИБ (ЭОК)	12		-	12	
3.5	Основы управления инцидентами ИБ (ЭОК)	9	1	-	8	
3.6	Контроль уровня обеспечения ИБ (ЭОК)	9	1	-	8	
4	**Модуль 4 «Методы и средства обеспечения безопасности информационных технологий»**	**76**	**6**	**6**	**64**	**зачет**
4.1	Защита информации от воздействия вредоносного кода: вредоносное программное обеспечение: тренды и направление развития	14	1	1	12	
4.2	Обеспечение ИБ в отрытых информационных системах (ОИС)	14	1	1	12	
4.3	Обеспечение ИБ веб-технологий	14	1	1	12	
4.4	Обеспечение доступности в информационных системах	14	1	1	12	
4.5	Криптографические методы защиты информации	20	2	2	16	
5	**Итоговая аттестация**	**4**	-	4	-	**экзамен**
	ИТОГО	**260**	**20**	**10**	**230**	

2.4. Рабочие программы

По каждому предмету (дисциплине, модулю) программы профессиональной переподготовки разрабатывается рабочая программа. Рабочие программы размещаются в приложении к учебной программе.

3. Материально-технические условия реализации программы (организационно-педагогические условия)

Специальные помещения представляют собой учебные аудитории для проведения всех занятий по программе профессиональной переподготовки «Информационная безопасность», предусмотренных учебным планом и соответствующие действующим санитарным и противопожарным правилам и нормам. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, в т.ч.:

- учебная мебель (парты аудиторные, столы аудиторные, стулья аудиторные, доска учебная);
- технические средства обучения (мультимедийный проектор, экран, ноутбук и персональные компьютеры с установленным программным обеспечением Microsoft Windows и Microsoft Office).

4. Формы аттестации и оценочные материалы

Уровни и критерии оценки результатов освоения программы и сформированности компетенций приводятся ниже.

Уровни		Критерии выполнения заданий ОС	Итоговая оценка
Недостаточный		Имеет представление о содержании программы, но не знает основные определения и понятия, не способен выполнить задание с очевидным решением, не владеет навыками самостоятельной работы	Неудовлетворительно
Базовый		Знает и воспроизводит основные методы определения в соответствии с заданием, применяет их для выполнения типового задания (организовать самостоятельный поиск и работу с различными источниками информации, использовать возможности компьютерной техники и информационных технологий при поиске источников и литературы)	Удовлетворительно
Повышенный	ПУ 1	Знает, понимает основные определения и методы анализа, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения. Анализирует элементы, устанавливает связи между ними	Хорошо
	ПУ 2	Знает, понимает основные определения и методы анализа, демонстрирует умение применять их для выполнения задания, в котором нет явно указанных способов решения. Анализирует элементы, устанавливает связи между ними, сводит их в единую систему, способен выдвинуть идею, правильно сформировать ответ	Отлично

4.1. Итоговая аттестация проводится в форме экзамена (вид – тестирование). Для сдачи итогового экзамена у слушателей формируются знания и компетенции в процессе обучения и на основе результатов промежуточной аттестации и при самостоятельной работе.

4.2. Образцы тестов, заданий

Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия

В) нет правильного ответа

Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

Атака – это…

А) попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

Окно опасности – это…

А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

Какие события должны произойти за время существования окна опасности?

А) должно стать известно о средствах использования пробелов в защите.

Б) должны быть выпущены соответствующие заплаты.

В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:

А) по спектру И.Б.

Б) по способу осуществления

В) по компонентам И.С.

По каким компонентам классифицируется угрозы доступности:

А) отказ пользователей

Б) отказ поддерживающей инфраструктуры

В) ошибка в программе

Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

В) все ответы правильные

Основными источниками внутренних отказов являются:

А) ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

Б) обрабатывать большой объем программной информации

В) нет правильного ответа

Какие существуют грани вредоносного П.О.?

А) вредоносная функция

Б) внешнее представление

В) способ распространения

По механизму распространения П.О. различают:

А) вирусы

Б) черви

В) все ответы правильные

Вирус – это…

А) код обладающий способностью к распространению путем внедрения в другие программы

Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов

В) небольшая программа для выполнения определенной задачи

Черви – это…

А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения

Б) код обладающий способностью к распространению путем внедрения в другие программы

В) программа действий над объектом или его свойствами

Конфиденциальную информацию можно разделить:

А) предметную

Б) служебную

В) глобальную

Природа происхождения угроз:

А) случайные

Б) преднамеренные

В) природные

Предпосылки появления угроз:

А) объективные

Б) субъективные

В) преднамеренные

К какому виду угроз относится присвоение чужого права?

А) нарушение права собственности

Б) нарушение содержания

В) внешняя среда

Отказ, ошибки, сбой – это:

А) случайные угрозы

Б) преднамеренные угрозы

В) природные угрозы

Отказ - это…

А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Б) некоторая последовательность действий, необходимых для выполнения конкретного задания

В) структура, определяющая последовательность выполнения и взаимосвязи процессов

Ошибка – это…

А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния

Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

В) негативное воздействие на программу

Сбой – это…

А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния

В) объект-метод

Побочное влияние – это…

А) негативное воздействие на систему в целом или отдельные элементы

Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

СЗИ (система защиты информации) делится:

А) ресурсы автоматизированных систем

Б) организационно-правовое обеспечение

В) человеческий компонент

Что относится к человеческому компоненту СЗИ?

А) системные порты

Б) администрация

В) программное обеспечение

Что относится к ресурсам А.С. СЗИ?

А) лингвистическое обеспечение

Б) техническое обеспечение

В) все ответы правильные

По уровню обеспеченной защиты все системы делят:

А) сильной защиты

Б) особой защиты

В) слабой защиты

По активности реагирования СЗИ системы делят:

А) пассивные

Б) активные

В) полупассивные

Правовое обеспечение безопасности информации – это…

А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) нет правильного ответа

Правовое обеспечение безопасности информации делится:

А) международно-правовые нормы

Б) национально-правовые нормы

В) все ответы правильные

Информацию с ограниченным доступом делят:

А) государственную тайну

Б) конфиденциальную информацию

В) достоверную информацию

Что относится к государственной тайне?

А) сведения, защищаемые государством в области военной, экономической … деятельности

Б) документированная информация

В) нет правильного ответа

Вредоносная программа - это…

А) программа, специально разработанная для нарушения нормального функционирования систем

Б) упорядочение абстракций, расположение их по уровням

В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

Основополагающие документы для обеспечения безопасности внутри организации:

А) трудовой договор сотрудников

Б) должностные обязанности руководителей

В) коллективный договор

К организационно - административному обеспечению информации относится:

А) взаимоотношения исполнителей

Б) подбор персонала

В) регламентация производственной деятельности

Что относится к организационным мероприятиям:

А) хранение документов

Б) проведение тестирования средств защиты информации

В) пропускной режим

Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) аппаратные

Б) криптографические

В) физические

Программные средства – это…

А) специальные программы и системы защиты информации в информационных системах различного назначения

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…

А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

4.3. Перечень вопросов к зачету (экзамену)

1. Перечень вопросов итогового экзамена по модулю «Нормативно-правовая база обеспечения безопасности информационных технологий»:

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.

2. Перечень вопросов итогового экзамена по модулю «Методология обеспечения информационной безопас-ности»:

16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
18. Способы наблюдения с использованием технических средств.
19. Каналы утечки информации. Технические каналы утечки
20. Классификация технических каналов утечки по физической природе носителя.
21. Классификация технических каналов утечки по информативности.
22. Классификация технических каналов утечки по времени функционирования.
23. Классификация технических каналов утечки по структуре.
24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
25. Перехват электромагнитных излучений.
26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
27. Понятия скрытия информации, виды скрытий. Информационный портрет.
28. Противодействие наблюдению. Способы маскировки.
29. Способы и средства противодействия подслушиванию.
30. Нейтрализация закладных устройств.
31. Состав инженерной защиты и технической охраны объектов.

3. Перечень вопросов итогового экзамена по модулю «Управление обеспечением безопасности ин-формационных технологий»:

32. Инженерные конструкции и сооружения для защиты информации. Их классификация.
33. Средства идентификации личности.
34. Классификация датчиков охранной сигнализации.
35. Классификация извещателей.
36. Телевизионные системы наблюдения.
37. Основные средства системы видеоконтроля.
38. Защита личности как носителя информации.

39. Системный подход к защите информации.
40. Параметры системы защиты информации.
41. этапы проектирования системы защиты информации.
42. Потенциальные каналы утечки информации.
43. Этапы разработки мер по предотвращению угроз утечки информации.
44. Угрозы сохранности данных в компьютере случайного характера.
45. Устройства электропитания компьютера, применяемые для защиты компьютера от неблагоприятных воздействий питающей электросети.

4. Перечень вопросов итогового экзамена по модулю «Методы и средства обеспечения безопасности информационных технологий»:

46. Дефекты магнитных дисков.
47. Простые приемы, используемые для защиты компьютера от умышленных действий.
48. Классификация вирусов.
49. Классификация антивирусных программ.
50. Компьютерная преступность. Виды преступной деятельности.
51. Преступления, связанные с нарушением частной тайны.
52. Информационные процессы.
53. Информационные технологии и их основные свойства.
54. Понятия сигнала, сообщения и данных.
55. Методы защиты информации от преднамеренного доступа.
56. Методы обеспечения безопасности каналов передачи данных.
57. Методы обеспечения достоверности передачи информации (методов защиты от ошибок).
58. Механизмы обеспечения безопасности радиолиний.
59. Криптографическая защита информации (основные понятия).
60. Методы шифрования данных.
61. Стандарт шифрования данных DES.

5. Составители программы

ФИО преподавателя, ученая степень, ученое звание, номер разработанного раздела (дисциплины, модуля), темы по учебно-тематическому плану.

№ п/п	Наименование разделов (дисциплин, модулей) и тем	ФИО преподавателя	Ученая степень, звание
1	Модуль 1 «Нормативно-правовая база обеспечения безопасности информационных технологий»	Таран В.Н.	Докт.физ.-мат.наук, профессор
2	Модуль 2 «Методология обеспечения информационной безопасности»	Таран В.Н.	Докт.физ.-мат.наук, профессор
3	Модуль 3 «Управление обеспечением безопасности информационных технологий»	Таран В.Н.	Докт.физ.-мат.наук, профессор
4	Модуль 4 «Методы и средства обеспечения безопасности информационных технологий»	Таран В.Н.	Докт.физ.-мат.наук, профессор

Подписи составителей:

Таран В.Н