Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Парадигма»

СОГЛАСОВАНО
Начальник I Управления
ФСТЭК России
_____ А.Г. Дротенко
"__" ____ мая ____ 2015 г.

УТВЕРЖДАЮ
Директор АНО ДПО
«Учебный центр «Парадигма»
_____ А.В. Гребенкина
"__" ____ мая ____ 2015 г.

СОГЛАСОВАНО
Первый заместитель начальника
Центра ФСБ России
_____ А.С. Кузьмин
"10" ____ 04 ____ 2015 г.

СОГЛАСОВАНО
Заместитель Председателя Совета УМО
по образованию в области
информационной безопасности
_____ Е.Б. Белов
"16" ____ 2015 г.

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

по направлению «Информационная безопасность»

Виды профессиональной деятельности:
организационно-управленческая, эксплуатационная

Трудоемкость обучения: 694 ч.
Срок действия согласования: до 1 июля **2016 г.**

Ярославль
2015

Цели реализации курса

Цель курса – раскрыть основы правового регулирования отношений в информационной сфере, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности. Дать знания о принципах и методах эффективного управления информационной безопасностью в современной организации. В рамках данного курса рассматриваются основные принципы и правила управления обеспечением информационной безопасности на предприятии, которые позволят повысить эффективность функционирования предприятия. Обеспечить освоение основ системы защиты государственной тайны, правил лицензирования и сертификации в области защиты информации, защиты информации, персональных данных, технологий шифрования и электронных подписей.

Планируемые результаты обучения

После прохождения обучающего курса слушатель должен:

1. Знать место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основные стандарты и нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области, соответствующие термины и понятия, правовые основы организации защиты конфиденциальной информации, особенности работы с персональными данными, риски, связанные с информацией, и способы их устранения, виды преступлений и ответственность по ним в сфере компьютерных и информационных технологий, принципы и методы организационной защиты информации, основные стандарты и алгоритмы шифрования данных.

2. *Уметь* анализировать и оценивать угрозы информационной безопасности объекта, анализировать и оценивать степень риска проявления факторов опасности системы "человек - среда обитания", осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности, вырабатывать и реализовывать комплекса мер по улучшению защиты информации на предприятии, мониторить и предотвращать возможные риски, управлять основными процессами реализации системы информационной безопасности, пользоваться нормативными документами по защите информации, составлять должностные инструкции пользователям информационных систем обработки персональных данных, определять классы и виды персональной информации, составлять акты обследования на уязвимость информационных систем, работать с инструментами шифрования данных и электронными подписями, предвидеть и пресекать нарушения в сфере информационных технологий.

3. *Владеть* средствами обработки информации, навыками выявления и уничтожения компьютерных вирусов, методами и средствами выявления угроз безопасности автоматизированным системам, методами формирования требований по защите информации, навыками безопасного использования технических средств в профессиональной деятельности, методами анализа и формализации информационных процессов объекта и связей между ними, методами организации и управления деятельностью служб защиты информации на предприятии, методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов, профессиональной терминологией, понимать важность системы информационной безопасности в общей системе корпоративной безопасности и системе управления рисками компании.

Все знания, умения и навыки, полученные в процессе обучения слушатель должен применять в своей дальнейшей профессиональной деятельности.

Требования к квалификации поступающего на обучение

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие высшее образование.

Программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.

Программа профессиональной переподготовки направлена на получение компетенции, необходимой для выполнения нового вида профессиональной деятельности, приобретение новой квалификации.

Характеристика новой квалификации и связанных с ней видов профессиональной деятельности, трудовых функций, уровней квалификации

Квалификационные характеристики призваны способствовать правильному подбору и расстановке кадров, повышению их деловой квалификации, рациональному разделению труда, созданию действенного механизма разграничения функций, полномочий и ответственности между указанными категориями работников, а также установлению единых подходов в определении их должностных обязанностей и предъявляемых к ним квалификационных требований.

К основным наиважнейшим квалификационным требованиям к выпускнику курса «Информационная безопасность» относятся:

Обязанности: Выполняет мероприятия по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Определяет возможные угрозы безопасности информации, уязвимость программного и аппаратного обеспечения, разрабатывает технологии обнаружения вторжения, оценивает и переоценивает риски, связанные с угрозами деструктивных информационных воздействий, способных нанести ущерб системам и сетям вследствие несанкционированного доступа, использования раскрытия, модификации или уничтожения информации и ресурсов информационно-управляющих систем. Определяет ограничения по вводу информации, процедуры управления инцидентами нарушения безопасности и предотвращает их развитие, порядок подключения к открытым информационным системам с учетом обеспечения безопасности, связанной с соглашениями о доступе, требования к местам резервного хранения, обработки и копирования информации, приоритеты обслуживания по использованию основных и резервных телекоммуникационных сервисов (услуг). Разрабатывает процедуры защиты носителей информации, коммуникаций и восстановления информационно-управляющих систем после сбоя или отказа. Осуществляет контроль деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры; информационное, материально-техническое и научно-техническое обеспечение безопасности информации; контроль состояния работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и их соответствие нормативным правовым актам Российской Федерации. Дает отзывы и заключения на проекты вновь создаваемых и модернизируемых объектов и других разработок по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Участвует в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, оценивает их соответствие действующим нормативным и методическим документам. Участвует в работах по внедрению новых средств технической защиты информации. Содействует распространению в организации передового опыта и внедрению современных организационно-технических мер, средств и способов обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Проводит оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Разрабатывает списки доступа персонала на объекты защиты, порядок и правила поведения работников, в том числе при их перемещении, увольнении и взаимодействии с персоналом сторонних организаций. Осуществляет руководство и обучение персонала действиям в кризисных ситуациях, включая порядок действий руководящих и других ответственных лиц ключевых систем информационной инфраструктуры.

Знания: Должен знать законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением безопасности информации; структуру управления, связи и автоматизации и основные элементы ключевой системы информационной инфраструктуры организации; подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации; порядок создания защищенного канала между взаимодействующими объектами через систему общего пользования с использованием выделенных каналов связи; порядок осуществления аутентификации взаимодействующих объектов и проверки подлинности отправителя и целостности, передаваемых через систему общего пользования данных; оснащенность организации основными и вспомогательными техническими средствами и системами, перспективы их развития и модернизации; перспективы и направления развития методов и средств технических и программно-аппаратных средств защиты информации от деструктивных информационных воздействий; порядок проектирования и аттестации объектов информатизации; контроль эффективности защиты информации на объектах информатизации; порядок осуществления контроля использования открытых каналов радиосвязи; методы и средства выявления угроз

безопасности информации, методики выявления каналов утечки информации; методы проведения научных исследований, разработок по технической защите информации; порядок обследования ключевых систем информационной инфраструктуры, составления актов проверки, протоколов испытаний, предписаний на право эксплуатации специальных средств обеспечения безопасности информации, а также положений, инструкций и других организационно-распорядительных документов; полномочия по вопросам обеспечения безопасности информации, возможности и порядок применения штатных технических средств обеспечения безопасности информации и контроля их эффективности; методы анализа результатов проверок, учета нарушений требований по обеспечению безопасности информации; методику подготовки предложений, методы и средства выполнения вычислительных работ в интересах планирования, организации и проведения работ по обеспечению безопасности информации и обеспечению государственной тайны; достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации; методы оценки профессионального уровня специалистов по обеспечению безопасности информации, аттестации специалистов; основы трудового законодательства; правила по охране труда и пожарной безопасности.

Характеристика компетенций, подлежащих совершенствованию и перечень новых компетенций, формирующихся в результате освоения программы

Совершенствованию подлежат общекультурные и профессиональные компетенции.

В результате освоения дисциплины формируются *общекультурные компетенции*:

способность осознавать необходимость соблюдения Конституции РФ, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма, способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм, способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления, способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства, способность к кооперации с коллегами, работе в коллективе, способность находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность.

В результате освоения дисциплины формируются *профессиональные компетенции*:

способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности, способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз, иметь навыки работы с компьютером как средством управления информацией, способность работать с информацией в глобальных компьютерных сетях, способность к организованному подходу к освоению и приобретению новых навыков и компетенций, способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов, способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности, способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

Форма обучения.

Очно-заочная с применением дистанционных технологий.

Учебный план

№ п/п	Наименование разделов	Всего час.	В том числе		Форма контроля
			Лекции	Практические/ самостоятельные занятия	
1	Основы информационной безопасности	34	29	5	Экзамен
2	Стандарты информационной безопасности	42	30	12	Экзамен
3	Математика и криптографические основы информационной безопасности	64	48	16	Экзамен
4	Протоколы безопасного сетевого взаимодействия. Защита информации с использованием средств криптозащиты	78	57	21	Экзамен
5	Алгоритмы и протоколы каналов и сетей передачи данных	32	32	0	Зачет
6	Основные протоколы и алгоритмы маршрутизации в Интернет	38	28	10	Экзамен
7	Безопасность компьютерных систем на основе операционных систем Windows	38	28	10	Зачет
8	Вирусы и средства борьбы с ними	28	22	6	Зачет
9	Сетевая безопасность на основе серверных продуктов Microsoft	42	32	10	Зачет
10	Технологии и продукты Microsoft в обеспечении информационной безопасности	32	24	8	Зачет
11	Технические средства и методы защиты информации	48	32	16	Зачет
12	Защита персональных данных	48	38	10	Экзамен
13	Стажировка	120		120	Зачет
14	Дипломная работа	50		50	Диплом
	Общая трудоемкость курса (ак. час)	**694**	**400**	**294**	

Календарный учебный график

2014-2015 г.г.																																																			
Сентябрь (01 сент. -28 сент.)				Октябрь (29 сент. – 02 нояб.)					Ноябрь (03 нояб. – 30 нояб.)				Декабрь (01 дек.-28 дек.)				Январь (29 дек. – 01 февр.)					Февраль (02 февр. – 1 мар.)				Март (02 мар. – 29 мар.)				Апрель (30 мар. – 26 апр.)				Май (27 апр. – 31 мая)					Июнь (01 июня – 28 июня)				Июль (29 июня – 02 августа)					Август (03 авг. – 30 авг.)			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

План-график распределения учебных недель в соответствии с рабочей программой

№ п/п	Наименование модуля	Количество недель
1	Основы информационной безопасности	1
2	Стандарты информационной безопасности	2
3	Математика и криптографические основы информационной безопасности	2,5
4	Протоколы безопасного сетевого взаимодействия. Защита информации с использованием средств криптозащиты	3,5
5	Алгоритмы и протоколы каналов и сетей передачи данных	2
6	Основные протоколы и алгоритмы маршрутизации в Интернет	2
7	Безопасность компьютерных систем на основе операционных систем Windows	1
8	Вирусы и средства борьбы с ними	1
9	Сетевая безопасность на основе серверных продуктов Microsoft	1
10	Технологии и продукты Microsoft в обеспечении информационной безопасности	1
11	Технические средства и методы защиты информации	3
12	Защита персональных данных	2
13	Стажировка	4
14	Дипломная работа	2
ИТОГО:		28

График учебной недели Учебного центра при очных лекциях, консультациях, аттестационных испытаний:

Понедельник - пятница, с 9 до 18 часов. Продолжительность рабочего дня, непосредственно предшествующего нерабочему праздничному дню, уменьшается на один час.

В случае реализации программ дополнительного профессионального образования с применением дистанционных образовательных технологий доступ обучающихся к серверу, на котором расположена учебная программа в формате электронного обучения осуществляется обучающимися круглосуточно за исключением времени регламентных (профилактических) работ.

Обучение начинается по мере формирования группы. Группа не менее 10 человек. Общая продолжительность обучения - 6 месяцев.

Рабочая программа учебного курса

Модуль 1. Основы информационной безопасности (всего 34 часа, из них 29 лекционных с использованием дистанционных технологий обучения и 5 практических/самостоятельных)

1. Понятие информационной безопасности. Основные составляющие. Важность проблемы.

Дается определение понятия «информационная безопасность», описываются ее составляющие – конфиденциальность, целостность, доступность. Приводится статистика нарушений ИБ, описываются наиболее характерные случаи.

2. Распространение объектно-ориентированного подхода на информационную безопасность.

В этой лекции кратко формулируются необходимые понятия объектно-ориентированного подхода, в соответствии с ним выделяются уровни мер в области ИБ с небольшим числом сущностей на каждом из них.

3. Наиболее распространенные угрозы.

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

4. Законодательный уровень информационной безопасности.

Эта лекция посвящена российскому и зарубежному законодательству в области ИБ и проблемам, которые существуют в настоящее время в российском законодательстве.

5. Стандарты и спецификации в области информационной безопасности.

Дается обзор международных и национальных стандартов и спецификаций в области ИБ - от "Оранжевой книги" до ISO 15408. Демонстрируются как сильные, так и слабые стороны этих документов.

6. Административный уровень информационной безопасности.

Вводятся ключевые понятия - политика безопасности и программа безопасности. Описывается структура соответствующих документов, меры по их разработке и сопровождению. Меры безопасности увязываются с этапами жизненного цикла информационных систем.

7. Управление рисками.

Информационная безопасность должна достигаться экономически оправданными мерами. В лекции описывается методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств.

8. Процедурный уровень информационной безопасности.

Описываются основные классы мер процедурного уровня. Формулируются принципы, позволяющие обеспечить надежную защиту.

9. Основные программно-технические меры.

Вводится понятие сервиса безопасности. Рассматриваются вопросы архитектурной безопасности, предлагается классификация сервисов.

10. Идентификация и аутентификация, управление доступом.

В данной лекции кратко описываются традиционные сервисы безопасности – идентификация и аутентификация, управление доступом. Сервисы безопасности мы будем рассматривать применительно к распределенным, разнородным системам, содержащим большое число компонентов.

11. Протоколирование и аудит, шифрование, контроль целостности.

Описываются протоколирование и аудит, а также криптографические методы защиты. Показывается их место в общей архитектуре безопасности.

12. Экранирование, анализ защищенности.

Рассматриваются следующие сервисы безопасности – экранирование и анализ защищенности.

13. Обеспечение высокой доступности.

Рассматриваются два вида средств поддержания высокой доступности: обеспечение отказоустойчивости (нейтрализация отказов, живучесть) и обеспечение безопасного и быстрого восстановления после отказов (обслуживаемость).

14. Туннелирование и управление.

Рассматриваются два сервиса безопасности очень разного масштаба — туннелирование и управление.

Модуль 2. Стандарты информационной безопасности (всего 42 часа, из них 30 лекционных с использованием дистанционных технологий обучения и 12 практических/самостоятельных)

1. Обзор наиболее важных стандартов и спецификаций в области информационной безопасности.

Выделяются наиболее важные стандарты и спецификации. Приводятся краткие сведения о стандартах, не являющихся предметом данного курса. Аннотируются спецификации, детально рассматриваемые в последующей части курса.

Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности. Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса. Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций

2. «Общие критерии». Часть 1.

Детально рассматриваются семейства функциональных требований безопасности, представленные в "Общих критериях". Анализируются достоинства и недостатки принятого в них подхода.

3. «Общие критерии». Часть 2. Функциональные требования безопасности.

Оценка профилей защиты и заданий по безопасности. Требования доверия к этапу разработки. Требования к этапу получения, представления и анализа результатов разработки. Требования к поставке и эксплуатации, поддержка доверия. Оценочные уровни доверия безопасности.

4. «Общие критерии». Часть 3. Требования доверия безопасности

Детально рассматриваются семейства требований и оценочные уровни доверия

безопасности, представленные в "Общих критериях". Анализируются достоинства и недостатки принятого в них подхода.

5. Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности.

Определяется роль профилей защиты, описывается их структура. Выделяются общие требования к сервисам безопасности. Общие положения. Общие предположения безопасности. Общие угрозы безопасности. Общие элементы политики и цели безопасности. Общие функциональные требования. Общие требования доверия безопасности.

6. Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности.

Описываются предположения и цели безопасности, функциональные требования и требования доверия, специфичные для конкретных сервисов безопасности. Основное внимание уделено функциональным требованиям, как наиболее важным для обеспечения безопасности.

7. Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности.

Описываются предположения и цели безопасности, функциональные требования и требования доверия, специфичные для конкретных сервисов безопасности. Основное внимание уделено функциональным требованиям, как наиболее важным для обеспечения безопасности.

8. Рекомендации семейства X.500.

Данные рекомендации очень важны в концептуальном плане. Служба директорий, формат сертификатов открытых ключей и атрибутов - это базовые элементы инфраструктуры программно-технического уровня информационной безопасности.

9. Британский стандарт BS 7799

Подробно рассматривается британский стандарт BS 7799, ставший основой международного стандарта ISO/IEC 17799. Он помогает решить проблемы административного и процедурного уровней информационной безопасности.

10. Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"

Рассматриваемый стандарт играет организующую роль, описывая внешний интерфейс криптографического модуля и общие требования к подобным модулям. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них.

Модуль 3. Математика и криптографические основы информационной безопасности (всего 64 часа, из них 48 лекционных с использованием дистанционных технологий обучения и 16 практических/самостоятельных)

1. Модульная арифметика.

Лекция имеет несколько целей: рассмотреть арифметику целых чисел, которая базируется на теории делимости и нахождении наибольшего общего делителя, обратить внимание на важность модульной арифметики (арифметики над вычетами по модулю n) и операций в ней, потому что они широко используются в криптографии.

2. Сравнения и матрицы

В данной лекции рассматриваются матрицы и операции с матрицами вычетов, которые широко используются в криптографии. Используя матрицы вычетов решается набор уравнений сравнения.

3. Традиционные шифры с симметричным ключом

Эта лекция представляет собой обзор традиционных шифров с симметричным ключом, которые использовались в прошлом. Изучение принципов таких шифров готовит читателя к следующим лекциям, которые рассматривают современные симметричные шифры.

4. Алгебраические структуры

Эта лекция имеет несколько целей: рассмотреть понятие алгебраических структур; определить и привести некоторые примеры алгебраических групп; определить и привести некоторые примеры алгебраических колец.

5. Поля.

Цели данной лекции: определить и привести некоторые примеры алгебраических полей; поговорить о таких операциях, как сложение, вычитание, умножение и деление с n-битовыми словами в современных блочных шифрах.

6. Введение в основы современных шифров с симметричным ключом

В этой лекции поставлено несколько целей. Показать различие между традиционными и современными шифрами с симметричным ключом. Привести современные блочные шифры и обсудить их характеристики. Объяснить, почему современные блочные шифры должны быть

спроектированы как шифры подстановки. Ввести компоненты блочных шифров, таких как P-блоки и S-блоки. Обсудить и показать различие между двумя классами шифров: шифры Файстеля и шифры не-Файстеля. Обсудить два вида атак, особо направленных на раскрытие современных блочных шифров: дифференциальный и линейный криптоанализ. Ввести понятие "шифры для потока" и показать различие между синхронными и несинхронными шифрами. Обсудить линейную и нелинейную обратную связь регистров сдвига для реализации поточных шифров.

7. Стандарт шифрования данных (DES).

В этой лекции мы обсуждаем Стандарт шифрования данных (DES — DATA ENCRIPTION STANDARD) — современный блочный шифр с симметричными ключами. Наши основные цели для этой лекции: рассмотреть короткую историю DES; определить основную структуру DES; описать детали основных элементов DES; описать процесс генерации ключей для раундов; провести анализ DES. Особое внимание уделяется тому, как DES использует шифр Файстеля, чтобы достигнуть перемешивания и рассеивания на выходе из битов исходного текста к битам зашифрованного текста.

8. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard)

Рассматривается разработка нового стандарта алгоритма симметричного шифрования – AES. Представлены критерии выбора стандарта и дана сравнительная характеристика пяти финалистов; описываются атаки на алгоритмы с уменьшенным числом раундов и вводится понятие резерва безопасности.Рассматриваются характеристики алгоритмов, являющихся финалистами конкурса AES. Представлены особенности программной реализации каждого из финалистов, возможность их реализации в окружениях с ограничениями пространства, возможность вычисления на лету подключей для каждого алгоритма.

9. Алгоритмы Rijndael и RC6.

Рассматриваются алгоритмы Rijndael и RC6. Приведены математические понятия, лежащие в основе алгоритма Rijndael. Описана структура раунда алгоритмов Rijndael и RC6.

10. Алгоритмы Blowfish, IDEA, ГОСТ 28147.

Рассматриваются алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения. Представлены различные способы создания псевдослучайных чисел.

11. Шифрование, использующее современные шифры с симметричным ключом

Эта лекция показывает, как могут быть зашифрованы длинные сообщения. Она также вводит два новых понятия шифра потока.

12. Простые числа.

Эта лекция имеет несколько целей: ввести простые числа и их приложения в криптографии, обсудить некоторые алгоритмы проверки простоты чисел и их эффективность, обсудить алгоритмы разложения на множители и их приложения в криптографии, описать китайскую теорему об остатках и ее приложения, ввести квадратичное сравнение, ввести возведение в степень по модулю и логарифмы.

13. Квадратичное сравнение.

Линейное сравнение уже рассматривалось в лекции 2, а китайская теорема об остатках была обсуждена в предыдущей секции. Для решения задач криптографии мы также должны уметь решать квадратичное сравнение, имеющее следующую форму $a2x2 + a1x + a0 = 0 \pmod n$.

14. Криптографическая система RSA.

В этой лекции рассматривается асимметрично-ключевая криптографическая система: RSA (RIVERST-SHAMIR-ADLEMAN).

15. Криптосистемы Рабина (Rabin), Эль-Гамаля (ElGamal).

В этой лекции рассматриваются несколько асимметрично-ключевых криптографических систем: Рабина (Rabin), Эль-Гамаля (ElGamal).

16. Криптография с использованием эллиптических кривых.

Рассматривается криптография с использованием эллиптических кривых. Описаны математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Дано описание аналога алгоритма Диффи-Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

17. Хэш-функции и аутентификация сообщений.

Рассматриваются сильные хэш-функции SHA-1, SHA-2 и ГОСТ 34.11. Представлены основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

18. Электронная подпись.

Рассматривается понятие электронной подписи, определяются службы безопасности,

обеспеченные электронной подписью, рассматриваются основные требования к электронным подписям, некоторые схемы электронной подписи, включая RSA, Эль-Гамаля (ElGamal), Шнорра (Schnorr), ГОСТ 34.10 и DSS.

19. Алгоритмы обмена ключей и протоколы аутентификации.

Рассматриваются основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Сравниваются протоколы аутентификации с использованием nonce и временных меток.

20. Методы криптоанализа.

В лекции проведен обзор современных методов криптоанализа. Наряду с классическими методами, особое внимание уделяется новому виду криптоанализа - атакам по побочным каналам и квантовому криптоанализу.

Модуль 4. Протоколы безопасного сетевого взаимодействия. Защита информации с использованием средств криптозащиты (всего 78 часов, из них 57 лекционных с использованием дистанционных технологий обучения и 21 практических/самостоятельных)

1. Управление ключами.

Рассматривается распределение и обслуживание ключей засекречивания в криптографии с симметричными ключами и открытых ключей в криптографии с асимметричными ключами. Разбирается два способа установления симметричного ключа – с использованием третьего лица, которому доверяют, и без использования такого лица. Обсуждается сертификация общедоступных ключей, использующая центры сертификации, на основе рекомендаций X.509. Кратко рассматривается идея относительно Инфраструктуры Открытого ключа (PKI).

2. Инфраструктура Открытого Ключа (часть 1).

Рассматривается стандартная нотация для определения типов и значений данных – Abstract Syntax Notation One (ASN.1). Определены простые и структурные типы. Введено понятие идентификатора объекта.Рассматриваются основные понятия, связанные с инфраструктурой открытого ключа: сертификат открытого ключа, удостоверяющий (сертификационный) центр, конечный участник, регистрационный центр, CRL, политика сертификата, регламент сертификационной практики, проверяющая сторона, репозиторий. Описана архитектура PKI.

3. Инфраструктура Открытого Ключа (часть 2).

Рассматривается сервис Каталога LDAP, описываются преимущества LDAP, приводится его сравнение с реляционными базами данных. Описывается информационная модель LDAP, рассматривается модель именования LDAP, определяется понятие дерева Каталога, DN, схемы, записи, атрибута записи, класса объекта.

4. Инфраструктура Открытого Ключа (часть 3).

Описаны основные свойства протокола LDAP, приведены типичные переговоры LDAP. Рассматриваютсяоперациипротокола LDAP: Bind, Unbind, Search, Modify, Add, Delete, Modify DN, Compare, Abandon.

5. Инфраструктура Открытого Ключа (часть 4).

Дается описание профиля сертификата третьей версии и профиля списка отмененных сертификатов второй версии. Рассматривается понятие сертификационного пути и доверия. Рассматриваются основные поля сертификата и расширения сертификата. Определяется понятие критичного и некритичного расширений. Рассматриваются стандартные расширения: использование ключа, альтернативные имена субъекта и выпускающего, ограничение имени субъекта и выпускающего, политики сертификата, точка распространения CRL.

6. Инфраструктура Открытого Ключа (часть 5).

Рассматривается профиль CRL второй версии и расширения CRL, вводится понятие области CRL, полного CRL, дельта CRL. Описывается алгоритм проверки действительности сертификационного пути. Рассмотрены проблемы безопасности, связанные с сертификатами и CRL.

7. Инфраструктура Открытого Ключа (часть 6).

Рассмотрены протоколы PKI управления сертификатом. Определены требования к управлению PKI, рассмотрены операции управления PKI: инициализация конечного участника, начальная регистрация/сертификация, доказательство обладания закрытым ключом, изменение ключа корневого CA, кросс-сертификация, запрос сертификата, изменение ключа. Также приведены соответствующие структуры данных.

8. Инфраструктура Открытого Ключа (часть 7).

Рассмотрен on-line протокол определения статуса сертификата, определены требования к протоколу и описаны детали протокола. Рассмотрены понятия политики сертификата и

регламента сертификационной практики. Описаны расширения сертификата CertificatePolicies, PolicyMappings и PolicyConstraints. Описано содержание множества постановлений, касающихся регламента сертификационной практики.

9. Безопасное сетевое взаимодействие (часть 1).

Рассматриваются наиболее распространенные на сегодня приложения, обеспечивающие безопасность сетевого взаимодействия. В первую очередь рассматривается аутентификационный сервис Kerberos. Рассматриваются требования, которым должен удовлетворять Kerberos, описан протокол Kerberos, определены функции AS и TGS, описана структура билета (ticket) и аутентификатора. Введено понятие области (realm) Kerberos. Описан протокол 5 версии.

10. Безопасное сетевое взаимодействие (часть 2).

Рассматривается протокол TLS/SSL. Описаны протокол Записи и протокол Рукопожатия, определено понятие "состояние соединения". Описаны используемые криптографические операции и PRF. Рассматриваются расширения, которые могут использоваться для добавления функциональностей в TLS.

11. Безопасное сетевое взаимодействие (часть 3).

Рассматривается протокол удаленного безопасного входа SSH.Определяется понятие ключа хоста, описан алгоритм транспортного уровня, способ аутентификации сервера и вычисление разделяемого секрета. Описаны методы аутентификации пользователя и механизм канала, обеспечивающий интерактивные входные сессии, удаленное выполнение команд, перенаправление TCP/IP-соединений, перенаправление X11-соединений.

12. Безопасное сетевое взаимодействие (часть 4).

Рассматриваются два протокола службы обеспечения безопасности для электронной почты: PGP и S/MIME. В лекции показывается как PGP и S/MIME могут дополнить службы безопасности почтовой системы. Особое внимание уделяется тому, как PGP и S/MIME могут менять криптографические алгоритмы, ключи засекречивания и сертификаты, не устанавливая сеанс между Алисой и Бобом.

13. Архитектура безопасности для IP (часть 1).

Рассматривается архитектура семейства протоколов IPsec. Рассматриваются протоколы безопасности – Authentication Header (AH) и Encapsulating Security Payload (ESP), Безопасные Ассоциации – что это такое, как они работают и как ими управлять, управление ключом – ручное и автоматическое (Internet Key Exchange – IKE), а также алгоритмы, используемые для аутентификации и шифрования.

14. Архитектура безопасности для IP (часть 2).

Рассматривается Безопасная Ассоциация Internet и Протокол Управления Ключом (ISAKMP), который определяет общие процедуры и форматы пакетов для ведения переговоров об установлении, изменении и удалении SA. В качестве протокола аутентификации и обмена ключа рассмотрен протокол IKE.

15. Назначение СКЗИ. Структура.

Рассматриваются функции защиты информации СКЗИ, механизмы защиты информации, требования к эксплуатации, структура СКЗИ, состав программного обеспечения СКЗИ. Нештатные ситуации при эксплуатации СКЗИ.

16. Ключевая система и ключевые носители.

Рассматриваются вопросы шифрования данных, формирование и проверка ЭП, ключевой контейнер, формирование ключей, ключевые носители, размеры ключей, сроки действия пользовательских ключей, уничтожение ключей на ключевых носителях, интерфейс управления ключами СКЗИ, обеспечение безопасности при обращении с носителями криптографических ключей, обеспечение защиты информации от несанкционированного доступа при ее хранении и обработке в организации с использованием средств криптографической защиты информации

17. Защита автоматизированных систем предприятия с применением средств криптографической защиты

Рассматривается место и роль средств криптографической защиты в системе защиты информации организации, необходимые организационные мероприятия (назначение ответственных лиц, разработка внутренних документов организации и т.д.), типовой перечень внутренних организационно-распорядительных документов, регламентирующих применение средств криптографической защиты в организации, требования к персоналу, помещению, специальному оборудованию, охране, порядок организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним.

18. Средство защиты информации ViPNet (часть 1).

В лекции рассматриваются общие сведения о системе защиты информации ViPNet, а также концепция защиты и разграничения доступа.

19. Средство защиты информации ViPNet (часть 2).

Рассматривается состав программного комплекса ViPNet (Administrator, Client, Coordinator), основные функции и возможности комплекса ViPNet.

20. Средство защиты информации ViPNet (часть 3).

В лекции описывается ключевая структура сети ViPNet (ключевая система, формирование и управления ключевой системой), и также функции и условия взаимодействия ЦУС и УКЦ.

21. Средство защиты информации ViPNet (часть 4).

Рассматривается формирование, модификация и межсетевое взаимодействие в сети ViPNet, логика обработки IP-трафика, а также работа с консольными утилитами.

22. Средство защиты информации ViPNet (часть 5).

28. Семейство продуктов «Континент» Описываются типовые схемы применения программного комплекса ViPNet. ViPNet CryptoService, ViPNet SafeDisk.

23. Средство защиты информации «КриптоПро» (часть 1).

В лекции рассматривается построение PKI на основе программного комплекса «КриптоПро УЦ». Описываются структура, состав, размещение и взаимодействие компонентов Удостоверяющего центра, рассматриваются центр сертификации и центр регистрации Удостоверяющего центра, компоненты и режимы их работы.

24. Средство защиты информации «КриптоПро» (часть 2).

В лекции рассматривается модуль сетевой аутентификации КриптоПро TLS , разбор конфликтных ситуаций, связанных с применением электронной подписи, действия при компрометации ключей, регистрация пользователя в сети, исключение пользователя из сети, периодичность издания списка отозванных сертификатов, ведение журналов.

25. Средство защиты информации «КриптоПро». Требования по защите от НСД (часть 1)

Рассматриваются общие требования по организации работ по защите от НСД, требования по размещению технических средств с установленным СКЗИ, требования по установке СКЗИ, общесистемного и специального ПО на ПЭВМ, меры по обеспечению защиты от НСД.

26. Средство защиты информации «КриптоПро». Требования по защите от НСД (часть 2)

Рассматриваются требования по подключению СКЗИ для работы по общедоступным каналам передачи данных, требования по использованию в СКЗИ программно-аппаратных средств защиты от НСД: программно – аппаратный комплекс «Аккорд –АМДЗ», электронный замок «Соболь», требования по криптографической защите.

27. Средство защиты информации СЗИ от НСД Secret Net

Рассматриваются основные структурные элементы и функциональные возможности: защита информации на рабочих станциях и серверах в соответствии с требованиями регулирующих органов, управление сертификатами, контроль утечек и каналов распространения защищаемой информации, защита VDI-инфраструктуры, разграничение доступа.

Рассматривается линейка продуктов «Континент», как одного из программно-аппаратных модулей для обеспечения сетевой безопасности при подключении к сетям общего пользования посредством межсетевого экранирования, построения частных виртуальных сетей (VPN) и системы обнаружения вторжений (СОВ): АПКШ «Континент», Детектор атак «Континент», СКЗИ «Континент-АП».

29. Средство защиты информации СКЗИ «Континент-АП».

Рассматриваются основные возможности: криптографическая защита, усиленная аутентификация, интегрированный межсетевой экран, централизованное управление, подключение малых филиалов (1-2 АРМ) к виртуальной частной сети организации, защищенный доступ в корпоративную сеть с удаленных рабочих станций и персональных компьютеров мобильных сотрудников.

30. Планшетный компьютер со встроенными средствами криптографической защиты конфиденциальной информации «Континент Т-10»

Рассматриваются основные возможности, назначение, технические характеристики, преимущества. Рассмотрены типовые схемы вариантов применения мобильного планшета «Континент Т-10»: доступ мобильных пользователей Wi-Fi сети, доступ мобильных пользователей 3G/4G сети, централизованное подключение АП, подключение АП по схеме «дерево», децентрализованное подключение АП, VPN Клиент под Android.

Модуль 5. Алгоритмы и протоколы каналов и сетей передачи данных (всего 32 часа, из них 26 лекционных с использованием дистанционных технологий обучения и 6 практических/самостоятельных)

1. Введение в новейшие телекоммуникационные технологии.

Введение в новейшие телекоммуникационные технологии. Каналы данных как продолжение органов чувств человека. Алгоритмы модуляции и кодирования при передаче данных, теорема Шеннона, природа шумов, шум дискретизации.

2. Особенности и алгоритмы кодирования голоса.

Особенности и методы кодирования голоса. Дифференциальные и адаптивные методы кодирования голоса. Дельта модуляция. Эхо-компенсация, эквилизация, эффект маскирования, VoCoDER, алгоритмы работы каналов.

3. Алгоритмы сжатия данных.

Алгоритмы сжатия данных. Алгоритм Зива-Лемпеля, Хаффмана и Барроуза-Виллера.

4. Алгоритмы обнаружения и коррекции ошибок.

Контроль по четности, CRC, алгоритм Хэмминга. Введение в коды Рида-Соломона: принципы, архитектура и реализация. Метод коррекции ошибок FEC (Forward Error Correction).

5. Алгоритмы работы с изображением.

Методы разложения, кодирования и отображения статических и движущихся изображений. Использование несовершенства человеческого зрения при кодировании и отображении. Стандарты MPEG-1 и -2. Интерактивное телевидение.

6. Стандарт mpeg-4, -7, -21.

Объектные подходы и описание сцены. Формирование аудио-визуальных сцен MPEG-4. Описание и синхронизация потоков данных для медийных объектов. Профайлы. Демультиплексирование, синхронизация и описание потоков данных, язык описания определений MPEG-7 (DDL). Альфа-маски.

7. Обзор каналов передачи данных.

Коаксиальные кабели и скрученные пары. Построение сетей передачи данных с использованием радио каналов. Сопоставление возможностей проводных, радио- и оптоволоконных каналов.

8. Мобильные телекоммуникации.

Мобильные телекоммуникации (802.11a-g, WiFi, GSM), CDMA. Bluetooth. Стандарт широкополосной беспроводной связи IEEE 802.16. Широкополосный канал для подключения периферийных устройств UWB.

9. Оптические каналы связи.

Оптические волокна, оптические каналы связи, одномодовый и мультимодовый режимы, беспроводные оптические каналы, протоколы PPP и L2TP.

10. Введение в сети передачи данных.

Сетевые топологии, методы доступа к сети, принципы построения сетевых программных интерфейсов. Алгоритмы и применения сетей, алгоритм клиент-сервер и P2P. Классификация сетей.

11. Методы организации и обработки очередей.

Методы организации и обработки очередей, FIFO, PQ, CQ, WFQ, CBWFQ, LLQ, методы работы в условиях перегрузки. Алгоритм leaky bucket ("дырявое ведро"), алгоритм "маркерное ведро", Алгоритмы RED и WRED.

12. Сетевые уровни.

7-уровневая эталонная модель ISO. Физический, канальный и сетевой уровни. Бит-ориентированная процедура управления HDLC. "Апокалипсис двух слонов". Некоторые примеры сетей. Маркерные сети. Сеть DQDB.

13. Интегрированные сети ISDN и ATM.

Модель сети ISDN, точки U, S и T. Интерфейсы NT1 и NT2. Синхронная и асинхронная передача данных. Адресация в ISDN и ATM, процедура setup, SAPI и TEI. Услуги, предлагаемые ISDN.

14. Протоколы frame relay, fibre channel, hippi.

Описание протокола межсетевого обмена Frame Relay. Форматы кадров FR. Интерфейс информационного канала. Мостовые кадры FR. Особенности сетей Fibre Channel. Закон Amdahl. Классы FC. Параллельный интерфейс HIPPI. HIPPI-IPI.

15. Синхронные каналы SDH/SONET, технологические сети CAN, коммутируемая мультимегабитная информационная служба SMDS и протокол IEEE 802.17.

Синхронная цифровая иерархия и PDH, виртуальные контейнеры, STM, архитектурные уровни SDH. Особенности протокола CAN, алгоритм доступа, механизм синхронизации станций.

Коммутируемая мультимегабитная информационная служба SMDS. Описание протокола адаптивных, кольцевых, высокоскоростных сетей IEEE 802.17.

16. Сети Ethernet.

Архитектура сетей Ethernet. Повторители, мосты, мультиплексоры, переключатели и маршрутизаторы, качество обслуживания в LAN. Fast Ethernet. Гигабитный Ethernet. 10-Гигабитный Ethernet. Интернет в Ethernet.

17. Моделирование сетей, сетевая надежность и сетевые драйверы.

Аналитическое и симуляционное моделирование. Элементы теории массового обслуживания. Проблемы оценки надежности сетей. Принципы работы сетевых драйверов.

Модуль 6. Основные протоколы и алгоритмы маршрутизации в Интернет (всего 38 часов, из них 28 лекционных с использованием дистанционных технологий обучения и 10 практических/самостоятельных)

1. Введение в Интернет.

История возникновения Интернет. Базовые принципы, позволившие Интернет выиграть в конкурентной борьбе. Нормативные документы RFC. Стек протоколов TCP/IP. Информационный обмен с и без установления соединения. Особенности IP-протоколов версий 4 и 6. IP-туннели.

2. Транспортные протоколы Интернет.

Описание транспортных протоколов Интернет UDP, TCP (со всеми модификациями). Проблемы и пути совершенствования транспортных протоколов.

3. Протокол передачи команд и сообщений об ошибках (ICMP). Протоколы DCCP и TFRC.

Описан протокол ICMP и его приложения, контроль доступности и управление перегрузкой, типы и коды ICMP, протокол управления перегрузкой для дейтаграмм DCCP.

4. Сокеты.

Описаны принципы организации сокетов и механизмы их применения при сетевом программировании, блокирующие и не блокирующие сокеты, классы услуг и группы сокетов.

5. Протоколы DNS (структура, обработка запросов, ресурсные записи), ARP и RARP.

Рассмотрен протокол DNS, структура, обработка запросов, преобразование имен в адреса и наоборот. Ресурсные записи, потенциальные уязвимости. Описаны также протоколы WINS, ARP и RARP.

6. Протокол динамического конфигурирования ЭВМ DHCP.

Описан протокол динамического конфигурирования машин DHCP, а также протоколы NAT, PAT и NETBIOS.

7. Гипертекстный протокол HTTP.

Протокол HTTP для реализации WWW-сервисов. Работа с проксисерверами и кэшами. Понятие метода, валидаторов, транспортного кодирования и типа среды, включая составные типы. Проблемы пригодности ресурсов и безопасность.

8. Маршрутные протоколы RIP, OSPF и BGP.

Постановка задачи маршрутизации. Принцип оптимальности. Метрика маршрута. Понятие вектора расстояния и алгоритм Белмана-Форда, алгоритм Дикстры, внутренние и внешние протоколы маршрутизации. Формирование и использование маршрутной таблицы.

9. Маршрутизация для групп ЭВМ.

Особенности маршрутизации для мультимедиа. Точки встречи и выделенные маршрутизаторы. Маршрутизация для VPN.

10. Алгоритмы мультимедиа.

Рассмотрены основные протоколы, используемые при работе с мультимедиа данными: IGMP, RTP/RTCP, RSVP и SIP, а также проблемы получения гарантированного качества обслуживания.

11. Передача данных с коммутацией по меткам.

Рассмотрены предпосылки появления технологии коммутации пакетов по меткам, особенности работы VPN, методы получения требуемого уровня качества обслуживания в рамках RSVPTE и GMPLS.

12. Спецификация LDP, RSVPTE, GMPLS.

Рассмотрены механизмы формирования маршрутов для систем с коммутацией по меткам. Описан протокол формирования маршрутных таблиц LDP.

13. Протокол определения адресов (ARP)и протокол определения сетевого адреса по местоположению (RARP).

Рассматриваются протокол преобразования логических адресов в физические и протокол обратного преобразования.

14. Протоколы прикладного уровня. TELNET.

В этой лекции рассматривается прикладная программа: TELNET. Стандартный протокол для услуг виртуального терминала, TELNET дает возможность устанавливать соединение с удаленным компьютером таким образом, что создается впечатление, как будто местный терминал – это терминал удаленной системы.

15. Протоколы передачи файлов (FTP и TFTP).

Рассматривается протокол передачи файлов (File Transfer Protocol – FTP) – это стандартный механизм для копирования файла от одного хоста другим.

16. Протоколы электронной почты: SMTP, POP, IMAP.

В данной лекции рассматриваются протоколы электронной почты. Приведены основные понятия, определения и свойства протоколов электронной почты. В TCP/IP протокол, который поддерживает сообщения электронной почты в Интернете, — это простой протокол электронной почты (SMTP — Simple Mail Transfer Protocol).

17. Подписные листы (LISTSERV) и поисковые системы.

В данной лекции рассматриваются подписные листы (LISTSERV) и поисковые системы. Приведены методы их практической реализации, принципы взаимодействия с другими протоколами, описаны базовые понятия и определения.

18. ICQ, WHOIS и Finger.

В данной лекции рассматриваются протоколы ICQ, WHOIS и Finger. Приведены базовые понятия и определения, связанные с этими протоколами, а также принципы взаимодействия с другими протоколами.

19. Сетевой протокол времени NTP.

В данной лекции внимание уделяется сетевому протоколу времени NTP. Приводятся основные определения и понятия, связанные с протоколом, названия основных переменных, используемых в протоколе, а также методы и принципы применения данного протокола.

20. Протокол SNMP.

В данной лекции рассматриваются вопросы сетевой диагностики и протокол SNMP. Приведены базовые понятия и определения, а также основные свойства и методы применения протокола SNMP.

21. Управляющая база данных MIB.

В данной лекции рассматривается управляющая база данных MIB. Приводятся названия основных переменных базы данных MIB, описаны базовые понятия и определения, связанные с данной базой.

22. Методы противодействия.

В данной лекции рассматриваются методы противодействия атакам. Рассматривается понятие Firewall и его основные типы и принципы работы.

Модуль 7. Безопасность компьютерных систем на основе операционных систем Windows (всего 38 часов, из них 28 лекционных с использованием дистанционных технологий обучения и 10 практических/самостоятельных)

1. Использование виртуальных машин для изучения операционных систем на примере Microsoft Virtual PC.

В связи с тем, что средства для создания виртуальных машин часто применяются, в данной лекции мы поговорим об использовании виртуальных машин для изучения ОС на примере Virtual PC. Данная программа позволяет пользователю одновременно выполнять несколько операционных систем без использования множества компьютеров или необходимости перезагружать основной компьютер.

2. Механизмы развертывания сетевой инфраструктуры на основе ОС Windows.

Данная лекция посвящена способам развертывания сетевой инфраструктуры на основе ОС Windows. Автоматическое развертывание ОС и клиентских рабочих мест является важной задачей для обеспечения безопасности сетевой инфраструктуры любой организации.

3. Обеспечение безопасности хранения данных в ОС Microsoft.

В этой лекции мы познакомимся с предоставляемыми возможностями ОС Microsoft Windows по обеспечению безопасности хранения данных в целом, несмотря на их степень значимости.

4. Центр обеспечения безопасности (Windows Security Center) в операционных системах Windows.

В этой лекции будет рассмотрен "Центр обеспечения безопасности Windows" (Windows Security Center), входящий в состав операционных систем Windows. Он разработан компанией Microsoft для автоматической проверки состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). С помощью этого инструмента пользователь

имеет возможность не только контролировать состояние перечисленных выше компонентов, но и получать рекомендации по устранению возникающих с этими компонентами проблем.

5. Системы анализа защищенности корпоративной сети (обнаружения уязвимостей) на примере сертифицированной системы обнаружения вторжений «Форпост».

Рассматривается обнаружение и блокирование сетевых атак в реальном масштабе времени, оперативное реагирование на выявленные сетевые атаки, поддержка обновления базы данных сигнатур атак в системе, наличие подсистемы собственной безопасности, наличие интуитивно-понятного русскоязычного интерфейса консоли администратора системы, использование системы обнаружения вторжений "Форпост" совместно с системой управления политикой безопасности "Урядник / Enterprise Guard" позволяющей обеспечить заданный уровень защищённости ИС в процессе её эксплуатации на основе принятой политики безопасности.

6. Управление электропитанием рабочих станций и серверов (на примере продуктов компании Raritan).

В этой лекции будут рассмотрены примеры практического применения продукции компании Raritan для защиты рабочих станций и серверов.

Модуль 8. Вирусы и средства борьбы с ними (всего 28 часов, из них 22 лекционных с использованием дистанционных технологий обучения и 6 практических/самостоятельных)

1. История вопроса.

В лекции рассказывается как и когда появились первые вирусы, их первоначальное назначение, дальнейшее развитие, мутации, принципы действия, дается перечень и краткое описание глобальных эпидемий.

2. Классификация вирусов.

В лекции рассматриваются существующие типы вредоносных программ. Даются их определения, характеристики, способы распространения, вредоносная нагрузка, жизненный цикл.

3. Что такое антивирусы.

В лекции дается определение антивирусной программы, ее задачи, подробно рассматриваются используемые для обнаружения вирусов технологии. Вводится понятие антивирусных комплексов, их классификация, описываются критерии выбора комплексов для построения оптимальной системы антивирусной защиты и этапы ее внедрения. Рассмотрены основные составляющие комплексной системы антивирусной защиты: организационные, правовые, программные меры.

4. Защита шлюзов.

Антивирус для шлюза – первый уровень защиты на пути проникновения вирусов в сеть организации. В лекции рассматриваются возможные схемы защиты сети с использованием антивируса для шлюзов, основные требования к антивирусам такого класса, вирусные угрозы, от которых они могут и не могут защитить, особенности эксплуатации.

5. Защита почтовых систем.

Задачи антивирусного комплекса по защите почтовых систем; возможные схемы защиты; требования к антивирусному комплексу; характеристики и сравнение основных известных АВ комплексов.

6. Защита серверов и рабочих станций.

В лекции рассматривается структура третьего уровня комплексной системы антивирусной защиты — средства защиты рабочих станций и сетевых серверов, инструменты удаленного централизованного управления ими. Для каждого из подуровней приводится обзор основных вирусных угроз, анализируются условия эксплуатации защищаемых компьютеров и необходимость применения тех или иных технологий выявления вирусов, формулируются требования к антивирусам такого класса.

7. Антивирусное программное обеспечение KasperskyEndpointSecurity (часть 1).

В лекции рассматриваются функциональные возможности, состав и предназначение продуктов, входящих в KasperskyEndpointSecurity и KasperskySecurityCenter, осуществление поддержки и мониторинга работы системы антивирусной защиты. Описывается внедрение системы антивирусной защиты рабочих станций и серверов Windows, построенной на базе KasperskyEndpointSecurity и KasperskySecurityCenter, в компьютерную сеть, осуществление обслуживания внедренной системы на всех стадиях эксплуатации.

8. Антивирусное программное обеспечение KasperskyEndpointSecurity (часть 2).

Рассматривается базовое устройство KasperskyEndpointSecurity 10. Разбирается защита файловой системы, защита сети, проактивная защита, диагностика угроз и диагностика состояния защиты.

9. Антивирусное программное обеспечение KasperskyEndpointSecurity (часть 3).

В рамках лекции рассматривается контроль запуски и активности программ, контроль устройств.

10. Антивирусное программное обеспечение KasperskyEndpointSecurity (часть 4).

Рассматриваются следующие разделы: статистика и отчета, обновление, управление лицензиями, взаимодействие с пользователями, создание и восстановление из резервной копии. Отдельное внимание уделено особенностям мобильных политик.

11. Антивирусное программное обеспечение Dr. Web.

В рамках лекции рассматриваются основные характерные особенности семейства антивирусов, разрабатываемых компанией «Доктор Веб».

Модуль 9. Сетевая безопасность на основе серверных продуктов Microsoft (всего 42 часа, из них 32 лекционных с использованием дистанционных технологий обучения и 10 практических/самостоятельных)

1. Сетевая безопасность. План защиты.

В данной лекции основное внимание уделено проблемам безопасности и составлению плана защиты сети. Рассматриваются основные принципы, которые учитываются при обеспечении сетевой безопасности.

2. Службы сертификации и их применение.

В данной лекции рассматриваются службы сертификации и их применение. Рассматривается классификация центров сертификации и понятие сертификата ключа проверки электронной подписи.

3. Защита серверных ролей.

В данной лекции рассматриваются вопросы защиты серверных ролей. Приводятся основные принципы открытия необходимых портов, репликации и реализации механизма разрешения имен.

4. Отношения доверия в лесах и доменах.

Рассматривается система отношений доверия между доменами и лесами в корпоративной сети.

5. Доступ к объектам в корпоративной сети.

В лекции рассмотрены типы доверия в лесах и доменах, их ограничение, и даны рекомендации к внедрению.

6. Защита беспроводных сетей.

В лекции рассматриваются основные механизмы защиты беспроводных сетей: проверка подлинности, шифрование, WPA.

7. Проектирование защиты Web-сервера.

В лекции рассмотрены базовые принципы защиты Web-сервера под управлением WS2003, созданного на базе технологии IIS 6.0.

Модуль 10. Технологии и продукты Microsoft в обеспечении информационной безопасности(всего 32 часа, из них 24 лекционных с использованием дистанционных технологий обучения и 8 практических)

1. Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни.

Перед студентами ставится задача собрать и систематизировать как можно больше информации друг о друге с использованием общедоступных Интернет-ресурсов, оценить угрозу злоумышленного применения информации и выработать рекомендации по обеспечению необходимого уровня безопасности частной жизни в мире цифровых зависимостей.

2. Криптопровайдеры. API для работы с криптосервисами Windows.

В данной лекции рассматривается эволюция криптографических сервисов в составе ОС Windows.

3. Криптографические функции в NET Framework.

В данной лекции .NET Framework изучается с точки зрения программиста, реализующего функции безопасности в корпоративных приложениях.

4. XML- криптография.

В данной лекции рассматривается круг вопросов, связанных с концепцией XML-криптографии и ее реализацией на платформе .NET Framework.

5. Шаблоны использования криптографических функций в корпоративных приложениях.

В данной лекции рассматриваются назначение, область применения и функции Enterprise Library на примере Cryptography Application Block.

6. Проблема аутентификации. Инфраструктура открытых ключей.

В рамках лекции рассматривается инфраструктура открытых ключей на примере ее реализации Microsoft.

7. Криптографические механизмы Windows.

Рассматривается системы шифрования данных, поставляемые в составе ОС Windows, BitLocker, Encrypted File System.

8. Безопасная вычислительная база нового поколения.

Рассматривается круг вопросов, связанных с концепцией "безопасных вычислений" и ее реализацией в продуктах Microsoft.

9. Системы управления идентичностью.

В лекции проведен обзор современных систем управления идентичностью. Подробно рассматриваются технологии Windows Live Id (также известной как Microsoft .NET Passport) и Windows CardSpace.

Модуль 11. Технические средства и методы защиты информации (всего 48 часов, из них 32 лекционных с использованием дистанционных технологий обучения и 16 практических/самостоятельных)

1. Общие сведения о технических каналах утечки информации.

В лекции рассматриваются структура, классификация и основные характеристики технических каналов утечки информации, а также физическая природа побочных электромагнитных излучений.

2. Технические каналы утечки информации при ее передаче по каналам связи.

Рассматриваются средства передачи электрических сигналов, пути утечки информативного сигнала по цепям электропитания и слаботочных линий, анализируются способы контроля и прослушивания телефонных каналов связи.

3. Технические каналы утечки речевой информации.

В рамках лекции рассматриваются краткие сведения об акустическом сигнале (линейные и энергетические характеристики звукового поля, виды звуковых волн: плоская и сферическая). Дается формальное определение понятности и разборчивости речи. Рассматриваются характеристики помещений, звукопоглощающие материалы и конструкции, которые могут быть использованы при отделке помещений для обеспечения их звукоизоляции. В лекции проведен обзор средств акустической разведки (микрофоны, диктофоны, стетоскопы, гидроакустические датчики, СВЧ- и ИК- передатчики). Отдельное внимание посвящено оптико-электронному каналу утечки речевой информации.

4. Технические каналы утечки видовой информации.

Рассматриваются способы скрытого видеонаблюдения и съемки.

5. Демаскирующие признаки объектов.

В лекции рассматриваются свойства объектов защиты, которые могут быть использованы технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.

6. Средства выявления каналов утечки информации.

Рассматриваются индикаторы электромагнитного поля, сканирующие радиоприемники, анализаторы спектра, радиочастотомеры, многофункциональные комплексы для выявления каналов утечки информации, комплексы измерения ПЭМИН, нелинейные локаторы, металлодетекторы, досмотровые эндоскопы.

7. Скрытие и защиты информации от утечки по техническим каналам.

В рамках лекции дается описание концепции и методов инженерно-технической защиты информации. Рассматриваются способы экранирования электромагнитных волн, безопасность оптоволоконных кабельных систем, подавление информационных сигналов в цепях заземления, пространственное и линейное зашумление, способы предотвращения утечки информации через ПЭМИН персонального компьютера, скрытие и защита от утечки информации по акустическому и виброакустическому каналам

8. Методы и средства инженерной защиты и технической охраны объектов.

Рассматриваются особенности охраны различных типов объектов защиты. Дается описание организации систем охранно-тревожной сигнализации, систем контроля и управления доступом, телевизионных систем, систем пожарной сигнализации.

9. Технический контроль эффективности мер защиты информации.

В рамках лекции приводится описание целей и задач технического контроля эффективности защиты информации, рассматриваются методы испытаний и контроля.

10. Концепция резидентного компонента безопасности (РКБ) и ее техническая реализация на примере СЗИ НСД семейства "Аккорд".

Обоснование безопасности, критерии отнесения СЗИ к РКБ, реализация защитных механизмов комплекса.

Выработка начальных умений и навыков установки, настройки и администрирования СЗИ

семейства. Логика построения линейки и оценки применимости СЗИ для решения типовых задач защиты информации в ГИС и корпоративных ИС различных архитектур.

10. Система защиты информации от несанкционированного доступа Dallas Lock (часть

Рассматриваются назначение и возможности системы защиты, а также установка/удаление системы защиты и вход на защищенный компьютер.

11. Система защиты информации от несанкционированного доступа Dallas Lock (часть

В лекции дается общее представление о пользовательском интерфейсе программы администрирования DallasLock и принципах работы, необходимых непосредственно администратору системы.

12. Система защиты информации от несанкционированного доступа Dallas Lock (часть

Подробно описываются функциональные возможности основных подсистем, модулей, механизсмой и настроек системы защиты DallasLock.

13. Система защиты информации от несанкционированного доступа Dallas Lock (часть

В лекции рассматриваются функциональные возможности модулей централизованного управления системы защиты «Сервер безопасности» и «Менеджер серверов безопасности».

14. Система защиты информации от несанкционированного доступа Dallas Lock (часть

Описывается процесс восстановления компьютера при сбое системы защиты DallasLock и восстановление данных жесткого диска.

Модуль 12. Защита персональных данных (всего 48 часов, из них 38 лекционных с использованием дистанционных технологий обучения и 10 практических/самостоятельных)

1. Введение в область знаний

Программа, цели и задачи модуля. Основные понятия, термины и определения. Информация, конфиденциальная информация, защита информации, коммерческая тайна, служебная информация, персональные данные. Нормативные правовые акты, регламентирующие вопросы, связанные с защитой конфиденциальной информации. Возможность страхования информационных рисков, как один из основных способов возмещения материального ущерба от нарушения конфиденциальности информации. Лицензирование деятельности по технической защите конфиденциальной информации. Место нормативных правовых актов, регулирующих вопросы защиты конфиденциальной информации в общей системе российского законодательства. Сертификация и аттестация информационных систем по требованиям безопасности.

2. Понятие «персональные данные»

«Персональные данные» как отдельная категория конфиденциальной информации. Специальные категории персональных данных. Биометрические персональные данные. Персональные данные в международном законодательстве, национальном законодательстве зарубежных стран, а также в российском законодательстве. Практика применения понятия «персональные данные» в органах государственной власти и организациях независимо от формы собственности.

3. Основные участники правоотношений в сфере организации работы с персональными данными

Субъекты персональных данных и операторы персональных данных. Модели взаимодействия при обработке персональных данных. Уполномоченный орган по защите прав субъектов персональных данных. Правовой статус. Реестр операторов. Проведение контрольно-надзорных мероприятий. Уполномоченные органы, на которые возлагается контроль и надзор за соблюдением требований по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требований к материальным носителям биометрических персональных данных, и технологиям хранения таких данных вне информационных систем персональных данных. Правовой статус. Нормативное правовое регулирование технической защиты персональных данных.

Лицензиаты уполномоченных органов в области защиты информации. Сертификация средств защиты. Разработка подсистем обеспечения безопасности персональных данных.

4. Особенности регулирования защиты персональных данных в различных сферах деятельности

Особенности регулирования защиты персональных данных в организациях различных форм собственности. Особенности регулирования защиты персональных данных в трудовых правоотношениях. Особенности регулирования защиты персональных данных в области связи. Правовой статус операторов связи. Особенности нормативного правового регулирования при обработке персональных данных. Технические и криптографические меры защиты. Особенности регулирования защиты персональных данных в международных правоотношениях. Трансграничная передача персональных данных. Особенности регулирования защиты

персональных данных в органах государственной власти. Особенности обработки персональных данных в государственных и муниципальных информационных системах персональных данных.

5. Основы технической и криптографической защиты персональных данных, обрабатываемых в информационных системах персональных данных.

Информация как объект защиты. Информация по форме представления. Информация по категориям доступа. Введение в область технической защиты информации. Правовая и нормативно-методическая база, регулирующая вопросы технической и криптографической защиты персональных данных. Понятие информационной системы персональных данных. Классификация информационных систем персональных данных. Типовые угрозы безопасности персональных данных при их обработке в информационных системах персональных данных. Классификация угроз безопасности персональных данных. Примеры угроз безопасности персональных данных. Модель угроз и модель нарушителя. Система моделей. Типизация моделей. Требования по защите персональных данных в соответствии с моделями угроз и нарушителя. Модель защиты персональных данных. Режим защиты персональных данных. Типовые документы по режиму защиты. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Типовые мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Основные методы и средства защиты персональных данных при их обработке в информационных системах персональных данных. Рекомендации по применению криптографических средств защиты. Защита персональных данных в процессе обработки их без средств автоматизации.

6. Организация работы с персональными данными в организации

Формирование локальной нормативной правовой базы: перечень сведений, относимых к персональным данным. Модель угроз и модель нарушителя. Оценка актуальности угроз. Меры и средства защиты. Дисциплинарная, административная и уголовная ответственность за нарушение законодательства о персональных данных. Делопроизводство. Взаимодействие с Уполномоченным органом по защите прав субъектов персональных данных.

7. Понятие «служебная и коммерческая тайна»

«Служебная и коммерческая тайна» как отдельная категория конфиденциальной информации. Практика применения понятия «служебная и коммерческая тайна» в органах государственной власти и организациях независимо от формы собственности.

8. Основные участники правоотношений в сфере защиты служебной и коммерческой тайны

Модели взаимодействия при обработке служебной и коммерческой тайны. Правовой статус участников взаимодействия при работе со служебной и коммерческой тайной. Проведение контрольных мероприятий. Органы, на которые возлагается контроль и надзор за соблюдением требований по обеспечению безопасности служебной и коммерческой тайны. Разработка подсистем обеспечения безопасности служебной и коммерческой тайны.

Условия реализации программы, организационно-педагогические условия

Чтение лекций по дисциплине проводится преимущественно с использованием электронных мультимедийных презентаций.

Использование презентации позволяет преподавателю чётко структурировать материал лекции, экономить время, затрачиваемое на рисование схем, диаграмм и других сложных графических объектов, что позволяет значительно увеличить объем излагаемого материала без потери его качества. Помимо этого, презентация позволяет очень хорошо иллюстрировать лекцию не только схемами и рисунками, но и цветными фотографиями.

Студентам предоставляется возможность копирования материала для самоподготовки и подготовки к экзамену.

При работе целесообразно использовать диалоговую форму ведения лекций с постановкой и решением проблемных задач, современных поправок в законодательстве РФ, обсуждением дискуссионных моментов и т.д.

При проведении лабораторных занятий создаются условия для максимально самостоятельного выполнения лабораторных работ. Проведение каждой лабораторной работы включает четыре этапа:

1. Постановка целей и задач лабораторной работы. Демонстрация и разбор примера.
2. Выполнение лабораторной работы.
3. Демонстрация результатов выполнения лабораторной работы и разбор ошибок.
4. Устранение ошибок и оценивание выполненной работы.

Каждая лабораторная работа включает самостоятельную проработку теоретического материала, изучение методики и технологий решения задачи, приобретение навыка решения задачпо управлению данными.

При проведении самостоятельных работ используются следующие формы:

· решение студентом самостоятельных задач обычной сложности, направленных на закрепление знаний и умений;

· выполнение самостоятельных работ, направленных на развитие у слушателей мышления и инициативы.

В преподавательский состав входят высококвалифицированные преподаватели, имеющие большой практический опыт в области информационной безопасности. Одним из них является Мурин Д.М., кандидат физико-математических наук по специальности 05.13.19.

Доля работников из числа руководителей и работников учебного центра, деятельность которых связана с направленностью (профилем) реализуемой программы и имеющих стаж работы в данной профессиональной области не менее 3 лет составляет 60%.

Материально-техническое обеспечение курса

Учебный центр имеет 1 учебную аудиторию вместимостью 32 места для слушателей, оснащенную стационарным мультимедийным оборудованием, компьютерный класс на 12 слушателей. Аудиторияучебного центра имеет возможность установки дополнительного технического оборудования: мультимедийных проекторов, звукоусиливающей аппаратуры.
Мультимедийное оборудование включает в себя: мультимедийный проектор, проекционный экран, акустическую систему, персональный компьютер, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI, трибуна преподавателя. Адитория оснащена высокоскоростным интернетом. Компьютерный класс включает компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети и находятся в едином домене.

Стажировка

Стажировка по специальности «Информационная безопасность» является завершающим этапом обучения и проводится с целью проверки профессиональной готовности будущего специалиста к самостоятельной трудовой деятельности.
Задачами стажировки являются:

- обеспечение готовности слушателей к выполнению основных профессиональных функций в соответствии с квалификационными требованиями.

Продолжительность стажировки – 4 недели.

Контроль работы слушателей осуществляет руководитель стажировки. Итоговый контроль проводится в форме зачета. Зачет проставляется руководителем стажировки на основании собеседования со слушателем, с учетом личных наблюдений за самостоятельной работой слушателя, отчета, индивидуального задания, а также характеристики, подготовленной руководителем практики.

Возможны следующие формы проведения стажировки:

- работа на должности;
- работа дублером на должности;
- прохождение стажировки по индивидуальному графику.

Тематический план стажировки

№№ тем	Наименование тем практики	Продолжительность в часах
	Вводный инструктаж	6
1	Ознакомление со структурой предприятия, роли отдела в общей структуре предприятия.	12
2	Организация защиты информации и управление доступом к информационным ресурсам в АИС.	50
3	Работа со стендом УЦ	36
4	Разработка инструктивной документации по сопровождению программных продуктов (индивидуальное задание)	8
	Обобщение материала, оформление отчета по стажировке	8
	Итого:	**120**

Слушатели во время прохождения стажировки:

• знакомятся с аппаратурой по защите информации:

программно-аппаратный комплекс «Удостоверяющий центр «КриптоПро УЦ» версии 1.5 (вариант исполнения 2) и организационно-технические мероприятия, предусмотренные регламентом ЖТЯИ.00067-01 90 17,

Dallas Lock – сертифицированная система защиты информации от несанкционированного доступа, использование которой в проектах по защите информации ограниченного доступа позволяет привести автоматизированные системы в соответствие требованиям законов РФ, стандартов и руководящих документов,

устройство защиты объектов информатизации выделенных помещений до 1 категории включительно Соната Р2.

• выполняют все работы, предусмотренные программой стажировки;

• осуществляют работу в соответствии с установленным в организации режимом и порядком работы;

• оформляют рабочие материалы и результаты практической работы в форме отчетов о практике.

Слушатели обязаны:

• выполнять правила внутреннего распорядка и техники безопасности, установленные в организации;

• нести ответственность за выполняемую работу и ее результаты наравне со штатными работниками предприятия.

Индивидуальное задание слушателя

Для проверки знаний, умений и навыков каждому слушателю выдается индивидуальное задание.

Индивидуальное задание составляет руководитель производственной практики.

Задание составляется так, чтобы выполнение его требовало от слушателя применения на производственной практике полученных в учебном центре теоретических знаний.

Результаты работы, выполненной в процессе прохождения производственной практики, представляются **в виде отчета**.

В первой части отчета кратко излагаются общие сведения об организации, на котором проходила производственная практика. Приводится структурная схема подразделения, где проходила практика.

В третьей части отчета излагается методика решения конкретной задачи и полученные результаты решения этой задачи.

На титульном листе отчета указываются все подразделения, в которых студент проходил производственную практику, фамилии и должности руководителей. Каждый руководитель визирует соответствующую часть отчета на титульном листе.

В отчете обязательно должен быть **список использованных литературных источников со ссылками на них в тексте.**

Форма аттестации. Оценочные материалы

Оценка качества освоения слушателями дополнительной профессиональной программы профессиональной переподготовки «Информационная безопасность» включает текущий контроль знаний, промежуточную и итоговую аттестацию слушателей.

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной и итоговой аттестации включают:

1) вопросы и задания для лабораторных работ, тематику дипломных работ, программы зачетов и экзаменов в виде компьютерного тестирования по отдельным дисциплинам программы.

2) планы проведения практических занятий по дисциплинам учебного плана;

3) программы самостоятельной работы слушателей.

Учебным планом предусмотрены следующие виды самостоятельной работы:

• самостоятельное изучение лекционных материалов;

• лабораторные работы (в компьютерных классах, на индивидуальном компьютерном рабочем месте);

• выполнение выпускной квалифицированной работы (дипломной работы).

В соответствии с учебным планом промежуточная аттестация предусматривает проведение экзаменов, зачетов в форме тестирования.

По всем перечисленным видам промежуточной аттестации разработаны комплекты оценочных средств.

Критерии оценки практической работы

Оценка	Предмет оценки
Отлично 86-100 баллов.	Практическая работа полностью раскрыта, имеются логические и обоснованные выводы, работа оформлена на высоком уровне. Автор свободно ориентируется в материале, владеет научной терминологией по рассматриваемой проблеме, умеет пользоваться Интернет ресурсами и самостоятельно находить нужную информацию и отвечать на возникающие вопросы.
Хорошо 70-85 баллов.	Практическая работа в целом раскрыта, сформулированы необходимые выводы. Имеются замечания/неточности в части изложения и отдельные недостатки по оформлению работы.
Удовлетворительно 51-69 баллов.	Практическая работа раскрыта недостаточно полно, выводы не обоснованы. Материал изложен непоследовательно, без соответствующей аргументации и необходимого анализа, имеются недостатки в оформлении.
Неудовлетворительно 50 и менее баллов.	Практическая работа не раскрыта Имеются недостатки в оформлении работы.

Критерии оценки самостоятельных работ

Оценка	Предмет оценки
Отлично 86-100 баллов.	86-100 баллов. Есть ответы на все тесты. Допущены незначительные неточности в 1-2 тестах.
Хорошо 70-85 баллов.	70-85 баллов. Допущена ошибка в 1-2 тестах.
Удовлетворительно 51-69 баллов.	Правильные ответы даны на более, чем 50% вопросов, но менее 69%
Неудовлетворительно 50 и менее баллов.	Менее 50% правильных ответов.

В случае использования сразу двух видов текущего контроля по одному разделу итоговая оценка выводится путем вычисления среднего арифметического двух оценок. Неудовлетворительная оценка не используется при выведении общей оценки, подлежит пересдаче.

Оценки за практические (лабораторные) и самостоятельные работы слушателей преподаватель выставляет в рабочую ведомость.

Итоговая аттестация слушателей по направлениюпрофессиональной переподготовки «Информационная безопасность» включает итоговый экзамен и защиту дипломной работы.

Итоговая аттестация организуется и проводится в соответствии с «Положением об итоговой аттестации АНО ДПО «Учебный центр «Парадигма».

Итоговый экзамен по программе «Информационная безопасность» является формой итоговой аттестации слушателей. Форма и содержание итогового экзамена обеспечивают контроль уровня подготовки слушателей для подтверждения их соответствия квалификационным признакам по компетенциям по направлению «Информационная безопасность». Итоговый экзамен имеет комплексный, междисциплинарный характер и проводится по программе, охватывающей широкий спектр фундаментальных вопросов по учебным дисциплинам рабочей программыпрофессиональной переподготовки «Информационная безопасность».

Дипломная работа подводит итоги теоретической и практической подготовки обучающегося и характеризует его подготовленность к предстоящей профессиональной деятельности.

Подготовка и защита дипломной работы предполагает наличие у слушателей умений и навыков проводить самостоятельное законченное исследование на заданную тему, свидетельствующее об усвоении слушателем теоретических знаний и практических навыков, позволяющих решать профессиональные задачи, соответствующие требованиям Федерального государственного образовательного стандарта высшего профессионального образования.

Дипломная работа должна свидетельствовать о способности и умении слушателя:

- решать практические задачи на основе применения теоретических знаний;
- вести поиск и обработку информации из различных видов источников;
- выявить управленческую задачу в сфере профессиональной деятельности;
- решить управленческую задачу с использованием аналитических методов с помощью

современных информационных технологий;

• грамотно и логично излагать материал, делать обоснованные выводы по результатам исследования.

Дипломная работа выполняется, как правило, в соответствии с установленным АНО ДПО «Учебный центр «Парадигма» перечнем тематики работ с учетом квалификационных требований к слушателям данной программы.

Требования к содержанию, объему и структуре дипломной работы определяются Учебный центром на основании действующего Положения об итоговой аттестации слушателей.

Методические пособия по изучению программы

Основным методическим материалом данного курса является электронный конспект лекций. Он состоит из 12 дисциплин в соответствии с учебным планом. Слушатели получают подбор литературы и информационный материал по каждой теме курса.

Источники

1. Правовые и нормативно-методические документы
2. Конституция Российской Федерации, принята 12 декабря 1993 г.
3. Закон РФ № 51-ФЗ от 30 ноября 1994 г. «Гражданский кодекс Российской Федерации. Часть первая».
4. Закон РФ № 230-ФЗ от 18 декабря 2006 г. «Гражданский кодекс Российской Федерации. Часть четвёртая».
5. Закон РФ № 138-ФЗ от 14 ноября 2002 г. «Гражданский процессуальный кодекс Российской Федерации».
6. Закон РФ № 95-ФЗ от 24 июля 2002 г. «Арбитражный процессуальный кодекс Российской Федерации».
7. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
8. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
10. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
11. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 27 декабря 2002 г. № 184 «О техническом регулировании».
14. Закон РФ от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений».
15. Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне».
16. Закон РФ № 195-ФЗ от 30 декабря 2001 г. «Кодекс Российской Федерации об административных правонарушениях».
17. Закон РФ № 63-ФЗ от 13 июня 1996 г. «Уголовный кодекс Российской Федерации».
18. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации 12 мая 2009 г. № 537.
19. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. №Пр-1895.
20. Указ Президента Российской Федерации от 12 мая 2008 г. №724 «Вопросы системы и структуры федеральных органов исполнительной власти».
21. Указ Президента Российской Федерации от 03 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
22. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
23. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
24. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года. Утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.
25. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».
26. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
27. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии

оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России. - М., 2002.
28.ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России. - М., 2002.
29.ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России. - М., 2002.
30.ISO/IEC 27001:2005. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
31.ISO/IEC 27002:2005. Информационные технологии. Методики безопасности. Практические правила управления информационной безопасностью.
32.ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
33.ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
34.ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
35.ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
36.Приказ ФАПСИ при Президенте РФ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
37.Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
38.«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.
39.«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.
40.Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
41.Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите информации».
42.Административный регламент ФСТЭК России по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации, утвержденный приказом ФСТЭК России от 28 августа 2007 г. № 181.
43.Приказ Директора ФСТЭК России от 5 февраля 2010 года № 58 «Положение о методах и способах защиты информации в информационных системах персональных данных».
44.Постановление Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
45.Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) (с изменениями от 15 июня 1999 г.)
46.Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации» ETS N 181 (Страсбург, 08 ноября 2001 г.).
47.Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г.о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года).
48.Директива Европейского Парламента и Совета Европейского Союза 2002/22/ЕС от 7 марта

2002 г.об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг (Директива об универсальных услугах).
49.Директива Европейского Парламента и Совета Европейского Союза 2002/58/ЕС от 12 июля 2002 г.в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи).

Основная литература

1. Панасенко С. «Алгоритмы шифрования». Специальный справочник. – М.: БХВ-Петербург, 2009.
2. Полянская О. Ю., Горбатов В. С. «Инфраструктуры открытых ключей». – М.: Интернет-университет информационных технологий, Лаборатория Знаний, 2007.
3. Тихонов В.А., Райх В.В. «Информационная безопасность: концептуальные, правовые, организационные и технические аспекты». Учебное пособие. - М.: Гелиос АРВ, 2006.
4. Галатенко В.А. «Основы информационной безопасности». - М.: Интернет-университет информационных технологий, 2004.
5. Галатенко В.А. «Стандарты информационной безопасности». М.: Интернет-университет информационных технологий, 2004.
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. «Технические средства и методы защиты информации». - М.: Машиностроение, 2009.
7. Шаньгин В.Ф. «Защита информации в компьютерных системах и сетях». - М.: ДМК Пресс, 2012.
8. Скиба В.Ю., Курбатов В.А. «Руководство по защите от внутренних угроз информационной безопасности». - СПб.: Питер, 2008.
9. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013.
10. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010.
11. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010.
12. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013.
13. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012.
14. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012.
15. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010.
16. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013.
17. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008.
18. *Гафнер В.В.* Информационная безопасность: учеб. пособие. – Ростов на Дону: Феникс, 2010.
19. *Малюк А.А.* Теория защиты информации. — М.:Горячая линия - Телеком, 2012.
20. *Щербаков А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
21. *Борисов М. А.* Особенности защиты персональных данных в трудовых отношениях. (Гриф УМО по дополнительному профессиональному образованию) М.: Книжный дом «ЛИБРОКОМ», 2013.
22. *Жданов О. Н., Чалкин В. А.* Эллиптические кривые: Основы теории и криптографические приложения. М.: Книжный дом «ЛИБРОКОМ», 2013.
23. *Борисов М. А., Заводцев И. В., Чижов И. В.* Основы программно-аппаратной защиты информации. (Гриф УМО по классическому университетскому образованию). Изд.2 М.: Книжный дом «ЛИБРОКОМ», 2013.
24. *Борисов М. А., Романов О. А.* Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). №2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014.
25. *Применко Э. А.* Алгебраические основы криптографии. №9. Изд.стереотип. М.: Книжный дом «ЛИБРОКОМ», 2014.
26. *Гуров С. И.* Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. Изд.2. М.: Книжный дом «ЛИБРОКОМ», 2013.

27. *Исамидинов А. Н.* Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.

Разработчики программы

Пышкина Н.Ю. – выпускник ЯГПУ им. Ушинского, профессиональная переподготовка по курсу Информационная безопасность – Национальный Открытый Университет «Интуит».

Лазарев И.В. – выпускник Ярославского государственного университета им. П.Г. Демидова, математический факультет, специальность – компьютерная безопасность.

Боровиков К.С. - выпускник Ярославского государственного университета им. П.Г. Демидова, математический факультет, специальность – компьютерная безопасность.