Саровский физико-технический институт – филиал федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский ядерный университет «МИФИ» **(СарФТИ НИЯУ МИФИ)**

УТВЕРЖДАЮ

Руководитель СарФТИ НИЯУ МИФИ

_____ Сироткина А.Г.

«_____» _____ 2015 г.

ОПИСАНИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«Безопасность информационно-технических систем»

(наименование программы)

Укрупненная группа направлений подготовки
10.03.01. Информационная безопасность

(направление)

Общие положения

Целью профессиональной переподготовки по направлению **"Безопасность информационно-технических систем"** является подготовка современного специалиста в области обеспечения информационной безопасности и комплексной защиты объектов информатизации.

Категория слушателей: профессорско-преподавательский состав вуза, руководители и специалисты структур, занимающихся организацией учебного процесса в вузе

Срок обучения: 360 часов (10 з.е.)
Режим занятий: 14 часов в неделю без отрыва от производства

Разработчик программы: Сплюхин Денис Валерьевич, старший преподаватель кафедры радиофизики и электроники СарФТИ НИЯУ МИФИ

Компетенции, подлежащие формированию по итогам обучения

Категория работника	Вид профессиональной (трудовой) деятельности	Компетенции/ готовность к выполнению трудовых действий в разрезе видов профессиональной (трудовой) деятельности
Профессорско-преподавательский состав	1. *организационно - управленческая:* • участие в совершенствовании системы управления информационной безопасностью; • осуществление организационно-правового обеспечения информационной безопасности объекта защиты; • организация работы малых коллективов исполнителей с учетом требований защиты информации; • изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны; • контроль эффективности реализации политики информационной безопасности объекта	ПК-14 Способен принимать участие в формировании комплекса мер по обеспечению информационной безопасности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью
		ПК-15 Способен организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации
		ПК-16 Способен изучать и обобщать опыт работы различных учреждений, организаций и предприятий в области повышения эффективности защиты информации
		ПК-20 Способен организовать технологический процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	2. *научно-педагогическая:* • преподавание дисциплин по направлению информационная безопасность в общеобразовательных учреждениях, образовательных учреждениях начального профессионального, среднего профессионального, высшего профессионального и дополнительного профессионального образования.	ПК-11 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности
		ПК-12 Способен принять участие в совершенствовании и разработке учебно-методического обеспечения дисциплин по направлению информационная безопасность
		ПК-13 Способен преподавать по направлению информационная безопасность в образовательных учреждениях различного уровня, используя существующие программы и учебно-методические материалы

Объем программы и виды учебной работы

Вид учебной работы	Всего часов
Общий объем программы	360
Лекционные занятия	100
Практические занятия	152
Подготовка и защита ВКР	108

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование разделов и тем профессионального модуля	Всего часов	Аудиторное обучение, в том числе		Применяемые образовательные технологии	Форма контроля
			Лекции	Практич. занятия		
Модуль 1. Безопасность информационных технологий						
1.1.	Основы безопасности информационных технологий	36	14	22	Лекция-беседа, тренинг	Участие в дискуссии
1.2.	Обеспечение безопасности информационных технологий	18	8	10	Работа в малых группах предполагает совместную учебно-познавательную и творческую деятельность слушателей в группе	Участие в дискуссии
1.3.	Средства защиты информации от несанкционированного доступа	32	10	22	Работа в малых группах	Ответы на контрольные вопросы
1.4.	Зачет	4	4	-		
	Итого	**90**	**36**	**54**		
Модуль 2. Безопасность компьютерных систем и сетей						
2.1.	Безопасность компьютерных сетей	36	14	22	Работа в малых группах предполагает совместную учебно-познавательную и творческую деятельность слушателей в группе	Участие в дискуссии
2.2.	Анализ защищенности сетей	18	8	10	Работа в малых группах	Ответы на контрольные вопросы

2.3.	Использование электронной подписи и инфраструктуры открытых ключей (PKI)	32	10	22	Работа в малых группах	Ответы на контрольные вопросы
2.4	Зачет	4	4	-		
	Итого	**90**	**36**	**54**		
Модуль 3. Защита персональных данных						
3.1	Основные понятия Федерального закона "О персональных данных"	20	8	12	Лекция-беседа, тренинг, моделирование ситуаций	Участие в дискуссии, Ответы на контрольные вопросы
3.2	Техническая защита персональных данных в информационных системах	32	12	20	Лекция-беседа, тренинг, моделирование ситуаций	Участие в дискуссии, Ответы на контрольные вопросы
3.3	Контроль и надзор за соблюдением законодательства о персональных данных	16	4	12	Работа в малых группах	Индивидуальное собеседование по отчетам практических работ
3.4	Зачет	4	4	-		
	Итого	**72**	**28**	**44**		
Всего		**252**	**100**	**152**		

Форма итоговой аттестации по программе: выполнение и защита аттестационной работы.

Слушателям после успешного окончания обучения (выполнившим все требования учебного плана) выдаются документы установленного образца о повышении квалификации (удостоверение о краткосрочном повышении квалификации)

Кадровое обеспечение образовательного процесса по программе

№ пп.	Фамилия, имя, отчество	Образование (вуз, год окончания, специальность)	Должность, ученая степень, звание. Стаж работы в данной или аналогичной должности, лет	Перечень основных научных и учебно-методических публикаций
Профессорско-преподавательский состав программы				
1.	Сплюхин Денис Валерьевич	Высшее (Пензенский государственный университет, 2014, Информационная безопасность телекоммуникационных систем)	Инженер-исследователь, 6 лет	1. Сплюхин Д.В. и др. Безопасная компоновка криптографических модулей как способ защиты информации. Сборник материалов IX

				НТК молодых специалистов Росатома «Высокие технологии атомной отрасли. Молодежь в инновационном процессе», Нижний Новгород 2014 г. 2. Сплюхин Д.В. и др. Формирование начального заполнения генераторов псевдослучайных последовательностей. Сборник материалов IX научная конференция Волжского регионального центра РАРАН «Современные методы проектирования и отработки ракетно-артиллерийского вооружения», Саров, 2015 г. 3. Сплюхин Д.В. и др. Отчёт о НИР «Разработка программно-математического обеспечения для исследования базовых характеристик, влияющих на функции распределения информационных массивов», ОТН03-2014, 2014 г. 4. Сплюхин Д.В. и др. Отчёт о НИР «Моделирование базовых характеристик, влияющих на функции распределения информационных массивов с помощью программно-математического обеспечения тестирования псевдослучайных последовательностей «Крона», ОТН09-2014, 2014 г.

Содержание модулей

Модуль 1. Безопасность информационных технологий.

Основы безопасности информационных технологий.

Раздел 1. Актуальность проблемы обеспечения безопасности информационных технологий.

Место и роль автоматизированных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.

Раздел 2. Основные понятия в области безопасности информационных технологий.

Что такое безопасность информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты автоматизированных систем и циркулирующей в них информации.

Раздел 3. Угрозы безопасности информационных технологий.

Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений. Основные источники и пути реализации угроз. Классификация угроз безопасности и каналов проникновения в автоматизированную систему и утечки информации. Основные непреднамеренные и преднамеренные искусственные угрозы. Неформальная модель нарушителя.

Раздел 4. Виды мер и основные принципы обеспечения безопасности информационных технологий

Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Основные принципы построения системы обеспечения безопасности информации в автоматизированной системе.

Раздел 5. Правовые основы обеспечения безопасности информационных технологий.

Законы Российской Федерации и другие нормативные правовые акты, руководящие и нормативно-методические документы, регламентирующие отношения субъектов в информационной сфере и деятельность организаций по защите информации. Защита информации ограниченного доступа, права и обязанности субъектов информационных отношений. Лицензирование деятельности, сертификация средств защиты информации и аттестация объектов информатизации. Требования руководящих документов ФСТЭК России и ФСБ России. Вопросы законности применения средств криптографической защиты информации. Ответственность за нарушения в сфере защиты информации.

Раздел 6. Государственная система защиты информации.

Состав государственной системы защиты информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. Финансирование мероприятий по защите информации.

Раздел 7. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.

Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированных систем. Регистрация и оперативное оповещение о событиях безопасности. Криптографические методы защиты информации. Контроль целостности программных и информационных ресурсов. Обнаружение атак. Защита периметра компьютерных сетей. Управление механизмами защиты.

Обеспечение безопасности информационных технологий.

Раздел 1. Организационная структура системы обеспечения безопасности информационных технологий.

Понятие технологии обеспечения безопасности информации и ресурсов в автоматизированной системе. Цели создания системы обеспечения безопасности информационных

технологий. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы. Политика безопасности предприятия. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации. Распределение функций по обеспечению безопасности информационных технологий. Система организационно-распорядительных документов по обеспечению безопасности информационных технологий.

Раздел 2. Обязанности конечных пользователей и ответственных за обеспечение безопасности информационных технологий в подразделениях.

Общие правила обеспечения безопасности информационных технологий при работе сотрудников с ресурсами автоматизированной системы. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения. Порядок работы с носителями ключевой информации.

Раздел 3. Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств автоматизированной системы.

Документы, регламентирующие правила парольной и антивирусной защиты. Инструкции по организации парольной и антивирусной защиты. Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей автоматизированной системы. Инструкция по внесению изменений в списки пользователей. Правила именования пользователей. Процедура авторизации сотрудников. Обязанности администраторов штатных и дополнительных средств защиты.

Раздел 4. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированных систем.

Регламентация процессов обслуживания и осуществления модификации аппаратных и программных средств. Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций. Экстренная модификация (обстоятельства форс-мажор).

Раздел 5. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.

Взаимодействие подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных подсистем.

Раздел 6. Определение требований к защите и категорирование ресурсов.

Положение о категорировании ресурсов. Проведение информационных обследований и анализ подсистем автоматизированной системы как объекта защиты. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Проведение обследований подсистем, инвентаризация, категорирование и документирование защищаемых ресурсов автоматизированных систем.

Раздел 7. Планы защиты и планы обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.

Регламентация действий при возникновении кризисных ситуаций.

Раздел 8. Основные задачи подразделения обеспечения безопасности информационных технологий.

Организация работ по обеспечению безопасности информационных технологий. Организационная структура, основные функции подразделения безопасности.

Раздел 9. Концепция безопасности информационных технологий предприятия.

Документальное оформление вопросов, отражающих официально принятую систему взглядов на проблему обеспечения безопасности информационных технологий, в качестве методологической основы для формирования и проведения в организации единой политики в области обеспечения информационной безопасности для принятия управленческих решений и разработки практических мер по воплощению данной политики в жизнь.

Средства защиты информации от несанкционированного доступа.

Раздел 1. Назначение и возможности средств защиты информации от несанкционированного доступа.

Задачи, решаемые средствами защиты информации от несанкционированного доступа.

Раздел 2. Рекомендации по выбору средств защиты информации от несанкционированного доступа.

Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК России к средствам защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа.

Раздел 3. Аппаратно-программные средства защиты информации от несанкционированного доступа.

Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Существующие средства аппаратной поддержки. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации.

Раздел 4. Возможности применения штатных и дополнительных средств защиты информации от несанкционированного доступа.

Стратегия безопасности и сертифицированные решения Microsoft. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Защита от несанкционированной модификации программ и данных. Защита данных от несанкционированного копирования и перехвата средствами шифрования. Регистрация событий, имеющих отношение к безопасности. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа. Управление средствами защиты.

Модуль 2. Безопасность компьютерных систем и сетей

Безопасность компьютерных сетей

Раздел 1. Проблемы обеспечения безопасности в компьютерных системах и сетях.

Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Сетевые угрозы, уязвимости и атаки. Средства защиты сетей.

Раздел 2. Назначение, возможности, и основные защитные механизмы межсетевых экранов (МЭ).

Назначение и виды МЭ. Основные защитные механизмы, реализуемые МЭ. Основные возможности и варианты размещения МЭ. Достоинства и недостатки МЭ. Основные защитные механизмы: фильтрация пакетов, трансляция сетевых адресов, промежуточная аутентификация, script rejection, проверка почты, виртуальные частные сети, противодействие атакам, нацеленным на нарушение работоспособности сетевых служб, дополнительные функции. Общие рекомендации по применению. Политика безопасности при доступе к сети общего пользования. Демилитаризованная зона. Назначение, особенности и типовая схема "HoneyNet".

Раздел 3. Анализ содержимого почтового и Web-трафика (Content Security).

Системы анализа содержимого. Компоненты и функционирование систем контроля контента (электронная почта и HTTP-трафик). Политики безопасности, сценарии и варианты применения и реагирования.

Раздел 4. Виртуальные частные сети (VPN).

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Структура защищенной корпоративной сети. Варианты, достоинства и недостатки VPN-решений. Общие рекомендации по их применению. Решение на базе ОС Windows 2003. VPN на основе аппаратно-программного комплекса шифрования "Континент". Угрозы, связанные с использованием VPN.

Раздел 5. Антивирусные средства защиты.

Общие правила применение антивирусных средств в автоматизированных системах. Технологии обнаружения вирусов. Возможные варианты размещение антивирусных средств. Антивирусная защита, как средство нейтрализации угроз.

Раздел 6. Обнаружение и устранение уязвимостей.

Назначение, возможности, принципы работы и классификация средств анализа защищенности. Место и роль в общей системе обеспечения безопасности. Сравнение возможностей с межсетевыми экранами. Средства обеспечения адаптивной сетевой безопасности. Варианты решений по обеспечению безопасности сети организации. Обзор средств анализа защищенности сетевого уровня и уровня узла. Специализированный анализ защищенности.

Раздел 7. Мониторинг событий безопасности.

Категории журналов событий. Способы построения, дополнительные компоненты и реализация инфраструктуры управления журналами событий. Технология обнаружения атак. Классификация систем обнаружения атак. Специализированные системы обнаружения атак.

Анализ защищенности сетей

Раздел 1. Терминология.

Понятие уязвимости. Классификация. Источники информации. Каталог уязвимостей CVE. Методы выявления уязвимостей. Системы анализа защищенности. Основные приёмы выявления уязвимостей. Обзор средств анализа защищенности. Варианты классификации.

Раздел 2. Сетевые сканеры безопасности.

Архитектура и принципы работы сканеров сетевого уровня. Методы сканирования на уровне сети. Методы сбора информации о сети. Информация, доступная через Интернет. Программа HTTrack. Foot Printing.

Раздел 3. Идентификация сетевых объектов.

Использование протокола ICMP. Использование протокола UDP. Использование протокола TCP. Использование протокола IP. Идентификация узлов с помощью протокола ARP. Определение топологии сети. Отслеживание маршрутов. Определение топологии сети за пакетным фильтром. Идентификация статуса порта. Способы сканирования портов. Сканирование портов TCP. Сканирование портов UDP. Идентификация сервисов и приложений. Идентификация TCP-служб. Идентификация UDP-служб. Сканирование протоколов. Идентификация операционных систем. Простейшие методы определения ОС. Опрос стека TCP/IP. Инструменты. SinFP. Использование протокола ICMP для идентификации ОС.

Раздел 4. Идентификация уязвимостей по косвенным признакам.

Методы идентификации уязвимостей по косвенным признакам. Баннерные проверки. Сетевые сервисы как объект сканирования. «Локальные» проверки. Сбор информации о Windows-системах. Методы и задачи Passive fingerprinting. Анализ сетевого трафика. Анализ запросов от сканируемого узла. Выявление уязвимостей с помощью тестов. «Эксплойты» и их разновидности. Проблема «отказа в обслуживании». Методы анализа результатов тестирования.

Раздел 5. Сетевой сканер Nessus.

Обзор возможностей. Архитектура сканера. Получение, установка и работа со сканером. Язык описания атак NASL. Структура сценария. Синтаксис языка. Подключаемые библиотеки. Написание пользовательских проверок.

Раздел 6. Примеры средств анализа защищенности.

Сетевой сканер XSpider. Программа Internet Scanner. Анализ защищенности уровня узла. Задачи и инструменты локального сканирования. Контроль целостности. Оценка стойкости паролей. Программа Assuria Auditor. Специализированные средства анализа защищённости. Анализ защищенности СУБД. Уязвимости СУБД. Сканирование СУБД.

Раздел 7. Методология анализа защищенности.

Ethical hacking (Penetration Testing). Разновидности Penetration Testing. Схема Penetration Testing. Централизованное управление уязвимостями. Инвентаризация информационных активов. Мониторинг состояния защищённости. Устранение уязвимостей. Контроль.

Использование электронной подписи и инфраструктуры открытых ключей (PKI)

Раздел 1. Электронные документы.

Угрозы безопасности субъектам электронного документооборота. Модель нарушителя. Электронная подпись. Виды электронной подписи. Правовые вопросы применения ЭП и СКЗИ в России. Особенности юридического определения ЭП. Федеральный закон "Об электронной подписи". Электронная цифровая подпись. Правовые вопросы применения ЭЦП и СКЗИ в России. Особенности юридического определения ЭЦП. Федеральный закон "Об электронной цифровой подписи".

Раздел 2. Криптографические методы защиты информации.

Криптография с симметричными ключами. Криптография с открытыми ключами. Доверие к открытому ключу и цифровые сертификаты. Электронный сертификат. Структура сертификата. Сертификаты стандарта X.509. Основной контекст сертификата. Расширения сертификатов. Классы сертификатов. Хранилища сертификатов. Закрытые ключи, риски использования по умолчанию. КриптоАРМ. Создание самоподписанного сертификата. Анализ сертификата. Импорт и экспорт сертификатов. Криптопровайдеры. Набор CSP (Cryptographic Service Provider) по умолчанию. Microsoft CSP.

Раздел 3. Создание электронной подписи. Установка и эксплуатация “КриптоАРМ”, “КриптоТри”. Электронные ключи eToken. Модели eToken. Российская криптография в eToken ГОСТ. Установка и настройка различных моделей eToken. Настройка параметров. Режимы работы. Получение сертификата с использованием электронных ключей eToken. Электронная подпись для Apple iOS. Решения и технологии применения российской криптографии для электронной подписи на iPad и iPhone. Электронные идентификаторы Рутокен. Модели Рутокен. Российская криптография в Рутокен ЭЦП. Рутокен Web. Установка и настройка различных моделей Рутокен. Настройка параметров. Режимы работы. Получение сертификата с использованием электронных ключей Рутокен.

Раздел 4. КриптоПро CSP.

Основные характеристики. Реализуемые алгоритмы. Установка. Настройка параметров. Получение сертификатов с использованием средства криптографической защиты "СКЗИ КриптоПро". Функциональный ключевой носитель. КриптоПро УЭК CSP. Практика применения КриптоПро eToken CSP и КриптоПро Рутокен CSP. КриптоПро OCSP Server. Краткое описание протокола Online Certificate Status Protocol (OCSP). Установка КриптоПро OCSP Server. Создание экземпляра Службы. Управление операторами Службы. Запуск Службы. Установка модуля поддержки OCSP. КриптоПро Revocation Provider. Ключевые особенности. Установка Revocation Provider. Как работает Revocation Provider. КриптоПро TSP Server. Для чего нужны штампы времени. Краткое описание протокола Time Stamping Protocol (TSP). Установка КриптоПро TSP Server. Запуск Службы. Установка модуля поддержки TSP КриптоАРМ. Усовершенствованная подпись КриптоПро. Доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент. Проверка подлинности ЭП/ЭЦП без сетевых обращений. Архивное хранение электронных документов. Формат усовершенствованной электронной цифровой подписи. Технологические процедуры создания усовершенствованной ЭП/ЭЦП. Проверка усовершенствованной ЭП/ЭЦП.

Раздел 5. Проблемы безопасности при применении электронных подписей.

Интернет-банкинг. Примеры атак на системы дистанционного банковского обслуживания. Обзор типовых методов атак на счета клиентов систем ДБО. Визуальный контроль содержания передаваемых в смарт-карту данных. Применение устройств доверенного ввода информации для защиты платежей. Просмотр содержания подписываемых до-

кументов в доверенной среде. Web-порталы и облачные сервисы. Особенности применения электронной подписи в решениях с облачной архитектурой. Квалифицированная электронная подпись. Неквалифицированная электронная подпись. Применение технологии OTP для защиты решений с использованием электронных подписей.

Раздел 6. Компоненты PKI.

Орган сертификации. Орган регистрации. Хранилище. Архив. Пользователи инфраструктуры. Принципы доверия PKI. Иерархическая модель доверительных отношений. Сетевая модель доверительных отношений. Регулируемые доверительные отношения. Базовые ограничения. Ограничения по именам. Ограничения по политике выдачи сертификатов. Ограничения по политике приложений. Получение и регистрация частного номера организации. Формирование объектных идентификаторов областей применения сертификатов открытых ключей. Регулируемые доверительные отношения.

Раздел 7. Эксплуатация PKI.

Создание файла конфигурации для корневого центра сертификации (ЦС). Установка и настройка корневого ЦС. Публикация списков отозванных сертификатов корневого ЦС. Установка подчиненного ЦС. Настройка WEB-интерфейса подчиненного ЦС. Проверка подлинности цифровых сертификатов в инфраструктуре Windows PKI. Процедуры сличения. Стандартная процедура обработки цепочки сертификатов. Обработка цепочки списков CTL. Обработка цепочки кросс-сертификатов. Получение сертификата пользователя. Организация защищенной электронной почты. Процедуры аннулирования сертификатов в Windows PKI. Списки аннулированных сертификатов (Certificate Revocation List, CRL). Риски, связанные с технологией CRL.

Модуль 3. Защита персональных данных

Основные понятия Федерального закона "О персональных данных"

Раздел 1. Введение. Персональные данные в организации.

Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни. Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных. Персональные данные в системе документооборота предприятия. Персональные данные в автоматизированных системах и приложениях. Значимые утечки персональных данных в России.

Раздел 2. Основные понятия Федерального закона "О персональных данных".

Содержание категории "персональные данные". Область применения закона. Ограничения. Обработка персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. Согласие в письменной форме. Общедоступные, подлежащие опубликованию или обязательному раскрытию персональные данные. Биометрические персональные данные. Обязанности оператора персональных данных. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных законом. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Ответственность за нарушение требований по обращению с персональными данными. Практика правоприменения.

Раздел 3. Работа с персональными данными на предприятии (в организации).

Мероприятия по защите сведений ограниченного доступа. Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства. Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением. Локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законода-

тельства, устранение последствий таких нарушений, их содержание, порядок разработки и ввода в действие. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

Техническая защита персональных данных в информационных системах.

Раздел 1. Требования Федерального закона "О персональных данных" и Постановления Правительства РФ 2012 г. № 1119 к обеспечению безопасности персональных данных.

Уровни защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) в зависимости от угроз безопасности этим данным, категорий персональных данных и количества субъектов, чьи данные обрабатываются в ИСПДн. • Модель угроз персональным данным. Базовая модель угроз. Перечень источников угроз. Уровень исходной защищенности. Методика актуализации угроз.

Раздел 2. Каналы утечки информации при обработке персональных данных в информационных системах.

Построение системы защиты персональных данных. Положения Приказа ФСТЭК 2013 г. № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", определение базовых, адаптивных и компенсирующих мер защиты.

Раздел 3. Лицензирование деятельности по технической защите конфиденциальной информации.

Понятие технической защиты как лицензируемого вида деятельности. Лицензионные требования. Ответственность за незаконную деятельность в области защиты информации. Незаконное предпринимательство. Оценка и управление риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации.

Контроль и надзор за соблюдением законодательства о персональных данных.

Раздел 1. Аутсорсинг обработки персональных данных и их технической защиты.

Требования, выдвигаемые законом к порядку обработки персональных данных внешней организацией, содержание договора на обработку персональных данных. Передача внешней организации функций технической защиты персональных данных. Передача внешней организации функций лица, ответственного за организацию обработки персональных данных. Достоинства и недостатки аутсорсинга обработки персональных данных и их защиты.

Раздел 2. Система государственного контроля и надзора за обеспечением безопасности персональных данных.

Область применения Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении госконтроля (надзора) и муниципального контроля" и регулируемые им вопросы. Принципы защиты прав юридических лиц, индивидуальных предпринимателей при осуществлении государственного контроля (надзора). Порядок планирования, организации и проведения проверок. Права и обязанности проверяемых и проверяющих. Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений.

Подготовка и защита выпускной квалификационной работы

5. ТРЕБОВАНИЯ К ОЦЕНКЕ КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММ

Формы и методы контроля и оценки результатов освоения модулей

Наименование модулей	Основные показатели оценки	Формы и методы контроля и оценки
Модуль 1. **Безопасность информационных технологий**	Проходной уровень освоения содержания модуля не менее 60%	*Устный опрос* *Зачет*
Модуль 2. **Безопасность компьютерных систем и сетей**	Проходной уровень освоения содержания модуля не менее 60%	*Выполнение практических заданий по тематике модуля* *Зачет*
Модуль 3. **Защита персональных данных**	Проходной уровень освоения содержания модуля не менее 60%	*Выполнение практических заданий по тематике модуля* *Зачет*
Итоговая аттестация	Проходной уровень освоения содержания программы не менее «удовлетворительно»	Защита выпускной квалификационной работы

Примерные темы ВКР и минимальные требования к ним

1) Теоретико-оценочная работа, представляющая собой анализ части одного из изучаемых криптографических алгоритмов с использованием методов анализа, рассмотренных в процессе изучения дисциплины;
2) Схемотехническая реализация, представляющая собой разработку аппаратной составляющей одного из изучаемых криптографических алгоритмов;
3) Программная реализация, представляющая собой разработку программного модуля, реализующего функции одно из изучаемых криптографических алгоритмов.

Работа выполняется на основе выданного преподавателем индивидуального для каждого слушателя задания.

Рекомендуемые программные средства: операционная система Windows XP и дополнения к ней в виде SP3, Microsoft Office Project (v.2007 SP3), авторское ПО.

По завершению выпускной аттестационной работы слушатели должны продемонстрировать результаты проведенной ими работы.