МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Пензенский государственный университет»
(ФГБОУ ВО «ПГУ»)

УТВЕРЖДАЮ
Ректор ПГУ
А.Д.Гуляков
«02.11» 2020 г.

РАБОЧАЯ ПРОГРАММА

дополнительной профессиональной программы
повышения квалификации

Управление информационной безопасностью объекта. Методы и средства обеспечения информационной безопасности

Наименование программы

Пенза 2020

1. Общая характеристика программы

1.1. Цель реализации программы

Целью повышения квалификации по данной специальности является актуализация профессиональных компетенций у обучаемых, связанных с применением программно-аппаратных средств защиты информации для защиты информации автоматизированных систем в области цифровой экономики..

1.2. Категория слушателей

Руководители и сотрудники государственных, муниципальных органов, органов местного самоуправления, организаций различных форм собственности, физические лица, организующие и (или) осуществляющие деятельность по защите информации автоматизированных систем с использованием программно-аппаратных средств защиты информации, руководители и сотрудники департаментов (отделов, служб) IT и информационной безопасности, специалисты по защите информации, знающие основы информационных технологий, имеющие навыки работы на персональном компьютере в ОС MS Windows, Linux, MacOS и имеющие навыки работы с офисными пакетами MS Office 2010 или выше, Libre Office 6.0 и выше.

1.3. Трудоемкость обучения

Нормативный срок освоения программы – 72 часа, включая все виды аудиторной и самостоятельной учебной работы слушателей.

Учебная нагрузка устанавливается не более 36 часов в неделю, включая все виды аудиторной и внеаудиторной учебной работы слушателя.

1.4. Форма обучения и форма организации образовательной деятельности

Форма обучения: очно-заочная.

Продолжительность учебной недели составляет: по очно-заочной форме обучения – 6 дней.

Программа реализуется с использованием дистанционных образовательных технологий.

2. Формализованные (планируемые) результаты освоения программы

Слушатель в результате освоения программы должен развить (актуализировать) следующие профессиональные компетенции:

– ПК-1 – способность обеспечить эффективное применение систем и средств защиты информации автоматизированной системы и их работоспособность при возникновении нештатных ситуаций;

– ПК-2 – способность администрировать подсистему защиты информации автоматизированной системы;

– ПК-3 – способность управлять защитой информации в автоматизированных системах.

3. Содержание программы

3.1. Календарный учебный график

Образовательный процесс по программе может осуществляться в течение всего учебного года.

Занятия проводятся по мере комплектования групп.

График обучения / Форма обучения	**Ауд. часов в день**	**Дней в неделю**	**Общая продолжительность программы (дней, недель, месяцев)**
очно-заочная	4	2	2 недели

3.2. Учебный план.

№ п/п	Наименование учебных модулей	ОТ, час	Аудиторные занятия, электронное обучение ДОТ, час		Сам. раб. час
			Лекционные занятия	Практические занятия	
1.	Система управления информационной безопасностью организации	6	3	–	3
2.	Система защиты информации Secret Net Studio	13	3	4	6
3.	ПАК СЗИ от НСД Аккорд. Структура и применение ПАК СЗИ от НСД «Аккорд»	15	4	4	7
4.	Основные компоненты и защитные механизмы программного комплекса DeviceLock	8	2	2	4
5.	Структура и принципы функционирования систем контроля и предотвращения утечек информации	12	2	4	6
6.	Администрирование подсистемы антивирусной безопасности	16	4	4	8
	Итоговая аттестация	2	–	–	2
ИТОГО		72	18	18	36

3.3. Содержание учебных дисциплин (модулей)

№ п/п	**Наименование учебных модулей**	**Содержание**
1	**Система управления информационной**	Цель управления информационной безопасностью объекта.

№ п/п	Наименование учебных модулей	Содержание
	безопасностью объекта	Модель системы управления информационной безопасностью объекта. Процессы управления информационной безопасностью. Цели, назначение, результаты.
	Самостоятельная работа слушателя	Выполнение контрольного теста по материалам лекционных занятий.
2	**Система защиты информации Secret Net Studio**	Состав устанавливаемых компонентов СЗИ Secret Net Studio. Режимы работы: автономный и сетевой. Управление функционированием СЗИ Secret Net Studio. Функциональные компоненты СЗИ Secret Net Studio. Механизмы защиты, реализуемые СЗИ Secret Net Studio. Применение СЗИ Secret Net Studio для реализации мер защиты, установленных Приказами ФСТЭК России №17 от 11.02.2013 и №21 от 18.02.2013
	Практическое занятие	Управление доступом к защищаемым ресурсам посредством применения СЗИ Secret Net Studio с имитацией событий НСД.
	Самостоятельная работа слушателя	Подготовка отчета о выполнении практического задания. Выполнение контрольного теста по материалам лекции и практического занятия.
3	**ПАК СЗИ от НСД Аккорд. Структура и применение ПАК СЗИ от НСД «Аккорд»**	Назначение и применение СЗИ от НСД «Аккорд». Аппаратные и программные компоненты СЗИ от НСД «Аккорд». Правила разграничения доступа (ПРД) к объектам доступа. Построение изолированной программной среды. Подсистема регистрации событий. Применение СЗИ от НСД «Аккорд» для реализации мер защиты, установленных Приказами ФСТЭК России №17 от 11.02.2013 и №21 от 18.02.2013.
	Практическое занятие	Управление доступом к защищаемым ресурсам посредством применения СЗИ от НСД «Аккорд» с имитацией событий НСД.
	Самостоятельная работа слушателя	Подготовка отчета о выполнении практического задания. Выполнение контрольного теста по материалам лекции и практического занятия.
4	**Основные компоненты и защитные механизмы программного комплекса DeviceLock**	Назначение ПК DeviceLock. Основные компоненты, входящие в состав ПК DeviceLock. Основные функциональные возможности ПК DeviceLock.
	Практическое занятие	Разграничение доступа к устройствам и портам ввода-вывода в ПК DeviceLock. Анализ записей в журнале регистрации событий.
	Самостоятельная работа слушателя	Подготовка отчета о выполнении практического задания. Выполнение

№ п/п	Наименование учебных модулей	Содержание
		контрольного теста по материалам лекции и практического занятия.
5	**Структура и принципы функционирования систем контроля и предотвращения утечек информации**	Общая характеристика систем контроля и предотвращения утечек информации. Структура и функциональные возможности систем контроля и предотвращения утечек информации. Контролируемые каналы утечки информации. Методы анализа информации при контроле каналов передачи. Возможности применения систем контроля и предотвращения утечек информации для реализации мер защиты, установленных Приказами ФСТЭК России №17 от 11.02.2013 и №21 от 18.02.2013.
	Практическое занятие	Применение программного комплекса DeviceLock для предотвращения утечек информации при доступе к устройствам с использованием правил контентного анализа.
	Самостоятельная работа слушателя	Подготовка отчета о выполнении практического задания. Выполнение контрольного теста по материалам лекции и практического занятия.
6	**Администрирование подсистемы антивирусной безопасности**	Классификация методов и средств обеспечения антивирусной безопасности. Основные виды вредоносного программного обеспечения. Архитектура и основные компоненты подсистемы антивирусной безопасности с сетевым центром управления. Требования к реализации антивирусной защиты. Процессы управления подсистемой антивирусной безопасности.
	Практические занятия	Применение средств антивирусной безопасности с сетевым центром управления для администрирования подсистемы антивирусной безопасности
	Самостоятельная работа слушателя	Подготовка отчета о выполнении практического задания. Выполнение контрольного теста по материалам лекции и практического занятия.
Используемые образовательные технологии		В преподавании курса частично используется электронной обучение и дистанционные образовательные технологии.

3.4. Требования к итоговой аттестации

Итоговая аттестация производится в форме тестирования.

Зачет выставляется, если слушатель:

– владеет материалом в пределах программы курса, обладает достаточными знаниями для прохождения тестирования;

– правильность ответов должна быть не менее 60% от общего количества вопросов.

Лицам, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Лицам, не прошедшим итоговой аттестации или получившем на итоговой аттестации неудовлетворительные результаты, выдается справка об обучении.

Вопросы для подготовки к итоговой аттестации

1. Цель управления информационной безопасностью организации.
2. Модель системы управления информационной безопасностью объекта.
3. Требования к документации системы управления информационной безопасностью объекта.
4. Управление рисками информационной безопасностью объекта.
5. Процессы оценки информационной безопасности объекта.
6. Состав программно-аппаратного комплекса (ПАК) СЗИ от НСД «Аккорд». Основные функции.
7. Реализация дискреционного механизма разграничения доступа в ПАК СЗИ от НСД «Аккорд».
8. Реализация мандатного механизма разграничения доступа в ПАК СЗИ от НСД «Аккорд».
9. Реализация изолированной программной среды в ПАК СЗИ от НСД «Аккорд».
10. Реализация подсистемы регистрации событий в ПАК СЗИ от НСД «Аккорд».
11. Функциональный компонент ПО «Secret Net Studio – Клиент», осуществляющий управление защитными подсистемами и компонентами, а также обеспечивает их взаимодействие. Его функциональные возможности.
12. Программный компонент СЗИ Secret Net Studio, устанавливаемый на защищаемых компьютерах (АРМ пользователей). Его назначение и функциональные возможности.
13. Программный компонент СЗИ Secret Net Studio, реализующий централизованное управление ПО «Secret Net Studio – Клиент» в сетевом режиме функционирования. Его задачи и функциональные возможности.
14. Действия, выполняемые СЗИ Secret Net Studio при осуществлении пользователем попытки НСД к защищаемым ресурсам.
15. Назначение программного комплекса DeviceLock. Функциональные модули, входящие в состав ПК DeviceLock. Базисный компонент.
16. Программный комплекс DeviceLock. Контроль доступа к устройствам: алгоритм контроля, настройка разрешений.
17. Программный комплекс DeviceLock. Управление и настройка списка администраторов. Защита от локального администратора.
18. Программный комплекс DeviceLock. Функциональные возможности.

19. Общая характеристика систем контроля и предотвращения утечек информации. Контролируемые каналы утечки информации.
20. Системы контроля и предотвращения утечек информации. Типовая структура. Основные компоненты.
21. Методы анализа содержимого информации, передаваемой по информационным каналам.
22. Применение контроля и предотвращения утечек информации для реализации мер защиты информации, установленных Приказами ФСТЭК России №17 от 11.02.2013 и №21 от 18.02.2013.
23. Основные виды вредоносного программного обеспечения.
24. Методы и средства обеспечения антивирусной безопасности.
25. Архитектура и основные компоненты подсистемы антивирусной безопасности с сетевым центром управления.
26. Основные требования к реализации антивирусной защиты.
27. Основные процессы управления подсистемой антивирусной безопасности

4. Условия реализации программы

4.1. Материально-технические условия реализации

Занятия проводятся в открытой образовательной среде ЭИОС ПГУ.

4.2. Учебно-методическое обеспечение программы

а) Основные источники:

1 Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=52182.— «БИБЛИОКОМПЛЕКТАТОР»

2 Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие – Москва : ДМК Пресс, 2014. – 702 с.

3 Семь безопасных информационных технологий: учеб. / А.В. Барабанов [и др.]. – Москва : ДМК Пресс, 2017. – 224 с.

4 Прокушев Я.Е. Программно-аппаратные средства защиты информации: Учебное пособие / Прокушев Я.Е. – СПб.: Интермедия, 2017. – 160 с.

5 Бирюков, А.А. Информационная безопасность: защита и нападение – Москва: ДМК Пресс, 2017. – 434 с.

6 Савельев А.О. Решения Microsoft для виртуализации ИТ-инфраструктуры предприятий / Савельев А.О. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 284 с.

7 Коробко, И.В. PowerShell как средство автоматического администрирования – Москва: ДМК Пресс, 2012. – 224 с.

8 Аппаратно-программные средства защиты информации: практикум / [сост. А.В. Душкин, А.С. Дубровин, В.В. Здольник, В.И.

Новосельцев, А.С. Кольцов, А.С. Кравченко, С.Л. Сахаров, В.И. Сумин] ; ФКОУ ВО Воронежский институт ФСИН России. - Воронеж : Издательско-полиграфический центр «Научная книга», 2017. - 198 с.

б) дополнительные источники

1 Обеспечение информационной безопасности бизнеса/ В.В. Андрианов, С.Л. Зефиров, В.Б. Голованов, Н.А. Голдуев; Под ред.А.П. Курило – М.: Издательство Альпина Паблишерз, 2011 – 373 с.

2 Нестеров, С.А. Основы информационной безопасности: учеб. пособие – Санкт-Петербург : Лань, 2017. – 324 с.

3 Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях: учеб. пособие – Москва: ДМК Пресс, 2012. – 592 с.

4 Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс]. – Электрон. текстовые данные. – 2013. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17, Загл. с экрана.

5 Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375). [Электронный ресурс]. – Электрон. текстовые данные. – 2013. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/692-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21, Загл. с экрана.

6 Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014). [Электронный ресурс]. – Электрон. текстовые данные. – 2014. Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument, Загл. с экрана.

7 Леандро, К. Windows Server 2012 Hyper-V. Книга рецептов – Москва : ДМК Пресс, 2013. – 302 с.

8 ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.

9 ГОСТ Р ИСО/МЭК 17203-2013 Информационная технология. Спецификация открытого формата визуализации (OVF).

10 Применение программно-аппаратных комплексов средств защиты информации от несанкционированного доступа семейства «АККОРД»: метод. указания к лабораторным работам / сост. А.П. Иванов. – Пенза: Изд-во ПГУ, 2011. – 92 с.

в) электронные и Интернет-ресурсы

1 www.securitycode.ru – официальный ресурс ООО «Код безопасности» (СЗИ Secret Net Studio)

2 www.accord.ru – официальный ресурс ОКБ САПР (СЗИ от НСД Аккорд)

3 www.devicelock.ru – официальный ресурс компании Смарт Лайн Инк (СЗИ DeviceLock)

4 http://dlp-expert.ru – ресурс, посвященный DLP-системам (системам контроля и предотвращения утечек информации)

5 www.cnews.ru – ресурс, содержащий материалы об информационных технологиях и обеспечении ИБ

6 www.servernews.ru – ресурс, содержащий информационные материалы о средствах ИТ и средствах обеспечения ИБ

7 https://support.kaspersky.ru/corporate – База знаний по продуктам для бизнеса

8 https://download.drweb.ru/doc/ - документация по продуктам Dr.Web

9 www.fstec.ru – сайт ФСТЭК РФ

10 https://www.microsoft.com/ru-ru/learning/virtualization-training.aspx – официальный ресурс компании Microsoft. Учебные курсы по виртуализации и учебные материалы от компании Microsoft.

5. Кадровое обеспечение программы

Образовательный процесс по модулям обеспечивается научно-педагогическими кадрами, имеющими базовое образование, соответствующее профилю модулю или опыт деятельности в соответствующей профессиональной сфере и систематически занимающимися научно-методической деятельностью.

6. Разработчики программы

Программу подготовили

Заведующий кафедрой «ИБСТ» _____ С.Л. Зефиров

Доцент кафедры «ИБСТ» _____ А.Г. Фатеев

Доцент кафедры «ИБСТ» _____ А.П. Иванов

Доцент кафедры «ИБСТ» _____ О.В. Липилин

СОГЛАСОВАНО

Директор МРЦПК и ДО _____ В.В. Сазонов