28.04.21 04.08-12/24

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

Институт современных образовательных технологий (ИСОТ)

УТВЕРЖДАЮ
Первый проректор-проректор
по учебной работе
_____Б.В. Падалкин
«28» 04 2021 г.

Дополнительное профессиональное образование

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Защищенные операционные системы

Регистрационный № 210407

Авторы программы:
д.ф.-м.н., доцент Басараб М.А.
Глинская Е.В.

Москва, 2021

СОГЛАСОВАНО:

Декан факультета Информатика и системы управления
МГТУ им. Н.Э. Баумана
д.т.н., профессор _____А.В. Пролетарский
_____(дата)

Начальник УМО ИСОТ
МГТУ им. Н.Э. Баумана _____А.Н. Козлова
01.04.2021 (дата)

Оглавление

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ 4
1.1. Цель ДПП 4
1.2. Планируемые результаты обучения 4
1.3. Дополнительные характеристики ДПП 4
1.4. Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения. Характеристика компетенций, подлежащих совершенствованию, и/или перечень новых компетенций, формирующихся в результате освоения программы 5
1.5. Соответствие видов деятельности и профессиональных компетенций и их составляющих 5
2. УЧЕБНЫЙ ПЛАН ДПП 6
2.1. Категория слушателей ДПП 6
2.2. Общая трудоёмкость программы, аудиторная и самостоятельная работа 6
2.3. Форма обучения 6
2.4. Учебный план 6
3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК 6
4. РАБОЧАЯ ПРОГРАММА ДПП 7
4.1. Рабочая программа модуля 7
5. УСЛОВИЯ РЕАЛИЗАЦИИ ДПП 9
5.1. Организационные условия реализации ДПП 9
5.2. Педагогические условия реализации ДПП 9
5.3. Учебно-методическое обеспечение ДПП 9
5.4. Методические рекомендации 10
6. ФОРМЫ ИТОГОВОЙ АТТЕСТАЦИИ ДПП 10
7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ИТОГОВОЙ АТТЕСТАЦИИ 11
7.1. Паспорт комплекта оценочных средств 11
7.2. Комплект оценочных средств 12
8. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ 14

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

Дополнительная профессиональная программа (ДПП) «Защищенные операционные системы» подготовлена на основе:

- Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- требований Приказа Минобрнауки России от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- методических рекомендаций-разъяснений Минобрнауки России по разработке дополнительных профессиональных программ на основе профессиональных стандартов от 22 апреля 2015 г. № ВК-1030/06;
- требований Приказа Министерства науки и высшего образования Российской Федерации от 19.10.2020 г. № 1316 «Об утверждении Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности».

Реализация ДПП направлена на совершенствование имеющихся и/или получение новых компетенций, необходимых для профессиональной деятельности и повышения профессионального уровня в рамках имеющейся квалификации.

1.1. Цель ДПП

Целью ДПП является: знакомство с основными методами и средствами обеспечения защиты информации при проектировании и использовании операционных систем, с основными теоретическими и практическими подходами к обеспечению безопасности информации в автоматизированных системах, использующих современные сетевые операционные системы.

Сформировать у слушателей необходимые компетенции в области обеспечения защиты современных операционных систем.

1.2. Планируемые результаты обучения

Планируемые результаты обучения по ДПП:

- успешное освоение профессиональных компетенций в процессе изучения перечисленных в учебном плане тем;
- успешное освоение программы повышения квалификации;
- успешное прохождение итоговой аттестации (зачет) и получение удостоверения о повышении квалификации по ДПП «Защищенные операционные системы».

1.3. Дополнительные характеристики ДПП

Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения, определен приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» (зарегистрировано в Минюсте России 28 сентября 2016 г., № 43857), регистрационный номер 843.

Наименование вида профессиональной деятельности: Обеспечение безопасности информации в автоматизированных системах (код 06.033).

Обобщенная трудовая функция: Разработка систем защиты информации автоматизированных систем.

Трудовая функция: Разработка проектных решений по защите информации в автоматизированных системах (D/02.7).

1.4. Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в результате обучения. Характеристика компетенций, подлежащих совершенствованию, и/или перечень новых компетенций, формирующихся в результате освоения программы

Реализация ДПП направлена на совершенствование имеющихся и/или получение новых компетенций, необходимых для профессиональной деятельности и повышения профессионального уровня в рамках имеющейся квалификации.

Профессиональные компетенции (ПК) базируются на основании Приказа Министерства образования и науки Российской Федерации от 01 декабря 2016 г. № 1513 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)» (зарегистрировано 20 декабря 2016 г, регистрационный № 44823).

Перечень профессиональных компетенций:

– способность разрабатывать программы и методики испытаний программных, программно-технических и технических средств и систем обеспечения информационной безопасности (ПК-4);

– способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества (ПК-5).

1.5. Соответствие видов деятельности и профессиональных компетенций и их составляющих

Трудовые функции			
Разработка проектных решений по защите информации в автоматизированных системах (D/02.7)			
Профессио-нальные компетенции	**Практический опыт**	**Умения**	**Знания**
ПК-4 **ПК-5**	Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах. Разработка моделей автоматизированных систем и подсистем безопасности автоматизированных систем	Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы. Применять действующую нормативную базу в области обеспечения защиты информации. Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации.	Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов. Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем.

2. УЧЕБНЫЙ ПЛАН ДПП

2.1. Категория слушателей ДПП

Для освоения ДПП допускаются лица, имеющие высшее образование уровня специалитет или магистратура в области информационной безопасности и/или освоившие дополнительное профессиональное образование в области информационной безопасности и имеющие практические навыки в данной области.

Программа так же будет интересна лицам, претендующим на должности: ведущий инженер-разработчик систем защиты информации, ведущий специалист по защите информации, руководитель проектов в области разработки систем защиты информации, руководитель отдела систем защиты информации, главный специалист по защите информации, руководитель отдела систем защиты информации, заместитель руководителя департамента (отдела) исследований и разработок, руководитель департамента (отдела) исследований и разработок.

2.2. Общая трудоёмкость программы, аудиторная и самостоятельная работа

Общая трудоемкость программы составляет 68 часов, из них 56 часов аудиторной работы и 12 часов самостоятельной работы.

2.3. Форма обучения

ДПП «Защищенные операционные системы» реализуется по очной форме обучения, возможна реализация программы с применением дистанционных образовательных технологий.

2.4. Учебный план

ДПП «Защищенные операционные системы» реализуется одним модулем.

№ п/п	Наименование тем	Всего, час	В том числе			Форма контроля
			Лекции	Практические занятия	Самостоятельная работа	
1.	Подсистемы безопасности оценки соответствия	34	20	8	6	–
2.	Средства обеспечения безопасности в оценке соответствия	34	20	8	6	–
Итоговая аттестация		68	40	16	12	зачет

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование тем	1 день	2 день	3 день	4 день	5 день	6 день	7 день	8 день
1.	Подсистемы безопасности оценки соответствия								
2.	Средства обеспечения безопасности в оценке соответствия								
Итоговая аттестация									

Минимальный срок освоения ДПП – 8 дней.

4. РАБОЧАЯ ПРОГРАММА ДПП

4.1. Рабочая программа модуля

4.1.1. Цель изучения модуля: изучение основных методов и средств обеспечения защиты информации при проектировании и использовании операционных систем, знакомство с основными теоретическими и практическими подходами к обеспечению безопасности информации в автоматизированных системах, использующих современные сетевые операционные системы.

4.1.2. Задачи изучения модуля:

- ознакомиться с терминологическим аппаратом по безопасности операционных систем, общих принципов защиты операционных систем;
- получить представления о возможных угрозах операционным системам;
- изучить нормативные требования и руководящие документы по обеспечению безопасности операционных систем;
- обучить слушателей методикам проведения мероприятий защиты операционных систем;
- ознакомиться с терминологическим аппаратом по безопасности систем баз данных, принципов защиты баз данных;
- получить представление о возможных угрозах системам баз данных;
- изучить нормативные требования к обеспечению безопасности систем баз данных;
- обучить слушателей методикам проведения мероприятий по защите систем баз данных.

4.1.3. Планируемые результаты обучения

Процесс изучения учебной дисциплины направлен на формирование следующих ПК:

Код компетенции	**Перечень планируемых результатов обучения по дисциплине**	**Формы и методы обучения, способствующие формированию и развитию компетенции**
ПК-4 **ПК-5**	***Знать:*** – критерии оценки эффективности защищенности; – типы и виды программных и программно-аппаратных систем защиты информации; – аппаратно-программные средства криптографической защиты информации; – методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; – физические основы образования технических каналов утечки информации; – назначение, принципы работы средств новых информационных технологий; – основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. ***Уметь:*** – производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; – осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;	Лекционные и практические занятия, самостоятельная работа с источниками информации и материалами аудиторных занятий

	– обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; – организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. ***Владеть:*** – навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; – навыками сопровождения программно-аппаратных средств защиты информации; – навыками применения современных информационных технологий к текущим реальным ситуациям, основными классификациям информационных систем, навыками развертывания основных программных комплексов и программ, реализующих ту или иную информационную технологию.	

4.1.4. Содержание модуля

Тема 1. Подсистемы безопасности оценки соответствия

Лекции (20 ч.). Определение оценки соответствия (ОС). Виды процедур оценки соответствия технических систем. Испытания. Аттестационные испытания. Тестирование программных средств. Аудит информационной безопасности. Анализ риска информационной безопасности. Определение сертификации средств защиты информации. Правила и участники сертификации средств защиты информации. Законодательно-правовые основы сертификации. Традиционные руководящие документы Гостехкомиссии России.

Классы защищенности средств вычислительной техники. Классы защищенности межсетевых экранов. Классы защищенности автоматизированных систем. Контроль отсутствия не декларированных возможностей. Требования к защите персональных данных. Требования к защите информационных систем общего пользования. Общие критерии оценки безопасности информационных технологий. Модель критериев оценки безопасности информационных технологий. Функциональные требования безопасности. Требования доверия к безопасности. Общая методология оценки безопасности информационных технологий.

Современные нормативные документы ФСТЭК России. Требованияк системам обнаружения вторжений. Требования к средствам антивирусной защиты. Показатели и метрики испытаний. Виды показателей объекта испытаний. Метрики сложности программного кода. Метрики покрытия программного кода. Метрики полноты функционального тестирования. Модели оценки технологической безопасности и планирования испытаний. Отладочные модели программ. Модели роста надежности от времени. Модели полноты тестирования. Модели сложности программного обеспечения. Выбор модели оценки и планирования испытаний. Модели управления доступом. Дискреционная модель управления доступом. Мандатная модель управления доступом. Ролевая модель управления доступом. Атрибутная модель управления доступом. Метрики парольных систем. Модели периодического инспекционного контроля. Модели инспекционного контроля средств защиты информации. Модели инспекционного контроля сред функционирования.

Практические занятия (8 ч.). Введение в аудит информационной безопасности автоматизированных систем. Понятия «этичный хакер» и «тестирование на проникновение». Сбор информации, сканирование и перечисление. Взлом системы. Перехват сеанса.

Самостоятельная работа (6 ч.). Проработка материалов аудиторных занятий, подготовка к практическим занятиям.

Тема 2. Средства обеспечения безопасности в оценке соответствия

Лекции (20 ч.). Формальный базис испытаний средств защиты информации. Методика испытаний средств вычислительной техники. Методика проверки дискреционного принципа контроля доступа. Методика проверки мандатного принципа контроля доступа. Методика проверки механизмов очистки памяти. Методика проверки механизмов изоляции модулей. Методика проверки механизмов идентификации и аутентификации субъектов доступа. Методика проверки механизмов контроля целостности. Методика испытаний межсетевых экранов. Проверка механизмов фильтрации данных и трансляции адресов. Проверка механизмов идентификации и аутентификации администраторов. Проверка механизмов контроля целостности. Методика испытаний автоматизированных систем. Методика проверки механизмов идентификации и аутентификации субъектов доступа. Методика проверки механизмов управления доступом. Методика проверки механизмов контроля целостности. Методика проведения испытания по требованиям «Общих критериев». Рекомендации по оптимизации испытаний. Рекомендации по контролю отсутствия не декларированных возможностей. Общий порядок проведения испытаний. Рекомендации по контролю наличия заданных конструкций.

Практические занятия (8 ч.). Взлом веб-серверов и атаки на веб-приложения. SQL инъекции. Атаки типа «отказ в обслуживании». Атаки на переполнение буфера.

Самостоятельная работа (6 ч.). Проработка материалов аудиторных занятий, подготовка к практическим занятиям.

5. УСЛОВИЯ РЕАЛИЗАЦИИ ДПП

5.1. Организационные условия реализации ДПП

Наименование аудитории	Вид занятия	Наименование оборудования, программного обеспечения
Специализированная аудитория / компьютерный класс	Лекции, практические занятия	Персональные компьютеры, мультимедийный проектор, экран, доска, маркер, Microsoft Office, СПС КонсультантПлюс, Интернет, средства виртуализации, средства защиты информации, средства разработки, средства оценки эффективности защиты информации

5.2. Педагогические условия реализации ДПП

В реализации программы принимают участие ведущие преподаватели кафедры Информационная безопасность (ИУ-8) МГТУ им. Н.Э. Баумана, известные своими научными достижениями, как в теоретической, так и в практической области информационной безопасности автоматизированных систем.

5.3. Учебно-методическое обеспечение ДПП

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов / 3-е изд. М.: Академия, 2007. 254 с.

2. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.

3. Девянин П.Н. Модели безопасности компьютерных систем. М.: Академия, 2005. 144 с.

4. Котенко И.В., Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. СПб.: ВУС, 2000. 190 с.

5. Ховард М., Лебланк Д. Защищённый код. М.: Русская редакция, 2004. 704 с.

6. Митник К. Искусство обмана. М.: Компания АйТи, 2004. 416 с.

7. Столингс В. Криптография и защита сетей. М.: Вильямс, 2001. 671 с.

5.4. Методические рекомендации

ДПП построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Преподавание программы основано на личностно-ориентированной технологии образования, сочетающей два равноправных аспекта этого процесса: обучение и учение. Личностно-ориентированный подход развивается при участии слушателей в активной работе на занятиях, направлен в первую очередь на развитие индивидуальных способностей, создание условий для развития творческой активности слушателя и разработку инновационных идей, а так же на развитие самостоятельности мышления, нахождение рационального варианта решения, сравнения и оценки нескольких подходов и т. п. Это способствует формированию приемов умственной деятельности по восприятию новой информации, ее запоминанию и осознанию, создания образов для сложных понятий и процессов, приобретению навыков поиска решений в условиях неопределенности.

Лекционные и практические занятия проводятся для приобретения навыков реализации знаний в предметной области. Занятия проводятся с использованием активных методов обучения.

Самостоятельная работа слушателей предназначена для внеаудиторной проработки материалов аудиторных занятий и источников информации не только рекомендованной, но из всех возможных источников, а также подготовки домашнего задания.

При изучении ДПП предусмотрены активные формы проведения занятий:

– управляемая дискуссия;

– разбор конкретных ситуаций.

6. ФОРМЫ ИТОГОВОЙ АТТЕСТАЦИИ ДПП

Итоговая аттестация проводится в форме зачета.

На зачете присутствуют преподаватели, принимающие участие в реализации программы.

По результатам итоговой аттестации слушателю выставляется оценка «Зачтено/Не зачтено»:

Оценка «Зачтено» выставляется слушателю, который:

- правильно ответил не менее чем на 75% вопросов зачета;
- продемонстрировал необходимые систематизированные знания и достаточную степень владения принципами предметной области программы, понимание их особенностей и взаимосвязь между ними в течение всего срока обучения по ДПП.

Оценка «Не зачтено» выставляется слушателю, который:

- ответил правильно менее чем на 75% вопросов зачета;
- имеет крайне слабые теоретические и практические знания, обнаруживает неспособность к построению самостоятельных заключений.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ИТОГОВОЙ АТТЕСТАЦИИ

7.1. Паспорт комплекта оценочных средств

Предметы оценивания	Объекты оценивания	Показатели оценки
ПК-4 **ПК-5**	***Знать:*** – критерии оценки эффективности защищенности; – типы и виды программных и программно-аппаратных систем защиты информации; – аппаратно-программные средства криптографической защиты информации; – методы защиты программ от несанкционированного копирования, методы защиты программных средств от исследования; – физические основы образования технических каналов утечки информации; – назначение, принципы работы средств новых информационных технологий; – основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем. ***Уметь:*** – производить установку, настройку и обслуживание программно-аппаратных средств защиты информации; – осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; – обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности; – организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности. ***Владеть:*** – навыками освоения, внедрения и сопровождения программно-аппаратных средств защиты информации на объектах различного типа; – навыками сопровождения программно-аппаратных средств защиты информации; – навыками применения современных информационных технологий к текущим реальным ситуациям, основными классификациям информационных систем, навыками развертывания основных программных комплексов и программ, реализующих ту или иную информационную технологию.	– умение сравнивать; – умение анализировать; – умение классифицировать; – умение устанавливать причинно-следственные связи; – умение формулировать выводы

7.2. Комплект оценочных средств

Примерные вопросы к зачету:

1. Типы сетевых узлов, сетевых подключений и их характеристика.
2. Структура документа HTML и способы создания WEB-страниц. Основные дескрипторы.
3. Технические характеристики сетевого оборудования, используемого для подключений типа Ethernet. Принципы построения одноранговой и клиент-серверной сетей.
4. Каскадные таблицы стилей CSS, их предназначение и виды. Приоритетность таблиц.
5. Стек протоколов. Эталонная модель взаимодействия открытых систем.
6. Настройка односегментных и клиент-серверных сетей на платформе Windows.
7. Расшифровка многоуровневой схемы стека.
8. Понятие фреймов, их предназначение. Организация простых фреймов. Привести примеры.
9. Понятие кадра. Что содержит структура кадра.
10. Описание web-страниц с помощью дескриптора <meta>. Использование графики на web-страницах.
11. Протокол TCP/IP.
12. Создание окна на языке HTML. Свойства границ окна.
13. Структура сетевых пакетов. Принцип формирования кадров. Формат кадра Ethernet.
14. Добавление бегущей строки, аудио- и видео-файлов на web-страницу.
15. Технология Ethernet, физические и логические топологии.
16. Создание таблиц в HTML. Управление рамкой таблицы.
17. Доступ к передаче данных по алгоритму «Множественный доступ с прослушиванием несущей и обнаружением коллизий».
18. Полное выравнивание объектов на web-странице. Привести примеры.
19. Схема стека TCP/IP. Установление и разрыв TCP-соединения.20.Создание вложенных и встроенных фреймов на HTML.
21. Средства сетевого тестирования. Привести примеры. 22.Определение правил CSS на HTML. Создание класса стилей.
23. Протоколы SMTP и POP3, их характеристика и предназначение. Штампы писем. Почта через Telnet.
24. Задание полей web-страницы. Управление полосой прокрутки и указателем мыши.
25. Сетевой интерфейс, IP-адрес, маска подсети, порт. Определения и примеры.
26. Основные сетевые компоненты C++ Builder и их характеристика.
27. Кнопки-гиперссылки. Интерактивные web-страницы. Текстовые поля ввода, раскрывающиеся списки.
28. Классификация информационных сетей и каналов связи. Четыре основных структуры интерфейсов каналов. Характеристики сетей с различными типами интерфейсов.
29. Интерактивные web-страницы. Флажки и переключатели. Кнопки управления.
30. Показатели эффективности каналов связи. Основные параметры для оптимизации каналов связи.
31. Динамические web-страницы. Привести примеры.
32. Схемы последовательного и параллельного каналов связи. Формулы расчета добротности и удельной стоимости.
33. Производительность сети, коэффициент использования канала, пропускная способность сети.
34. Основные параметры и характеристики физических каналов связи. Витая пара, коаксиальный кабель, волоконно-оптический кабель.
35. Апертура.
36. Шумы в канале связи. Отношение сигнал-шум.

37. Задержка распространения и задержка передачи сигналов.

38. Предназначение и возможности прокси-сервера.

39. Характеристики модели вычислительной системы из двух ЛВС, объединенных через глобальную сеть.

40. Способы управления ошибками при передаче информации. Эхо-контроль. Автоматический запрос на повторение.

Авторы программы:

Заведующий кафедрой ИУ-8
МГТУ им. Н.Э. Баумана
д.ф.-м.н., доцент М.А. Басараб

Старший преподаватель кафедры ИУ-8
МГТУ им. Н.Э. Баумана Е.В. Глинская

8. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ