05.07.19 04.08-08/64

Министерство науки и 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

УТВЕРЖДАЮ
Директор ИСОТ
МГТУ им. Н.Э. Баумана
В.Г. Брекалов
«__» _____ 2019 г.

Дополнительное профессиональное образование

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Анализ информационных рисков

Регистрац. № 19042402

Москва, 2019

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО:

Заведующий кафедрой ИУ8

_____ _____ (Басараб М.А.)

_____ (дата)

Начальник УМО ИСОТ
МГТУ им. Н.Э. Баумана

_____ _____ (Шмаков А.Ю..)

_____ (дата)

СОДЕРЖАНИЕ

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 5

2.1. Категория слушателей ДПП 5

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 6

4.1. Цель изучения модуля 6

4.2. Задачи изучения модуля 6

4.3. Планируемые результаты обучения 7

4.4. Содержание модуля 8

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 9

6. ФОРМЫ ИТОГОВОЙ АТТЕСТАЦИИ ДПП 10

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ИТОГОВОЙ АТТЕСТАЦИИ 10

7.1. Паспорт комплекта оценочных средств 10

7.2. Комплект оценочных средств 11

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

Дополнительная профессиональная программа (ДПП) подготовлена на основе:

– Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– требований Приказа Минобрнауки России от 1 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 Минобрнауки России от 5 декабря 2013 г. № 1310 «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

Подготовить высококвалифицированных и конкурентоспособных специалистов в области информационной безопасности автоматизированных систем.

Сформировать у слушателей компетенции в области выявления угрозы и оценки уязвимости информационных рисков автоматизированных систем.

1.2. Планируемые результаты обучения

Планируемые результаты обучения по ДПП:

– освоение профессиональных компетенций в процессе изучения перечисленных в учебном плане тем;

– успешное освоение программы повышения квалификации;

– успешное прохождение итоговой аттестации (зачет);

– получения удостоверения о повышении квалификации по ДПП «Анализ информационных рисков».

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 (регистрац. № 843)

Наименование вида профессиональной деятельности: обеспечение безопасности информации в автоматизированных системах.

Основная цель вида профессиональной деятельности: обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите.

Обобщенная трудовая функция: разработка систем защиты информации автоматизированных систем.

Трудовые функции: 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 базируются на основании Приказа Минобрнауки России от 01 декабря 2016 г. № 1513 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)» (регистрац. № 44823).

Перечень компетенций:

– способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности (ПК-2);

– способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности (ПК- 4).

1.5. Соответствие видов деятельности и профессиональных компетенций и их составляющих

Разработка проектных решений по защите информации в автоматизированных системах (D/02.7.)			
Профессиональные компетенции	Практический опыт	Умения	Знания
ПК-2: способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	Разработка модели угроз безопасности информации и модели нарушителя в автоматизированных системах	Выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	–
ПК- 4: способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности	–	Применять действующую нормативную базу в области обеспечения защиты информации	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.

2.2. Общая трудоёмкость программы, аудиторная и самостоятельная работа

Общая трудоемкость программы составляет 40 часов, из них 16 часов аудиторной работы и 24 часа самостоятельной работы.

2.3. Форма обучения

ДПП «Анализ информационных рисков» реализуется по очной форме обучения.

2.4. Учебный план

ДПП «Анализ информационных рисков» реализуется 1 модулем.

№ п/п	Наименование темы	Форма контроля	Всего, час	В том числе		
				Лекции	Практические занятия	Самостоятельная работа
1	Основы анализа информационных рисков	домашнее задание	20	4	4	12
2	Организация защиты информации	домашнее задание	20	4	4	12
ИТОГО		**зачет**	**40**	**8**	**8**	**24**

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

№ п/п	Наименование темы	1 день	2 день	3 день	4 день	5 день
1	Основы анализа информационных рисков					
2	Организация защиты информации					
	Итоговая аттестация					**зачет**

Минимальный срок освоения ДПП - 5 дней.

4. РАБОЧАЯ ПРОГРАММА ДПП

4.1. Цель изучения модуля

Целью изучения модуля является получение слушателями знаний, навыков и умений, позволяющих идентифицировать информационные риски, определение вероятности их осуществления и потенциального воздействия, а также контрмер, уменьшающих это воздействие.

4.2. Задачи изучения модуля

Задачами изучения модуля являются:

– теоретические и практические основы теории рисков;

– основные понятия и методы управления рисками реагирования на инциденты;

– современные подходы и инструментальные средства анализа рисков.

4.3. Планируемые результаты обучения

Процесс изучения модуля направлен на формирование следующих профессиональных компетенций:

Код компетенции	Перечень планируемых результатов обучения модуля	Формы и методы обучения, способствующие формированию и развитию компетенции
ПК-2 ПК-4	***Знать:*** – основные требования по повышению уровня защищенности предприятия; – основные принципы выбора наилучшего состава средств защиты информации на предприятии; – основные понятия архитектуры системы информационной безопасности предприятия; – существующие методы и алгоритмы качественного и количественного анализа информационных рисков; – отечественную и зарубежную нормативную правовую базу в области рисков нарушения информационной безопасности и программные продукты на их основе. ***Уметь:*** – составлять технические задания, направленные на повышение уровня защищенности предприятия и снижение риска нарушения информационной безопасности; – разрабатывать программные средства, реализующие методы анализа риска нарушения информационной безопасности, составления перечня наилучших вариантов выбора программных/аппаратных и программно- аппаратных средств защиты информации. ***Владеть:*** – способами формирования технического задания для повышения уровня защищенности и снижения информационных рисков на предприятии; – способами разработки программных средств, реализующих методы анализа риска нарушения информационной безопасности, составления перечня наилучших вариантов выбора программных/аппаратных и программно- аппаратных средств защиты информации.	Лекционные и практические занятия, самостоятельная работа

4.4. Содержание модуля

Тема 1. Основы анализа информационных рисков

Лекции (4 часа). Цели и задачи анализа рисков нарушения информационной безопасности. Эталонная модель рисков. Анализ критичных активов предприятия, разработка модели бизнес-процессов предприятия, выявление основных источников угроз на предприятии. Оценка информационных рисков на основе анализа по информационным потокам с помощью программных продуктов. Оценка информационных рисков на основе анализа требований стандартов. Технологии анализа информационных рисков

Практические занятия (4 часа). Уровни правового обеспечения информационной безопасности идентификации и аутентификации пользователя. Основные механизмы реализации удалённых атак.

Самостоятельная работа (12 ч.).

Наименование темы	**Дидактические единицы, вынесенные на самостоятельное изучение**	**Формы самостоятельной работы**	**Учебно-методическое обеспечение**	**Форма контроля**
Разработка итоговых отчетов по анализу и управлению рисками.	перечень рисков, система управления риска; оценка рисков	самостоятельная проработка аудиторных занятий, доп. источники информации	материалы лекционных и практических занятий, [1,2]	домашнее задание

Тема 2. Организация защиты информации

Лекции (4 часа) Оценка рисков с помощью нечетких когнитивных карт. Системы нечеткого логического вывода. Оценка рисков с помощью нейронных сетей. Инструментальные средства (программные пакеты) для оценки информационных рисков. Аудит информационной безопасности. Понятие аудита, виды аудита информационной безопасности.

Практические занятия (4 часа). Работа с международной базой уязвимости (NVD), определение уровня уязвимости компонентов локальной вычислительной сети предприятия. Расчет рисков информационной безопасности с помощью системы нечеткого логического вывода. Требования к классам защищённости. Межсетевые экраны. Программные закладки. Программные средства защиты информации.

Самостоятельная работа (12 ч.).

Наименование темы	**Дидактические единицы, вынесенные на самостоятельное изучение**	**Формы самостоятельной работы**	**Учебно-методическое обеспечение**	**Форма контроля**
Расчет рисков информационной безопасности с помощью системы нечеткого логического вывода.	оценка рисков, информационные измерения, нечеткая кластеризация	самостоятельная проработка аудиторных занятий, доп. источники информации	материалы лекционных и практических занятий, [1,2]	домашнее задание

5. УСЛОВИЯ РЕАЛИЗАЦИИ ДПП

5.1. Организационные условия реализации ДПП

Наименование аудитории	Вид занятия	Наименование оборудования, программного обеспечения
Специально оборудованная аудитория	Лекции, практические занятия	Компьютер, мультимедийный проектор, экран, доска, маркер, лазерная указка, Microsoft Office, СПС КонсультантПлюс, Интернет

5.2. Педагогические условия реализации ДПП

В реализации программы принимают участие ведущие преподаватели кафедры Информационная безопасность 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

Основная литература:

1. Организационно – правовое обеспечение информационной безопасности: учеб. пособие для вузов / А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова [и др.]; ред. А.А.Стрельцов. М.: Академия, 2008. 248 с.

2. Организационное обеспечение информационной безопасности: учебник для вузов/ О.А. Романов, С.А. Бабин, С.Г. Жданов М.: Академия, 2008. 188 с.

Дополнительная литература:

3. Медведев Н.В., Троицкий И.И., Цирлов В.Л. К вопросу об использовании аппарата теории нечетких множеств при анализе рисков информационной безопасности// Вестник МГТУ им. Н. Э. Баумана. Сер. Приборостроение. 2011. Спец. вып. Технические средства. С. 25-30.

4. Васильев В.И. Информационные системы защиты информации: учеб. пособие для вузов/ 2-е изд. М.: Машиностроение, 2012. 152 с.

5. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

6. Варфоломеев А.А. Управление информационными рисками: учеб. пособие/ М.: Изд-во РУДН, 2008. 158 с.

Электронные ресурсы:

1. Научная электронная библиотека http://elibrary.ru

5.4. Методические рекомендации

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

Преподавание модуля 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 практических занятиях и при выполнении самостоятельных заданий, направлен в первую очередь на развитие индивидуальных способностей обучающихся, создание условий для развития творческой активности слушателя и разработке инновационных идей, применимых в педагогике.

Самостоятельная работа слушателей предназначена для внеаудиторной работы по самостоятельному изучению отдельных разделов дисциплины, приобретения практических навыков по анализу и систематизации полученной информации.

Текущий контроль самостоятельной работы слушателей проводится на занятиях в виде проверки домашнего задания и общей дискуссии по тематике дисциплины.

Приступая к работе над ДПП каждый слушатель должен принимать во внимание следующие положения: освоение материала его успешное закрепление на стадии промежуточного контроля возможно только при регулярной работе во время занятий и планомерном выполнении самостоятельных заданий.

Самостоятельная работа предусматривает не только проработку материалов лекционного курса, но и их расширение в результате поиска, анализа, структурирования и представления в компактном виде современной информации из всех возможных источников.

6. ФОРМЫ ИТОГОВОЙ АТТЕСТАЦИИ ДПП

Освоение ДПП завершается итоговой аттестацией в форме зачета.

На зачете присутствуют преподаватели, принимающие участие в реализации программы.

Зачет проходит в форме общей дискуссии, по итогам которой выставляется оценка – зачет или незачет. Итоговая оценка, учитывает:

– активность слушателя;

– ответ на вопросы преподавателя;

– итоговое обсуждение результатов обучения.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ИТОГОВОЙ АТТЕСТАЦИИ

7.1. Паспорт комплекта оценочных средств

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки
ПК-2 ПК- 4	***Знать:*** – основные требования по повышению уровня защищенности предприятия; – основные принципы выбора наилучшего состава средств защиты информации на предприятии; – основные понятия архитектуры системы информационной безопасности предприятия. – существующие методы и алгоритмы качественного и количественного анализа информационных рисков; – отечественную и зарубежную нормативную правовую базу в области рисков нарушения информационной безопасности и программные продукты на их основе. ***Уметь:*** – составлять технические задания, направленные на повышение уровня защищенности предприятия и снижение риска нарушения информаци-	«зачет» - ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Раскрываются причинно-следственные связи между явлениями и событиями. Обосновываются выводы. Демонстрируются знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи. При этом может допускаться ухудшение качества показателей оценки, которые не представляют собой существенного искажения системы знаний по ДПП; «незачет» - материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний. Не раскрываются причинно-следственные связи. Не проводится анализ. Выводы от-

	онной безопасности; – разрабатывать программные средства, реализующие методы анализа риска нарушения информационной безопасности, составления перечня наилучших вариантов выбора программных/аппаратных и программно-аппаратных средств защиты информации. ***Владеть:*** – способами формирования технического задания для повышения уровня защищенности и снижения информационных рисков на предприятии – способами разработки программных средств, реализующих методы анализа риска нарушения информационной безопасности, составления перечня наилучших вариантов выбора программных/аппаратных и программно-аппаратных средств защиты информации.	сутствуют. Ответы на дополнительные вопросы отсутствуют. Имеются нарушения норм литературной речи

7.2. Комплект оценочных средств

1. Характеристики информационного ресурса как объекта защиты.
2. Угрозы случайные и преднамеренные.
3. Внешние и внутренние угрозы.
4. Угрозы стихийного и искусственного характера.
5. Проявления угроз.
6. Последствия угроз.
7. Основные способы реализации угроз.
8. Способы несанкционированного доступа к информации и защиты от него.
9. Идентификация подлинности пользователя.
10. Механизмы подтверждения подлинности пользователя
11. Взаимная проверка подлинности пользователя.
12. Протоколы идентификации с нулевой передачей знаний.
13. Упрощенная схема идентификации с нулевой передачей знаний.
14. Способы аутентификации пользователей компьютерных систем.
15. Протоколы аутентификации при удаленном доступе.
18. Методы управления доступом к объектам компьютерных систем.
19. Средства защиты информации в глобальных вычислительных сетях.
20. Способы симметрического шифрования.
21. Современные алгоритмы симметрического шифрования.
22. Принципы создания асимметрических криптосистем.
23. Свойства асимметрических криптосистем.
24. Примеры асимметрических криптосистем.
25. Электронная цифровая подпись и ее использование.
26. Функции хеширования.
27. Принципы использования криптографического интерфейса ОС Windows.

28. Компьютерная стеганография и ее применение.

29. Режим функционирования межсетевых экранов и их основные компоненты.

30. Шлюзы сетевого уровня.

31. Основные схемы сетевой защиты на базе межсетевых экранов.

32. Применение межсетевых экранов для организации виртуальных корпоративных сетей.

33. Программные методы защиты.

34. Методы средства ограничения доступа к компонентам сети.

35. Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям.

Авторы программы:

	/М.А. Баскаев/

ЛИСТ ИЗМЕНЕНИЙ

УТВЕРЖДАЮ
Руководитель НУК ИУ
_____ А.В. Пролетарский
«__22__» ____04____ 20__19__ г.

ЗАКЛЮЧЕНИЕ
о возможности открытого опубликования

программы повышения квалификации *«Анализ информационных рисков»*
(наименование материалов, подлежащих экспертизе)

Экспертная комиссия в составе председателя экспертной комиссии Научно-учебного комплекса «Информатика и системы управления» МГТУ им. Н.Э.Баумана Министерства образования и науки РФ к.т.н. доцента кафедры ИУ1 Звягина Ф.В., д.т.н. профессора кафедры ИУ1 Неусыпина К.А., заместителя заведующего кафедры ИУ8 к.т.н. доцента Троицкого И.И.

в период с «__22__» ____04____ 20__19__ г. по «__25__» ____04____ 20__19__ г.
провела экспертизу материалов программы повышения квалификации
(наименование материалов, подлежащих экспертизе, список авторов)
«Анализ информационных рисков» на предмет отсутствия (наличия) в них сведений, составляющих государственную тайну, и возможности (невозможности) их открытого опубликования.

Руководствуясь Законом Российской Федерации «О государственной тайне», Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995г. № 1203, а также Перечнем сведений, подлежащих засекречиванию, Министерства образования и науки Российской Федерации (Минобрнауки РФ), утвержденным приказом Минобрнауки РФ от 10 ноября 2014 г. № 36с,
комиссия установила:

1. Сведения, содержащиеся в рассматриваемых материалах, **находятся в компетенции** федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет им. Н.Э. Баумана (национальный исследовательский университет)» (**МГТУ им. Н.Э. Баумана**) Министерства образования и науки Российской Федерации.

2. Сведения, содержащиеся в рассматриваемых материалах, **не подпадают под действие Перечня сведений,** составляющих государственную тайну (статья 5 Закона Российской Федерации «О государственной тайне»), не относятся к Перечню сведений, отнесенных к государственной тайне, утвержденному Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203, **не подлежат засекречиванию и данные материалы могут быть открыто опубликованы.**

Члены комиссии

_____ Ф.В. Звягин
(подпись, инициалы и фамилия)
_____ К.А. Неусыпин
(подпись, инициалы и фамилия)
_____ И.И. Троицкий
(подпись, инициалы и фамилия)