

Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»
ИНЖЕНЕРНО - ЭКОНОМИЧЕСКИЙ ИНСТИТУТ

СОГЛАСОВАНО

ООО НТЦ «ТЕЗИС +»
Генеральный директор

_____ А.К. Туркин
«__» _____ 201__ г.



УТВЕРЖДЕНА

Решением Ученого совета МЭИ
от «__» _____ 201__ г. № ____
Ректор _____ Н.Д. Роголев



ОСНОВНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ВЫСШЕГО ОБРАЗОВАНИЯ

Направление подготовки (специальность): 10.03.01 Информационная безопасность

Профиль(и) подготовки: Защита информации в автоматизированных информационных системах

Вид(ы) профессиональной деятельности:

- эксплуатационная;
- проектно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая.

Квалификация выпускника: Бакалавр

Москва 2013

1. ОБЩИЕ ПОЛОЖЕНИЯ

Основная профессиональная образовательная программа (далее – образовательная программа), реализуемая в МЭИ, представляет собой комплект документов, разработанный и утвержденный в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВПО) с учетом профессиональных стандартов.

Образовательная программа представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий, форм аттестации, который представлен в виде общей характеристики программы, учебного плана, календарного учебного графика, рабочих программ дисциплин (модулей), программ практик, оценочных средств, методических материалов.

Образовательная программа позволяет осуществлять обучение инвалидов и лиц с ограниченными возможностями здоровья. С этой целью в вариативную часть образовательной программы, при необходимости, включаются специализированные адаптационные и адаптированные дисциплины и практики.

Нормативные документы для разработки образовательной программы

Нормативную правовую базу разработки образовательной программы составляют:

Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» (с последующими дополнениями и изменениями);

«Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры», утвержденный приказом Минобрнауки России от 19 декабря 2013 г. № 1367 (с последующими дополнениями и изменениями);

Федеральный государственный образовательный стандарт по направлению подготовки 090900 «Информационная безопасность» высшего профессионального образования, утвержденный приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 496.

Нормативно-методические документы Минобрнауки России;

Устав МЭИ;

Локальные акты МЭИ;

Профессиональные стандарты: отсутствуют.

2. ОБЩАЯ ХАРАКТЕРИСТИКА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цель образовательной программы:

Подготовка высокопрофессиональных и конкурентоспособных на рынке труда специалистов в области информационной безопасности и защиты информации для инновационной экономики и энергетики страны, способных обеспечить, на основе системного подхода, защищенность информационной системы (активов) организации от вредоносных программно-технических и информационных воздействий. Подготовка осуществляется на основе эффективного сочетания фундаментального и прикладного образования с использованием передовых образовательных технологий.

Форма обучения: очно-заочная.

Объем программы: 240 зачетных единиц.

Сроки получения образования: 5 лет.

Использование электронного обучения, дистанционных образовательных технологий и сетевой формы при реализации образовательной программы.

В рамках данной образовательной программы создан электронный образователь-

ный ресурс «Кафедра информационной и экономической безопасности Инженерно-экономического института» на платформе Moodle.

Каждый обучающийся обеспечен доступом к сервисам и информационным активам ресурса (личный кабинет, преподаватели, учебные дисциплины, курсы, учебные группы, электронный контент в виде учебно-методических комплексов дисциплин). Также создана версия ресурса для мобильных гаджетов.

Каждый обучающийся имеет индивидуальный непосредственный и удаленный, с использованием сервисов Интернет, доступ к электронно-библиотечной системе НИУ «МЭИ».

Для повышения эффективности управления образовательным процессом и индивидуальными образовательными траекториями обучающихся каждому из них в информационной системе НИУ «МЭИ» создан индивидуальный почтовый ящик и предоставлена возможность размещения личных образовательных активов в «облачных» сервисах университета.

Язык обучения: русский.

Требования к абитуриенту (*бакалавриат*): абитуриент должен иметь документы в соответствии с Правилами приема в МЭИ, которые устанавливаются решением Ученого совета МЭИ.

3. ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВЫПУСКНИКОВ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Область профессиональной деятельности выпускника:

Область профессиональной деятельности бакалавра информационной безопасности включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Выпускник по направлению подготовки «Информационная безопасность» готовится для осуществления профессиональной деятельности в органах государственной власти и органах местного самоуправления, на предприятиях и в организациях любых форм собственности и направлений деятельности, в научно-исследовательских и проектных организациях.

Объекты профессиональной деятельности выпускника:

Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере; технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах; процессы управления информационной безопасностью защищаемых объектов.

Виды профессиональной деятельности выпускника:

- эксплуатационная деятельность;
- проектно-технологическая;
- экспериментально-исследовательская;
- организационно-управленческая.

Задачи профессиональной деятельности выпускника:

А) При осуществлении эксплуатационной деятельности;

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- администрирование подсистем информационной безопасности объектов;

Б) При осуществлении проектно-технологической деятельности;

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов;

В) При осуществлении экспериментально-исследовательской деятельности;

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств;

Г) При осуществлении организационно-управленческой деятельности.

- осуществление организационно-правового обеспечения информационной безопасности объектов защиты;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- совершенствование системы управления информационной безопасностью;
- 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.

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения образовательной программы у выпускника должны быть сформированы следующие компетенции:

Общекультурные компетенции (выпускник должен обладать):

- 1) способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма (ОК-1);
- 2) способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм (ОК-2);
- 3) способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия (ОК-3);
- 4) способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные

положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач (ОК-4);

5) способностью к кооперации с коллегами, работе в коллективе (ОК-5);

6) способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК-6);

7) способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной со- стязательной деятельности в условиях информационного противоборства (ОК-7);

8) способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);

9) способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии (ОК-9);

10) способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного (ОК-10);

11) способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства (ОК-11);

12) способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков (ОК-12);

13) способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (ОК-13).

Общепрофессиональные компетенции (выпускник должен обладать):

1) способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);

2) способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);

3) способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);

4) способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);

5) способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);

6) способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);

7) способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);

8) способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-8);

Профессиональные компетенции (выпускник должен обладать)::

При осуществлении эксплуатационной деятельности:

- 1) способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9);
- 2) способностью администрировать подсистемы информационной безопасности объекта (ПК-10);
- 3) способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-11);

При осуществлении проектно-технологической деятельности:

- 4) способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);
- 5) способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-13);
- 6) способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-14);
- 7) способностью применять программные средства системного, прикладного и специального назначения (ПК-15);
- 8) способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-16);
- 9) способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-17);
- 10) способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-18);

При осуществлении экспериментально-исследовательской деятельности:

- 11) способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-19);
- 12) способностью применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);
- 13) способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);
- 14) способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов (ПК-22);
- 15) способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-23);
- 16) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24);

При осуществлении организационно-управленческой деятельности:

- 17) способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-25);
- 18) способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-26);
- 19) способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27);
- 20) способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28);
- 21) способностью участвовать в работах по реализации политики информационной

безопасности (ПК-29);

22) способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-30);

23) способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации (ПК-31);

24) способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПК-32);

25) способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю (ПК-33).

Компетентностно-формирующая часть учебного плана, определяющая этапы формирования компетенций дисциплинами учебного плана, представлена в приложении 1 к ОПОП.

5. УЧЕБНЫЙ ПЛАН И КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Учебный план определяет перечень и последовательность освоения дисциплин, практик, промежуточной и государственной итоговой аттестаций, их трудоемкость в зачетных единицах и академических часах, распределение контактной работы обучающихся с преподавателем (в том числе лекционные, практические, лабораторные виды занятий, консультации) и самостоятельной работы обучающихся.

Календарный учебный график определяет сроки и периоды осуществления видов учебной деятельности и периоды каникул.

Учебный план и календарный учебный график представлены в приложении 2 к ОПОП.

6. РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН

Аннотации всех учебных дисциплин представлены в приложении 3 к ОПОП.

7. ПРОГРАММЫ ПРАКТИК

Аннотации всех практик представлены в приложении 4 к ОПОП.

8. ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ

Государственная итоговая аттестация является обязательной и осуществляется после освоения всех предусмотренных образовательной программой дисциплин и практик в полном объеме. Государственная итоговая аттестация включает в себя подготовку к защите и защиту выпускной квалификационной работы.

9. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды оценочных средств представлены в приложении 5 к ОПОП.

10. ФАКТИЧЕСКОЕ РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Кадровое обеспечение образовательного процесса приведено в приложении 6 к ОПОП.

Для реализации образовательной программы используется материально-техническая база, обеспечивающая проведение всех предусмотренных учебным планом видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической, научно-исследовательской и самостоятельной работы обучающихся.

Перечень материально-технического обеспечения включает в себя:

А) Учебный лабораторный комплекс в составе:

- лаборатория «Программно-аппаратная защита информации» (ауд. К-303);
- лаборатория «Защита информационных процессов в компьютерных системах» (ауд. К-307);

- лаборатория «Технические средства обеспечения безопасности» (ауд. И-610);

- лаборатория «Инженерно-техническая защита информации» (ауд. И-601е);

Кроме этого:

- лаборатория физики (ауд. А-104, А-106);

- лаборатория аппаратных средств вычислительной техники (ауд. Е-702);

- лаборатория электротехники (ауд. Е-803);

Б) Компьютерные классы (ауд. К-302, К-303, К-307, И-610);

В) Аудитории, оборудованные мультимедийным и (или) презентационным оборудованием (ауд. К-301, К-302, К-303, К-307);

Г) Комплект лицензионного программного обеспечения.

Описание материально-технического обеспечения образовательной программы приведено в соответствующих рабочих программах дисциплин и практик.

Учебно-методическое обеспечение образовательной программы приведено в соответствующих рабочих программах дисциплин и практик.

ОБРАЗОВАТЕЛЬНУЮ ПРОГРАММУ СОСТАВИЛ:

Профессор кафедры информационной и экономической безопасности
к.т.н., доцент

А.Ю. Невский

Зав. кафедрой информационной и экономической безопасности
д.т.н., профессор

А.С. Минзов

Директор Инженерно-экономического института
к.т.н., доцент

А.Ю. Невский

СОГЛАСОВАНО:

Первый проректор – проректор по учебной работе

Т.А. Степанова

Начальник учебного управления

Д.А. Иванов

Начальник отдела методического обеспечения
и управления качеством образования

А.В. Носов