УТВЕРЖДЕНА НА ЗАСЕДАНИИ АС

23.06.2018 ПРОТОКОЛ № 3

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ   
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет бизнеса и менеджмента

Школа бизнес-информатики

**Концепция образовательной программы «Управление информационной безопасностью»**

**Подготовки магистров по направлению**

38.04.05 «Бизнес-информатика»

### Общая характеристика образовательной программы

Форма обучения – очная.

Срок обучения: 2 года.

Язык преподавания – русский.

Набор 2018 года предполагает 20 бюджетных мест, 10 платных мест, 7 платных мест для иностранцев

На программе предполагаются бюджетные и платные места.

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики» (далее – НИУ ВШЭ) имеет Лицензию Федеральной службы по надзору в сфере образования и науки на право ведения образовательной деятельности рег. № 2593 от 24 мая 2017 года.

Магистерская программа «Управление информационной безопасностью» по направлению 38.04.05 разработана в соответствии с «Положением о магистерской подготовке (магистратуре) в системе многоуровневого высшего образования Российской Федерации» и «Образовательным стандартом федерального государственного автономного образовательного учреждения высшего профессионального образования “Национальный исследовательский университет “Высшая школа экономики”», утвержденным учёным советом Национального исследовательского университета “Высшая школа экономики” (Протокол от 02.02.2018 г. № 1)

Основной целью магистерской программы «Управление информационной безопасностью» является подготовка специалистов, умеющих определять цели, стратегии и политику корпоративной безопасности, которые необходимы для обеспечения эффективной безопасности информационных технологий организации, обеспечение информационной безопасности в достаточном объёме для реализации функции управления проектами создания, эксплуатации и развития современных информационно-телекоммуникационных систем (ИТКС).

Программа ориентирована на подготовку профессиональных специалистов в

и получивших комплекс технических, экономических, организационных и правовых знаний. Выпускники будут обладать высокими компетенциями в области теоретических и организационно-правовых аспектов безопасности компьютерных систем, криптографических и статистических методов защиты, типовых подсистем и решений обеспечения информационной безопасности.

***Стратегической целью и раскрывающими ее задачами магистерской программы является:***

- подготовка специалистов, обладающих необходимыми компетенциями для управления процессом разработки и использования систем информационной безопасности;

- приобретение навыков описания основных компонентов безопасности информационных технологий, их взаимосвязи;

- мониторинг новых источников угроз в сфере информационных технологий и связанных с ними рисков в условиях современного информационного общества и оперативная корректировка содержания курсов и даже структуры самой программы;

- участие в международных процессах в сфере управления информационной безопасностью и вхождение в число международных лидеров в исследованиях и разработках, посвященных проблеме управления информационной безопасностью;

- формирование на площадке НИУ ВШЭ сообщества российских и зарубежных исследователей в сфере проблем применения информационных технологий с возможностью анализа проблем и проведения дискуссий;

- формирование уникального, узнаваемого в мире бренда НИУ ВШЭ, выход НИУ ВШЭ на международный рынок образовательных и интеллектуальных услуг.

Магистерская программа «Управление информационной безопасностью» напрямую соотносится с положениями Программы развития НИУ ВШЭ в части формирования на базе университета передового научно-образовательного, аналитического, консалтингового и проектного центра в области социальных и экономических наук, входящего в число ведущих мировых исследовательских университетов по качеству своих компетенций и разработок и осуществляющего значительный практический вклад в инновационное развитие и глобальную конкурентоспособность России.

### Анализ и потребности рынка труда в выпускниках данной ОП

Принципиальной особенностью магистерской программы является то, что она ориентирована на подготовку высоквалифицированных специалистов в области управления информационной безопасностью информационно-коммуникационных технологий и систем (Management Security Information или Security Information and Event Management).

Вместе с тем проблемы управления информационной безопасностью стали актуальны и для систем, обрабатывающих общедоступную информацию. Если ранее информационная безопасность понималась, как совокупность трех направлений обеспечения конфиденциальности, целостности и доступности, то теперь востребованы системы, в которых необходимо обеспечение комплексного подхода по каждому из направлений или сочетаниям пар направлений.

В первую очередь это:

- обеспечение менеджмента информационной безопасности в крупных корпоративных информационных системах, информационных системах государственного сектора, электронном правительстве;

* построение модели информационной безопасности в Интернет-системах взаимодействия органов государственной власти и организаций с гражданским обществом, где конфиденциальность требуется в минимальной степени;.
* управление информационной безопасностью в мобильных системах, таких, как клиент-банк, мобильные пункты (рабочие места) управления организациями, распределенное проектирование, где целостность является определяющим свойством;.
* обеспечение информационной безопасности в системах, обрабатывающих, хранящих и передающих персональные данные граждан, где доступность не является первостепенным качеством системы и. т.д.

Характеризуя спрос работодателей на специалистов в области управления информационной безопасностью, обращает на себя внимание то обстоятельство, что управление информационной безопасностью является одним из наиболее актуальных направлений развития информационной инфраструктуры государственных и частных компаний. Важно отметить, что это направление является областью конвергенции различных инструментов, методов контроля и управления информационными рисками, в том числе, включающей и традиционно изучаемые в наших вузах вопросы создания программных и аппаратных средств и программных систем обеспечения информационной безопасности.

Одной из особенностей этого направления является то, что оно сегодня развивается в двух направлениях: создание внутрикорпоративных систем управления информационной безопасностью и аутсорсинг этих услуг.

Предлагаемая магистерская программа ориентирована на модель подготовки специалистов в сфере информационной безопасности, сочетающей в себе изучение теоретических основ с одновременным изучением прикладных дисциплин, с использованием современного математического инструментария, что обеспечивает преемственность теоретических и прикладных курсов. Построенная таким образом система подготовки магистров позволит студентам после завершения обучения приступить к практической работе в сфере управления информационной безопасностью.

### Описание преимуществ и особенностей ОП с точки зрения позиционирования на рынке образовательных услуг

В настоящее время подготовка магистров в сфере управления информационной безопасностью осуществляется рядом зарубежных Университетов, к числу которых можно отнести: University of Texas at Austin, Clark university, Wright State University, University of Warwick (Coventry, UK), University of Southampton, University of Oxford (Cyber Security Global Centre for Cyber Security Capacity) и др.

Создание системы управления информационной безопасностью предполагает создание программно-технической, правовой и кадровой подсистем. В западной терминологии данные системы обозначаются аббревиатурой SIM (Security Information Management), SIEM (Security Information and Event Management), Cyber Security and Management (CSM); Cyber Security; Master of Cyber Security (MCS); Master of Science in Cyber Security (MSCS); Magister Science in information technology (MSit).

Зарубежные магистерские программы в сфере управления информационной безопасностью, основной акцент подготовки специалистов делают, с одной стороны, на уникальность образования в данной сфере, с другой стороны, на значительный дефицит специалистов в области информационной безопасности.

При этом магистерские программы осуществляют подготовку по направлениям корпоративной информации (безопасность и технологии команд); консультанты государственных и частных информационных служб безопасности; управление информацией треков в критическом состоянии организаций; исследование кибербезопасности.

При занятиях по программам рассматриваются ряд аспектов кибербезопасности, учащиеся получают знания в сфере электроники и компьютерных наук, права, менеджмента, математики, оптоэлектроники и психологии.

Осуществляется проведение занятий по дисциплинам: Архитектуры безопасности и обороны сети; Информационные системы управления; Криптосистемы и защита данных; Глобализация и аутсорсинг; Информация управления рисками и руководства; Финансовые системного анализа и управления; Промышленный шпионаж и подделка; Цифровая криминалистика и др.

Область компетенции выпускников связана с приобретением навыков, умений и знаний по следующим отраслям:

- сетевая безопасность, компьютерная безопасность и информационная безопасность;

- защита критически важных инфраструктур, пользователей, их данных и интересов (деятельность электронных и программных систем, передовых сетей и протоколов, рискованного поведения, социальной и правовой приемлемости и физической и киберидентичности управления);

- архитектура компьютеров и сетей для разработки и осуществления безопасных систем.

Уникальность настоящей магистерской программы в нашей стране определяется тем обстоятельством, что в настоящее время приказами Министерства образования Российской Федерации утвержден ряд федеральных ГОСов по направлению подготовки «информационная безопасность», квалификации магистр[[1]](#footnote-1), область профессиональной деятельности которых включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Область профессиональной деятельности квалификации бакалавр [[2]](#footnote-2) включает: сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

Характеризуя профессиональную деятельность направления 090900, определены: эксплуатационная, проектно-технологическая, экспериментально-исследовательская и организационно-управленческие виды деятельности, каждая из которых решает ограниченный круг зада. В целях формирования надлежащих компетенций предусмотрен ряд подлежащих изучению дисциплин профессионального цикла, к которым можно отнести: защищенные информсистемы, информационно- аналитические средства безопасности, аппаратные средства вычислительной техники; программно-аппаратные средства защиты информации; техническая защита информации; сети и системы передачи информации; безопасность жизнедеятельности; языки и методы программирования и т.д.

При этом обращает на себя внимание программа подготовки специалистов в соответствии с положениями ГОСов среднего специального образования по специальности 090303 «Информационная безопасность телекоммуникационных систем», в соответствии с которым осуществляется подготовка выпускников, профессиональная деятельность которых направлена на организацию и проведение работ по техническому обслуживанию и обсечению информационной безопасности телекоммуникационных сетей и систем[[3]](#footnote-3).

Анализируя существующие программы по направлению «информационная безопасность», можно выделить ь существующие подходы к информационной безопасности, как к системе знаний:

Магистерская программа НИУ ВШЭ

«Управление информационной безопасностью»

УПРАВЛЕНЧЕСКИЙ

Осуществляется по программам

подготовки в США и странах

ТЕХНОЛОГИЧЕСКИЙ

Евросоюза

включено в программы

БАЗОВЫЙ

магистратур Российских ВУЗов

Программы подготовки

Бакалавров и среднего образования

При этом можно выделить три уровня формирования компетенций:

- в основе находится базовый уровень, формирующий фундаментальные основы знаний в сфере информационной безопасности, в процессе формирования которого формируются навыки использования математических методов и моделей для решения прикладных задач, приобретаются навыки анализа процессов обработки, поиска и передачи информации;

- технологический уровень предполагает освоение выпускником методов программирования и методов разработки эффективных алгоритмов решения прикладных задач на основе применения современных средств разработки и анализа программного обеспечения для выбора необходимых инструментальных средств обеспечения политики безопасности информационных систем;

- третий уровень – управление информационной безопасностью информационно-телекоммуникационных систем государственного и коммерческого сектора предполагает фактическое управление рисками в контексте создания систем информационной безопасности для крупных корпоративных информационных систем, информационных систем государственного сектора и электронного правительства.

Обращает на себя внимание то обстоятельство, что разработанные на основе существующего ГОСа рядом ВУЗов программы подготовки магистров направления информационной безопасности, ориентированы прежде всего на формирование компетенций базового и технологического уровня.

При этом программами подготовки магистров, с одной стороны, основной акцент делается на изучение принципов и методов противодействия несанкционированному информационному воздействию, анализу каналов утечек информации, с другой стороны, - явно недостаточное внимание уделяется проблеме организации производственных процессов и информационных систем в соответствии с требованиями по защите информации.

Совершенно за рамками обучения в высшей школе остаются вопросы подготовки специалистов в вопросах разработки комплексного подхода управления информационной безопасностью, формированию предложений по совершенствованию системы управления информационной безопасностью, разработки и реализации политики информационной безопасности в государственных и корпоративных информационных системах.

В то же время ряд западных школ уделяет значительное внимание проблеме подготовки кадров в сфере именно подготовки высшего звена менеджеров в области управления информационной безопасностью.

Таким образом, в настоящее время в нашей стране осуществляется формирование новой отрасли знаний ***отражающей возможность управления рисками в контексте создания системы информационной безопасности***, включающей в себя методологические, философские и правовые аспекты сферы информационной безопасности и защиты информации применительно к проблемам крупных корпоративных информационных систем частного сектора экономики и электронного правительства.

### Требования к абитуриенту

Лицо, поступающее на обучение по программе «Управление информационной безопасностью» должно иметь специальное образование в области экономики, менеджмента, права и инфокоммуникационных технологий, быть знакомым с основами проектирования, анализа, внедрения и сопровождения корпоративных информационных систем.

Учащийся должен обладать способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем в сфере управления информационной безопасностью, характеризовать комплекс мер по управлению информационной безопасностью, организовывать и поддерживать его.

Порядок и содержание конкурсного отбора абитуриентов, включая состав конкурсных процедур, определяется с учетом Концепции программы и в соответствии с Положением НИУ ВШЭ о порядке приема для обучения по программам магистратуры НИУ ВШЭ.

На программу принимаются лица, имеющие высшее образование и выдержавшие конкурсные испытания, свидетельствующие о способности абитуриента к приобретению знаний и навыков в рамках магистерской программы. При поступлении на программу предполагаются вступительные испытания в форме портфолио (конкурс документов), включающие следующие документы:

- диплом о высшем образовании и приложение к нему;

- дипломы победителей, призеров и лауреатов студенческих конкурсов научных работ, исследовательских проектов и олимпиад различных уровней;

- дипломы и сертификаты, свидетельствующие о повышении профессиональной квалификации, о наградах и поощрениях;

-мотивационное письмо;

-рекомендательные письма известных преподавателей или практиков, занимающихся информационной безопасностью;

- научные работы абитуриента в электронном и бумажном виде (опубликованные или рукописные), авторские свидетельства, свидетельства об отраслевой регистрации разработок;

-сведения о получении именных стипендий (справка из деканата/учебной части вуза, подтверждающая получение именной стипендии вуза, города, региона, правительства, Президента РФ, фондов общественных организаций и т.п.

### Характеристика профессиональной деятельности выпускника ОП

Выпускник указанной магистерской программы помимо компетенций магистра по направлению бизнес- информатика дополнительно приобретает ряд компетенций, к числу которых можно отнести способности и навыки:

- проектировать и создавать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объекта защиты;

- производства и детального обоснования выбора архитектуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты;

- оценивать риски в сфере обеспечения безопасности информационных систем и информационно- коммуникационных технологий;

- понимать и анализировать направления развития ИКТ объекта защиты;

- прогнозировать эффективность функционирования систем информационной безопасности,

- самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности.

Выпускник НИУ-ВШЭ, завершивший обучение на магистерской программе «Управление информационной безопасностью», получает высококачественную теоретическую университетскую подготовку, обладает знаниями и практическими навыками аналитической поддержки процессов принятия решений в сфере управления информационной безопасностью, навыками ведения самостоятельной научной работы, включая дальнейшее повышение уровня знаний в аспирантуре и докторонтуре.

Основной акцент подготовки магистров делается на необходимость обладать высокими компетенциями в области теоретических и организационно-правовых аспектов безопасности компьютерных систем, криптографических и статистических методов защиты, типовых подсистем и решений обеспечения информационной безопасности.

С этой целью студенты должны изучить содержание работ по управлению информационной безопасностью на уровне известных и достаточно широко применяемых решений для основных программно-аппаратных сред. В конце обучения студент должен твердо ориентироваться в законодательно-правовой базе, регулирующей применение средств информационной безопасности в организациях различных форм собственности. Студент должен иметь представление о структуре и составе требований государственных органов, предъявляемых к системам ИБ, подлежащих развертыванию и применению в современных ИТКС различного назначения.

Компетенции учащихся ориентированы на решение задач и приобретение навыков в следующих сферах:

- определение организационных целей и стратегий защиты информационных технологий;

- идентификация и анализ угроз требованиям защиты информационных технологий;

- идентификация и анализ угроз активам информационных технологий в пределах организации;

- идентификация и анализа рисков;

- определение соответствующих защитных мер;

- контроль выполнения и функционирования защитных мер, которые являются необходимыми для обеспечения эффективной защиты информации и услуг в пределах организации;

- разработка и реализация программы осведомленности о защите;

- обнаружение инцидентов и реагирование на них.

Подготовка студентов и аспирантов включает ведение, в том числе ими, научно исследовательской работы с целью подготовки магистерской или, соответственно, кандидатской диссертации.

Подготовка студентов осуществляется по следующим основным видам их будущей деятельности: аналитическая, организационно-управленческая, проектная, научно-исследовательская, консалтинговая, иновационно- предпринимательская.

### Планируемые образовательные результаты, формируемые в результате освоения ОП

При подготовке магистра по программе «Управление информационной безопасностью» профессорско-преподавательский состав исходит из того, что выпускник должен обладать следующим набором компетенций, формируемых в процессе обучения:

- способность к самостоятельному освоению новых методов исследования, изменению научного и научно-производственного профиля своей профессиональной деятельности;

- способность принимать организационно-управленческие решения и готовность нести за них ответственность, в т.ч. и в нестандартных ситуациях;

- способность пользоваться иностранными языками как средством профессионального общения;

- умение применять методы системного анализа и моделирования для разработки комплекса мер по обеспечению информационной безопасности организации (учреждения);

- разрабатывать стратегию развития системы информационной безопасности предприятия, планировать процессы управления жизненным циклом и организовывать исполнение указанных процессов;

- осуществлять моделирование бизнес-процессов, осуществлять исследования и поиск новых моделей и методов совершенствования системы информационной безопасности;

- знать основания и пределы ограничения конституционных прав на информацию, характеризовать правовой режим информации, осуществлять комплекс мер по реализации правового режима.

### Организация проектной и/или научно-исследовательской работы обучающихся.

В рамках реализации проекта кафедрой информационной безопасности осуществляется проведение ежегодных международных научно-практических конференций «Актуальные проблемы управления информационной безопасностью», участие в которой принимает ряд ведущих российских и иностранных специалистов в указанной сфере.

Программа конференции ориентирована на решение вопросов управления информационной безопасностью. В рамках конференции осуществляется проведение секций, выступление наиболее авторитетных аналитиков по исследованию и практической реализации системы информационной безопасности.

В работе конференции активное участие принимают студенты ВШЭ, представившие ряд докладов по проблематике управления информационной безопасностью.

В процессе обучения на магистерской программе студенты с первого курса прикрепляются к научному руководителю для подготовки магистерской диссертации по наиболее актуальным научным направлениям.

Научный семинар, в концептуальном плане реализовывается в форме мозговых штурмов тех или иных актуальных проблем, как теоретических (фундаментальных), так и прикладных. В первом случае приоритет отдается разработке теоретической концепции решения проблемы, во втором – разработке комплекса мероприятий по обеспечению информационной безопасности. Для проведения научных семинаров задействуется как штатный профессорско-преподавательский состав, так и приглашенные лекторы, являющиеся признанными специалистами в обеспечении информационной безопасности.

Предполагается, что в качестве направлений научно-исследовательской работы будут избраны актуальные проблемы организационно-правового обеспечения информационной безопасности, криптографических и статистических методов, правоприменительной практики в сфере информационной безопасности.

В ходе научно-исследовательской работы учащиеся осуществляют подготовку экспертиз по конкретным заданиям преподавателей, а затем представлящищают их в процессе коллективного обсуждения.

1. Приказ Министерства образования и науки Российской Федерации № 497 от 28 октября 2009 года [↑](#footnote-ref-1)
2. Приказ Министерства образования и науки Российской Федерации № 496 от 28 октября 2009 года; [↑](#footnote-ref-2)
3. Приказ Министерства образования и науки Российской Федерации № 683 от 23 июня 2010 г., Приказ Министерства образования и науки Российской Федерации № 708 от 24 июня 2010 г. [↑](#footnote-ref-3)