Федеральное государственное бюджетное учреждение науки
Институт проблем региональной экономики Российской академии наук

«УТВЕРЖДАЮ»

Директор ФГБУН Институт проблем региональной экономики Российской академии наук

Д.э.н., проф. А.Д. Шматко
«22» сентября 2025 г.

Утверждена на заседании Ученого совета ФГБУН Институт проблем региональной экономики Российской академии наук протокол №13 от «22» сентября 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
профессиональной переподготовки

«Информационная безопасность»

(форма обучения – очная, с применением дистанционных технологий, 250 часов, итоговая аттестация в форме экзамена)

г. Санкт-Петербург
2025 г.

Авторы программы:

Руководитель образовательной программы:

1. Афанасьева Наталья Владимировна, д.э.н., проф., главный научный сотрудник Лаборатории комплексного исследования пространственного развития регионов Института проблем региональной экономики Российской академии наук

Программа разработана:

2. Песоцкий Андрей Алексеевич, к.э.н., доц., научный сотрудник Лаборатории комплексного исследования пространственного развития регионов Института проблем региональной экономики Российской академии наук
3. Назарова Евгения Андреевна, к.э.н., старший научный сотрудник Лаборатории комплексного исследования пространственного развития регионов Института проблем региональной экономики Российской академии наук

Программа рассмотрена на заседании
научно-методической комиссии ИПРЭ РАН «18» сентября 2025г., протокол №7

СОДЕРЖАНИЕ:

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Цель реализации программы.

Целями реализации программы «Информационная безопасность» являются совершенствование имеющихся и/или формирование у обучающихся (слушателей) новых необходимых компетенций (знаний и умений), необходимых для последующего ведения нового вида профессиональной деятельности и выполнения трудовых функций в сфере информационной безопасности (по обеспечению информационной безопасности автоматизированных систем от вредоносных технических воздействий в рамках ОКВЭД 75.24 «Деятельности по обеспечению общественного порядка и безопасности. Обеспечение безопасности средств связи и информации»).

При разработке содержания Программы в части требований к результатам освоения образовательных программ учтены требования обеспечения преемственности по отношению к федеральным государственным образовательным стандартам высшего профессионального образования (ФГОС ВПО) по направлению подготовки «Информационная безопасность», а именно ФГОС ВПО 10.05.01 «Компьютерная безопасность» (квалификация (степень) «специалист») по специализации «Информационная безопасность объектов информатизации на базе компьютерных систем».

Программа относится к дополнительным профессиональным программам в области информационной безопасности (далее - ИБ) и разработана на основании установленных квалификационных требований (видов профессиональной деятельности, трудовых функций и уровней квалификации) профессионального стандарта для «Специалиста по информационной безопасности» приказом Министерства труда и социальной защиты Российской Федерации, а также с учётом иных доступных квалификационных требований, указанных в квалификационных справочниках, утверждаемых в порядке, устанавливаемом Правительством Российской Федерации, по соответствующим должностям, профессиям, специальностям (в соответствии с Приказом Минтруда России №148н от 12 апреля 2013 г. «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов»).

Кроме того, при разработке программы учитывались требования и положения:

- Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»;

- Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499), зарегистрированного в Минюсте РФ 20 августа 2013 г. Регистрационный № 29444;

- Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);

- ранее использовавшегося Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090301 «Компьютерная безопасность» (квалификация (степень) "специалист")" (утв. приказом Минобрнауки РФ от 17.01.2011 № 69, ред. от 31.05.2011, Зарегистрировано в Минюсте РФ 20.04.2011 Регистрационный № 20544).

Плановая (нормативная) продолжительность освоения Программы составляет 512 и более академических часов аудиторных занятий (в зависимости от набора выбранных программ, модулей, курсов вариативной части программы).

Программа разработана Учебным центром в инициативном порядке (Приказ Директора УЦ от «16 » декабря 2014 г. № 01/11).

Обучение по данной дополнительной образовательной Программе направлено на решение следующих основных задач:

- получение и углубление профессиональных знаний и умений обучающихся по правовым основам защиты информации, организационным мерам и техническим средствам обеспечения безопасности при использовании современных информационных технологий на предприятиях;

- удовлетворение потребности специалистов в получении знаний об актуальных нормативных требованиях к защите и о новейших достижениях в области защиты конфиденциальной информации и систем её обработки (в комплексном обновлении их профессиональных компетенций, в рамках того же вида профессиональной деятельности);

- популяризация передовых технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации предприятий (объединений), организаций и учреждений, распространение передового опыта по успешному решению задач обеспечения информационной безопасности;

- оказание помощи предприятиям (объединениям), организациям и учреждениям в повышении квалификации и переподготовке руководителей и инженерно-технических работников (специалистов) служб безопасности и подразделений защиты информации по вопросам построения и эффективного применения комплексных систем защиты информации;

- профессиональная переподготовка руководителей и инженерно-технических работников (специалистов по защите информации) предприятий и организаций, в соответствии с квалификационными требованиями к персоналу в штате у соискателя лицензии (лицензиата) на осуществление лицензируемых видов деятельности по направлениям ФСБ России и ФСТЭК России.

Программа ориентирована на следующие категории обучающихся (специалистов, слушателей):

- начальников служб безопасности, руководителей подразделений обеспечения информационной безопасности (900ИБ), технической защиты конфиденциальной информации (ТЗКИ), ответственных за состояние и обеспечение ИБ и организацию работ по созданию комплексных систем защиты конфиденциальной информации предприятий. Возможное наименование должностей:

- Начальник службы/ отдела/ департамента/ лаборатории/ сектора ИБ/ ТЗИ/ ПДиТР/ ПДТР/ ЗИ (защите информации)

- Руководитель службы/отдела/департамента ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ

- Заместитель руководителя по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ

- Заместитель руководителя службы/отдела/департамента корпоративной безопасности по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ

- Главный специалист по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ

- Главный инженер по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ

- аналитиков подразделений ОИБ (ТЗКИ), отвечающих за анализ состояния информационной безопасности, определение требований к защищенности различных подсистем ИС и путей обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации. Возможное наименование должностей:

- Специалист/эксперт/инженер в области ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
- Специалист/эксперт/инженер по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
- Специалист/эксперт/инженер по безопасности компьютерных систем
- Специалист/эксперт/инженер по анализу защищенности компьютерных систем
- Специалист/эксперт/инженер по безопасности распределенных компьютерных систем
- Специалист/эксперт/инженер по безопасности информационных ресурсов и информационных систем
- Специалист/эксперт по обеспечению безопасности информации
- Консультант по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ

- администраторов средств защиты и специалистов подразделений ОИБ (ТЗКИ), ответственных за защиту конфиденциальной информации техническими средствами. Возможное наименование должностей:

- Техник/администратор по ИБ/ТЗИ/ПДиТР/ПДТР/ЗИ
- Администратор безопасности операционных систем и систем управления базами данных

1.2 Характеристика нового вида профессиональной деятельности, новой квалификации.

Слушатель, успешно завершивший обучение по данной Программе, должен решать профессиональные задачи по обеспечению защищенности компьютерных систем от вредоносных технических воздействий в рамках «Деятельности по обеспечению общественного порядка и безопасности. Обеспечение безопасности средств связи и информации» (Код ОКВЭД75.24).

А. Область профессиональной деятельности слушателей, прошедших обучение по Программе для выполнения нового вида профессиональной деятельности по обеспечению защищенности компьютерных систем от вредоносных технических воздействий включает сферы техники и технологии, охватывающие совокупность проблем, связанных с:

- анализом и оценки уровня защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий в условиях существования угроз в информационной сфере
- эксплуатацией и администрированием средств и систем защиты информации компьютерных систем.

Б. Объектами профессиональной деятельности являются:

- автоматизированные системы, входящие в них средства обработки, хранения и передачи информации и информационно-технологические ресурсы, подлежащие защите и функционирующие в условиях существования угроз в информационной сфере;
- технологии обеспечения информационной безопасности автоматизированных систем;
- системы управления информационной безопасностью автоматизированных систем;
- методы и реализующие их средства защиты информации в компьютерных системах;

- процессы, возникающие при защите информации, обрабатываемой в компьютерных системах;

- методы и реализующие их системы и средства контроля эффективности защиты информации в компьютерных системах.

В. Виды профессиональной деятельности и решаемые задачи.

Программа ориентирована на подготовку к следующим подвидам профессиональной деятельности:

- организационно-управленческая;
- эксплуатационная;
- контрольно-аналитическая.

Слушатели, успешно завершившие обучение по данной Программе, должны решать следующие профессиональные задачи в соответствии с подвидами профессиональной деятельности:

Организационно-управленческая деятельность:

- управление информационной безопасностью объекта;
- организация работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа;
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- контроль эффективности реализации политики информационной безопасности объекта;
- разработка проектов нормативных и методических документов, регламентирующих работу по защите информации и иных организационно-распорядительных документов;
- организация работы малых коллективов исполнителей с учетом требований защиты информации;
- организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядок выполнения работ;
- участие в определении потребности в средствах защиты информации, контроль их поставки и эксплуатации;
- поиск рациональных решений при выборе средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения.

Эксплуатационная деятельность:

- выполнение работ по защите информации;
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта;
- проверка технического состояния и остаточного ресурса оборудования защиты информации, организация профилактических проверок и текущего ремонта;
- приемка и освоение программно-аппаратных средств защиты информации;
- составление инструкций по эксплуатации аппаратно-программных средств защиты информации;
- обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы;
- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;
- проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

Контрольно-аналитическая деятельность:

- контроль эффективности реализации политики информационной безопасности объекта;

- проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;

- предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;

- применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;

- участие в обследовании объектов информатизации, их категорировании и аттестации по требованиям безопасности информации;

- проведение экспериментально-исследовательских работ при аттестации объектов с учетом требования к обеспечению защищенности компьютерной системы;

- проведение инструментального мониторинга защищенности компьютерных систем;

- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей;

- сбор и анализ исходных данных для проектирования систем защиты информации.

Г. Уровень квалификации в соответствии с профессиональным стандартом**

Профессиональная переподготовка по настоящей Программе осуществляется на базе высшего и среднего профессионального образования.

К освоению данной дополнительной профессиональной Программы переподготовки допускаются лица:

- имеющие среднее профессиональное и (или) высшее образование;

- получающие среднее профессиональное и (или) высшее образование.

1.3 Планируемые результаты обучения.

1.3.1. Приобретаемые профессиональные компетенции.

Слушатель, успешно завершивший обучение по данной Программе, должен обладать следующими профессиональными и общепрофессиональными компетенциями (коды ПК даны в соответствии с ФГОС ВПО 10.05.01 (090301)):

Общепрофессиональные:

- понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ОПК-3);

- использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-5);

- учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности (ОПК-7);

- работать с программными средствами прикладного, системного и специального назначения (ОПК-8);

- разрабатывать формальные моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ОПК-11);

- организовать антивирусную защиту информации при работе с компьютерными системами (ОПК-13);

Профессиональные:

В проектной деятельности:

- проводить сбор и анализ исходных данных для проектирования систем защиты информации (ПК-21);

- участвовать в разработке проектной документации (ПК-22);

- проводить анализ проектных решений по обеспечению защищенности компьютерных систем (ПК-23);

- участвовать в разработке системы защиты информации предприятия (организации) и подсистемы информационной безопасности компьютерной системы (ПК-24);

- оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи (ПК-25);

В контрольно-аналитической деятельности:

- участвовать в проведении экспериментально-исследовательских работ при аттестации системы защиты информации с учетом требований к уровню защищенности компьютерной системы (ПК-26);

- к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей (ПК-27);

- обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения (ПК-28);

- оценивать эффективность систем защиты информации в компьютерных системах (ПК-29);

В организационно-управленческой деятельности:

- организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (ПК-30);

- разрабатывать оперативные планы работы первичных подразделений (ПК-31);

- разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы (ПК-32);

- разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-33);

В эксплуатационной деятельности:

- производить установку, тестирование программного обеспечения и программно-аппаратных средств по обеспечению информационной безопасности компьютерных систем (ПК-34);

- принимать участие в эксплуатации программного обеспечения и программно-аппаратных средств обеспечения информационной безопасности компьютерных систем (ПК-35);

- производить проверку технического состояния и профилактические осмотры оборудования по защите информации (ПК-36);

- выполнять работы по приему, настройке, регулировке, освоению и восстановлению работоспособности оборудования защиты информации (ПК-37);

- разрабатывать и составлять инструкции и руководства пользователей по эксплуатации средств обеспечения информационной безопасности компьютерных систем и аппаратно-программных средств защиты информации (ПК-38).

1.3.2. Приобретаемые знания и умения

Слушатель, успешно завершивший обучение по данной Программе, должен обладать знаниями и умениями в следующих областях науки, техники и технологии, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере:

Знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации

- сущность и понятие информационной безопасности, характеристику ее составляющих

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области

- правовые основы организации защиты государственной тайны и конфиденциальной информации

- методики оценки и разработки моделей угроз информационной безопасности

- правовые нормы и стандарты по лицензированию в области обеспечения защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну и сертификации средств защиты информации

- систему организации комплексной защиты информации ограниченного доступа в системе, включая защиту персональных данных

- технические каналы утечки информации, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации

- методы и способы несанкционированного доступа (НСД) к информации, способы и средства защиты от НСД к информации на объектах информатизации

- методы и способы защиты информации с использованием СКЗИ

- принципы и методы управления системой обеспечения информационной безопасности в ведомстве (предприятии, организации)

- существующие криптографические алгоритмы, используемые для ЗИ, и принципы построения защищенного документооборота с использованием электронной подписи и виртуальных частных систем

- принципы организации информационных систем в соответствии с требованиями по защите информации

- источники угроз информационной безопасности и меры по их предотвращению

- современные программно-аппаратные средства и способы обеспечения информационной безопасности в КС

- состав и принципы работы защищенных компьютерных систем, операционных систем и средств

- особенности применения программно-аппаратных и технических средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных

- источники угроз информационной безопасности и меры по их предотвращению

- требования по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации

- основные виды политик управления доступом и информационными потоками в компьютерных системах

- принципы построения современных операционных систем и особенности их применения для решения задач защиты информации

- механизмы реализации вредоносных программно-технических и информационных воздействий в компьютерных системах

- защитные механизмы и средства обеспечения сетевой безопасности

- средства и методы предотвращения и обнаружения вторжений

- основные средства и методы анализа программных реализаций

- технические каналы утечки информации и методы защиты

- содержание и порядок аттестации компьютерных систем на предмет их соответствия требованиям по защите

- принципы работы и правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты и другого оборудования

- организацию ремонта и технического обслуживания средств и систем безопасности

- порядок оформления технической документации по защите информации инструкции по соблюдению режима проведения специальных работ

- методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации

- порядок оформления документации по приемке и постановке на учет в организации приобретаемых программно-аппаратных средств защиты информации

- правила и нормы охраны труда, техники безопасности, производственной (промышленной) санитарии и противопожарной защиты.

Уметь:

- применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах

- осуществлять техническое обслуживание и текущий ремонт программно-аппаратных средств обеспечения ИБ

- проводить мониторинг эффективности программно-аппаратных средств обеспечения ИБ в КС

- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации

- применять технические средства обеспечения информационной безопасности

- участвовать в эксплуатации технических средств обеспечения информационной безопасности

- проводить мониторинг эффективности технических средств обеспечения ИБ в КС

- участвовать в эксплуатации компонентов подсистем безопасности КС, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности

- выполнять работы по администрированию подсистем безопасности компьютерных систем

- производить установку и адаптацию компонентов подсистем безопасности компьютерных систем

- вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в компьютерных системах

- формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе

- применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

- проводить анализ показателей качества сетей и систем связи

- анализировать и оценивать угрозы информационной безопасности объекта

- оценивать полноту и качество выполнения работниками организации требований политики безопасности

- иметь навыки по установке, настройке, эксплуатации и обслуживанию аппаратно-программных средств защиты информации

- анализировать и оценивать угрозы информационной безопасности объекта

- пользоваться нормативными документами по защите информации

- разрабатывать концепции, политики и иные организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации

- разрабатывать документы, необходимые для аттестации объектов информатизации по требованиям безопасности информации

- правильно эксплуатировать систем и средства, предназначенные для эффективного функционирования комплексной системы защиты информации в подразделениях организации

Владеть:

- профессиональной терминологией;

- навыками применения средств антивирусной защиты;

- навыками организации и обеспечения режима защиты информации;

- навыками эксплуатации комплексов удостоверяющих центров;
- методами технической защиты информации;
- методами организации и управления деятельностью;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

1.3.3. Достигаемый уровень квалификации

Настоящая Программа обеспечивает достижение 5 (пятого) уровня квалификации (при исходном среднем профессиональном образовании) или 6 (шестого) уровня квалификации (при исходном высшем образовании) в соответствии с требованиями Профессионального стандарта «Специалист по информационной безопасности», указанного в п. 1.1.

Наименование вида профессиональной деятельности: деятельность по обеспечению защищенности компьютерных систем от вредоносных технических воздействий.

Функциональная карта вида профессиональной деятельности:

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень квалификации
A	Эксплуатация защищенных КС и применение методов и средств обеспечения их безопасности	Пятый	Применение программно-аппаратных средств обеспечения информационной безопасности в КС	A/01.5	Пятый
			Применение технических средств обеспечения информационной безопасности защищенных КС	A/02.5	Пятый
			Эксплуатация комплексных систем обеспечения информационной безопасности в КС	A/03.5	Пятый
B	Администрирование и эксплуатация аппаратно-программных средств защиты информации в компьютерных системах	Шестой	администрирование систем безопасности КС	B/01.6	Шестой
			организация профилактических проверок регламентов технического обслуживания и текущего ремонта систем безопасности КС	B/02.6	Шестой
			приемка и освоение программно-аппаратных средств защиты информации	B/03.6	Шестой

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план

Настоящая Программа разработана и реализуется с учётом основных особенностей профессиональной деятельности руководителей и специалистов подразделений информационной безопасности и защиты конфиденциальной информации, а именно:

- сложностью единовременного отрыва от работы на продолжительное время для освоения учебных дисциплин, обусловливающей необходимость реализации возможности поэтапного модульного обучения;
- высокой динамикой изменений в сфере ИТ, в области угроз безопасности, технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации, требующей постоянной актуализации соответствующих модулей (курсов, дисциплин) обучения;
- наличием существенных различий в исходных образовательных уровнях и профессиональной подготовленности обучающихся.

С учетом вышесказанного, Программа построена по модульному принципу и предполагает определённую вариативность, позволяющую в наибольшей степени обеспечить соответствие обучения конкретным направлениям и подвидам профессиональной деятельности (специализациям) и адаптивность к задачам, решаемым специалистами в рамках своих должностных или функциональных обязанностей (в дальнейшем называемую актуализацией).

Часть плановых часов обучения по специальному (профессиональному) циклу Программы) отводятся на вариативную часть для актуализации знаний и углубленного изучения нескольких выбранных для специализации модулей (курсов, дисциплин).

Модули актуализации (курсы вариативной части для углубленного изучения материала отдельных разделов и тем) выбираются из заданного для данного направления списка самим обучающимся (специалистом) либо организацией, направившей его на обучение, в соответствии с поставленными перед ним задачами и его профессиональными интересами.

Возможность обучения по Программе специалистов с различными исходными образовательными уровнями и профессиональной подготовленностью обеспечивается наличием в Учебном плане и Программе переподготовки дисциплин (модулей, курсов) подготовительного естественнонаучного (инженерно-технического) цикла и вариативной части специального (профессионального) цикла.

При освоении Программы может производиться перезачет учебных дисциплин (модулей, курсов) как естественнонаучного, так и профессионального цикла, освоенных обучающимися ранее (или изучаемых параллельно) в ходе освоения ими основных образовательных программ профессионального образования соответствующего уровня, и (или) дополнительных профессиональных образовательных программ того же направления, в т.ч. в иных образовательных организациях/учреждениях.

2.2 Рабочие программы дисциплин

Наименование дисциплин (модулей курсов) разделов тем	Общее кол-во часов	В том числе			Контроль (зачет экзамен)
		Лекции	Практические занятия, семинары	Самостоятельная работа	
2	3	4	5	6	7
Естественнонаучный цикл					
Дискретная математика	**30**	**8**	**8**	**10**	**4**
Основы теории множеств	6	2	1	2	
Комбинаторика	4	1	1	2	
Математическая логика	5	1	2	2	
Переключательные функции	3	1	1	1	
Теория алгоритмов	3	1	1	1	
Основы теории конечных автоматов	3	1	1	1	
Теория графов	3	1	1	1	
Контрольные занятия	4				4
Теория вероятностей и математическая статистика	**30**	**8**	**8**	**10**	**4**
Случайные события	5	2	1	2	
Случайные величины	5	2	1	2	
Случайные векторы	5	1	2	2	
Случайные последовательности	3	1	1	1	
Математическая статистика	13	1	1	1	
Приложения математической статистики	5	1	2	2	
Контрольные занятия	4				4
Информационные технологии	**30**	**8**	**8**	**10**	**4**
Информация ИТ и ИС	4	1	1	2	
Технологии обработки различных видов информации	4	1	1	2	
Информационные хранилища Архивирование файлов Файловые серверы и базы данных	3	1	1	1	
Централизованные и распределённые системы обработки данных Облачные ИТ	3	1	1	1	

Сетевые технологии обработки и передачи информации	3	1	1	1	
Интеграция ИТ на рабочем месте пользователя Корпоративные ИС	3	1	1	1	
Системы удалённого доступа к государственным и коммерческим услугам	3	1	1	1	
Информационные сервисы сети Интернет	3	1	1	1	
Контрольные занятия	4				4
ИТОГО	**90**	**24**	**24**	**30**	**12**
Профессиональный цикл					
Базовая (обязательная) часть					
Безопасность информационных технологий	**20**	**6**	**6**	**6**	**2**
Основы безопасности ИТ	4	2		2	
Правовые основы обеспечения информационной безопасности	2	2			
Организационные меры защиты	6	2	2	2	
Средства защиты от внутренних нарушителей	2	0	2		
Обеспечение безопасности компьютерных сетей	4	0	2	2	
Контрольные занятия	2				2
Безопасность компьютерных сетей	**20**	**6**	**6**	**6**	**2**
Типовая IP-сеть организации	2	1		1	
Классификация сетевых уязвимостей и атак Работа с базами атак и уязвимостей	1		1		
Защитные механизмы и средства обеспечения безопасности	2	1		1	
Базовые принципы сетевого взаимодействия	1			1	
Безопасность физического и канального уровней	1	1			
Проблемы безопасности протокола разрешения адресов ARP	1		1		

Стандарт 8021х Безопасность на уровне порта	2	1		1	
Защита периметра сети	1		1		
Защита трафика на сетевом уровне	1			1	
Безопасность транспортного уровня модели OSI	1	1			
Анализ защищённости корпоративной сети как превентивный механизм защиты	1			1	
Защита трафика на транспортном уровне	1		1		
Обнаружение сетевых атак	1	1			
Общие проблемы безопасности служб прикладного уровня	1		1		
«Honeynet» или сеть-приманка для изучения поведения нарушителей	1		1		
Контрольные занятия	2				2
Работа органа криптографической защиты	**22**	**8**	**6**	**6**	**2**
Основы криптографии	4	2	1	1	
Нормативное регулирование вопросов криптографической защиты информации	4	2	1	1	
Организация и обеспечение безопасности хранения обработки и передачи по каналам связи с использованием СКЗИ	4	2	1	1	
Обеспечение юридической значимости электронных документов	4	1	1	2	
Корпоративные информационные и телекоммуникационные системы защищенные с использованием шифровальных (криптографических)	4	1	2	1	
Контрольные занятия	2				2
Использование ЭП и ИОК (PKI)	**18**	**6**	**4**	**6**	**2**
Традиционные бумажные и	1	1			

электронные документы					
Правовые вопросы применения ЭП и СКЗИ в России	2		1	1	
Криптографические методы защиты информации	1	1			
Электронный сертификат структура сертификата издание импорт и экспорт сертификатов	1		1		
Электронные ключи	1	1			
Электронные идентификаторы	1			1	
Криптопровайдеры (CSP)	1	1			
Интернет-банкинг Проблемы безопасности при применении электронных подписей	1		1		
Компоненты PKI	1			1	
Принципы доверия PKI	1		1		
Управление доверием	2	1		1	
Проверка подлинности цифровых сертификатов в инфраструктуре PKI	1			1	
Процедуры аннулирования сертификатов в PKI Списки отозванных сертификатов OCSP Server Revocation Provider	1	1			
Сервер меток времени (TSP Server)	1			1	
Усовершенствованная подпись	1			1	
Контрольные занятия	2				2
Безопасность операционных систем	**20**	**6**	**6**	**6**	**2**
Риски угрозы уязвимости атаки	2	1		1	
Встроенные средства защиты Windows	2		1	1	
Идентификация и аутентификация	2	1	1		
Разграничение доступа к ресурсам	2		1	1	
Защита сетевого взаимодействия	2	1	1		

Повышение уровня защищенности рабочей среды пользователей	2	1		1	
Анализ параметров безопасности и конфигурирование безопасности	2		1	1	
Обеспечение объективного контроля работы пользователей и системных администраторов	2	1		1	
Повышение защищенности служб	2		1	1	
Поддержание программного обеспечения в актуальном состоянии	1	1			
Контрольные задания	2				2
ИТОГО	**100**	**32**	**28**	**30**	**10**

Набор курсов вариативной части профессионального цикла.

Профессиональный цикл: Вариативная (актуализируемая) часть (дисциплины на выбор обучающихся по направлениям не менее час.)	**60**
Дисциплины по теме «Криптографическая защита информации PKI и электронная подпись» (не менее час.)	**10**
Использование ЭП и PKI	10
Автоматизация управления жизненным циклом сертификатов изданных с помощью "КриптоПро УЦ"	10
Разработка и управление инфраструктурой открытых ключей на базе Microsoft Windows	10
Использование ЭП и PKI с применением продуктов «Сигнал-КОМ»	10
Организационно-правовые основы применения ЭП и деятельности удостоверяющих центров	10
Оператор удостоверяющего центра	10
Инфраструктура открытых ключей на Microsoft Windows Server 2008 R2	10
Дисциплины по теме «Администрирование средств защиты информации» (не менее час.)	**10**
Порядок развертывания и применения PKI на основе ПАК "КриптоПро УЦ" 2.0	10
Эксплуатация и техническое обслуживание PKI на основе ПАК «КриптоПро УЦ»	10
Применение «КриптоПро IPsec» для обеспечения защиты данных передаваемых в IP-сетях	10
Порядок миграции на ПАК "КриптоПро УЦ" 2.0	10
Внедрение системы управления доступом Cisco Secure ACS Implementing Cisco Secure Access Control System (ACS)	10

ArcSight Express 4.0 администрирование и эксплуатация (ArcSight Express 4.0 CORR-Engine Administration and Operations)	10
ArcSight ESM Administrator 6 CORR Engine	10
ArcSight ESM Security Analyst	10
Построение и эксплуатация инфраструктуры аутентификации на основе продуктов электронные ключи eToken и SafeNet Authentication Manager 8.0	10
Эксплуатация инфраструктуры аутентификации на основе продуктов электронные ключи eToken и SafeNet Authentication Manager 8.0	10
Построение корпоративной системы защиты конфиденциальной информации на основе линейки продуктов Secret Disk компании «Аладдин Р.Д.»	10
Построение инфраструктуры аутентификации на основе продуктов компании Аладдин Р.Д. Электронные ключи eToken и система Token Management System	10
Aladdin Token Management System 2.0: установка настройка и эксплуатация системы	10
Система анализа защищенности Assuria Auditor	10
Внедрение Cisco Clean Agent для контроля доступа к сети	10
Внедрение системы защиты безопасности информации при помощи Check Point Endpoint Security R80	10
Администрирование Check Point Security Administration 2013 (R76)	10
Управление безопасностью средствами Check Point R77 (Check Point Security Administration R77)	10
Расширенные возможности по поиску неполадок в продуктах компании Check Point (Advanced troubleshooting Check Point)	10
Check Point - рекомендованная практика (Check Point best practice)	10
Учебный модуль по управлению работой приложений Check Point	10
Учебный модуль Check Point DLP	10
Учебный модуль Check Point IPS	10
Вводный курс по операционной системе JUNOS	10
Маршрутизация в ОС JUNOS (JUNOS Intermediate Routing (JIR))	10
Контроль доступа средствами JunosPulse (Junos Pulse Access Control (JPAC))	10
Изучение оборудования безопасного удаленного доступа JunosPulse (Junos Pulse Secure Access (JPSA))	10
Программное обеспечение JUNOS. Основные вопросы маршрутизации	10
Внедрение межсетевых экранов Cisco ASA	10

Многофункциональные межсетевые экраны FortiGate. Часть 1	10
Многофункциональные межсетевые экраны FortiGate. Часть 2	10
Использование сетевого оборудования Cisco®. Часть 1	10
Использование сетевого оборудования Cisco®. Часть 2	10
Применение системы сетевой безопасности на базе Cisco IOS	10
Реализация технологий VPN на оборудовании Cisco IOS	10
Внедрение системы предотвращения вторжений Cisco	10
Kaspersky Endpoint Security and Management. Базовый курс.	10
Kaspersky Endpoint Security and Management. Расширенный курс.	10
Kaspersky Endpoint Security for Windows. Расширенный курс	10
Планирование внедрение и поддержка инфраструктуры службы каталога Microsoft Windows Server 2003	10
Поддержка баз данных в Microsoft SQL Server 2005	10
Разработка безопасности для Microsoft SQL Server 2005	10
Разработка и управление инфраструктурой открытых ключей на базе Microsoft Windows	10
Внедрение и администрирование защиты в сети на базе Microsoft Windows Server 2003	10
Новые возможности Windows Server 2012	10
Управление System Center Operations Manager 2007	10
Deploying and Administering Microsoft Forefront Client Security	10
Deploying and Administering Microsoft Forefront Security for Exchange Server Forefront Security for SharePoint and Microsoft Forefront Server Security Microsoft	10
Обслуживание баз данных в Microsoft SQL Server 2008 R2	10
Установка и настройка операционной системы Windows 7	10
Планирование и управление развертыванием Windows 7	10
Настройка управление и обслуживание серверов Windows Server 2008	10
Основы Windows Server 2008 R2	10
Настройка сетевой инфраструктуры Windows Server 2008 и устранение неполадок	10

Настройка доменных служб Active Directory на базе Windows Server 2008 и устранение неполадок в их работе	10
Конфигурирование решений идентификации и доступа в среде Active Directory Windows Server 2008	10
Планирование развертывание и управление Microsoft Systems Center Configuration Manager 2007	10
Регулирование доступа пользователей в сеть с помощью Cisco NAC фаза 2	10
Основы инсталляции настройки и управления межсетевым экраном Palo Alto	10
Углубленный курс управления межсетевым экраном Palo Alto	10
Построение защищенных виртуальных сетей на основе IPsec с использованием алгоритмов шифрования ГОСТ на базе шлюзов безопасности S-Terra CSP	10
Обеспечение безопасности сетей с помощью маршрутизаторов и коммутаторов Cisco	10
Система централизованного управления Stonesoft Management Center (SMC) 5.4	10
Система защиты от атак Stonesoft IPS and Layer 2 Firewall 5.4	10
Межсетевой экран Stonesoft Firewall/VPN 5.4	10
Внедрение виртуальных частных сетей средствами Cisco ASA	10
Средство криптографической защиты информации «Верба-OW>>>	10
Система защиты информации «Vipnet»	10
Дисциплины по теме «Защита информации от утечек по техническим каналам» (не менее час.)	**10**
Защита информации от утечки по техническим каналам	10
Организация защиты от закладочных устройств	10
Дисциплины по теме «Защита персональных данных» (не менее час)	**10**
Защита персональных данных	10
Техническая защита персональных данных	10
Сложные проблемы применения законодательства о персональных данных в кредитно- финансовых учреждениях	10
Нетехнические методы защиты персональных данных и коммерческой тайны	10
Регулирование отношений при осуществлении проверок операторов персональных данных	10
Дисциплины по теме «Защищенный электронный документооборот» (не менее час)	**10**
Организация конфиденциального делопроизводства	10
Применение технологии управления правами AD RMS для защиты документов	10

Безопасность систем электронной почты	10
Дисциплины по теме «Управление информационной безопасностью» (не менее час)	**10**
Управление рисками (Risk Management)	10
Управление информационной безопасностью (InfoSecurity Governance)	10
Система управления инцидентами как основа обеспечения ИБ организации	10
Управление рисками безопасности информационных систем организаций	10
Расследование компьютерных инцидентов	10
Аудит ИБ на соответствие стандартам	10

2.3 Календарный учебный график

На освоение Программы Слушателю отводится 1 календарный год с даты зачисления в Центр образовательных программ ИПРЭ РАН

Обучение по Программе может проводиться как единовременно (непрерывно), так и поэтапно (дискретно), в том числе через освоение отдельных учебных курсов, предметов, дисциплин, модулей, прохождения практик, а также с использованием сетевого дистанционного взаимодействия. Порядок обучения определяется образовательной Программой, договором на обучение и индивидуальным план-графиком освоения программы.

Модули (дисциплины) Программы представлены в виде отдельных курсов, которые можно осваивать в разное время и в различной последовательности (в соответствии с индивидуальным графиком обучения и расписанием занятий). Однако рекомендуется начинать обучение с модулей базового естественнонаучного и обязательного специального (профессионального) циклов.

Наименование дисциплины	Нагрузка, акад. час.	Порядок прохождения дисциплин			
		Первая очередь	Вторая очередь	Третья очередь	Четвертая очередь
1	2	3	4	5	6
Естественнонаучный цикл	**90**	**90**			
Дискретная математика	30	30			
Теория вероятностей и математическая статистика	30	30			
Информационные технологии	30	30			
Профессиональный цикл	**160**				
Базовая (обязательная) часть	**100**		**100**		
Базовый курс по безопасности информационных технологий	20		20		
Безопасность компьютерных сетей	20		20		

Безопасность операционных систем	20		20		
Работа органа криптографической защиты	22		22		
Использование ЭП и ИОК (PKI)	18		18		
Вариативная (актуализируемая) часть (дисциплины на выбор обучающихся по направлениям специализации не менее час.)	**60**			**32**	**28**
Дисциплины по теме «Криптографическая защита информации PKI и электронная подпись» (не менее час.)	10				10
Дисциплины по теме «Администрирование средств защиты информации» (не менее час.)	10			6	4
Дисциплины по теме «Защита информации от утечек по техническим каналам» (не менее час.)	10			6	4
Дисциплины по теме «Защита персональных данных» (не менее час.)	10			10	
Дисциплины по теме «Защищенный электронный документооборот» (не менее час.)	10			10	
Дисциплины по теме «Управление информационной безопасностью» (не менее час.)	10				10

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1 Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

Обучение по Программе осуществляется на основе договоров об образовании, заключаемых со слушателями и (или) с физическими или юридическими лицами, обязующимися оплатить обучение слушателей, зачисляемых на обучение.

Профессиональная переподготовка по настоящей Программе осуществляется на базе высшего и среднего профессионального образования. Лица, желающие освоить дополнительную профессиональную программу, должны иметь:

- имеющие среднее профессиональное и (или) высшее образование;
- получающие среднее профессиональное и (или) высшее образование, при условии, что они получат дипломы об первичном образовании в процессе обучения по программе.

Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования. Наличие указанного образования должно подтверждаться документом государственного или установленного образца. Желательно иметь стаж работы (не менее 1 года), связанной с процессами обеспечения информационной безопасности в компаниях или организациях, или связанного с внедрением/эксплуатацией информационных систем.

При зачислении обучающегося экспертной комиссией учебного центра на основе предоставленных документов осуществляется анализ и зачёт (перезачёт) дисциплин (курсов, модулей) естественнонаучного цикла и вариативной части профессионального цикла, освоенных слушателем в процессе предшествующего обучения по основным профессиональным образовательным программам и (или) дополнительным профессиональным программам, после чего для него формируется индивидуальный План-график изучения базовых дисциплин и дисциплин вариативной части Программы.

Формы обучения и конкретные сроки освоения Программы определяются с учётом исходного уровня основного образования (квалификации и компетенций) слушателя, набора выбранных им курсов вариативной части Программы, расписания проведения назначенных курсов в Учебном центре и указываются в договоре об образовании.

3.2 Трудоемкость обучения

Нормативная трудоемкость обучения по данной программе – не менее 250 часов, включая все виды очной, дистанционной и самостоятельной учебной работы слушателя.

3.3 Форма обучения

Переподготовка специалистов по данной Программе реализуется в форме обучения с частичным отрывом от работы.

Обучение по модулям (курсам, дисциплинам) Программы проводится в очной форме с отрывом от работы и/или с использованием дистанционных образовательных технологий в форме онлайн-вебинаров с частичным отрывом от работы.

Обучение по Программе осуществляется на основе модульного принципа построения её содержания и индивидуальных учебных планов слушателей по освоению дисциплин (курсов) Программы, с использованием различных форм обучения и образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

Конкретная форма обучения устанавливается при зачислении слушателей на прохождение программы на этапе составления индивидуального плана-графика обучения.

Освоение программы может проводится как в очной, так и дистанционной форме. При этом, объем дистанционно изученных учебных курсов не может превышать 80% лекционного и 50% лабораторных и практических занятий (семинаров).

3.4 Режим занятий

При любой форме обучения учебная нагрузка устанавливается не более 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

Учебные занятия организованы в одну смену.

Продолжительность академического часа соответствует нормативным требованиям (45 мин).

Время проведения очных занятий и онлайн-вебинаров проводятся по рабочим дням с 10:00 до 17:30 по московскому времени.

Доступ к учебным пособиям и стендам для дистанционного выполнения лабораторных работ предоставляется слушателям круглосуточно.

3.5 Материально-технические условия реализации программы

Аудиторные занятия по модулям (курсам, дисциплинам) Программы включают лекции с демонстрацией презентаций на экране, практические работы с конкретными аппаратно-программными и техническими средствами защиты, а также лабораторные практикумы в специально оборудованных лаборатория.

3.6 Учебно-методическое обеспечение программы

Учебная литература предоставляется Центром через университетскую библиотеку biblioclub.ru, приобретенную ИПРЭ РАН на основании договора. Научные публикации имеются в открытом доступе на портале elibrary.ru

Учебные пособия и учебники:

1.Целых, А. Н. Информационно-аналитические системы обеспечения информационной и финансовой безопасности : учебное пособие : [16+] / А. Н. Целых, Э. М. Котов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2024. – 123 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=724382 (дата обращения: 01.10.2025). – Библиогр. – ISBN 978-5-9275-4787-6.
2. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 01.10.2025). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0.
3.Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 01.10.2025). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0.
4. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет им. А. А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694670 (дата обращения: 01.10.2025). – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670.
5. Помазанов, А. В. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А. В. Помазанов ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2024. – 134 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=724469 (дата обращения: 01.10.2025). – Библиогр.: с. 103-105. – ISBN 978-5-9275-4851-4.

Статьи:

1. Карепова С.Г., Костоломова М.В., Некрасов С.В., Пинчук А.Н. Информационная безопасность в условиях новой социальной реальности: специфика и способы сохранения // Социальные и гуманитарные знания. 2022. Т. 8. № 2 (30). С. 190-203.
2. Стоякина Е.Н., Калинина Г.В. Информационная безопасность в цифровых реалиях // Инновационная экономика: перспективы развития и совершенствования. 2023. № 3 (69). С. 146-151.

3. Карепова С.Г., Некрасов С.В., Пинчук А.Н. Информационная безопасность: специфика феномена, методы и способы ее обеспечения // Вестник Московского университета. Серия 18. Социология и политология. 2023. Т. 29. № 4. С. 200-220.
4. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51-57.
5. Кипкеева А.М., Урусов А.А. Информационная безопасность - важнейший элемент обеспечения экономической безопасности организации // Вестник Академии знаний. 2020. № 40 (5). С. 157-161.
6. Мустафаев А.Г., Кобзаренко Д.Н., Бучаев А.Я. Информационная безопасность - критическая составляющая цифровой экономики // УЭПС: управление, экономика, политика, социология. 2020. № 4. С. 38-43.
7. Яриков В.Г., Пашков М.В. Информационная безопасность и защита информации на предприятии // НБИ технологии. 2023. Т. 17. № 4. С. 47-51.
8. Мирабова Л. Современная защита информации и кибербезопасность // Ceteris Paribus. 2023. № 4. С. 56-59.
9. Кондрашова Н.Г. Защита информации как важная составляющая экономической безопасности // Modern Economy Success. 2022. № 6. С. 149-153.
10. Бирюков А.С. Защита информации в компьютерной сети предприятия // Молодой ученый. 2020. № 15 (305). С. 81-84.

3.7 Требования к кадровым условиям реализации программы

Реализация программы обеспечивается научными сотрудниками Института проблем региональной экономики РАН, ведущими образовательную деятельность, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора из числа специалистов, имеющих опыт практической работы в различных областях обеспечения информационной безопасности, включая проектирование, разработку, эксплуатацию и оценку средств и систем защиты информации. Для проведения занятий по дисциплинам естественнонаучного цикла могут привлекаться преподаватели ведущих вузов страны (на основе договоров).

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ (ФОРМЫ АТТЕСТАЦИИ, ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ)

Оценка качества освоения программы включает текущую, промежуточную и итоговую аттестацию обучающихся.

Кандидаты на зачисление на обучение по данной Программе документально подтверждают свой уровень образования (уровень образования специалистов, проходящих профессиональную переподготовку, должен быть не ниже уровня образования, требуемого для нового вида профессиональной деятельности).

При зачислении обучающегося экспертной комиссией учебного центра на основе предоставленных документов осуществляется анализ и зачёт (перезачёт) дисциплин (курсов, модулей) естественнонаучного цикла и вариативной части профессионального цикла, освоенных слушателем в процессе предшествующего обучения по основным профессиональным образовательным программам и (или) дополнительным профессиональным программам, после чего для него формируется индивидуальный План-график изучения базовых дисциплин и дисциплин вариативной части Программы.

Помимо документов о высшем или среднем профессиональном образовании к рассмотрению принимаются государственные документы и документы установленного образца о краткосрочном повышении квалификации по направлению информационной безопасности и защите информации, а так же сертификаты и свидетельства о прохождении учебных дисциплин (модулей, курсов) как естественнонаучного цикла, так и вариативной части профессионального цикла, изученных обучаемыми ранее (или изучаемых

параллельно) в ходе освоения ими основных образовательных программ профессионального образования Центре образовательных программ ИПРЭ РАН или иных образовательных учреждениях (выданные не ранее 5 лет с даты зачисления Слушателя в Центр).

Прохождение каждого курса/модуля/дисциплины Программы завершается зачетом. Зачет принимает преподаватель Учебного центра при предъявлении Слушателем документа, удостоверяющего личность. Зачет может проводиться в форме собеседования или в форме теста, который подразумевает: ответы на контрольные вопросы (обязательно); выполнение контрольных задач и заданий (опционально); выполнение контрольных лабораторных работ (опционально); собеседование с представителями работодателя (опционально).

Тестирование при помощи контрольных вопросов, контрольных задач и заданий может быть организованно в: устной форме; бумажной форме; с использованием электронных методов тестирования.

Для каждого теста разрабатывается система оценки, параметрами которой являются количество вопросов, их сложность, полнота ответа на вопрос. По результатам ответа на вопрос испытуемому присваивается определенное системой оценки количество баллов. Итоговое решение о прохождении теста принимается на основании превышения суммарно набранного количество баллов по всем вопросам над определенным системой оценки пороговым значением.

При использовании средств электронного тестирования, зачет может содержать от 10 до 40 вопросов 3-х уровней сложности. К вопросам предлагаются по три или четыре варианта ответов, сформулированных по принципам:

- Выбора: правильный, похожий на правильный, но имеющий неточность, совершенно неправильны, относящийся к смежной предметной области.

- Перечисления, когда из набора правильных и неправильных ответов необходимо выбрать наиболее полный правильный вариант.

Выполнение лабораторных работ производится на компьютерных стендах, воссоздающих или эмулирующих реальные объекты информационных систем, или с реальными приборами/установками/системами. Выполнение работ может проводится как под контролем преподавателя, так и самостоятельно.

Результаты зачета вносятся преподавателем в зачетную ведомость Слушателя. В случае неуспешной попытки, Слушатель вправе запросить время на самоподготовку и углубленное изучение дисциплины и пересдать зачет в любое согласованное с Учебным центром время.

Освоение дополнительной профессиональной образовательной Программы переподготовки завершается обязательной итоговой аттестацией обучающихся в форме зачёта. Итоговая аттестация Слушателей проводится в форме тестирования (возможно в электронном виде) по основным темам изученных базовых дисциплин профессионального цикла и заключительного собеседования с членами аттестационной комиссии. К собеседованию допускаются только успешно прошедшие тестирование Слушатели.

Итоговый аттестационный тест содержит 45 вопросов, выбираемых случайным образом из пула в 120 вопросов. На прохождение теста отводится полтора часа. Проходной бал 2/3 (30) правильных ответов. Допускается использование в Итоговой аттестации вопросов из зачетных материалов к составляющим Программу курсам/модулям/дисциплинам. В случае неуспешной попытки сдачи итогового теста, Слушателю предоставляется время на самоподготовку и возможность повторно пройти тестирование. По результатам успешного тестирования и собеседования по каждому Слушателю оформляется отдельное решение о прохождении (не прохождении) итоговой аттестации.

Считается, что обучающийся освоил Программу переподготовки, если он успешно завершил обучение по всем модулям (дисциплинам, курсам) циклов Программы в

соответствии со своим индивидуальным учебным планом (План-графиком) в объеме не менее 512 часов с обязательным прохождением базовой части (базовых специальных модулей) профессионального цикла Программы и прошёл итоговую аттестацию.

Слушателям, успешно освоившим Программу, выполнившим все требования учебного плана и прошедшим итоговую аттестацию, по решению аттестационной комиссии (состав которой утверждается руководителем образовательного учреждения) выдаются дипломы о профессиональной переподготовке по направлению «Информационная безопасность», которые удостоверяют право (соответствие квалификации) специалистов заниматься профессиональной деятельностью в сфере «Информационной безопасности».

Слушателям, не прошедшим итоговой аттестации или показавшим на итоговой аттестации неудовлетворительные результаты, а также слушателям, освоившим лишь часть Программы и/или отчисленным из организации, выдается справка об обучении.

При освоении Программы слушателем параллельно с получением среднего профессионального образования и (или) высшего образования диплом о профессиональной переподготовке выдаётся ему после получения соответствующего документа об основном образовании и о квалификации.

Темы практических работ по дополнительной профессиональной программе «Информационная безопасность»:

- принципы защиты информации на предприятии;
- условия, сопутствующие утечки информации;
- методы защиты информации;
- система защиты информации в банковских организациях;
- состав угроз информационной безопасности;
- методика отбора персонала для работы с конфиденциальной информацией;
- построение системы защиты информационной инфраструктуры на предприятии;
- система защиты коммерческой тайны на предприятии;
- защита информации в системах электронного документооборота;
- роль информационного права в информационной безопасности;
- защита информации в государственных информационных системах;
- защита информации в образовательных системах;
- защита информации в процессе переговоров;
- современные средства выявления угроз информационной безопасности;
- обзор методов и программного обеспечения для анализа сетевого трафика;
- программно-аппаратные комплексы анализа каналов утечки информации;
- методика инструктирования персонала правилам защиты секретов предприятия;
- разработка резервной модели комплекса для управления банком в кризисных случаях;
- разработка программного комплекса для защиты корпоративной сети;
- разработка программного комплекса для обнаружения вредоносного кода по сигнатурам;
- разработка механизмов защиты информационного портала для органов гос. власти;
- моделирование защищенных частных сетей по средствам VPN;
- разработка систем обнаружения и предотвращения компьютерных атак;
- защита информации при использовании платежных систем;
- защита информации при использовании банковских карт;
- анализ защищенности мобильных приложений от вредоносного кода;
- разработка предложений по противодействию угрозам в социальных сетях и мессенджерах;

Перечень примерных вопросов к экзамену по дополнительной профессиональной программе «Информационная безопасность»:

1. Основные понятия информационной безопасности.

2. Информационные технологии и необходимость ИБ.

3. Система защиты информации и ее структуры.

4. Экономическая информация как товар и объект безопасности.

5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.

6. Персональные данные и их защита.

7. Информационные угрозы, их виды и причины возникновения.

8. Информационные угрозы для государства.

9. Информационные угрозы для компании.

10. Информационные угрозы для личности (физического лица).

11. Действия и события, нарушающие информационную безопасность.

12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.

13. Способы воздействия информационных угроз на объекты.

14. Внешние и внутренние субъекты информационных угроз.

15. Компьютерные преступления и их классификация.

16. Исторические аспекты компьютерных преступлений и современность.

17. Субъекты и причины совершения компьютерных преступлений.

18. Вредоносные программы, их виды.

19. История компьютерных вирусов и современность.

20. Деятельность международных организаций в сфере информационной безопасности.

21. Государственное регулирование информационной безопасности в РФ.

22. Задачи ИБ в программе « цифровая экономика».

23. Доктрина информационной безопасности России.

24. Федеральные законы в сфере информатизации и информационной безопасности в РФ.

25. Уголовно-правовой контроль над компьютерной преступностью в РФ.

26. Политика безопасности и ее принципы.

27. Фрагментарный и системный подход к защите информации.

28. Методы и средства защиты информации.

29. Организационное обеспечение ИБ.

30. Организация конфиденциального делопроизводства.

31. Организационно-экономическое обеспечение ИБ.

32. Инженерно-техническое обеспечение компьютерной безопасности.

33. Организационно-правовой статус службы безопасности.

34. Защита информации в Интернете.

35. Электронная почта и ее защита.

36. Защита от компьютерных вирусов.

37. «Больные» мобильники и их «лечение».

38. Популярные антивирусные программы и их классификация.

39. Этапы и освоение защиты информации экономических объектов.

40. Криптографические методы защиты информации.

41. Оценка эффективности инвестиций в информационную безопасность.

42. Российские компании в сфере ИБ.

43. Фирмы, оценивающие работу персонала в компании.

44. Менеджмент и аудит ИБ на уровне предприятия.

45. Аудит ИБ автоматизированных банковских систем.

46. Аудит ИБ электронной коммерции.

47. Информационная безопасность предпринимательской деятельности.