

АННОТАЦИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ
ПРОГРАММЫ ПО СПЕЦИАЛЬНОСТИ
**10.05.05 БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В
ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ**

Специализация – Технологии защиты информации в правоохранительной сфере

Квалификация (степень) выпускника – Специалист по защите информации

Форма обучения – Очная, очно-заочная

Нормативный срок освоения образовательной программы – 5 лет

1.Цель образовательной программы

Целью образовательной программы является формирование у студентов общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВПО по специальности «Безопасность информационных технологий в правоохранительной сфере», подготовка высококвалифицированных специалистов, способных решать задачи комплексной защиты информации, обеспечения безопасности информационных систем и технологий в правоохранительной сфере.

2.Область и объекты профессиональной деятельности

Область профессиональной деятельности специалистов по защите информации включает области науки, техники и технологии, охватывающие совокупность проблем по обеспечению защищенности объектов информатизации с учётом специфики правоохранительной сферы в условиях информационных угроз.

Объектами профессиональной деятельности специалистов являются: информационные технологии и системы, информационные процессы и ресурсы в правоохранительной деятельности; методы и технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы, регламентирующие информационно-аналитическую деятельность в правоохранительной сфере; процессы управления информационной безопасностью на защищаемых объектах.

Выпускник сможет работать в профильных подразделениях правоохранительных органов и других государственных и муниципальных структурах власти, а также на предприятиях (в том числе в сфере ОПК) и в специализированных компаниях, являющихся производителями средств защиты информации и системными интеграторами в области обеспечения информационной безопасности.

3.Виды и задачи профессиональной деятельности

Выпускник подготовлен к решению разнообразных задач в рамках эксплуатационной, правоохранительной, организационно-управленческой, информационно-аналитической, научно-исследовательской, проектно-технологической и педагогической деятельности.

Эксплуатационная деятельность

Задачи:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации;
- участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- администрирование подсистем обеспечения информационной безопасности на объекте.

Организационно-управленческая деятельность

Задачи:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации;
- участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- администрирование подсистем обеспечения информационной безопасности на объекте.

Правоохранительная деятельность

Задачи:

- обеспечение законности и правопорядка;
- участие в предупреждении, выявлении, пресечении, раскрытии преступлений и иных правонарушений;
- участие в информационно-аналитическом и информационно-психологическом обеспечении оперативно-розыскных мероприятий и следственных действий.

Организационно-управленческая деятельность

Задачи:

- организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
- разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
- организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.

Информационно-аналитическая деятельность

Задачи:

- получение и обработка поступающей информации;
- участие в анализе и отборе данных и сведений для формирования информационных ресурсов;
- мультимедийная обработка акустических и видеозаписей, фотоматериалов с целью получения информации, необходимой для формирования ресурсов и оперативного реагирования;
- участие в противодействии деструктивным и негативным информационно-психологическим воздействиям;
- формирование автоматизированных справочных, оперативно-розыскных, криминалистических и иных учетов;
- осуществление информационного и оперативно-аналитического поиска;
- участие в осуществлении оперативно-розыскного анализа, идентификации, диагностики и прогнозирования, криминалистической диагностики;

Научно-исследовательская деятельность

Задачи:

- сбор, изучение, систематизация и обобщение научно-технической информации, отечественного и зарубежного опыта по проблемам информационно-аналитической работы и обеспечения защиты информации;

- анализ прикладных проблем информационно-аналитического обеспечения правоохранительной деятельности, защиты информации и обеспечения безопасности информационных технологий;
- разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок;
- проведение экспериментов по заданным методикам;
- выполнение прикладных научных исследований, подготовка отчетов, докладов на научно-практических семинарах и конференциях.

Проектно-технологическая деятельность

Задачи:

- сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации;
- участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации;
- адаптация к защищаемым объектам современных информационных технологий и методов обеспечения безопасности информации на основе отечественных и международных стандартов.

Педагогическая деятельность

Задачи:

- преподавание в общеобразовательных учреждениях, образовательных учреждениях начального профессионального, среднего профессионального, высшего профессионального и дополнительного образования дисциплин в области информационных технологий и информационной безопасности.

4.Профессиональные дисциплины

Формирование общекультурных компетенций студентов происходит в процессе изучения широкого спектра гуманитарных, социально-экономических, математических, естественнонаучных дисциплин. Профессиональные компетенции специалиста по защите информации в правоохранительной сфере обеспечиваются изучением профессиональных дисциплин, в частности:

История защиты информации и современное информационное противоборство, Теория информационной безопасности и методология защиты информации, Программирование: языки, методы и технологии; Системы и сети передачи информации, Основы электротехники и радиоэлектроники, Основы электро-, радиоизмерений, Средства вычислительной техники, Документоведение, Защита и обработка документов ограниченного доступа; Информационное право, Правовая защита информации; Организационная защита информации; Основы безопасности информационных технологий, Криптографическая защита информации, Программно-аппаратная защита информации, Инженерно-техническая защита информации; Стандарты информационной безопасности; Управление информационной безопасностью, Безопасность жизнедеятельности; Управление проектированием информационных систем и систем защиты информации; Специальные информационные технологии в правоохранительной сфере; Правоохранительные органы; Криминология; Информационно-аналитическое обеспечение правоохранительной деятельности, Информационно-психологическое обеспечение правоохранительной деятельности, Противодействие коррупции и незаконным финансовым операциям; Аудит информационной безопасности, Расследование инцидентов информационной безопасности; Методы и средства обнаружения компьютерных атак, комплексная система защиты объектов информатизации, Тактико-специальная подготовка, Огневая подготовка и др.

Для студентов 4-5 курса организован факультативный практикум по технологиям

безопасности и научно-исследовательский семинар по информационной безопасности

При проведении занятий используются традиционные и инновационные технологии обучения: интерактивные лекции, групповые дискуссии и проектное обучение, анализ деловых ситуаций, проведение деловых и ролевых игр, тренингов и т.п. Студенты активно вовлекаются в выполняемые кафедрой информационной безопасности исследовательские и прикладные проекты в интересах совершенствования образовательного процесса и решения практических задач НГУЭУ.

5. Возможные места практик

Базой для прохождения практик и подготовки выпускных квалификационных работ студентов, могут являться:

- Территориальные (региональные) структуры Федеральных правоохранительных органов Российской Федерации (МВД, ФСКН, ФТС, МЧС, Следственного комитета, Прокуратуры, др.);
- Управление ФСТЭК по Сибирскому Федеральному округу;
- Правительство Новосибирской области;
- Мэрия Новосибирска;
- Организации-лицензиаты ФСТЭК России и ФСБ России, имеющие право предоставлять услуги по проектированию, разработке и сопровождению систем и средств технической и криптографической защиты информации, в частности (Новосибирский НТЦ ФГУП «Научно-производственное предприятие ГАММА»; Новосибирский филиал ФГУП НТЦ «АТЛАС»; ООО Аттестационный технический центр; ООО «Безопасные информационные технологии»; ООО «Региональный аттестационный центр»; Группа компаний «АКСТЕЛ» и др.).

НГУЭУ является членом Межрегиональной общественной организации «Ассоциация защиты информации», включающей более 100 ведущих российских компаний, работающих в сфере информационной безопасности и информационных технологий, а также сотрудничает с Межрегиональной общественной организацией «Ассоциация руководителей служб защиты информации», что позволяет содействовать в организации практики студентов и трудоустройству в различных регионах.

6. Условия реализации образовательной программы

Учебно-методическое обеспечение

Уровень обеспеченности образовательной программы специалитета учебно-методической документацией и информационными материалами по всем дисциплинам. Библиотечный фонд НГУЭУ укомплектован актуальными печатными и/или электронными изданиями по дисциплинам базовой части всех циклов.

Электронно-библиотечная система [«znanium.com»](http://znanium.com) обеспечивает возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет.

Учебно-методические материалы представлены на информационном ресурсе сайта НГУЭУ (<http://nsuem.ru>) и специализированном сервере учебного полигона кафедры информационной безопасности.

Кадровое обеспечение

Реализация образовательной программы обеспечена научно-педагогическими кадрами, имеющими базовое образование, и/или ученую степень в соответствии с профилями преподаваемых дисциплин, активно занимающимися научной и методической деятельностью.

Ведущие преподаватели

Основу кадрового персонала образовательной программы составляет профессорско-преподавательский состав кафедры информационной безопасности (выпускающая кафедра) и других кафедр НГУЭУ, а также привлечённые специалисты-практики из государственных и коммерческих структур:

- Пестунова Тамара Михайловна, канд. техн. наук, доцент, зав. кафедрой
- Белов Виктор Матвеевич, профессор, д-р техн. наук, профессор
- Лисс Александр Андреевич, нач. отдела технической защиты персональных данных, ведущий инженер по ИБ лаборатории компьютерной и сетевой безопасности
- Мошегова Антонина Тадеушевна, канд. социол. наук, доцент,
- Пузынин Николай Георгиевич, заведующий лабораторией инженерно-технической защиты информации;
- Прокопов Максим Дмитриевич, генеральный директор ООО «Сибирская академия информационной безопасности»
- Пестунов Андрей Игоревич, канд. физ.-мат. наук, доцент, заведующий лабораторией компьютерной и сетевой безопасности
- Ревнивых Александр Владимирович, канд. техн. наук, доцент, проректор по науке НГУЭУ;
- Рыжов Владимир Анатольевич, канд. техн. наук, доцент,
- Свиридов Игорь Владимирович, канд. филос. наук, доцент
- Селифанов Валентин Валерьевич, начальник отдела Управления ФСТЭК России по СФО
- Соловьёв Владимир Александрович, коммерческий директор ГК «АКСТЕЛ»
- Ханин Андрей Геннадьевич, руководитель образовательных проектов ЗАО «Д-Линк Интернэшнл ПТЕ Лтд»

Материально-техническое обеспечение

Материально-техническое обеспечение учебного процесса включает в себя современные компьютерные классы, лингафонные кабинеты, лекционные аудитории с мультимедийными средствами обучения и др. В компьютерных классах установлено лицензионное программное обеспечение, используемое при изучении различных дисциплин, в т.ч.: системы моделирования бизнес-процессов Business Studio, ORG-MASTER Educational и ARIS Express, программное обеспечение в рамках лицензии MSDN, системы электронного документооборота Ефрат, ДЕЛО и др., система моделирования электронных схем Multisim Electronics Workbench, инструментарий разработки бизнес-планов ProjectExpert, виртуальный практикум по физике на основе интерактивных моделей «Открытая физика», пакеты для математического моделирования и расчётов Matlab и Mathcad, программы статистического анализа данных SPSS и Statistica, инструменты проектирования и документирования баз данных Erwin Community Edition, система имитационного моделирования AnyLogic Educational и многое другое специализированное программное обеспечение, в том числе авторские разработки преподавателей.

Для формирования практико-ориентированных профессиональных компетенций, приобретения исследовательского и практического опыта при кафедре информационной безопасности созданы учебно-исследовательские лаборатории (УИЛ).

На базе УИЛ компьютерной и сетевой безопасности создан учебный полигон для изучения аппаратных средств вычислительной техники, основ администрирования компьютерных сетей, программных и программно-аппаратных средств анализа уязвимостей, защиты информации и контроля их эффективности. Установлено современное лицензионное программное обеспечение. Студенты изучают сертифицированные программно-аппаратные средства защиты информации, многие из них предоставлены компаниями-производителями и ИТ-интеграторами в рамках договоров о сотрудничестве и академических лицензий. В лаборатории, в частности, представлены сертифицированные средства линейки «Аккорд», «Соболь», «Шипка», «Secret Net», «Континет», «E-token», «Аура» и др., средства анализа

защищённости сетей «XSpider», «MAX Patrol», средства контроля защищённости «Фикс», «Terrier», «Ревизор», а также широкий спектр средств на основе бесплатных свободных лицензий. Класс проектирования и защиты компьютерных сетей оборудован при содействии компании Д-Линк.

Специализированный кабинет электротехники и электроники создан на базе компьютерного класса с установленным программным обеспечением САПР «MULTISIM» и профессиональных мобильных учебных стендов KL-200, KL-210, Учебный стенд КС-900.

На базе УИЛ инженерно-технической защиты информации развёрнут полигон технической защиты информации, включающий более десяти специализированных учебных стендов для выявления технических каналов утечки информации и изучения соответствующих средств защиты. На их базе студенты изучают физические явления, порождающие технические каналы утечки информации, учатся выявлять несанкционированные источники излучения, применять средства подавления сигналов побочных электромагнитных излучений и наводок, обеспечивать защиту переговоров по сотовой связи и проводным телефонным линиям, предотвращать утечку информации по цепям электросети и заземления, оптическому, акустическому, виброакустическому и другим техническим каналам. В состав лаборатории входит специальное учебное помещение, аттестованное по требованиям безопасности.

Для изучения специальных дисциплин, связанных с расследованием преступлений, в НГУЭУ имеются криминалистическая лаборатория, для отработки практических навыков огневой подготовки используется тир.