

АННОТАЦИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ  
ПРОГРАММЫ ПО НАПРАВЛЕНИЮ  
**10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**Направленность (профиль)** – Информационная безопасность

**Квалификация (степень) выпускника** – Бакалавр

**Форма обучения** – Очная, очно-заочная

**Нормативный срок освоения образовательной программы** – 4 года

**1.Цель образовательной программы**

Целью образовательной программы является развитие у студентов формирование общекультурных и профессиональных компетенций в соответствии с требованиями ФГОС ВПО по направлению «Информационная безопасность».

**2.Область профессиональной деятельности**

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

Выпускник может работать в госструктурах, предприятиях и организациях разных форм собственности, в которых решаются задачи обеспечения информационной безопасности, а также в специализированных компаниях, предоставляющих услуги в сфере защиты информации, являющихся производителями и поставщиками средств технической защиты информации, системными интеграторами в области информационной безопасности.

**3.Виды и задачи профессиональной деятельности**

Выпускник подготовлен к решению разнообразных задач в рамках проектно-технологической, экспериментально-исследовательской, эксплуатационной и организационно-управленческой деятельности по информационной безопасности.

***Организационно-управленческая деятельность***

*Задачи:*

- анализ нормативно-правовой базы в области информационной безопасности и её применение в практической деятельности;
- разработка и обоснование политики безопасности, организационных мер, инструкций и регламентов с целью защиты информации;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, сохранения государственной и других видов тайн;
- контроль эффективности политики безопасности и совершенствование системы управления информационной безопасностью;
- организация работы малых коллективов исполнителей с учетом требований защиты информации.

***Проектно-технологическая деятельность***

*Задачи:*

- проведение аудита информационной безопасности на предприятии, сбор и анализ исходных данных для проектирования систем защиты информации;
- проведение проектных расчетов для элементов систем обеспечения информационной безопасности;
- участие в разработке технической документации;
- сравнительный анализ проектно-технологических решений; технико-экономическое обоснование проектных расчетов;

- участие в проектировании, разработке и внедрении программного обеспечения для решения задач информационной безопасности.

### **Экспериментально-исследовательская деятельность**

#### *Задачи:*

- сбор и анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение расчётов и экспериментов с целью решения задач защиты информации, обработка и анализ результатов;
- разработка и исследование программного обеспечения для решения задач защиты информации в проблемно-ориентированных информационных технологиях;
- проведение вычислительных экспериментов с использованием стандартных программных средств.

### **Эксплуатационная деятельность**

#### *Задачи:*

- установка, настройка и эксплуатация средств и подсистем информационной безопасности в соответствии установленными требованиями;
- администрирование подсистем информационной безопасности объектов информатизации;
- проведение мониторинга информационной безопасности объектов информатизации;
- участие в проведении специсследований, спецпроверок и аттестации объектов информатизации по требованиям защиты информации.

## **4.Профессиональные дисциплины**

Формирование компетенций специалиста по информационной безопасности обеспечивает в процессе изучения следующих дисциплин.

*Профессиональные дисциплины:* история защиты информации и современное информационное противоборство, основы информационной безопасности, технологии и методы программирования, электротехника, электроника и схемотехника, аппаратные средства вычислительной техники, теория и методология защиты информации, информационные технологии, системы и сети передачи информации, основы безопасности информационных технологий, криптографические методы защиты информации, программно-аппаратные средства защиты информации, технические методы защиты информации, проектирование инженерно-технических систем защиты информации, документооборот и конфиденциальное делопроизводство, организационно-правовое обеспечение информационной безопасности, модели и стандарты компьютерной безопасности, методики и технологии выявления угроз и нарушений информационной безопасности, управление информационной безопасностью, проектирование информационных систем и технологии управления проектами, защита информации в специализированных информационных системах, администрирование информационных систем и баз данных, аудит информационной безопасности, методы и средства обнаружения компьютерных атак, комплексное обеспечение информационной безопасности на предприятии и др.

Для студентов 3-4 курса организован дополнительный 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 метод проектов, анализ деловых ситуаций на основе кейс-метода и имитационных моделей, проведение деловых, 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, являются:

- Территориальные органы государственной власти РФ, органы власти субъекта РФ и местного самоуправления, в частности:
  - Управление Федеральной службы по техническому и экспортному контролю по Сибирскому федеральному округу;
  - Новосибирская таможня Сибирского таможенного управления Федеральной таможенной службы;
  - 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»;
  - ЗАО «Софтлайн Трейд»;
  - ООО Аттестационный технический центр;
  - ООО «Безопасные информационные технологии»;
  - ООО «Региональный аттестационный центр»;
  - ЗАО «Д-Линк Интернэшнл» (Новосибирское представительство);
  - ООО «Сибирская академия информационной безопасности»;
  - Группа компаний «АКСТЕЛ»

Студенты в рамках практик и (или) дипломирования участвовали в решении практических задач на крупных предприятиях: ОАО «РусГидро» – «Саяно-Шушенская ГЭС им. П.С.Непорожнего»; ОАО «Енисейская территориальная генерирующая компания», филиал «Абаканская ТЭЦ»; ФГУП ПО «СЕВЕР», Новосибирский завод химконцентратов, Новосибирский авиационный завод им. В.П.Чкалова, и др., в передовых ИТ-компаниях: ЗАО «Центр финансовых технологий», ООО «Центр консалтинга и информационных систем», ООО «ДГ-Софт», Новосибирское представительство СКБ «Контур», Сибирский банк Сбербанка России, Газпромбанк 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, что позволяет содействовать в организации практики студентов и трудоустройству в различных регионах.

## 6. Условия реализации образовательной программы

### *Учебно-методическое обеспечение*

Уровень обеспеченности образовательной программы бакалавриата учебно-методической документацией и информационными материалами по всем дисциплинам соответствует требованиям п. 7.17 ФГОС ВПО.

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 бакалавриата по информационной безопасности 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***

- Белов Виктор Матвеевич, 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, начальник корпоративного учебного центра ОАО «Россельхозбанк»
- Пестунова Тамара Михайловна, канд. техн. наук, доцент
- Пузынин Николай Георгиевич, старший преподаватель, 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
- 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 ООО «АКСТЭЛ»
- 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 ElectronicsWorkbench, 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 ErwinCommunity Edition, система имитационного моделирования AnyLogic Educational и многое другое специализированное программное обеспечение, в том числе авторские разработки преподавателей.

Для формирования практико-ориентированных профессиональных компетенций, в сфере информационной безопасности, приобретения исследовательского и практического опыта при кафедре информационной безопасности созданы две учебно-исследовательские лаборатории.

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.

На базе УИЛ инженерно-технической защиты информации развёрнуты 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 защищаемое помещение, аттестованное по требованиям безопасности.