**Институт т автоматики и информационных технологий**
**Кафедра «Кибербезопасность, обработка и хранение информации»**

# ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

**«7М06303 - Комплексное обеспечение информационной безопасности»**

**шифр и наименование образовательной программы**

Код и классификация области образования: **7М06**
**Информационно-коммуникационные технологии**
Код и классификация направлений подготовки: **7М063**
**Информационная безопасность**
Группа образовательных программ: **М095**
**Информационная безопасность**
Уровень по НРК: **7**
Уровень по ОРК: **7**
Срок обучения: **1 года**
Объем кредитов: **60 кредитов**

**Алматы 2025**

Образовательная программа «7М06303 - Комплексное обеспечение информационной безопасности» утверждена на заседании Учёного совета КазНИТУ им. К.И.Сатпаева.
Протокол № _10__ от "_06___" _март_ 2025 г.

Рассмотрена и рекомендована к утверждению на заседании Учебно-методического совета КазНИТУ им. К.И.Сатпаева.
Протокол № _3__ от "_20_" _декабрь 2024 г.

Образовательная программа «7М06303 - Комплексное обеспечение информационной безопасности» разработан академическим комитетом по направлению «7М063 Информационная безопасность»

| Ф.И.О. | Учёная степень/учёное звание | Должность | Место работы | Подпись |
|---|---|---|---|---|
| **Председатель академического комитета:** | | | | |
| Покусов Виктор Владимирович | | Председатель | Казахстанская Ассоциация Информационной безопасности | |
| **Профессорско-преподавательский состав:** | | | | |
| Айтхожаева Евгения Жамалхановна | Кандидат технических наук, доцент | Профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Рахметулаева Сабина Батырхановна | Доктор PhD | Профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Сатыбалдиева Рысхан Жакановна | Кандидат технических наук | Ассоциированный профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Сербин Василий Валерьевич | Кандидат технических наук | Ассоциированный профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Жумагалиев Биржан Изимович | Кандидат технических наук, доцент | Ассоциированный профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Алимсеитова Жулдыз Кенесхановна | Доктор PhD | Ассоциированный профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Юбузова Халича Ибрагимовна | Доктор PhD | Ассоциированный профессор | НАО «КазНИТУ им.К.И.Сатпаева» | |
| **Представители работодателей:** | | | | |
| Мамырбаев Оркен Жумажанович | Доктор PhD, ассоциированный профессор | Заместитель генерального директора | РГП «Институт информационных и вычислительных технологий» | |
| Конысбаев Әмірет Тұяқұлы | Кандидат физико-математических наук | Президент | Ассоциация инновационных компаний СЭЗ «ПИТ» | |
| Батыргалиев Асхат Болатханович | Доктор PhD, ассоциированный профессор | Погранслужба КНБ, контрразведки | В/ч № 01068, | |
| **Обучающиеся:** | | | | |
| Абилкайырова Алина Сериккызы | | Обучающийся 3 курса | НАО «КазНИТУ им.К.И.Сатпаева» | |
| Элле Венера | | Обучающийся 1 курса, докторантура | НАО «КазНИТУ им.К.И.Сатпаева» | |

# Оглавление

## Список сокращений и обозначений

**ОП** – образовательная программа
**БК** – базовые компетенции
**ПК** – профессиональные компетенции
**РО** – результаты обучения
**МООС** – массовые открытые онлайн курсы
**НРК** – Национальная рамка квалификаций
**ОРК** – Отраслевая рамка квалификаций
**БД** – база данных
**ИБ** – информационная безопасность
**ИКТ** – информационно-коммуникационные технологии

## 1. Описание образовательной программы

Образовательная программа 7М06303 «Комплексное обеспечение информационной безопасности» направлена на обучение магистрантов профильного направления. Программа включает базовые и профильные дисциплины с достижением соответствующих компетенций, а также прохождение различных видов практик (производственная, экспериментально-исследовательская и стажировка).

Профессиональная деятельность магистров направлена на область защиты и безопасности информации, а именно на комплексное обеспечение информационной безопасности и инженерно-техническую защиту информации.

Подготовка магистров профильного направления по информационной безопасности будет осуществляться по обновленной образовательной программе 7М06303 «Комплексное обеспечение информационной безопасности». Программы дисциплин и модулей образовательной программы имеют междисциплинарный и мультидисциплинарный характер, разрабатываются с учетом соответствующих образовательных программ ведущих университетов мира и международного классификатора профессиональной деятельности по направлению информационная безопасность.

Образовательная программа обеспечивает применение индивидуального подхода к обучающимся, трансформацию профессиональных компетенций из профессиональных стандартов и стандартов квалификаций в результаты обучения и пути их достижения.

Образовательная программа разрабатывалась на основе анализа трудовых функций администратора по информационной безопасности, аудитора информационной безопасности, инженера по защите информации, заявленных в профессиональных стандартах.

Основным критерием завершенности обучения по программам магистратуры является освоение всех видов учебной и профессиональной деятельности магистранта.

В случае успешного завершения полного курса обучающемуся присваивается степень магистр техники и технологий по образовательной программе 7М06303 «Комплексное обеспечение информационной безопасности».

Выпускник может выполнять следующие виды трудовой деятельности: - проектно-конструкторская;

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

В разработке образовательной программы участвовали представители казахстанских компаний и ассоциаций, специалисты ведомственных структур в области защиты и безопасности.

## 2. Цель и задачи образовательной программы

**Цель ОП:** Подготовка высококвалифицированных специалистов, умеющих решать задачи планирования работы по аудиту информационной безопасности, выявления и устранения уязвимостей, проведение мониторинга и расследования инцидентов ИБ

**Задачи ОП:**

Подготовка высококвалифицированных специалистов, умеющих решать следующие задачи:

- планирование работы по аудиту информационной безопасности;
- организационное обеспечение аудита информационной безопасности;
- проведение анализа соответствия проектной, эксплуатационной и технической документации по информационной безопасности требованиям в сфере ИКТ и обеспечения ИБ объекта аудита ИБ;
- анализ текущего состояния защищенности объекта аудита ИБ;
- выявление и устранение уязвимостей;
- проведение мониторинга и расследования инцидентов ИБ;
- разработка модели угроз безопасности информации в предприятиях;
- разработка технического задания на создание системы защиты информации.

Магистр техники и технологий по образовательной программе 7М06303 «Комплексное обеспечение информационной безопасности» ориентирован на самостоятельное определение цели профессиональной деятельности и выбора адекватных методов и средств их достижения, осуществление инновационной деятельности по получению новых знаний. Кроме того, ориентирован на организацию, проектирование, разработку, управление и аудит систем защиты и безопасности информации прикладного назначения для всех отраслей экономики, государственных организаций и других областей деятельности.

## 3. Требования к оценке результатов обучения образовательной программы

Образовательная программа разработано в соответствии с Государственными общеобязательными стандартами высшего и послевузовского образования, утвержденными приказом Министра науки и высшего образования Республики Казахстан от 20 июля 2022 года №2 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 28916) и отражает результаты обучения, на основании которых разрабатываются учебные планы (рабочие учебные планы, индивидуальные учебные планы обучающихся) и рабочие учебные программы по дисциплинам (силлабусы). Освоение дисциплин не менее 10% от общего объема кредитов образовательной программы с применением МООС на официальной платформе https://polytechonline.kz/cabinet/login/index.php/, а также посредством изучения дисциплин через международную образовательную платформу Coursera https://www.coursera.org/

Оценивание результатов обучения проводится по разработанным тестовым заданиям в рамках образовательной программы в соответствии с требованиями государственного общеобязательного стандарта высшего и послевузовского образования.

При проведении оценивания результатов обучения для обучающихся создаются единые условия и равные возможности для демонстрации уровня своих знаний, умений и навыков.

При проведении промежуточной аттестации в онлайн форме применяется онлайн прокторинг.

## 4. Паспорт образовательной программы

### 4.1. Общие сведения

| № | Название поля | Примечание |
|---|---|---|
| 1 | Код и классификация области образования | 7М06 Информационно-коммуникационные технологии |
| 2 | Код и классификация направлений подготовки | 7М063 Информационная безопасность |
| 3 | Группа образовательных программ | М095 Информационная безопасность |
| 4 | Наименование образовательной программы | 7М06303 - Комплексное обеспечение информационной безопасности |
| 5 | Краткое описание образовательной программы | Профессиональная деятельность выпускников включает в себя: образование, государственные и ведомственные структуры, экономику и промышленность государства, область здравоохранения.<br>Объектами профессиональной деятельности выпускников магистерских программ по образовательной программе 7М06303 «Комплексное обеспечение информационной безопасности» являются:<br>− органы государственного управления;<br>− отделы информационной безопасности и департаменты ведомственных организаций;<br>− отделы информационной безопасности, IT отделы и департаменты финансовых организаций;<br>− отделы информационной безопасности, IT отделы и департаменты промышленных предприятий;<br>− отделы и департаменты информационной безопасности государственных организаций и коммерческих структур. Основными функциями профессиональной деятельности магистрантов являются: проведение исследовательских работ в сфере защиты и безопасности информации; аудит, анализ уязвимостей и расследование инцидентов в системах информационной безопасности; проектирование, внедрение, эксплуатация, администрирование, сопровождение и тестирование систем информационной безопасности предприятий<br>Направления профессиональной деятельности, следующие:<br>− проектирование, разработка, внедрение и эксплуатация систем информационной безопасности;<br>− анализ, тестирование и выявление уязвимостей системы;<br>− аудит информационной безопасности |
| 6 | Цель ОП | Подготовка высококвалифицированных специалистов, умеющих решать задачи планирования работы по аудиту информационной безопасности, выявления и устранения уязвимостей, проведение мониторинга и расследования инцидентов ИБ |
| 7 | Вид ОП | новая |
| 8 | Уровень по НРК | 7 |
| 9 | Уровень по ОРК | 7 |
| 10 | Отличительные особенности ОП | нет |

| | | |
|---|---|---|
| 11 | Перечень компетенций образовательной программы: | Выпускников профильной магистратуры, должен:<br>1) иметь представление:<br>– о противоречиях и социально-экономических последствиях процессов глобализации;<br>– о профессиональной компетентности в области защиты и безопасности информации;<br>– о технологии виртуализации ресурсов и платформ;<br>– об интеллектуализации средств обеспечения информационной безопасности;<br>– о технологиях защиты БД;<br>– об алгоритмах криптографической защиты информации;<br>– об анализе больших данных.<br>2) знать:<br>– алгоритмы криптографической защиты информации;<br>– стандарты ИБ и критерии оценки безопасности ИТ;<br>– технологии виртуализации ресурсов и платформ и системы виртуализации от ведущих производителей<br>; – угрозы и риски систем виртуализации, принципы построения гипервизоров и их уязвимости;<br>– организацию IP-сетей,<br>структуру IP-пакетов и IPпротоколов;<br>– внутреннюю организацию носителей информации ОС;<br>– методы и средства хранения ключевой информации и шифрования;<br>– разновидности и принципы аутентификации;<br>– технологии защиты БД и методы проектирования безопасных БД;<br>– организацию системы защиты и безопасности БД;<br>– методы и инструменты активного аудита.<br>3) уметь:<br>– использовать полученные знания для оригинального развития и применения идей в контексте экспериментальных исследований;<br>– критически анализировать существующие концепции и подходы к анализу процессов и явлений;<br>– интегрировать знания, полученные в рамках разных дисциплин для решения исследовательских задач в новых незнакомых условиях;<br>– путем интеграции знаний выносить суждения и принимать решения на основе неполной или ограниченной информации;<br>– проводить информационно-аналитическую и информационно-библиографическую работу с привлечением современных информационных технологий;<br>– креативно мыслить и творчески подходить к решению новых проблем и ситуаций;<br>– свободно владеть иностранным языком на профессиональном уровне, позволяющим проводить исследования;<br>– обобщать результаты исследовательской и аналитической работы в виде диссертации, статьи, отчета, аналитической записки и др.;<br>– применять алгоритмы криптографической защиты информации; |

| | | |
|---|---|---|
| | | – применять стандарты ИБ и проводить оценку безопасности ИТ;<br>– применять системы виртуализации от ведущих производителей;<br>– выявлять угрозы и риски систем виртуализации;<br>– применять методы и средства хранения ключевой информации и шифрования;<br>– применять технологии защиты БД и методы проектирования безопасных БД;<br>– организовать систему защиты и безопасности БД;<br>– применять методы и инструменты активного аудита;<br>– применять инструменты анализа больших данных.<br>4) иметь навыки:<br>– использования современных информационных технологий;<br>– профессионального общения и межкультурной коммуникации;<br>– правильного и логичного оформления своих мыслей в устной и письменной форме;<br>– организации и защиты безопасности БД;<br>– проведения аудита информационной безопасности;<br>– применения алгоритмов криптографической защиты информации;<br>– выявления угроз и противодействия им;<br>– работы с Big Data;<br>– расширения и углубления знаний, необходимых для повседневной профессиональной деятельности и продолжения образования в докторантуре.<br>5) быть компетентным:<br>– в выполнении проектов и исследований в профессиональной области;<br>– в организации систем информационной безопасности;<br>– в проведении аудита информационной безопасности;<br>– в обеспечении информационной безопасности организации;<br>- в способах обеспечения постоянного обновления знаний, расширения профессиональных навыков и умений. |
| 12 | Результаты обучения образовательной программы: | **РО1:** Применять на практике знания фундаментальных и прикладных разделов дисциплин, определяющих направленность (профиль) программы магистратуры<br>**РО2:** Способность проводить самостоятельное исследование, включая навыки и умения анализа, синтеза, оценки, и получения оригинальных научных результатов, способствующие развитию в области защиты информации<br>**РО3:** Самостоятельно приобретать, осмысливать, структурировать и использовать в профессиональной деятельности новые знания и умения, развивать свои инновационные способности для создания комплексной стойкой защищенной инфраструктуры организаций.<br>**РО4:** Применять технологии виртуализации ресурсов и платформ, обладая знаниями принципов организации безопасного использования систем виртуализации и облачных технологий. Разрабатывать и управлять |

| | | |
|---|---|---|
| | | программными средствами автоматизации обработки больших данных.<br>**РО5:** Применять технологии защиты БД и методы проектирования безопасных БД, организовать систему защиты и безопасности БД, а также применять инструменты анализа больших данных.<br>**РО6:** Анализировать угрозы и разрабатывать системы информационной безопасности в организации с применением алгоритмов криптографической защиты<br>**РО7:** Руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия. Готов коммуникации в устной и письменной формах на иностранном языке для решения задач профессиональной деятельности для партнерства в интересах устойчивого развития.<br>**РО8:** Применять алгоритмы криптографической защиты информации, стандарты информационной безопасности. Умение проводить аудиторскую проверку по определению уровня информационной безопасности и осуществлять критерии оценки безопасности информационных технологий.<br>**РО9:** Демонстрирует владение инструментами проведения расследовании компьютерных инцидентов. Применяет системы предотвращения утечки данных. |
| 13 | Форма обучения | Очное, онлайн |
| 14 | Срок обучения | 1 года |
| 15 | Объем кредитов | 60 кредитов |
| 16 | Языки обучения | Казахский, русский, |
| 17 | Присуждаемая академическая степень | магистр технических наук |
| 18 | Разработчик(и) и авторы: | Айтхожаева Е.Ж.,<br>Сатыбалдиева Р.Ж., |

## 4.2. Взаимосвязь достижимости формируемых результатов обучения по образовательной программе и учебных дисциплин

| № | Наименование дисциплины | Краткое описание дисциплины | Кол-во кредитов | Формируемые результаты обучения (коды) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | РО1 | РО2 | РО3 | РО4 | РО5 | РО6 | РО7 | РО8 | РО9 |
| **Цикл базовых дисциплин Вузовский компонент** | | | | | | | | | | | | |
| 1 | Иностранный язык (профессиональный) | Цель курса: совершенствование и развитие иноязычных коммуникативных умений в профессиональной и академической сфере. Содержание курса: общие принципы профессионального и академического межкультурного устного и письменного общения с использованием современных педагогических технологий (круглый стол, дебаты, дискуссии, анализ профессионально-ориентированных кейсов, проектирование). | 2 | | | v | | | | v | | |
| 2 | Менеджмент | Цель дисциплины - формирование научного представления об управлении как виде профессиональной деятельности; освоение обучающимися общетеоретических положений управления социально-экономическими системами; овладение умениями и навыками практического решения управленческих проблем; изучение мирового опыта менеджмента, а также особенностей казахстанского менеджмента, обучение решению практических вопросов, связанных с управлением различными сторонами деятельности организаций. | 2 | | | v | | | | v | | |
| 3 | Психология управления | Цель: Приобретение навыков принятия | 2 | | | v | | | | v | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | стратегических и управленческих решений с учётом психологических особенностей индивидуума и коллектива. Содержание: современная роль и содержание психологических аспектов в управленческой деятельности, методы улучшение психологической грамотности, состав и устройство управленческой деятельности, как на местном уровне так и в зарубежном, психологическая особенность современных управленцев. | | | | | | | | | | |
| **Цикл базовых дисциплин<br>Компонент по выбору** | | | | | | | | | | | | |
| 4 | Безопасность систем виртуализации и облачных технологий | Целью освоения дисциплины является изучение вопросов безопасности облачных технологий, источники угроз в облачных вычислениях. Курс нацелен на изучение модели развертывания облаков: публичные, частные, гибридные облака, модели облачных технологий, особенности и характеристики облачных вычислений, стандарты информационной безопасности в сфере облачных технологий и систем виртуализации, средства обеспечения защиты облачных вычислений, шифрование, VPN-сети, аутентификация, изоляция пользователей. | 4 | v | | | v | v | | | | |
| 5 | Phyton для решения задач ИБ | Курс нацелен на изучение вопросов решения высокоуровневых математических и технических задач с использованием пакетов NumPy и SciPy, анализа данных с помощью пакета Pandas. Спообствует развитию навыков работы с данными, связанными с информационной | 4 | v | v | v | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | безопасностью: загрузка, фильтрация, преобразование, анализ и интерпретация данных с использованием известных моделей классификации, кластеризации, регрессии и пр. Изучаются основные методы работы с матрицами и матричными операциями. Изучаются инструменты визуализации данных. | | | | | | | | | | |
| **Цикл профилирующих дисциплин<br>Вузовский компонент** | | | | | | | | | | | | |
| 6 | Организация защиты и безопасности БД | Аспекты и критерии безопасности, политика безопасности. Угрозы безопасности данных. Защита и безопасность баз данных, целостность и надежность данных. Методы и средства защиты и защиты данных. Разработайте безопасную базу данных. CASE-инструменты дизайна. Инструменты администрирования базы данных. Впечатления как инструменты повышения безопасности данных. Влияние курсоров на безопасность базы данных. Управление транзакциями. Хранимые процедуры. Триггеры. Мандатное и дискреционное управление доступом к СУБД. Роль и отчеты. Мониторинг и аудит СУБД. Криптографические инструменты для защиты базы данных. Репликация и восстановление данных. Инструменты высокой подготовки. | 5 | **v** | **v** | | | **v** | | | | |
| 7 | Организация систем информационной безопасности | Концепция систем информационной безопасности. Стандарты систем информационной безопасности. Выберите объект для организации системы. Анализ угроз и разработка программного | 5 | | **v** | | | | | | **v** | **v** |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | обеспечения для безопасности. Административный и процедурный уровни информационной безопасности. Анализ и выбор методов защиты информации. Обеспечение и оценка объектов | | | | | | | | | | |
| 8 | Управление IT проектами и информационными рисками | Целью освоения дисциплины является формирование знаний, умений и навыков в сфере управления рисками IT проектов, теоретическое и практическое овладение современными средствами анализа и оценки рисков, изучение требований к разработке документации по выявлению и оценке рисков, ознакомление с принципами и методами обработки рисков для совершенствования бизнес-процессов и IT инфраструктуры предприятия. | 5 | | v | | | | v | | v | |
| **Цикл профилирующих дисциплин Компонент по выбору** | | | | | | | | | | | | |
| 9 | Аудит информационной безопасности | Аудит информационной безопасности Управление информационной безопасностью. Аудит информационной безопасности. Базовые термины, определения, понятия и принципы в сфере аудита информационной безопасности. Основные направления аудита информационной безопасности. Виды и цели аудита. Основные этапы аудита безопасности. Перечень исходных данных, необходимых для проведения аудита безопасности. Оценка текущего состояния системы информационной безопасности. Оценка уровня безопасности. Анализ рисков, оценка уровня защищенности, разработка политик безопасности и других | 5 | v | v | | | | | | v | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | организационно-распорядительных документов по защите информации. Международные стандарты и лучшие практики проведения ИТ-аудита. | | | | | | | | | | |
| 10 | Риск менеджмент в кибербезопасности | Риск менеджмент в кибербезопасности Программа учебного курса «Риск менеджмент в кибербезопасности» направлена на изучение международных и национальных стандартов риск менеджмента в кибербезопасности, методов определения и управления рисками, практического применения стандартов и методов, изучения специализированных программных комплексов для оценки рисков. | 5 | | | | v | | | | | v |
| 11 | Big Data и анализ данных | Цель изучения курса - формирование у студентов профессиональной компетенции в области разработки и использования систем обработки и анализа больших массивов данных. Содержание дисциплины рассматривает методы анализа и хранения больших объемов данных, этапы жизненного цикла обработки больших данных, языки, наиболее приспособленные для обработки и аналитики больших данных, способы организации хранения и доступа к большим данным. | 5 | | v | | v | v | | | | |
| 12 | Machine Learning & Deep Learning | Курс посвящен моделям глубокого обучения. Являясь областью в рамках машинного обучения, модели глубокого обучения иллюстрируют количественно-качественный переход. Новые модели и их свойства требуют отдельного изучения и практики настройки метапараметров таких | 5 | | v | | v | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | моделей. В этом курсе изучаются основы глубокого обучения, нейронные сети, сверточные сети, RNN, LSTM, Adam, Dropout, BatchNorm, инициализации Xavier/He. | | | | | | | | | | |

# 5. Учебный план образовательной программы