

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## Модели безопасности компьютерных систем

по специальности 10.05.03 информационная безопасность автоматизированных систем

### 1. Цели и задачи освоения дисциплины

Цель освоения дисциплины: обучение студентов принципам формального моделирования и анализа безопасности компьютерных систем, реализующих управление доступом и информационными потоками.

Задачи освоения дисциплины:

- развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций;
- изучение основных формальных моделей политик безопасности, моделей дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков;
- приобретение практических навыков разработки математических моделей безопасности для защищаемых компьютерных систем;
- формирование у будущего специалиста в области компьютерной безопасности таких качеств, как строгость в суждениях, творческое мышление, организованность и работоспособность, дисциплинированность, самостоятельность и ответственность.

### 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Модели безопасности компьютерных систем» относится к числу дисциплин блока Б1.В.1 программы подготовки специалистов по направлению 10.05.03 – «Информационная безопасность автоматизированных систем». Дисциплина читается в 8-ом семестре студентам очной формы обучения.

### 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Информатика и программирование» направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат	<b>Знать:</b> основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела;

<p>для формализации и решения профессиональных задач</p>	<p>физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации;</p> <p>основные методы управления информационной безопасностью;</p> <p>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах</p> <p><b>Уметь:</b></p> <p>определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач</p> <p>определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач</p> <p>строить математические модели физических явлений и процессов;</p> <p>решать типовые прикладные физические задачи;</p> <p>анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;</p> <p>применять математические методы исследования моделей шифров</p> <p>основы физической защиты объектов информатизации</p> <p>выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем</p> <p><b>Владеть:</b></p> <p>навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры</p> <p>навыками построения дискретных моделей при решении профессиональных задач</p> <p>методами теоретического исследования физических явлений и процессов;</p> <p>навыками проведения физического эксперимента и обработки его результатов</p>
<p>ОПК-2</p> <p>способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики,</p>	<p><b>Знать:</b> математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> <p><b>Уметь:</b> применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p> <p><b>Владеть:</b> навыками корректного применения при</p>

<p>теории алгоритмов, теории информации, в том числе с использованием вычислительной техники</p>	<p>решении профессиональных задач соответствующего математического аппарата алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники.</p>
<p>ОПК-3 способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p>	<p><b>Знать:</b>          принципы построения и функционирования, примеры реализаций современных операционных систем;          принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;          основные информационные технологии, используемые в автоматизированных системах;          показатели качества программного обеспечения;          язык программирования высокого уровня (объектно-ориентированное программирование);          возможности, классификацию и область применения макрообработки;          способы обработки исключительных ситуаций</p> <p><b>Уметь:</b>          создавать объекты базы данных;          выполнять запросы к базе данных;          разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;          исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;          формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;          работать с интегрированной средой разработки программного обеспечения;          использовать шаблоны классов и средства макрообработки;          использовать динамически подключаемые библиотеки</p> <p><b>Владеть:</b>          навыками использования ЭВМ в анализе простейших шифров;          навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;          навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ;          навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;          навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электрон-</p>

	<p>ных аппаратных средств автоматизированных систем;          навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;          навыками проектирования программного обеспечения с использованием средств автоматизации;          навыками разработки программной документации</p>
<p>ПК-2          способностью создавать и исследовать модели автоматизированных систем</p>	<p><b>Знать:</b>          модели шифров и математические методы их исследования;          основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;          основные характеристики сигналов электросвязи, спектры и виды модуляции;          эталонную модель взаимодействия открытых систем;          принципы построения и функционирования систем и сетей передачи информации</p> <p><b>Уметь:</b>          разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;          исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений</p> <p><b>Владеть:</b>          навыками математического моделирования в криптографии;          методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;          навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;          навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;          навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</p>
<p>ПК-3          способностью проводить анализ защищенности автоматизированных систем</p>	<p><b>Знать:</b>          требования к шифрам и основные характеристики шифров;          модели шифров и математические методы их исследования;          программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;          технические каналы утечки информации;          возможности технических средств перехвата информа-</p>

	<p>ции;  организацию защиты информации от утечки по техническим каналам на объектах информатизации;</p> <p><b>Уметь:</b>  разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;  исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений</p> <p><b>Владеть:</b>  навыками математического моделирования в криптографии;  методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;  навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;  навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;  навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;  навыками организации и обеспечения режима секретности</p>
--	--

#### 4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 часов)

#### 5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение лабораторных занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение зачета.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к лабораторным работам, их оформление.

#### 6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля:

Подготовка ответов на вопросы по темам при выполнении лабораторных работ.  
Промежуточная аттестация проводится в форме зачета.