

АННОТАЦИЯ
рабочей программы учебной дисциплины
Б1.В.ДВ.04.02. «КИБЕРБЕЗОПАСНОСТЬ»
по направлению подготовки 09.03.02 Информационные системы и технологии
по профилю подготовки Банковские информационные системы и технологии

Цель дисциплины	Целью освоения дисциплины «Кибербезопасность» является развитие профессиональных компетенций студентов, связанных в сфере технологий и проблем обеспечения кибербезопасности, защиты информационных систем в различных сценариях угрозы.
Место дисциплины в структуре бакалавриата	Дисциплина «Кибербезопасность» относится к дисциплинам части, формируемой вузом Б1.В.ДВ.04.02. Освоение данной дисциплины является основой для последующего изучения дисциплин вариативной части «Автоматизация основных и вспомогательных бизнес-процессов банка», «Финтех: инструментарий и модели бизнеса», а также для последующего прохождения практики, подготовки к государственной итоговой аттестации.
Компетенции, формируемые в результате освоения учебной дисциплины	В результате освоения дисциплины обучающийся должен обладать следующими компетенциями бакалавра экономики: УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.
Содержание дисциплины	Введение в кибербезопасность. Теоретические основы кибербезопасности. Классификация угроз в информационных системах. Анализ способов борьбы с фишингом. Выявление и устранение возможности организации социальной инженерии в профессиональной деятельности. Связь обновления программного обеспечения с возникновением киберугроз. Анализ информационных ресурсов предоставляющих характеристики современных угроз. Методы применения полученной актуальной информации о принципах работы нового вредоносного программного обеспечения. Анализ автоматизированного рабочего места на предмет выявления киберугроз.
Знания, умения и навыки, получаемые в процессе изучения дисциплины	В результате изучения дисциплины студент должен: <i>Знать:</i> - основные причины выявления киберугроз; методы выявления угроз информационной безопасности; правила первичного блокирования киберугроз; методы проведения профилактических работ по устранению киберугроз; основные критерии фильтрации трафика в глобальной сети; методы противодействия с фишингом. <i>Уметь:</i> - проводить первичный анализ на предмет выявления киберугроз; осуществлять первичное блокирование киберугроз; выявлять вложенные и скрытые гиперссылки для предотвращения XSS уязвимости; управлять COOKIE данными с целью сокращения работы открытых сессий пользователя. <i>Владеть:</i> - навыком работы со стандартным набором инструментов пользователя, для выявления угроз информационной безопасности автоматизированного рабочего места; техниками выявления методов социальной инженерии; приемами отражения

	латентных кибератак; навыками оценки устойчивости информационной безопасности автоматизированного рабочего места.		
Объем дисциплины и виды учебной работы	Вид учебной работы	Всего часов	8 семестр
	Общая трудоемкость дисциплины	108	108
	Аудиторные занятия	48	48
	Лекции	24	24
	Практические занятия (ПЗ)	24	24
	Самостоятельная работа	60	60
Используемые ресурсы информационно-телекоммуникационной сети «Internet», информационные технологии, программные средства и информационно-справочные системы	<p>В ходе обучения используются средства для обеспечения коммуникации, которые включают несколько форм: электронную почту, специализированные ресурсы Internet, специализированное ПО, ЭБС</p> <p>Размещение базовой и дополнительной информации, необходимой для учебного процесса, на сайте кафедры</p> <p>Размещение ссылок на разнообразные базы данных ведущих библиотек, информационных, научных и учебных центров</p> <p>Используется стандартное программное обеспечение (MSExcel и др.)</p>		
Формы текущего и рубежного контроля	Групповые дискуссии, тесты, домашние задания, презентации, рефераты		
Форма итогового контроля	Зачет в 8 семестре.		