АННОТАЦИЯ
рабочей программы учебной дисциплины
Б1.В.ДВ.05.01. «ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»
по направлению подготовки 09.03.02 Информационные системы и технологии
по профилю подготовки Банковские информационные системы и технологии

Цель изучения дисциплины	Целью освоения дисциплины «Основы кибербезопасности» является развитие профессиональных компетенций студентов, связанных в сфере технологий и проблем обеспечения кибербезопасности, защиты информационных систем в различных сценариях угрозы.
Место дисциплины в структуре ОПОП бакалавриата	Дисциплина «Основы кибербезопасности» относится к дисциплинам части, формируемой вузом Б1.В.ДВ.05.01. 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: *Знать:* - 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 противоборства с фишингом. *Уметь:* - 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. *Владеть:* - навыком работы со стандартным набором инструментов пользователя, для выявления угроз информационной безопасности автоматизированного рабочего места; техниками выявления методов социальной инженерии; приемами отражения

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