

«Информационная безопасность»

Аннотация рабочей программы

Цель дисциплины «Информационная безопасность» является ознакомление обучающихся с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации.

Задачи дисциплины:

- сформировать у обучающихся целостную систему знаний о методах и средствах информационной безопасности;
- дать понятийно-терминологический аппарат информационной безопасности;
- дать методику оценки эффективности информационной безопасности;
- научить обучающихся, правильно оценивать перспективы и особенности информационной безопасности.

Дисциплина «Информационная безопасность» относится к обязательной части Б1.В.01 основной профессиональной образовательной программы бакалавриата направления 09.03.03 Прикладная информатика направленность (профиль) Прикладная информатика в экономике.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции:

| Код и наименование компетенции | Код и наименование индикатор достижения компетенции | Основание (ПС, анализ опыта) |
|--|--|------------------------------|
| УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.1. Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач. УК-1.2. Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности. УК-1.3. Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений. | |
| УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения. УК-2.2. Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах. | |
| ПК-10. Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью. | ПК-10.1. Знает методы и модели организации ИТ-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; основы конфигурационного управления; основы управления изменениями. ПК-10.2. | |

| | | |
|--|---|--|
| | <p>Умеет применять методы и модели организации ИТ- инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; работать с системой контроля версий. ПК-10.3.</p> <p>Владеет навыками организации ИТ- инфраструктуры и управления информационной безопасностью, в т.ч., обеспечения и контроля соответствия технических, программных и коммуникационных средств для функционирования ИС, разграничение прав доступа к ИС.</p> | |
|--|---|--|

В результате изучения учебной дисциплины обучающиеся должны:

знать:

- имеет представление об основных видах угроз информационной безопасности, принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач; классификацию угроз в зависимости от обрабатываемой информации, способа ее хранения и средств обработки. (УК -1.1);
- типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду (УК -2.1);
- методы и модели организации ИТ- инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; основы конфигурационного управления; основы управления изменениями. (ПК-10.1).
- типовые разработанные средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем. (ПК-10.1).

уметь:

- анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности; осуществлять обоснованный выбор средств и систем защиты информации; (УК -1.2);
- анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ (УК -2.2);
- реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации.; применять методы и модели организации ИТ- инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ИС; работать с системой контроля версий (ПК-10.2).

владеть:

- навыками применения методов аудита организации защиты информации на предприятии; методиками анализа предметной области; (УК -1.3);
- методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах; навыками применения технических средств защиты информации (УК -2.3);
- навыками организации ИТ- инфра-структуры и управления информационной безопасностью, в т.ч., обеспечения и контроля соответствия технических, программных и коммуникационных средств для функционирования ИС, разграничение прав доступа к ИС; навыками администрирования систем и устройств защиты информации. (ПК-10.3).

Краткое содержание тем дисциплины:

1. Международные стандарты информационного обмена. Понятие угрозы Информационная безопасность в условиях функционирования в России глобальных сетей2. Основные положения теории информационной безопасности информационных систем. Процедуры и механизмы обеспечения информационной безопасности и их применение. 3. Модели безопасности и их применение. Анализ способов нарушений информационной безопасности.4.Использование защищенных компьютерных систем. Методы криптографии. Основные технологии построения защищенных ЭИС.

Для студентов очной формы обучения. Общая трудоемкость освоения дисциплины: 144 часа/4зач.ед.

Промежуточный контроль: экзамен.