Аннотация к рабочей программе дисциплины

Автор: Урбан В.А, доцент, канд.техн.наук
Наименование дисциплины: Б2.В.01(ПД) Производственная (преддипломная) практика
Цель освоения дисциплины: закрепление и углубление знаний, полученных студентами в процессе теоретического обучения, получения профессиональных умений и навыков для работы по избранной специальности и защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	*Знать:* основные меры по выполнения обеспечения информационной безопасности *Уметь:* разрабатывать меры по обеспечению информационной безопасности *Владеть:* навыками разработки мер поддержки обеспечения информационной безопасности
	ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	*Знать:* основные этапы контрольных проверок технических средств защиты информации *Уметь:* Разрабатывать методику контрольных проверок технических средств защиты информации *Владеть:* Навыками применения контрольных проверок
ПК-2 Способен администрироватьсредства защиты информации в компьютерных системах и сетях	ПК-2.1 Осуществляет выбори настройку средств защиты информации в компьютерныхсистемах и сетях	*Знать:* об установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты *Уметь:* принимать участие в установке,

		настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты *Владеть:* способностью принимать участие в установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объектазащиты
ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* источники угроз безопасности информации и меры по их предотвращению *Уметь:* классифицироватьпотенциальные угрозы безопасностиинформации *Владеть:* комплексом мер по информационной безопасности
	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* источники угроз безопасности информации и меры по их предотвращению *Уметь:* классифицировать защищаемую информацию по видам тайны и степеням секретности *Владеть:* методами разработки компонентов по обеспечению информационной безопасности объекта защиты
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.1 Оценивает информационные риски в автоматизированных системах	*Знать:* основные методики анализа угроз и рисков информационной безопасности *Уметь:* анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации *Владеть:* технологиями обеспечения

		информационной безопасности в части проведения риск-анализа и управления риска
	ПК-4.2 Способен классифицировать и оценивать угрозы безопасности информации	*Знать:* источники и классификацию угроз информационной безопасности *Уметь:* классифицировать и оценивать угрозы информационной безопасности *Владеть:* способностью классифицировать и оценивать угрозы безопасности информации
	ПК-4.3 Определяет подлежащие защите информационные ресурсы автоматизированных систем	*Знать:* состав и принципы работы автоматизированных систем *Уметь:* осуществлять настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем *Владеть:* навыками определения и настройка компонентов систем защиты информации автоматизированных (информационных) систем
	ПК-4.4 Применяет нормативные документы по противодействию технической разведки	*Знать:* основные руководящие и нормативные документы в сфере инженерно-технической защите информации *Уметь:* использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации *Владеть:* навыками работы с профессиональными аппаратными средствами инженерно-технической защиты информации
ПК-6 Способен	ПК-6.1 Проводит	*Знать:*

проводитьанализ рисков информационной безопасности автоматизированной системы	оценкурисков информационной безопасности на основе существующих методик	методики оценки риска и управления рисками, а также тестирования средств обеспечения информационной безопасности *Уметь:* анализировать угрозы иоценивать рискиинформационной безопасности с целью обеспечения безопасности объектов информатизации *Владеть:* средствами обеспечения информационной безопасности, анализа угроз, риск-анализа иуправления рисками
ПК-7 Способен разрабатывать комплексмероприятий по защите информации в автоматизированных системах финансовых и экономических структур	ПК-7.1 Учитывает и использует правовые нормы реализации профессиональной детельности в облсти обеспечения инфрмационной безопсности и защиты интересов личности , обества и государства	*Знать:* технологии и нормы обеспечения информационной безопасности *Уметь:* обеспечивать информационную безопасность при интеграции в государственную и международную информационную среду *Владеть:* способами практического обеспечения норм информационной безопасности при интеграции в государственную и международную информационную среду
	ПК-7.2 Реализует комплексмероприятий по защите информации в автоматизированн ых системахфинансовых и экономических структур	*Знать:* принципы организации информационных систем в соответствии с требованиями по защите информации *Уметь:* осуществлять меры противодействия нарушениям информационной безопасности *Владеть:* навыками безопасного использования технических

		сред
ПК-8 Способен проводитьанализ информационной безопасности объектов и систем на соответсвие требований стандартов и нормативно-правовых актов в области информационной безопасности	ПК-8.1 Применяет стандартыи нормативно-правовые акты вобласти информационной безопасности	*Знать:* правила и нормативные требования к оформлению технической документации с учетом действующих методических документов *Уметь:* применять действующие нормативные и методические документы в области информационной безопасности *Владеть:* навыками оформлять рабочую техническую документацию с учетом действующих нормативных иметодических документов
ПК-9 Способен применятьтехнические средства защиты информации на основе знаний физических законов	ПК-9.1 Выявляет техническиеканалы утечки на основе знаний физических законов	*Знать:* основные способы физической защиты объектов информатизации *Уметь:* применять инженерно-технические средства физической защиты объектов информатизации *Владеть:* навыками применения основных типов технических средств защиты информации
	ПК-9.2 Осуществляет сбор ианализ исходных данных для расчета и проектирования радиоэлектронны х устройств исистем	*Знать:* принцип работы *Уметь:* самостоятельно проектировать *Владеть:* навыками осуществлять сбори анализ исходных данных для расчета и проектирования
ПК-10 Способен разрабатывать компьютерные модели исследуемых процессов и систем и применять их для определения оптимальных	ПК-10.1 Использует современное программное обеспечение в области разработки компьютерной графики	*Знать:* понятийный аппарат (используемые термины и определения) современной сферы компьютерной графики *Уметь:* создавать и редактировать изображения в

вариантов проектных, конструкторских и технологических решений		специализированных программах обработки графической информации *Владеть:* методами использования информационных технологий для решения задач компьютерной графики
ПК-11 Способен участвовать в проектировании системы управления информационной безопасностью	ПК-11.1 Осуществляет проектирование средств защиты информации автоматизированных систем	*Знать:* методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации *Уметь:* применять программные и программно-аппаратные средства для защиты информации в базах данных *Владеть:* навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами

2. Содержание дисциплины:

Тема 1. Ознакомление со структурой и работой основных подразделенийпредприятия, лицензией и уставом,решаемыми задачами,наличием документовразрешающих основные виды деятельности

Тема 2. Ознакомление со структурой органов защиты информации. Ознакомление с видами угрозбезопасности информации,характерными для Предприятия

Тема 3. Ознакомление с видами,методами, средствами информационной защиты, применяемыми напредприятии

3. Общая трудоемкость дисциплины: 6 ЗЕ