

Утверждено
Генеральный директор
ООО «ДИАС-К»

А.А. Шинкин

М.П.



**Курс повышения квалификации
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
Учебная программа курса**

Авторы курса	Бушин Сергей Алексеевич – кандидат технических наук; Власов Денис Николаевич – магистр по направлению Информационная безопасность
Цель	Повышение профессионального уровня обучающихся (слушателей) в рамках имеющейся квалификации путём совершенствования имеющихся и/или формирования у них новых компетенций (знаний и умений), необходимых им для выполнения трудовых функций в рамках нового вида профессиональной деятельности (исполнения должностных обязанностей в области профессиональной деятельности) в сфере информационной безопасности (деятельность по обеспечению информационной безопасности автоматизированных систем, обеспечению защищенности объектов информатизации на базе компьютерных систем и сетей от вредоносных технических воздействий).
Задачи	1. Получение и углубление профессиональных знаний и умений обучающимися (слушателями) по правовым основам защиты информации, организационным мерам и техническим средствам обеспечения безопасности при использовании современных информационных технологий на предприятиях и в организациях. 2. Удовлетворение потребности специалистов в получении знаний об актуальных нормативных требованиях к защите и о новейших достижениях в области защиты конфиденциальной информации и систем её обработки (в приобретении или комплексном обновлении их профессиональных компетенций, в рамках указанного вида профессиональной деятельности). 3. популяризация передовых технологий, подходов, решений, методов и средств обеспечения защиты конфиденциальной информации предприятий (объединений), организаций и учреждений, распространение передового опыта по успешному решению задач обеспечения информационной безопасности. 4. Оказание помощи предприятиям (объединениям), организациям и учреждениям в повышении квалификации руководителей и инженерно-технических работников (специалистов) служб безопасности и подразделений защиты информации по вопросам построения и эффективного применения комплексных систем и средств защиты информации.

Категории обучающихся	Техники по защите информации, инженеры по защите информации, специалисты по защите информации, инженеры-программисты по технической защите информации, инженеры-программисты, ведущие инженеры-разработчики систем защиты информации, ведущие специалисты по защите информации, руководители проектов в области разработки систем защиты информации, руководители отдела систем защиты информации, главные специалисты по защите информации, руководители отдела систем защиты информации.
Оценка качества	Освоение данной учебной дисциплины (модуля, курса) завершается зачетом (без оценки) в форме онлайн опроса, который подразумевает ответы на контрольные вопросы по материалу курса. Зачет проводится с использованием программных средств аудио-видеосвязи (основной вариант) или в бумажной форме (резервный вариант).
Форма обучения	Заочная. В процессе обучения применяются исключительно дистанционные образовательные технологии и электронное обучение.
Прогнозируемые результаты	В результате обучения на курсе обучающиеся приобретут: <u>знания:</u> о сущности понятия информационной безопасности, характеристики ее составляющих; о месте и роли информационной безопасности в системе национальной безопасности Российской Федерации; об основных нормативных правовых актах в области информационной безопасности и защиты информации, а также о нормативных методических документах ФСТЭК России, ФСБ России в данной области; об основах построения информационных систем и формирования информационных ресурсов ограниченного доступа; о правовых основах организации защиты государственной тайны и конфиденциальной информации; об основах лицензирования деятельности по технической защите информации и деятельности по разработке и производству средств защиты информации; об основах действующей системы сертификации средств защиты информации по требованиям безопасности информации; о принципах построения и управления системой обеспечения информационной безопасности в ведомстве (организации, на предприятии); об источниках угроз информационной безопасности и мерах по их предотвращению; о механизмах реализации вредоносных программно-технических и информационных воздействий в компьютерных системах; о методах и способах несанкционированного доступа (НСД) к информации, способах и средствах защиты от НСД к информации на объектах информатизации; о принципах организации информационных систем в соответствии с требованиями по защите информации; о системе организации комплексной защиты информации ограниченного доступа, включая защиту персональных данных; о требованиях по составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методах их практической реализации; об основных видах политик управления доступом и информационными потоками в компьютерных системах; о методах и способах защиты информации; о защитных механизмах и средствах обеспечения сетевой безопасности; о современных программно-аппаратных средствах и способах обеспечения информационной безопасности в компьютерных системах; о

	<p>средствах и методах предотвращения и обнаружения вторжений; об основных средствах и методах анализа уязвимостей программных средств.</p> <p><u>Умения:</u> проводить информационные обследования, анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; планировать защиту и рационально распределять соответствующие функции и ответственность между подразделениями и сотрудниками предприятия, организовывать их взаимодействие на различных этапах жизненного цикла автоматизированных систем; участвовать в организации деятельности служб технической защиты информации в действующих и проектируемых системах защиты информации; разрабатывать концепции, политики и иные организационно-распорядительные документы, необходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации в организации; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; оценивать полноту и качество выполнения работниками организации требований политики безопасности; ориентироваться в проблемах информационной безопасности в сетях Интернет/Интранет, уязвимостях сетевых протоколов и служб, атаках в IP-сетях; ориентироваться в средствах защиты информации от несанкционированного доступа, межсетевых экранах, средствах контроля контента, средствах анализа защищенности и средствах обнаружения атак для обеспечения информационной безопасности в IP-сетях; обоснованно выбирать необходимые программные и программно-аппаратные средства защиты информации в автоматизированных системах; организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для обеспечения информационной безопасности данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.</p>
<p>Выдаваемый документ</p>	<p>По окончании курса обучающийся получит печатное удостоверение о повышении квалификации установленного образца. Удостоверение высылается Почтой России.</p>

Учебный план

№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	Распределение времени по видам занятий, час			Самостоятельная работа	Формы аттестации и контроля знаний
			Лекции	Практические занятия	Промежуточная аттестация		
1.	Раздел I. Основы безопасности информационных технологий	36	28			8	Ответы на вопросы для самоконтроля
2.	Раздел II. Обеспечение безопасности информационных технологий	48	40			8	Ответы на вопросы для самоконтроля
3.	Раздел III. Средства защиты информации от несанкционированного доступа	26	12	6		8	Ответы на вопросы для самоконтроля
4.	Раздел IV. Обеспечение безопасности компьютерных систем и сетей	30	20	2		8	Ответы на вопросы для самоконтроля
	Итоговая аттестация	4			4		Зачёт в форме онлайн опроса или в бумажной форме
	Итого:	144	100	8	4	32	