ООО «АНТКОЛОНИ»

УТВЕРЖДЕНА

Приказ № 4

от «28» февраля 2025 г.

Левин М.В.

Дополнительная профессиональная программа

«Информационная безопасность»

502 часа

Разработчик: Левин М.В.

Санкт-Петербург

2025

1.ВВЕДЕНИЕ

Направление подготовки: Информационная безопасность

Цель: формирование знаний, умений и навыков, необходимых для выполнения нового вида профессиональной деятельности в сфере информационной безопасности

Категория слушателей: лица, имеющие или получающие высшее образование и (или) среднее профессиональное образование

Форма обучения – с применением дистанционных образовательных технологий

Режим занятий – определяется совместно с Заказчиком

Квалификация (степень) выпускника: дополнительное профессиональное образование

Компетенции выпускника, формируемые в результате освоения курса:

Выпускник должен обладать следующими профессиональными компетенциями (ПК):

Общепрофессиональными:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-5: способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-6: способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;

ПК-7: способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

ПК-8: способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

в эксплуатационной деятельности:

ПК-9: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-10: способностью администрировать подсистемы информационной безопасности объекта;

ПК-11: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

в проектно-технологической деятельности:

ПК-12: способностью участвовать в разработке подсистемы управления информационной безопасностью;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-14: способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-15: способностью применять программные средства системного, прикладного и специального назначения;

ПК-16: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-17: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;

ПК-18: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

в экспериментально-исследовательской деятельности:

ПК-19: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20: способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-21: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

ПК-22: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;

ПК-23: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;

ПК-24: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

в организационно-управленческой деятельности:

ПК-25: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

ПК-26: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;

ПК-27: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

ПК-28: способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

ПК-29: способностью участвовать в работах по реализации политики информационной безопасности;

ПК-30: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;

ПК-31: способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;

ПК-32: способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

ПК-33: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю.

2. СТРУКТУРА И СОДЕРЖАНИЕ КУРСА

Всего, час.	Лекции, час.	Практич. самост	Форма промежуточного контроля (тесты) час.
502	**406**	**90**	**6**

2.1. Учебно-тематический план

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Лекции	Практика	
1	2	3	4	5	6
1.	**МОДУЛЬ 1. Критерии защищенности информации.**	**20**	**12**	**8**	
	1.1. Конфиденциальность, целостность, доступность				
	1.2. Контроль доступа и его типы				
	1.3. Механизмы контроля доступа				
	1.4. Архитектура корпоративной кибербезопасности				

2.	**МОДУЛЬ 2. Моделирование угроз и оценка рисков кибербезопасности.**	**20**	**12**	**8**	
	2.1 Методики моделирования угроз 2.2. Методики оценки и управления рисками 2.3. Построение процессов и архитектуры кибербезопасности на основе модели угроз				
3.	**МОДУЛЬ 3. Безопасность сетей TCP/IP.**	**20**	**12**	**8**	
	3.1 Функциональная классификация механизмов защиты TCP/IP сетей 3.2 Контроль доступа к локальной сети. Защита от ARP и DHCP атак 3.3 Контроль доступа к локальной сети. 802.1x 3.4 Репутационная аналитика. IP, DNS и URL фильтрация 3.5 Фильтрация сетевого трафика. Firewall и IPS 3.6 Защита от DoS и DDoS атак 3.7 Защита Wi-Fi сетей				
4.	**МОДУЛЬ 4. Криптография и VPN.**	**20**	**12**	**8**	
	4.1. Принципы шифрования данных 4.2. Симметричные шифры 4.3 Асимметричные шифры 4.4 PKI 4.5 Принципы обеспечения целостности данных				

	4.6 Алгоритмы создания MAC 4.7 Принципы построения защищенных каналов связи 4.8 Принципы работы VPN 4.9 Классификация и архитектуры VPN				
5.	**МОДУЛЬ 5. Безопасность операционных систем.**	**20**	**12**	**8**	
	5.1 Принципы обеспечения защиты информации внутри ОС 5.2. Управление учетными записями 5.3. Модели безопасности ОС 5.4. Безопасность ОС Windows 5.5. Безопасность ОС Linux 5.6. Безопасность macOS 5.7. Безопасность мобильных ОС				
6.	**МОДУЛЬ 6. Безопасность приложений.**	**70**	**62**	**8**	
	6.1. Безопасность Web-приложений 6.2. Безопасность электронной почты. 6.3. Безопасность IP-телефонии 6.4. Безопасность облачной инфраструктуры Microsoft365 6.5. Безопасность платформ виртуализации				
7.	**МОДУЛЬ 7. Безопасность индустриальных объектов.**	**70**	**62**	**8**	
	7.1 Объекты и системы индустриальной инфраструктуры. 7.2 Компоненты обеспечения кибербезопасности индустриальных				

	объектов 7.3 Архитектура кибербезопасности индустриальных объектов				
8.	**МОДУЛЬ 8. Кибербезопасность информации.**	**45**	**37**	**8**	
	8.1 Работа с персональными данными и приватность информации 8.2 Защита от утечек данных 8.3 Защита авторского права средствами кибербезопасности				
9.	**МОДУЛЬ 9. Операционная кибербезопасность.**	**70**	**62**	**8**	
	9.1 Мониторинг событий и инцидентов кибербезопасности 9.2 Реагирование на события и инциденты кибербезопасности 9.3 OSINT – Open-Source Intelligence 9.4 Threat intelligence 9.5 Анализ уязвимостей 9.6 Reverse Engineering вредоносного п/о 9.7 Проведение Pentest'а 9.8 Цифровая криминалистика				
10.	**МОДУЛЬ 10. Проектирование и управление кибербезопасностью.**	**71**	**61**	**10**	
	10.1 Принципы управления кибербезопасностью 10.2 Построение процессов управления кибербезопасностью 10.3 Политики кибербезопасности 10.4 Оценка и метрики работы процессов				

	кибербезопасности 10.5 Построение корпоративного SoC'a				
11.	**МОДУЛЬ 11. Государственная политика Российской Федерации и национальные интересы в области обеспечения информационной безопасности**	**70**	**62**	**8**	
	11.1. Государственная политика Российской Федерации в области организационно-правового обеспечения информационной безопасности в условиях новых вызовов и угроз 11.2. Стратегические задачи и приоритетные направления правового регулирования в области обеспечения информационной безопасности в России 11.3 Организационное обеспечение информационной безопасности как составляющая реализации государственной политики в этой сфере				
ИТОГОВАЯ АТТЕСТАЦИЯ ПО КУРСУ		**6**		**6**	**тесты**
Всего часов:		**502**	**406**	**96**	

4. СОДЕРЖАНИЕ КУРСА

МОДУЛЬ 1. Критерии защищенности информации

Критерии защиты информации, основанные на конфиденциальности, целостности, доступности. Типы контроля доступа (дискреционный, обязательный, ролевой, атрибутный) и соответствующие механизмы (аутентификация, авторизация, шифрование, цифровые подписи, журналирование). Архитектура корпоративной кибербезопасности, включая оценку рисков, разработку политик, внедрение защитных мер, мониторинг и реагирование на инциденты.

МОДУЛЬ 2. Моделирование угроз и оценка рисков кибербезопасности

Методики моделирования угроз для выявления потенциальных уязвимостей и сценариев атак. Методы оценки и управления рисками, включая количественные и качественные подходы к определению вероятности и последствий угроз. Использование результатов моделирования угроз и оценки рисков для построения

эффективных процессов и архитектуры кибербезопасности, позволяющих минимизировать воздействие угроз.

МОДУЛЬ 3. Безопасность сетей TCP/IP

Классификация механизмов защиты сетей TCP/IP, методы контроля доступа к локальным сетям, включая защиту от атак на ARP и DHCP протоколы, а также использование стандарта 802.1x. Техники репутационной аналитики, фильтрация IP, DNS и URL адресов, применение межсетевых экранов (Firewall) и систем предотвращения вторжений (IPS) для фильтрации трафика. Защита от DoS и DDoS атак и меры безопасности для Wi-Fi сетей.

МОДУЛЬ 4. Криптография и VPN

Принципы шифрования данных, включая симметричные и асимметричные шифры, а также инфраструктуру открытых ключей (PKI). Принципы обеспечения целостности данных с использованием алгоритмов создания кодов аутентификации сообщений (MAC). Принципы построения защищенных каналов связи и разбор принципов работы VPN, их классификацию и различные архитектуры.

МОДУЛЬ 5. Безопасность операционных систем

Общие принципы защиты информации внутри операционной системы, управление учетными записями и различные модели безопасности. Изучение аспектов безопасности для Windows, Linux, macOS и мобильных операционных систем с учетом специфических для каждой платформы механизмов и уязвимостей.

МОДУЛЬ 6. Безопасность приложений

Аспекты безопасности веб-приложений, электронной почты и IP-телефонии. Безопасность облачной инфраструктуры Microsoft 365 и платформ виртуализации, специфические угрозы и методы защиты для каждого из этих сценариев.

МОДУЛЬ 7. Безопасность индустриальных объектов

Типы объектов и систем в индустриальной инфраструктуре. Компоненты, обеспечивающие их кибербезопасность, общая архитектура безопасности для таких объектов.

МОДУЛЬ 8. Кибербезопасность информации

Кибербезопасности информации при работе с персональными данными, защита приватности. Методы защиты от утечек данных и применение кибербезопасности для защиты авторских прав.

МОДУЛЬ 9. Операционная кибербезопасность

Мониторинг и реагирование на события и инциденты кибербезопасности, использование открытых источников информации (OSINT) и данных об угрозах (Threat Intelligence), анализ уязвимостей, обратный инжиниринг вредоносного ПО, проведение пентестов и основы цифровой криминалистики.

МОДУЛЬ 10. Проектирование и управление кибербезопасностью.

Принципы управления кибербезопасностью и построение соответствующих

процессов. Разработка политик кибербезопасности, оценка эффективности и метрики работы процессов, а также построение корпоративного центра безопасности (SoC).

МОДУЛЬ 11. Государственная политика Российской Федерации и национальные интересы в области обеспечения информационной безопасности

Государственная политика Российской Федерации в области организационно-правового обеспечения информационной безопасности в условиях новых вызовов и угроз. Стратегические задачи и приоритетные направления правового регулирования в области обеспечения информационной безопасности в России. Организационное обеспечение информационной безопасности как составляющая реализации государственной политики в этой сфере

Самостоятельная работа при изучении учебной дисциплины.

Виды работ:

Систематическая проработка материалов для подготовки к тестированию в соответствие с методическими рекомендациями.

40 закрытых вопросов с 4 вариантами ответа к каждому вопросу для самоконтроля в конце изучения курса.