Автономная Некоммерческая Организация
Дополнительного Профессионального Образования
«ТЮМЕНСКИЙ МЕЖРЕГИОНАЛЬНЫЙ ЦЕНТР АТТЕСТАЦИИ ПЕРСОНАЛА»

«УТВЕРЖДАЮ»
Исполнительный директор АНО
ДПО «ТМЦАП»
_____ Е.В. Ильина
«___» _____ 2020 г.

Дополнительная профессиональная образовательная программа повышения квалификации по циклу «Информационная безопасность».

	Должность	**Фамилия**	**Подпись**	**Дата**
Разработал	Преподаватель АНО ДПО «ТМЦАП»	Калугина Л.В.		

Тюмень 2020

Актуальность: В современном мире вопросы информационной безопасности являются одними из наиважнейших при внедрении и эксплуатации информационных систем. Связано это в первую очередь с расширением влияния информационных технологий в различные области деятельности человека. И так как все большее количество обрабатываемых данных и людей вовлечено в этот процесс наблюдается все большее число попыток получить несанкционированный доступ к ресурсам и данным информационных систем. Это в свою очередь ставит на первый план необходимость построения систем защиты информации.

Цель: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи:
- изучение концепции инженерно-технической защиты информации;
– изучение теоретических основ инженерно - технической защиты информации;
– изучение физических основ инженерно-технической защиты информации;
– изучение технических средств добывания и защиты информации;
– изучение организационных основ инженерно-технической защиты информации;
– изучение методического обеспечения инженерно-технической защиты информации.

Форма обучения: заочная (по желанию слушателя или заказчика возможны очная, очно – заочная, а также сочетание всех форм обучения) с применением электронного обучения, дистанционных образовательных технологий.

Срок обучения: 16 часов.

В результате изучения программы курса должны:

- знать основы информационной безопасности и защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду;

- уметь реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации;

- иметь представление о типовых разработанных средствах защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных систем.

Учебно-тематический план программы повышения квалификации

№п/п	Наименование темы, модуля	Всего часов	теория	Самост	Вид контроля
1	Понятие информационной безопасности. Понятие угрозы. Международные стандарты информационного обмена	1	0,5	0,5	опрос
2	Информационная безопасность в условиях функционирования в России глобальных сетей.	2	1	1	опрос

3	Виды противников или "нарушителей". Понятия о видах вирусов. Понятие угрозы. Наиболее распространенные угрозы. Классификация угроз	2	1,5	0,5	опрос
4	Виды возможных нарушений информационной системы. Виды защиты. Типовая операция враждебного воздействия	2	0,5	1,5	опрос
5	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	2	1	1	опрос
6	Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	1	0,5	0,5	опрос
7	Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Криптографические методы защиты информации	2	0,5	1,5	опрос
8	Основные технологии построения защищенных ЭИС. Защита от разрушающих программных воздействий. Программные закладки. RAID-массивы и RAID - технология.	2	1,5	0,5	опрос
	Итоговое тестирование	**2**	**2**		зачет
	ИТОГО	**16**	**8**	**8**	

Календарный учебный график
по программе дополнительной профессиональной
образовательной программы повышения квалификации

Календарный учебный график разработан в соответствии с Правилами внутреннего учебного распорядка в автономной некоммерческой организации дополнительного профессионального образования «Тюменский Межрегиональный Центр аттестации персонала» от 11.01.2019г №51.21;

- Федеральным законом от 29 декабря 2012 г. № 273 - ФЗ «Об образовании в Российской Федерации»,

-приказом Минобрнауки России от 01.07.2013г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»,

- приказом Минобрнауки РФ от 18.04. 2013 г. № 292 «Об утверждении Порядка организации и осуществления образовательной деятельности по основным программам профессионального обучения»,

- Уставом АНО ДПО «Тюменский межрегиональный центр аттестации персонала»

Календарный учебный график учитывает в полном объеме заявки организаций, заявления от физических лиц, возрастные особенности обучаемого контингента, и отвечает требованиям охраны их жизни и здоровья в процессе обучения.

Продолжительность обучения в АНО ДПО «Тюменский межрегиональный центр аттестации персонала»:

Учебным годом в АНО ДПО «Тюменский межрегиональный центр аттестации персонала» считается календарный год с 1 января по 31 декабря.

Режим работы АНО ДПО «Тюменский межрегиональный центр аттестации персонала»:
Продолжительность рабочего времени в день- 8 часов
Продолжительность рабочего времени в предпраздничные дни - сокращены на 1 час.
Начало работы в- 9час.00 мин.
Перерыв-с 12-00 до 13-00 час.
Окончание работы в 18-00 час.
Режим рабочего дня преподавателей определяется учебной нагрузкой.
Регламент образовательного процесса:
Продолжительность учебной недели 40 часов - 5 дней (понедельник-пятница),
Регламентирование образовательной деятельности на день 6-8 часов.
Учебные занятия организуются в одну смену (при необходимости в 2 смены).
Начало учебных занятий в 9:00 , окончание в 16.15 (с часовым перерывом на обед).
Продолжительность уроков (академический час): 45 мин. Перерыв между уроками-10 мин
Наполняемость групп: не более 20 человек

Оценочные и методические материалы

Основная литература

1. .Безопасность информационных технологий. Системный подход / . - Киев : ДС, 2004. - 992 с. : ил.
2. Информационная безопасность и защита информации: учебное пособие для студентов вузов / , , . - М. : Академия, 2011. - 336 с. - (Высшее профессиональное образование). Б. Шнайер. Прикладная криптография. 2-е издание. –
3. В. Столлингс, Криптография и защита сетей. Принципы и практика. 2-е издание. – М., «Вильямс», 2001
1. Nik Goots, Boris Izotov, Alex Moldovyan and Nik Moldovyan. Modern Cryptography: Protect Your Data with Fast Block Ciphers. - A-LIST Publishing, 2003
2. D. Bishop. Introduction to cryptography with Java Applets. – Jones and Bartlett Publishers, Inc., 2003
3. Allan Liska, The Practice of Network Security: Deployment Strategies for Production Environments. - Prentice Hall PTR., 2002
4. R. J. Shimonski, W. Schmied, T. W. Shinder, V. Chang, D. Simonis, D. Imperatore. DMZs for enterprise networks. – Syngress Publishing, Inc., 2003.
5. N. Doraswamy, D. Harkins. IPSec. The New Security Standard for the Internet, Intranets, and VPN. Second Edition. – Prentice Hall PTR., 2003

Дополнительная литература

1. Бабаш безопасность. Лабораторный практикум: учебное пособие для студентов вузов / , , . - М. : КНОРУС, 2012. - 136 с.
2. . Телекоммуникационные технологии (Сети TCP/IP) - Владивосток: Изд-во ВГУЭС, 1999.
3. М. Мамаев, С. Петренко. Технологии защиты информации в Интернете. Специальный справочник - СПб: "Питер", 2002.

Итоговая аттестация

Проходит в последний день обучения в тестовой форме по вопросам изучаемых тем/модулей.

Цель:

Проверка теоретических знаний, полученных в ходе изучения курса повышения квалификации «Информационная безопасность».

1. Основная масса угроз информационной безопасности приходится на:
а) Троянские программы
б) Шпионские программы
в) Черви

2. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли
в) одноразовые пароли

3. Под какие системы распространение вирусов происходит наиболее динамично:
а) Windows
б) Mac OS
в) Android

4. Заключительным этапом построения системы защиты является:
а) сопровождение
б) планирование
в) анализ уязвимых мест

5. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ

6. Какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный
в) логический

7. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про

8. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви

9. Stuxnet – это:
а) троянская программа
б) макровирус
в) промышленный вирус

10. Таргетированная атака – это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия
в) атака на конкретный компьютер пользователя

11. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или

преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа

12. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности

в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

13. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации

14. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур
в) защита от несанкционированного доступа к информации

15. Для чего создаются информационные системы:
а) получения определенных информационных услуг
б) обработки информации
в) оба варианта верны

16. Кто является основным ответственным за определение уровня классификации информации:
а) руководитель среднего звена
б) владелец
в) высшее руководство

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники

18. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

19. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности

20. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

21. Процедурой называется:
а) пошаговая инструкция по выполнению задачи
б) обязательные действия
в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

22. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:
а) проведение тренингов по безопасности для всех сотрудников
б) поддержка высшего руководства
в) эффективные защитные меры и методы их внедрения

23. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:
а) когда риски не могут быть приняты во внимание по политическим соображениям
б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски
в) когда стоимость контрмер превышает ценность актива и потенциальные потери

24. Что такое политика безопасности:
а) детализированные документы по обработке инцидентов безопасности
б) широкие, высокоуровневые заявления руководства
в) общие руководящие требования по достижению определенного уровня безопасности

25. Какая из приведенных техник является самой важной при выборе конкретных защитных мер:
а) анализ рисков
б) результаты ALE
в) анализ затрат / выгоды

26. Что лучше всего описывает цель расчета ALE:
а) количественно оценить уровень безопасности среды
б) оценить потенциальные потери от угрозы в год
в) количественно оценить уровень безопасности среды

27. Тактическое планирование:
а) среднесрочное планирование
б) ежедневное планирование
в) долгосрочное планирование

28. Эффективная программа безопасности требует сбалансированного применения:
а) контрмер и защитных механизмов
б) процедур безопасности и шифрования
в) технических и нетехнических методов

29. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
а) уровень доверия, обеспечиваемый механизмом безопасности
б) внедрение управления механизмами безопасности
в) классификацию данных после внедрения механизмов безопасности

30. Что из перечисленного не является целью проведения анализа рисков:
а) выявление рисков
б) делегирование полномочий
в) количественная оценка воздействия потенциальных угроз