АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ТИХООКЕАНСКАЯ ВЫСШАЯ ШКОЛА ЭКОНОМИКИ И УПРАВЛЕНИЯ»

«УТВЕРЖДАЮ»
Ректор АНОО ДПО «ТВШЭУ»
_____ /Ваганова Т.Д./
«20» 02 2020 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«Управление безопасностью на предприятии»

Категория слушателей - лица, имеющие высшее или среднее специальное образование

Форма обучения – очная, очно-заочная с применением дистанционных технологий, дистанционная

1. ОБЪЕМ УЧЕБНОЙ НАГРУЗКИ И ОТЧЕТНОСТЬ

Лекции	30
Практические занятия	45
Самостоятельная работа	120
Форма отчетности (текущая: зачетная, итоговая: ВКР/тестирование)	65
Всего	260

Хабаровск, 2020

Дополнительная образовательная программа
профессиональной переподготовки
«Управление безопасностью на предприятии»

Цель обучения: формирование и расширение профессиональных компетенций, необходимых для выполнения профессиональных задач.

Задачи курса:

- дать слушателям представление о информационной безопасности на предприятии, её организационном и правовом сопровождении;
- рассмотреть существующие угрозы информационной безопасности и методы защиты данных в информационных системах.

Условия для реализации программы:

- Дистанционная форма обучения.
- Сопровождение куратора на весь период обучения

Примерный перечень тем и краткое содержание

Модуль 1.Понятие и сущность безопасности на предприятии. Организационное и правовое обеспечение безопасности. Нормативно-правовая база в информационной безопасности. Структура информационного законодательства в РФ.

Модуль 2.Концепция безопасного кадрового развития предприятия. Психологические основы обеспечения кадровой безопасности. Профайлинг. Методы профайлинга. Основные направления обеспечения собственной безопасности компании. Мониторинг персонала.

Модуль 3. Причины и источники случайных воздействий на информационные системы. Понятие и классификация угроз. Угрозы информационной безопасности Каналы утечки информации.

Модуль 4. Способы неправомерного доступа к информации. Методы и средства защиты компьютерной информации. Организационные средства защиты информации. Технические средства защиты информации. Аутентификация и идентификация.

Модуль 5. Криптографические средства и методы защиты информации. Симметричные криптосистемы. Криптосистемы с открытым ключом. Электронная подпись. Управление ключами.

Модуль 6. Защита информации. Программные и аппаратные средства защиты информации. Основные принципы защиты информации. Антивирусные программы

Модуль 7. Защита персональных данных при их обработке в информационных системах. Персональные данные. Конфиденциальная информация. Нормативно-правовая база защиты персональных данных.

Модуль 8. Аудит и в информационных системах. Цель и задачи аудита. Виды аудита. Этапы проведения аудита информационной безопасности.

Примерный тематический план программы
«Управление безопасностью на предприятии» по часам

№	Наименование темы	Контактная работа	Самостоятельная работа	Нормоконтроль	Примечание
1	**Модуль 1.** Организационное и правовое обеспечение безопасности.	14	14	зачет	Лекция; тестирование
2	**Модуль 2.** Психологические основы обеспечения кадровой безопасности. Профайлинг.	14	14	зачет	Лекция; тестирование
3	**Модуль 3.** Угрозы информационной безопасности.	14	14	зачет	Лекция; тестирование
4	**Модуль 4** Методы и средства защиты компьютерной информации.	14	14	зачет	Лекция; тестирование
5	**Модуль 5** Криптографические средства и методы защиты информации.	14	14	зачет	Лекция; тестирование
6	**Модуль 6** Программно-аппаратные средства защиты информации.	14	14	зачет	Лекция; тестирование
7	**Модуль 7** Защита персональных данных при их обработке в информационных системах.	14	14	зачет	Лекция; тестирование
8	**Модуль 8** Аудит и в информационных системах.	14	14	зачет	Лекция; тестирование
9	**Итоговая аттестация Защита выпускной квалификационной работы (Итоговое тестирование)**	8	28	оценка	Защита ВКР / итоговое тестирование
10	**Итого**	120	140	х	х

№	Наименование темы	Контак-тная работа	Самосто-ятельная работа	Нормо-контроль	Примечание
	ВСЕГО	260		x	x

СПИСОК ЛИТЕРАТУРЫ И ИНТЕРНЕТ-ИСТОЧНИКОВ

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Федеральный закон от 16.02.95 № 15-ФЗ «О связи».
4. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
5. «Концепция национальной безопасности Российской Федерации», утверждена Указом Президента Российской Федерации от 17.12.97 № 1300.
6. «Доктрина информационной безопасности Российской Федерации», утверждена Указом Президента Российской Федерации от 09.09.2000 № Пр.–1895.
7. Указ Президента Российской Федерации от 16.08.04 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера».
9. «Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», утверждено Указом Президента Российской Федерации от 30.05.2005 № 609.
10. Постановление Правительства Российской Федерации от 11.02.0 № 135 «О лицензировании отдельных видов деятельности».
11. Постановление Правительства Российской Федерации от 15.08.06 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
12. Постановление Правительства Российской Федерации от 31.08.06 № 532 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».
13. «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено Постановлением Правительства Российской Федерации от 17.11.2007 № 781.
14. «Положение об особенностях обработки персональных данных, осуществляемой без использования
15. средств автоматизации», утверждено Постановлением Правительства Российской Федерации от 15.09.2008 № 687.

16. «Специальные требования и рекомендации по технической защите конфиденциальной информации» Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.

17. «Положение о ведении реестра операторов, осуществляющих обработку персональных данных»

18. Утверждено приказом Россвязьохранкультуры от 28.03.2008 № 154.

19. «Об утверждении Порядка проведения классификации информационных систем персональных данных»,приказ Федеральной службы по техническому и экспортному контролю ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008 № 55/86/20.

20. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15.02.2008;

21. «Методика определения актуальных угроз безопасности персональных данных при их обработке

22. в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14.02.2008;

23. «Административный регламент проведения проверок». Приказ Роскомнадзора от 01.12.2009 № 630

24. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа

25. к информации. Классификация автоматизированных систем и требования по защите информации.

26. Решение председателя Гостехкомиссии России от 30 марта 1992 года

27. Руководящий документ Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года.

28. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного

29. доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 года.

30. Руководящий документ Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение председателя Гостехкомиссии России от 30 марта 1992 года.

31. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Государственной

технической комиссии при Президенте Российской Федерации от 25 июля 1997года.

32. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования.

33. ГОСТ Р 51583-00. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

34. Анализ рисков в области защиты информации/ Электронное информационно- методическое пособие/ под ред. Петренко С.А.- СПб.: Афина, 2009

35. Аудит информационной безопасности/Электронное информационно- методическое пособие /под ред. Петренко С.А.- СПб.: Афина, 2012

36. Идентификация и аутентификация пользователей при удаленном электронном взаимодействии/ Электронное информационно-методическое пособие/Сабанов А.Г. - СПб.: Афина,2015

37. Методы защиты критически важной инфраструктуры /Электронное информационно-методическое пособие/ под ред. Петренко С.А - СПб.: Афина,2014

38. Обеспечение безопасности персональных данных/ Электронное информационно-методическое пособие/ под ред. Петренко С.А - СПб.: Афина,2013

39. Петренко С. А., Курбатов С. А. Политика информационной безопасности. – М.: ДМК Пресс, 2006.

40. Специалист объекта информатизации по технической защите информации/ Электронное информационно- методическое пособие / Е. Г. Воробьев, С. В. Войцеховский, А. В. Зотова. – СПб.: Афина,2014

41. Федотов Н.Н. Форензика – компьютерная криминалистика – М.: Юридический Мир, 2007 – 432 с.

42. Чумарин И. Г. Тайна предприятия: что и как защищать. – СПб: Изд-во ДНК, 2001.