МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

АНО «ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ»

УТВЕРЖДАЮ:
Директор
АНО «Профессиональный стандарт»

_____ А.В. Постюшков

25 апреля 2018 года

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

дополнительного профессионального образования
профессиональной переподготовки
«Основы кибербезопасности»

САРАТОВ - 2018

Содержание

1. Общая характеристика программы

1. Цель реализации программы

Целью изучения программы является формирование общих представлений о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

К задачам дисциплины относятся

- формирование общих представления о безопасности в информационном обществе;
- описать общие принципы технологий, применяемых в информационной безопасности;
- привить умения применять правила кибербезопасности во всех сферах деятельности
- освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах;
- овладение умением использовать компьютерную технику как практический инструмент для работы с информацией в повседневной жизни;
- развитие навыков ориентирования в информационных потоках;

В результате освоения программы профессиональной переподготовки слушателем будут приобретены следующие знания, навыки и умения:

знать:

– объекты компьютерных технологий, используемые в обеспечении кибербезопасности;
- понятийный аппарат информационных технологий и особенности терминологии кибербезопасности;
- базовые составляющие в области развития систем информационной безопасности
- объекты компьютерно-технической экспертизы;

уметь:

- ставить цели, формулировать задачи, связанные с обеспечением кибербезопасности;
- анализировать тенденции развития систем обеспечения кибербезопасности;
- применять знания о кибербезопасности в решении поставленных задач;

владеть:

– знаниями о современных технологиях, применяемых в области кибербезопасности;
методами проведения анализа в области обеспечения кибербезопасности.

2. Категория слушателей

Выпускники ВУЗов, колледжей, обучающихся по техническим направлениям, преподаватели, работники служб, занимающихся организацией кибербезопасности в организациях и на предприятиях.

3. Планируемые результаты обучения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОК – 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
ОК – 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях;
ОК – 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития;
ОК – 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности;

ОК – 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий;
ПК – 36. Способностью составлять прогнозы динамики основных показателей деятельности хозяйствующих субъектов;
ОК – 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях;
ОК – 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития;
ОК – 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности;
ОК – 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий;
ПК – 1. Способен разрабатывать модели средств, систем и процессов в инфокоммуникациях, проверять их адекватность на практике и использовать пакеты прикладных программ анализа и синтеза инфокоммуникационных систем, сетей и устройств.
ПК – 13. Способен к выполнению работ по обеспечению функционирования телекоммуникационного оборудования корпоративных сетей с учетом требований информационной безопасности;

Трудоемкость освоения – 520 академических часов (3 месяца).

2. Учебный план

№ п/п	Наименование Дисциплин	Общее число часов по дисциплине	Аудиторных часов, всего	В том числе:		Форма аттестации
				Лекции	Практические занятия	
1	Правовые основы профессиональной деятельности	28	28	20	8	Зачет
2	Компьютерные сети, информационно-аналитические системы и системы моделирования в технике	28	28	20	8	Зачет
3	Киберпространство и основы кбербезопасности, векторы риска	28	28	20	8	Зачет
4	Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	28	28	20	8	Зачет
5	Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	28	28	20	8	Зачет
6	Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	28	28	20	8	Зачет
7	Теоретические основы и практические аспекты защиты киберпространства	28	28	20	8	Зачет
8	Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности	28	28	20	8	Зачет
9	Государственная политика в области кибербезопасности и государственный аудит	28	28	20	8	Зачет
10	Информационное противоборство в бизнесе, обеспечение сохранности и конфиденциальности данных	28	28	20	8	Зачет
11	Внутренние и внешние угрозы, связанные с новыми информационными технологиями	28	28	20	8	Зачет
12	Управление ИТ-проектами и ИТ-процессами	28	28	20	8	Зачет
13	Организация и проведение работ по технической защите информации в компьютерных сетях и системах	28	28	20	8	Зачет
14	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	28	28	20	8	Зачет
15	Судебная компьютерно-техническая экспертиза	28	28	20	8	Зачет
ИТОГОВАЯ АТТЕСТАЦИЯ		**100**	**–**	**–**	**–**	**Итоговая аттестация**
ВСЕГО		**520**	**420**	**300**	**120**	

3. Календарный учебный план

3.1. Учебно-тематический план

№	Наименование дисциплины	Месяц 1				Месяц 2				Месяц 3			
		Нед.1	Нед.2	Нед.3	Нед.4	Нед.1	Нед.2	Нед.3	Нед.4	Нед.1	Нед.2	Нед.3	Нед.4
1	Правовые основы профессиональной деятельности	+/з	-	-	-	-	-	-	-	-	-	-	-
2	Компьютерные сети, информационно-аналитические системы и системы моделирования в технике	-	+/з		-	-	-	-	-	-	-	-	-
3	Киберпространство и основы кибербезопасности, векторы риска	-	+	+/з			-	-	-	-	-	-	-
4	Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	-	-	+	+/з	-	-	-	-	-	-	-	-
5	Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы	-	-	-	+	+/з	-	-	-	-	-	-	-
6	Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм	-	-	-	-	+/з	-	-	-	-	-	-	-
7	Теоретические основы и практические аспекты защиты киберпространства	-	-	-	-	-	+/з	-	-	-	-	-	-
8	Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности	-	-	-	-	-		-	-	-	-	-	-
9	Государственная политика в области кибербезопасности и государственный аудит	-	-	-	-	-	-	+	+/з		-	-	-
10	Информационное противоборство в бизнесе, обеспечение сохранности и конфиденциальности данных	-	-	-	-	-	-	-	-	+/з	-	-	-
11	Внутренние и внешние угрозы, связанные с новыми информационными технологиями	-	-	-	-	-	-	-	-	+	+/з	-	-
12	Управление ИТ-проектами и ИТ-процессами	-	-	-	-	-	-	-	-	-	-	+/з	
13	Организация и проведение работ по технической защите информации в компьютерных сетях и системах	-	-	-	-	-	-	-	-	-	-	+/з	
14	Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации	-	-	-	-	-	-	-	-	-	-	+	+/з
15	Судебная компьютерно-техническая экспертиза	-	-	-	-	-	-	-	-	-	-		+/з

\+ время изучение дисциплины (недели); з – зачет.

3.2 Содержание программы

Раздел 1. Правовые основы профессиональной деятельности
Концептуальные основы кибербезопасности. Структура стандарта по киберпезопасности. Базовые меры по кибербезопасности. Национальные стандарты в области киберпезопасности.

Раздел 2. Компьютерные сети, информационно-аналитические системы и системы моделирования в технике.
Информационная безопасность. Функциональная безопасность. Уязвимости, угрозы и риски. Вредоносное программное обеспечение. Векторы и поверхности атаки. Последствия кибератак. Нетехнические способы компрометации систем безопасности. Социальная инженерия. Информационная безопасность. Функциональная безопасность. Уязвимости, угрозы и риски. Вредоносное программное обеспечение. Векторы и поверхности атаки. Последствия кибератак.

Раздел 3. Киберпространство и основы кибербезопасности, векторы риска.
Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации. Проверка подлинности (аутентификация) в Интернете. Меры безопасности для пользователя WiFi. Настройка безопасности. Настройка компьютера для безопасной работы. Ошибки пользователя. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях

Раздел 4. Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости.
Понятие безопасности персонального компьютера. Интернет и виды угроз компьютерной безопасности. Проблемы безопасности информационных систем. Методы обеспечения защиты данных в СУБД. Безопасность при удаленном доступе к ресурсам компьютера. Новые технологии и новые угрозы информационной безопасности. Опасная информация в сети. Проблемные сайты. Риски интернета (контентные, электронные, коммуникационные, потребительские). Проблемы интернет зависимости.

Раздел 5. Методы обеспечения безопасности ПК и интернета, вирусы и антивирусы
Технологии защиты. Стратегии снижения рисков. Аудит безопасности. Мониторинг инцидентов кибербезопасности. Реагирование на инциденты кибербезопасности. Адаптивная архитектура безопасности.

Раздел 6. Мошеннические действия в интернете, киберпреступления против личности, общества и государства, хакерские атаки и кибертерроризм.
Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов. Понятие и виды хакерских атак. Способы защиты от хакерских атак. Кибертерроризм: понятие, приемы, способы предотвращения.

Раздел 7. Теоретические основы и практические аспекты защиты киберпространства.
Задачи и уровни обеспечения защиты киберпространства. Аспекты кибербезопасности. Доктрина информационной безопасности РФ.

Раздел 8. Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности.
Кибербезопасность как основной фактор национальной и международной безопасности. Государственные стратегии кибербезопасности: ЕС, США, Канада Япония. Общие принципы стратегии кибербезопасности. Руководство по кибербезопасности для развивающихся стран. Международные нормы по кибербезопасности.

Раздел 9. Государственная политика в области кибербезопасности и государственный аудит.
Концепция стратегии кибербезопасноти в РФ. Вопросы кибербезопасности в современной государственной политике в области обеспечения национальной безопасности. Государственный аудит в области киберпезопасности. Задачи, стоящие в области государственной политике по обеспечению национальной кибербезопасности.

Раздел 10. Информационное противоборство в бизнесе, обеспечение сохранности и конфиденциальности данных.
Информационное противоборство в бизнесе и кибербезопаснсть. Конфиденциальность информации. Угрозы конфиденциальной безопасности. Механизмы обеспечения конфиденциальности файлов и требования к ним. Система защиты информации и требования, предъявляемые к ней.

Раздел 11. Внутренние и внешние угрозы, связанные с новыми информационными технологиями.
Особенности современных информационных систем как объекта защиты информации. Классификация угроз безопасности информации. Характеристика основных угроз НСД и способов их реализации. Характеристика основных классов атак, реализуемых в сетях общего пользования. Методы оценки опасности угроз.

Раздел 12. Управление ИТ-проектами и ИТ-процессами.
Управление IT-проектами, среда проекта. Классификация ИТ-проектов, их место в деятельности компании. Жизненный цикл ИТ-проекта. Продукт ИТ-проекта. Стандарты управления проектами и их применимость в сфере ИТ. Основы управления проектами и процессами в области информационных технологий.

Раздел 13. Организация и проведение работ по технической защите информации в компьютерных сетях и системах
Организационно-технические мероприятия по защите информации. Вопросы проектирования, внедрения и эксплуатации АС и их систем зашиты информации.

Раздел 14. Проведение аттестации объектов вычислительной техники на соответствие требованиям по защите информации
Деятельность по аттестации объектов информатизации по требованиям безопасности информации. Добровольная и обязательная аттестация. Органы входящие в структуру системы аттестации. Документы и данные необходимые для проведения аттестации объектов вычислительной техники.

Раздел 15. Судебная компьютерно-техническая экспертиза
Предмет, объект и задачи компьютерно-технической экспертизы. Методы экспертизы. Возможности компьютерно-технической экспертизы

4. Организационно-педагогические условия реализации программы

4. 1. Материально-технические условия реализации программы

Приводятся сведения об условиях проведения лекций, лабораторных и практических занятий, а также об используемом оборудовании и информационных технологиях.

№ п/п	***Наименование специализированных аудиторий, кабинетов, лабораторий***	***Вид занятий***	***Наименование оборудования, программного обеспечения***
1.	*Аудитория*	*лекции*	*Ноутбук Lenovo (2,4 Ghz), мультимедийный проектор Sony, экран, доска*
2.	*Аудитория*	*практические занятия*	*учебные макеты, плакаты, слайды для изучения основ бюджетирования*

4.2. Организация образовательного процесса

Профессиональная программа подготовки «Основы кибербезопасности» обеспечена учебной литературой, учебно-методической документацией и материалами. Библиотечный фонд укомплектован печатными (электронными) изданиями основной литературы по всем дисциплинам. Учебники (печатные или электронные), обновляются с учетом степени успеваемости литературы.

Список рекомендуемой литературы по дисциплине включает научные, официальные, справочные, библиографические издания, периодические издания по профилю дисциплины.

4.3 Кадровое обеспечение образовательного процесса

Реализация рабочей программы обеспечивается педагогическими кадрами, имеющими высшее и среднее профессиональное образование, соответствующее профилю преподаваемой темы. Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации в соответствии с требованиями нормативных документов.

5. Формы аттестации, оценочные материалы

5.1 Формы и методы контроля

Итоговая аттестация после дополнительной профессиональной образовательной программы повышения квалификации «Основы кибербезопасности» осуществляется посредством подготовки и защиты аттестационной работы и должна выявлять теоретическую и практическую часть в соответствии с содержанием образовательной программы.

Темы для подготовки аттестационной работы:

• национальные стандарты России в области киберпезопасности;
• проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации;
• характеристика современного вредоносного программного обеспечения и виды кибератак;
• новые технологии и новые угрозы информационной безопасности;
• особенности современных информационных систем как объекта защиты информации;
• основные международные стандарты и наборы рекомендаций в области проектного и процессного управления;
• основные угрозы, риски и уязвимости в сфере кибербезопасности и критической информационной инфраструктуры;
• основные понятия в сфере функциональной безопасности;
• положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
• архитектура основных подсистем обеспечения ИБ объектов КИИ;
• основные определения СМИБ и особенности построения СМИБ для объектов КИИ на промышленных объектах;
• положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.
• основные средства обеспечения кибербезопасности (архитектура, принципы построения);
• принципы проектирования систем безопасности значимых объектов КИИ;
• состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ;
• основные риски и проблемы усовершенствования системы кибербезопасности
• состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз;

В процессе подготовки аттестационной работы слушателю следует:

- изучить отечественную и зарубежную научную литературу, и аналитические материалы по теме исследования, имеющиеся статистические данные;
- определить современные разработки в научной литературе
- провести анализ основных научно-теоретических концепций по изучаемой проблеме;
- раскрыть возможности применения полученных решению практических задач в сфере бюджетирования сформулировать выводы и предложения.

Рекомендуемая литература:

а) Основная литература:

- Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032. Вопросы кибербезопасности № 1(12) 2014. С. 28-35
- Петренко С. А., Смирнов М. Б. Безопасность АСУТП и критической информационной инфраструктуры // СПб.: ООО «ИД «Афина». – 2018. ISBN 978-5-9909868-1-7. Учебно-методическое пособие [Электронная версия]

- Куприяновский В.П. Кибер-физические системы как основа цифровой экономики / В.П. Куприяновский, Д.Е. Намиот, С.А. Синягов // International Journal of Open Information Technologies. – 2016. – Т.4 – №2. – С. 18-25.
- Васильева Т.В. «Интернет Вещей» – стратегическое направление инновационных преобразований в экономике России / Т.В. Васильева // Вопросы современной науки и практики. Университет им. В.И. Вернадского. – 2013. – № 2 (46). – С. 187-193.
- Никифоров О.Ю. Базовые технологии Интернета вещей / О.Ю. Никифоров // Символ науки. – 2015. – №9-1.
- Дроздов С. EurotEch, «Интернет вещей» и «облако устройств» / С. Дроздов, С. Золотарев // Control Engineering. – 2012. – № 8. – С.19.
- Маркеева А.В. Интернет вещей (iot): возможности и угрозы для современных организаций / А.В. Маркеева // Общество: социология, психология, педагогика. – 2016. – № 2. – С. 42–46.
- Что такое Интернет вещей (Internet of Things, IoT) [Электронный ресурс]. Режим доступа: http://tadviser.ru/a/135141 (дата обращения 25.06.2018).
- Лаврова Д.С. Обнаружение инцидентов безопасности в Интернете Вещей / А.И. Печенкин, Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. – СПб.: Изд-во Политехн. Ун-та. – 2015. – №2. – С. 69-79.

б) Дополнительная литература:

- Концепция основных мер защиты критической инфраструктуры Германии. Разработана Федеральным министерством внутренних дел, Федеральным ведомством по вопросам за-щиты населения и ликвидации последствий чрезвычайных ситуаций и Федеральным ве-домством криминальной полиции, а также рядом внешних экспертов. Первое издание, ян-варь 2006. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/Sprachvarianten/Basisschutzkonzept_kritische_Infrastrukturen_russisch.pdf?__blob=publicationFile
- ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements - See more at: https://www.isa.org/store/products/product-detail/?productId=116181#sthash.Nus3KyIn.dpuf / https://www.isa.org/store/products/product-detail/?productId=116181
- ОБСЕ. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства. 5 марта 2013 г. http://www.osce.org/ru/secretariat/110472
- Обеспечение безопасности АСУТП – краткий обзор семейства стандартов IEC 62443 http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystva-standartov-iec-62443
- Шаги к разработке безопасных продуктов Интернета вещей. 13.10.2016. Альянс «Облачная безопасность» (CSA) опубликовал новое руководство, что помочь дизайнерам и разработчикам Интернета Вещей, а также сопутствующих товаров и услуг, в понимании основных мер безопасности, которые должны быть частью всего процесса разработки. http://www.securitylab.ru/blog/personal/tsarev/318190.php
- Практические рекомендации по совершенствованию кибербезопасности для промышленных автоматизированных систем. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016/ https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

в) программное обеспечение и Интернет-ресурсы:

Лицензионные программы, используемые для учебного процесса:

Microsoft Office 2010 профессиональный плюс
Нормативно-справочная система Консультант Плюс
Интернет-ресурсы:
Интернет-ресурс Центрального банка России URL: www.cbr.ru
Сайт информационного агентства АК&М. URL: www.akm.ru
Интернет-ресурс «Инновации - инвестиции – индустрия». URL: http://www.rvca.ru
Универсальный портал для экономистов. URL: http://www.cfin.ru
Технологии управления проектами. URL: http://www.project.km.ru/