АНО ДПО «Учебный центр «Парадигма»
150047, г. Ярославль,
ул. Угличская, д.36/44
ИНН 7604200936 / КПП 760601001
ОГРН 1117600002178

Автономная некоммерческая организация дополнительного профессионального образования "Учебный центр "Парадигма"

«УТВЕРЖДАЮ»
Исполнительный директор
АНО ДПО "Учебный центр "Парадигма"

Гребенкина А.В. _____

«13» августа 2018 г.

Дополнительная профессиональная программа,
программа повышения квалификации

«Информационная безопасность автоматизированных систем»

Виды профессиональной деятельности:
организационно-управленческий, эксплуатационный

Трудоемкость - 120 часов
Форма обучения – заочная, с применением дистанционных образовательных технологий
Дополнительное профессиональное образование – повышение квалификации «*Информационная безопасность автоматизированных систем*»

Ярославль
2018 год

АНО ДПО «Учебный центр «Парадигма»
150047, г. Ярославль,
ул. Угличская, д.36/44
ИНН 7604200936 / КПП 760601001
ОГРН 1117600002178

1. Общая характеристика программы

1.1. Общие положения

Настоящая дополнительная профессиональная программа, программа повышения квалификации «Информационная безопасность автоматизированных систем» (далее - Программа) разработана на основании Федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовнаии в Российской Федерации», приказа Минобрнауки России от 5 декабря 2013 года № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» и приказа Минобрнауки России от 01.07.2013 года № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Минобрнауки России от 01.12.2016 № 1509.

Программа повышения квалификации реализуется в АНО ДПО Учебный центр «Парадигма». Программа повышения квалификации разработана по заказу ООО «Компания «Тензор» г. Ярославль.

1.2. Цели реализации программы

Целью реализации программы является ознакомление слушателей с основами комплексного подхода к обеспечению информационной безопасности (ИБ) автоматизированных систем (АС), проблемами защиты информации и подходами к их решению.

1.3. Категории слушателей

Программа предназначена для повышения квалификации руководителей и специалистов структурных подразделений органов государственной власти, органов местного самоуправления, предприятий, учреждений и организаций, занимающихся обеспечения информационной безопасности, технической, криптографической, физической и правовой защиты информации на объектах информатизации, включающих в себя компьютерные системы.

Повышение квалификации осуществляется только на базе высшего профессионального образования.

1.4. Планируемые результаты обучения

Слушатель, успешно освоивший Программу повышения квалификации, должен

- Знать:
  основные угрозы безопасности информации и модели нарушителя в АС;
  АС как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
  содержание и порядок деятельности персонала по эксплуатации защищенных АС;
  законодательные акты в области защиты информации;
  основные задачи подразделения защиты информации;
  основные меры по защите информации в АС (организационные, правовые, программно-аппаратные, физические, технологические);
  основные защитные механизмы, применяемые в АС;
- Уметь:
  разрабатывать модели угроз и нарушителей в АС;

анализировать и оценивать риски информационной безопасности;
разрабатывать структуру системы обеспечения безопасности АС;
классифицировать уязвимости АС;
правильно выбирать средства защиты АС;

- Владеть:
использования основных защитных механизмов подсистем безопасности АС;
разработки системы организационно-распорядительных и нормативно-методических документов по защите информации;
определения требований к защите и категорирования ресурсов АС;
применения штатных и дополнительных средств защиты информации от несанкционированного доступа (НСД);
построения инфраструктуры управления событиями.

Все знания, умения и навыки, полученные в процессе обучения слушатель должен применять в своей дальнейшей профессиональной деятельности.

1.5. Трудоемкость программы

Нормативная трудоемкость обучения по программе повышения квалификации – 120 часов.

1.6. Форма и сроки обучения

Обучение по программе профессиональной переподготовки осуществляется в заочной (без отрыва от работы) форме с использованием дистанционных образовательных технологий.

Срок обучения составляет 6 недель.

1.7. Режим занятий

Нагрузка устанавливается - 20 часов в неделю.

Для занятий устанавливается академический час продолжительностью 45 минут.

АНО ДПО «Учебный центр «Парадигма»
150047, г. Ярославль,
ул. Угличская, д.36/44
ИНН 7604200936 / КПП 760601001
ОГРН 1117600002178

2. Содержание программы

2.1. Учебный план

№ п/п	Наименование учебных дисциплин	Всего учебных часов
1.	Основы безопасности автоматизированных систем	10
2.	Правовые основы обеспечения безопасности автоматизированных систем	20
3.	Обеспечение безопасности автоматизированных систем	30
4.	Средства защиты информации от несанкционированного доступа	32
5.	Обеспечение безопасности компьютерных сетей	26
6.	Итоговая аттестация	2
	Итого:	120

2.2. Рабочие программы модулей

2.2.1. Учебная программа дисциплины «Информационная безопасность автоматизированных систем»

План-график распределения учебных недель в соответствии с рабочей программой

№ п/п	Наименование модуля	Количество недель
1.	Основы безопасности автоматизированных систем	0,5
2.	Правовые основы обеспечения безопасности автоматизированных систем	1
3.	Обеспечение безопасности автоматизированных систем	1,5
4.	Средства защиты информации от несанкционированного доступа	1,5
5.	Обеспечение безопасности компьютерных сетей	1,5
6.	Итоговая аттестация	—
	Итого:	6

Доступ слушателей к серверу, на котором расположена учебная программа в формате электронного обучения осуществляется слушателями круглосуточно за исключением времени регламентных (профилактических) работ.

Обучение начинается по мере формирования группы. Общая продолжительность обучения – 6 недель.

2.2.2. Рабочая программа учебного курса

Модуль 1. Основы безопасности автоматизированных систем

Лекция 1. Определение безопасности автоматизированных систем

Лекция 2. Угрозы безопасности автоматизированных систем

Лекция 3. Классификация угроз безопасности и каналов проникновения в АС

Лекция 4. Неформальная модель нарушителя

Модуль 2. Правовые основы обеспечения безопасности автоматизированных систем

Лекция 1. Правовые основы обеспечения безопасности автоматизированных систем

Лекция 2. Защищаемая информация

Лекция 3. Лицензирование

Лекция 4. Сертификация средств защиты информации и аттестация объектов информатизации

Лекция 5. Специальные требования и рекомендации по технической защите конфиденциальной информации

Лекция 6. Юридическая значимость электронных документов с электронной подписью

Лекция 7. Ответственность за нарушения в сфере защиты информации

Лекция 8. Изменения в законодательстве Российской Федерации в сфере ИТ в 2018г.

Модуль 3. Обеспечение безопасности автоматизированных систем

Лекция 1. Организационная структура системы безопасности автоматизированных систем

Лекция 2. Обязанности пользователей и ответственных за обеспечение информационной безопасности

Лекция 3. Ответственность за нарушения требований обеспечения безопасности

Лекция 4. Порядок работы с носителями ключевой информации

Модуль 4. Средства защиты информации от несанкционированного доступа

Лекция 1. Назначение и возможности средств защиты информации от несанкционированного доступа

Лекция 2. Защита периметра компьютерных сетей и управление механизмами защиты

Лекция 3. Страхование информационных рисков

Лекция 4. Аппаратно-программные средства защиты информации от несанкционированного доступа

Лекция 5. Обзор существующих на рынке средств защиты информации от несанкционированного доступа

Лекция 6. Средства аппаратной поддержки

Лекция 7. Способы аутентификации

Лекция 8. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа

Лекция 9. Разграничение доступа зарегистрированных пользователей к ресурса АС

Лекция 10. Оперативное оповещение о зарегистрированных попытках

несанкционированного доступа

Модуль 5. Обеспечение безопасности компьютерных сетей

Лекция 1. Защита периметра корпоративной сети

Лекция 2. Межсетевые экраны

Лекция 3. Анализ содержимого почтового и веб-трафика

Лекция 4. Виртуальные частные сети

3. Условия реализации программы, организационно-педагогические условия

3.1 Требования к уровню подготовки поступающего на обучение, необходимые для освоения программы

Лица, желающие освоить программу повышения квалификации, должны иметь высшее техническое образование смежное с УГНПС 10.00.00 «Информационная безопасность». Наличие указаного образования должно подтверждаться документом государственного или установленного образца.

3.2 Требования к кадровым условиям реализации программы

Реализация программы профессиональной переподготовки обеспечивается руководящими и научно-педагогическими работниками организации, а также лицами, привлекаемыми к реализации программсы на условиях гражданско-правового договора.

Все научно-педагогические работники, участвующие в реализации программы профессиональной переподготовки, должны иметь образование, соответствующее профилю преподаваемой дисциплины (модуля), конкретный опыт реализации научно-прикладных разработок или иной формы практической деятельности в области информационной безопаснсоти.

Студентам предоставляется возможность копирования материала для самоподготовки и подготовки к зачету.

3.3 Требования к информационному и учебно-методическому обеспечению программы

Каждый Слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке), содержащей обязательные и дополнительные издания учебной, учебно-методической и иной литературы. Перечисленной в рабочих программах дисциплин (моулей), практик, с выполнением установленных требований по защите информации. Библиотечный фонд учебного центра укомплектован печатными изданиями. Фонд дополнительной литературы включает официальные, справочно-библиографические и специализированные отечественные и зарубежные периодические издания, в том числе, правовые нормативные акты и нормативные методические документы в области информационной безопасности.

4. Форма аттестации. Оценочные материалы

Оценка качества освоения слушателями программы повышения квалификации «Информационная безопасность автоматизированных систем» включает итоговую аттестацию слушателей в виде зачета.

4.1 Критерии оценки зачета

Оценка	Предмет оценки
Отлично 86-100 баллов.	86-100 баллов. Есть ответы на все вопросы. Допущены незначительные ошибки.
Хорошо 70-85 баллов.	70-85 баллов. Правильные ответы даны на более, чем 70% вопросов, но менее 86%.
Удовлетворительно 51-69 баллов.	Правильные ответы даны на более, чем 50% вопросов, но менее 70%
Неудовлетворительно 50 и менее баллов.	Менее 50% правильных ответов.

Итоговая аттестация слушателей по программе повышения квалификации включает итоговый зачет.

Итоговая аттестация организуется и проводится в соответствии с «Положением об итоговой аттестации АНО ДПО «Учебный центр «Парадигма».

5. Литература и нормативные акты

5.1. Постановления Правительства Российской Федерации

1. Постановление Правительства РСФСР от 05 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».
2. Постановление Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).
3. Постановление Правительства Российской Федерации от 03 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
4. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».
5. Постановление Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
6. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
7. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
8. Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об

особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

9. Постановление Правительства Российской Федерации от 04 марта 2010 г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».
10. Постановление Правительства Российской Федерации от 21 апреля 2010 г. № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации»,
11. Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)».
12. Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
13. Постановление Правительства Российской Федерации от 03 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
14. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
15. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию

шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

16. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5.2. Иные информационные акты

1. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 25.11.1994).
2. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 27,10,1995, приказ № 199).
3. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утв. Государственной технической комиссией при Президенте РФ от 30.08.2002, приказом № 282).
4. Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации (утв. ФСТЭК России 25.04.2006).
5. Методические рекомендации по технической защите информации, составляющей коммерческую тайну (утв. ФСТЭК России 25.12.2006).
6. Пособие по организации технической защиты информации, составляю¬щей коммерческую тайну (утв. ФСТЭК России 25.12.2006).
7. Методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007 и 19.11.2007).

5.3. Литература

1. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум. М.: КноРус, 2013, 136 с.
2. Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. 2011, № 4.
3. Волков П.П. Экспертный анализ методов защиты информации от утечки по техническим каналам // Эксперт-криминалист. 2009, № 4.
4. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция. 2011, № 2.
5. Воротников В.Л. О правовой защите компьютерной информации // Администратор суда. 2009, № 2.
6. Гафнер В.В. Информационная безопасность. Ростов н/Д: Феникс. 2012, 324 с.
7. Громов Ю.Ю., Драчев В. О., Иванова О.Г. Информационная безопасность и защита информации. Ст. Оскол: ТНТ. 2013, 384 с.
8. Забегайло Л.А., Назарова И.А. Актуальные вопросы охраны коммерческой тайны в

отношениях с органами государства // Современное право. 2011, № 7.
9. Кузнецова Т.В. Организация работы с персональными данными // Трудовое право. 2011, № 5.
10. Партыка Т.Л., Попов И.И. Информационная безопасность. М.: Форум, 2012, 432 с.
11. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи. 2006, 400 с.
12. Петров С.В., Слинькова И.П., Гафнер В.В. Информационная безопасность. АРТА. 2012, 296 с.
13. Савчишкин Д.Б. Административная ответственность как средство обеспечения информационной безопасности // Административное и муниципальное право. 2011, № 6.
14. Семененко В.А. Информационная безопасность. М, 2010, 277 с.
15. Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журнал российского права. 2011, № 5.