Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
"ТОМСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ"

пл. Соляная, 2, г. Томск, 634003, телефон (3822) 65-39-30,факс (3822) 65-25-52, e-mail: rector@tsuab.ru

ИНСТИТУТ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ

УТВЕРЖДАЮ
Проректор по учебной работе

_____ О.Г. Волокитин

«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА

повышения квалификации

«Обеспечение информационной безопасности персональных данных в кредитной организации»

Наименование программы

направление подготовки (специальности):

Код и наименование

Томск
2018

1. Общая характеристика программы.

1.1. Цель и задачи реализации программы.

Целью реализации программы повышения квалификации является совершенствование и освоение специалистами актуальных изменений в области информационной безопасности персональных данных, обновление теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности персональных данных в кредитной организации. В курсе проанализированы требования вступающих в силу поправок в закон о персональных данных, требования смежных законов, актуальные нормативные правовые акты, в частности, изменения в Трудовом и Гражданском процессуальном кодексах РФ, законах о банках и банковской деятельности, и о судебных приставах. Рассматривается допустимость и порядок обработки персональных данных кандидатов на вакантные должности организации, близких родственников работников, различных категорий субъектов, не состоящих с банками в договорных отношениях, но чьи персональные данные обрабатываются банками (лиц, имеющих право распоряжения средствами на счетах клиентов, пользователей банковских ячеек, посетителей, представителей контрагентов и т.д.). Детально рассматриваются вопросы передачи третьим лицам персональных данных заемщиков по кредитам с целью взыскания просроченной задолженности, архивного хранения персональных данных, передачи третьим лицам персональных данных заемщиков по кредитам с целью взыскания просроченной задолженности и архивного хранения персональных данных. Специальный раздел программы курса посвящен проблемам соотнесения персональных данных и банковской тайны, принятым в последнее время законодательным актам, расширяющим возможность доступа к банковской тайне налоговых органов, Банка России.

Для достижения указанной цели предлагается решение следующих задач*:*

- изучение организационно-правовых основ обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
- овладение методами и приемами осуществления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- изучение перечня и содержания документов, определяющих порядок хранения и уничтожения персональных данных клиентов на бумажных носителях;
- изучение условий конфиденциальности персональных данных клиентов организации;
- изучение классификации программных и технических средств защиты информации;
- проведение анализа объекта информатизации;
- построение модели угроз и модели злоумышленника;
- осуществление контроля средств защиты информации.

В процессе обучения слушатель выполняет проектную работу — разрабатывает пакет организационно-распорядительной документации для организации в отношении персональных данных.

1.2. Категория слушателей.

Лица, желающие освоить программу повышения квалификации, должны иметь высшее или среднее - специальное образование, иметь общее представление об организации бизнес-процессов, связанных с обработкой персональных данных в кредитной организации.

Желательно наличие у слушателей общих знаний в области информационных технологий, знание бизнес-процессов, касающихся обработки персональных данных в организации.

Сфера профессиональной деятельности – защита персональных данных.

1.3. Трудоемкость обучения.

1.3. Трудоемкость обучения и режим занятий слушателей.

Нормативный срок освоения программы – 72 часа, включая все виды аудиторной и самостоятельной учебной работы слушателей.

Учебная нагрузка устанавливается не более 36 часов в неделю, включая все виды аудиторной и внеаудиторной учебной работы слушателя.

1.4. Форма обучения и форма организации образовательной деятельности.

Форма обучения: очно-заочная, заочная.

Продолжительность учебной недели составляет: по очно-заочной форме обучения – 2 недели, по заочной форме обучения – 4 недели.

Программа реализуется с использованием дистанционных образовательных технологий.

2. Формализованные (планируемые) результаты освоения программы.

Изучение данной программы направлено на формирование у слушателей следующих компетенций:

общекультурных компетенций:

ОК1 умение использовать нормативные правовые документы в своей деятельности;

ОК2 способность разрабатывать локальные организационно-распорядительные документы;

ОК3 умение обеспечивать конфиденциальность персональных данных клиентов организации;

профессиональных компетенций:

расчетно-экономическая деятельность

ПК1 способность собрать и проанализировать исходные данные, необходимые для расчета и оценки технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений;

ПК2 проведение исследований с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации;

аналитическая деятельность:

ПК3 способность осуществлять сбор, анализ и обработку данных, необходимых для решения поставленных задач информационной безопасности;

ПК4 умение определять актуальные угрозы безопасности персональных данных;

ПК5 умение определять требуемые уровни защищённости персональных данных, обрабатываемых в информационных системах персональных данных

ПК6 , умение классифицировать и выбирать программные и технические средства защиты информации;

организационно-управленческая деятельность:

ПК7 способность эффективно организовать процесс обработки персональных данных в организации (компании);

ПК8 умение составлять и совершенствовать внутренние положения организации, предусматривающие персональную ответственность сотрудников, которые занимаются обработкой данных клиентов;

ПК9 способность составлять документы, определяющие порядок хранения и уничтожения персональных данных клиентов на бумажных носителях;

ПК10 умение разрабатывать предложения по совершенствованию текущей системы управления информационной безопасностью;

ПК11 умение организации контроль средств защиты информации;

ПК12 способность участвовать в работах по реализации политики информационной безопасности.

ПК13 В результате освоения программы у слушателя должен сформироваться комплекс знаний, умений и навыков в области информационной безопасности персональных данных субъектов при их обработке в кредитных организациях в рамках требований законодательства Российской Федерации, а также практические навыки по их применению.

В результате изучения программы слушатели должны:

знать:

- основные понятия, используемые при работе с персональными данными;
- принципы и условия хранения персональных данных;
- права субъекта персональных данных;
- права и обязанности оператора персональных данных;
- ответственность за нарушение законодательства Российской Федерации в области персональных данных.

уметь:

- обосновывать управленческие решения в области информационной безопасности на предприятии;
- обеспечивать конфиденциальность персональных данных клиентов;
- обращаться с документами, содержащими персональные данные;
- составлять нормативно-правовые документы в области информационной безопасности предприятия;
- осуществлять порядок работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

владеть:

- методикой выявления угроз безопасности информации;
- методикой оценки состояния защиты персональных данных;
- организационными и техническими методами обеспечения безопасности персональных данных.

3. Содержание программы.

3.1. Календарный учебный график.

Образовательный процесс по программе может осуществляться в течение всего учебного года.

Занятия проводятся по мере комплектования групп. Возможно индивидуальное обучение.

Таблица 1. Форма календарного учебного графика

График обучения / **Форма обучения**	**Ауд. часов в день**	**Дней в неделю**	**Общая продолжительность программы (дней, недель, месяцев)**
очно-заочная	6	6	2 неделя
заочная	3	6	4 недели

3.2. Учебный план.

Таблица 2. Форма учебного плана программы, реализуемой в полном объеме с использованием аудиторных занятий (дистанционных образовательных технологий).

№ п/п	**Наименование дисциплин (модулей)**	**ОТ*, час.**	**Аудиторные/ дистанционные занятия, час.**		**ВЗ* час.**	**СРС*, час.**	**Форма контроля**
			Лк*	**ПЗ, СЗ, ЛЗ***			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1.	Модуль 1. Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации	13	5	3	-	5	Тест
2.	Модуль 2. Структура, задача и основные функции системы защиты ПДн	15	6	4	-	5	Тест зачет

3.	Модуль 3. Системы обработки ПДн	19	7	4	-	8	Тест зачет
4.	Модуль 4. Рекомендации по защите ПДн	21	8	6	-	7	Тест зачет
Практики (стажировки)		-					Не предусмотрено
Итоговая аттестация		4		2	-	2	зачет
	ИТОГО:	**72**	26	19	-	27	

[*] *ОТ – общая трудоемкость, Лк – лекции, ПЗ – практические занятия, СЗ – семинарские занятия, ЛЗ – лабораторные занятия, ВЗ – выездные занятия, СРС – самостоятельная работа слушателя*

3.3. Содержание учебных дисциплин (модулей).

Таблица 4. Форма содержания учебных дисциплин (модулей).

Модуль 1. Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации.

№ п/п	Наименование тем	Содержание обучения по темам, наименование и тематика лабораторных (практических и/или семинарских) занятий, самостоятельной работы слушателя и используемых образовательных технологий
1.1	Основные понятия ФЗ "О персональных данных".	Основные понятия, термины и определения в области информационной безопасности. Персональные данные в банке и банковских системах.
1.2	Категории данных.	Общедоступные, подлежащие опубликованию или обязательному раскрытию персональные данные. Биометрические персональные данные. Специальные категории персональных данных и особенности их обработки. Данные о судимости. Доступ к банковской тайне.
1.3	Права субъекта ПДн и обязанности оператора.	Условия обработки персональных данных. Согласие субъекта. Согласие в письменной форме. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных законом.
1.4	Ответственность за нарушение требований ФЗ "О персональных данных"	Гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством Российской Федерации ответственность.
Практические и/или семинарские занятия		Составление перечня персональных данных, подлежащих защите и перечня бизнес-процессов для заданной модели информационной системы
Лабораторные работы		Не предусмотрены
Самостоятельная работа слушателя		Разбор Федерального закона №149-ФЗ "Об информации, информационных технологиях и о защите информации.
Используемые образовательные технологии		В преподавании курса используются преимущественно традиционные образовательные технологии: лекции, практические занятия, самостоятельное изучение разделов.

Модуль 2. Структура, задача и основные функции системы защиты ПДн

№ п/п	Наименование тем	Содержание обучения по темам, наименование и тематика лабораторных (практических и/или семинарских) занятий, самостоятельной работы слушателя и используемых образовательных технологий
2.1	Управление информационной безопасностью в организации.	Анализ Федерального закона Российской Федерации № 152-ФЗ «О персональных данных». Область применения закона. Ограничения. Анализ Постановления Правительства РФ 2012 г. № 1119, Постановления Правительства РФ от 15 сентября 2008 г. № 687. Обзор систем типа «Банк-Клиент», обзор ДБО.
2.2	Структура локальной нормативной документации.	Локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений, их содержание, порядок разработки и ввода в действие
2.3	Классификация угроз информационной безопасности и каналов утечки информации.	Условия обработки персональных данных. Согласие субъекта. Согласие в письменной форме. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных законом.

Практические и/или семинарские занятия	Составление локальных нормативных документов
Лабораторные занятия	Не предусмотрены
Самостоятельная работа слушателя	Разбор Постановления Правительства РФ №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
Используемые образовательные технологии	В преподавании курса используются преимущественно традиционные образовательные технологии: лекции, практические занятия, самостоятельное изучение разделов.

Модуль 3. Системы обработки ПДн

№ п/п	Наименование тем	Содержание обучения по темам, наименование и тематика лабораторных (практических и/или семинарских) занятий, самостоятельной работы слушателя и используемых образовательных технологий
3.1	Организация работ по классификации ИСПДн.	Методология определения класса ИСПДн. Проведение инвентаризации документов в ИСПДн на наличие в них ПДн.
3.2	Модель угроз.	Базовая модель угроз. Перечень источников угроз. Уровень исходной защищенности. Методика актуализации угроз. Акт классификации ИСПДн.
3.3	Классификация нарушителей. Модель нарушителя.	Определение угроз безопасности информации. Банк данных угроз безопасности информации.
3.4	Особенности обработки персональных данных, осуществляемой без использования средств автоматизации.	Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных".
Практические и/или семинарские занятия		Определение класса защищенности и уровня защищенности ПДн для заданной информационной системы персональных данных
Лабораторные занятия		Не предусмотрены
Самостоятельная работа слушателя		Методика определения актуальных угроз безопасности персональных данных, порядок разработки модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
Используемые образовательные технологии		В преподавании курса используются преимущественно традиционные образовательные технологии: лекции, практические занятия, самостоятельное изучение разделов.

Модуль 4. Рекомендации по защите ПДн

№ п/п	Наименование тем	Содержание обучения по темам, наименование и тематика лабораторных (практических и/или семинарских) занятий, самостоятельной работы слушателя и используемых образовательных технологий
4.1	Обеспечение безопасности ПДн в ИСПДн	Место и роль системы защиты ПДн в общей системе обеспечения информационной безопасности.
4.2	Организация защиты ПДн от несанкционированного доступа.	Угрозы несанкционированного доступа к информации. Архивное хранение. Доступ клиентов к персональным данным, находящимся на архивном хранении в банке.
4.3	Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств.	Позиции Банка России и ФСТЭК России.Порядок обращения с криптосредствами и криптоключами к ним. Учет криптосредств. Порядок действий при компрометации криптоключей.
4.4	Аттестация	Аттестат соответствия. Порядок проведения аттестации объектов информатизации. Надзорные органы. Организация проверок, права, обязанности надзорных органов и проверяемых организаций.
Практические и/или семинарские занятия		Перечень и краткое содержание организационно-распорядительной документации, регламентирующей вопросы организации обработки и обеспечения безопасности персональных данных
Лабораторные занятия		Не предусмотрены
Самостоятельная работа слушателя		разбор разъяснений Роскомнадзора по работе с персональными данными

Используемые образовательные технологии	В преподавании курса используются преимущественно традиционные образовательные технологии: лекции, практические занятия, самостоятельное изучение разделов.

3.4. Требования к промежуточной и итоговой аттестации.

Промежуточная аттестация проводится по каждому модулю. Аттестация по первому модулю осуществляется в форме теста, по остальным – прохождением теста и выполнением задания на тему пройденного материала. Итоговая оценка уровня освоения дисциплины осуществляется по двухбалльной системе («зачет», «незачет»).

Информационная система персональных данных определяется слушателем самостоятельно из предоставленного преподавателем перечня.

Возможные варианты вопросов для промежуточного контроля перечислены в Приложении А.

Лицам, успешно освоившим программу повышения квалификации и получившим оценку «зачет», выдается удостоверение о повышении квалификации.

4. Условия реализации программы.

4.1. Материально-технические условия реализации.

Занятия проводятся дистанционно с использованием системы управления курсами Moodle (izido.ru).

4.2. Учебно-методическое обеспечение программы.

Доступ к электронным образовательным ресурсам происходит через единую информационно-образовательную среде MOODLE.

Основная литература:

Нормативные правовые акты:

1. Федеральный закон Российской Федерации от 27.07.2006 г. № 149- ФЗ "Об информации, информационных технологиях и о защите информации" (принят ГД ФС РФ 08.07.2006)
2. Федеральный Закон Российской Федерации от 27.07.2006 г. № 152-ФЗ "О персональных данных".
3. Постановление Правительства Российской Федерации от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
4. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных осуществляемой без использования средств автоматизации»
5. Постановление Правительства Российской Федерации от 15 апреля 1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»
6. Указ президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
7. О государственной тайне Закон РФ от 21 июля 1993 г. N 5485-I (в ред. от 18, 19 июля 2011 г.).

8. О связи Федеральный закон от 07 июля 2003 г. N 126-ФЗ (ред. от 18 июля 2011 г.) (с изм. и доп., вступающими в силу с 29 сентября 2011 г).
9. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.
10. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России.
11. Приказ ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах
12. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности
13. Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
14. КоАП РФ Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных
15. ТК РФ Глава 14. Защита персональных данных работника
16. Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных"
17. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных

Дополнительная литература:

18. Вычисления в системах управления: учебное пособие / А. Е. Городецкий, В. В. Козлов, Ю. Н. Артеменко, И. Л. Тарасова. - СПб.: Изд-во Политехн. ун-та, 2006.
19. Информационное право: учебное пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин. М.: «Юнити-Дана», 2015 – 336 с.
20. Специальные вопросы информационной безопасности: Монография / Мещеряков Р. В., Шелупанов А. А. – Томск: Изд-во Института оптики атмосферы СОРАН.2003. – 224 с.
21. Общие вопросы технической защиты информации./ Д.А. Скрипник – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012 – 231 с.

Электронные и Internet-ресурсы:

22. Информационная безопасность открытых систем: Учебник для вузов в 2-х частях. Часть 1. /С.В.Запечников, Н.Г.Милославская, А.И.Толстой, Д.В.Ушаков. -М.: Горя-чая линия - Телеком, 2006. - 686 с. Н.В. Шишлина Автор электронного курса. Учеб-но-методическое пособие. Ижевск, 2015. http://weblabor.ru/docs/aek-2015.pdf
23. Информационно-правовой портал – Гарант URL: http://www.garant.ru
24. Официальный сайт компании Консультант Плюс – URL: http://www.consultant.ru
25. Банк данных угроз ФСТЭК - URL: https://bdu.fstec.ru/

5. Кадровое обеспечение программы.

Образовательный процесс по модулям обеспечивается кадрами, имеющими специальное образование, соответствующее профилю модуля, и опыт деятельности в соответствующей профессиональной сфере.

Преподавательский состав, работающий по данной программе представлен в приложении В.

6. Разработчики программы.

А.В. Солдатова, специалист по защите информации ЦИТ ТГАСУ

(подпись)

А.Н. Хуторной, к.т.н., доцент директор ИНО - ТГАСУ (разделы учебного плана)

(подпись)

СОГЛАСОВАНО:

Руководитель программы:

_____ (А.В. Солдатова)

Директор ИНО-ТГАСУ А.Н. Хуторной

Пример.

Приложение А

Возможные варианты вопросов для промежуточного контроля

1. Понятие персональных данных.
2. Понятие системы защиты ПДн.
3. Угрозы и каналы утечки информации.
4. Законодательство РФ в области ПДн.
5. Понятие субъекта ПДн.
6. Понятие оператора ПДн.
7. Правовое основание для обработки ПДн.
8. Условия обработки ПДн.
9. Общедоступные источники ПДн.
10. Специальные категории данных.
11. Биометрические ПДн.
12. Случаи, не требующие согласия на обработку субъекта ПДн.
13. Понятие ИСПДн.
14. Основные внутренние нормативные документы, регулирующие действия с ПДн субъекта.
15. Понятие и виды несанкционированного доступа.
16. Порядок обращения с ПДн.
17. Контроль и учет соблюдения мер по конфиденциальности ПДн.
18. Существующие модели удостоверяющих центров.
19. Классы ИСПДн, требующие обязательной сертификации (аттестации).
20. Правовое основание для обработки ПДн.
21. Понятие лицензирования.
22. Процедура аттестации ИСПДн.
23. Органы, осуществляющие надзор за соблюдением требований ФЗ-152.
24. Процедур контроля СЗИ.
25. Аттестация СЗИ.
26. Срок аттестата соответствия.

Приложение В

Кадровое обеспечение программы

№ п/п	Наименование дисциплин (модулей), разделов (тем, элементов и т.д.)	Фамилия, имя, отчество, год рождения	Ученая степень, ученое звание	Стаж	Основное место работы, должность	Место работы и должность по совместительству (если есть)
1.	Модуль 1. Нормативно-правовое обеспечение защиты персональных данных в Российской Федерации	Солдатова Анна Валерьевна, 1991	-	5 лет	ТГАСУ, ЦИТ, Специалист по защите информации	-
2.	Модуль 2. Структура, задача и основные функции системы защиты ПДн	Солдатова Анна Валерьевна, 1991	-	5 лет	ТГАСУ, ЦИТ, Специалист по защите информации	
3.	Модуль 3. Системы обработки ПДн	Солдатова Анна Валерьевна, 1991	-	5 лет	ТГАСУ, ЦИТ, Специалист по защите информации	
4.	Модуль 4. Рекомендации по защите ПДн	Солдатова Анна Валерьевна, 1991	-	5 лет	ТГАСУ, ЦИТ, Специалист по защите информации	