

УДК 004.56(06) (075.8)
ББК 32.973.26-018.2 я73
П 30

Печатается по решению
редакционно-издательского совета
Северо-Кавказского федерального
университета

Петренко В. И.

П 30 Защита персональных данных в информационных системах:
учебное пособие. – Ставрополь: Изд-во СКФУ, 2016. – 201 с.

Пособие предоставляет собой курс лекций, способствующих приобретению необходимых знаний для обеспечения безопасности персональных данных, в нем рассмотрены основные термины и законодательство Российской Федерации в данной предметной области. Приведены этапы построения системы защиты персональных данных.

Предназначено для студентов, обучающихся по направлению подготовки 10.03.01 – Информационная безопасность.

УДК 004.56(06) (075.8)
ББК 32.973.26-018.2 я73

Рецензенты:

д-р физ.-мат. наук, доцент *Ф. Б. Тебуева*,
канд. техн. наук, доцент *К. А. Катков*

© ФГАОУ ВО «Северо-Кавказский
федеральный университет», 2016

Предисловие

Информационные технологии никогда не стояли и не стоят на месте, мы постоянно видим их бурный рост. Но в последнее время наблюдается особенно стремительное их развитие, проявляющееся в регулярном появлении новых и модернизации старых программных и аппаратных средств. В свою очередь, такой бурный рост сопряжён с появлением новых уязвимостей в продуктах информационных технологий и новых угроз информационной безопасности. Параллельно идёт процесс постоянного совершенствования нормативно-правовой и нормативно-методической базы в области обеспечения информационной безопасности и защиты информации. Указанные и ещё многие другие причины обуславливают необходимость наличия в штате организаций различных форм собственности грамотных, обученных специалистов в указанной предметной области, а также необходимость повышения уровня осведомлённости рядовых сотрудников в вопросах информационной безопасности. Деятельность структурных подразделений по защите информации в Российской Федерации регламентируется различными нормативно-правовыми и нормативно-методическими документами. Однако необходимо отметить, что, несмотря на постоянное совершенствование указанных документов, имеет место их несоответствие актуальным угрозам и современному уровню развития информационных технологий, иногда расплывчатость формулировок, нечёткое определение понятий, отсутствие конкретизации требований, носящих порой общих, формальный характер.

Вопросы информационной безопасности, в том числе касающиеся защиты персональных данных, необходимость их эффективного решения признаются приоритетными и требуют мобилизации усилий как на основе анализа ситуации и использования накопленного за предыдущие годы опыта работы, так и посредством применения новых подходов в деятельности, связанной с защитой информации.

Целью дисциплины «Защита персональных данных в информационных системах» является обеспечение студентов теоретическими знаниями и практическими навыками, необходимыми для формирования компетенций по обеспечению безопасности пер-

сональных данных при их обработке в информационных системах персональных данных, а также работ по технической защите конфиденциальной информации (ТЗКИ) в соответствии с современными требованиями.

В ходе курса студенты изучают вопросы защиты персональных данных и подготовки предприятий к выполнению требований Федерального Закона «О персональных данных» от 27.07.06 года № 152-ФЗ, правовые и организационные основы обеспечения безопасности в информационных системах персональных данных (ИСПДн), методы и процедуры выявления угроз безопасности персональных данных (ПДн) и оценки степени их опасности.

При изучении дисциплины особое внимание уделяется требованиям российского законодательства, нормативно-методическим документам по организации защиты ПДн при их обработке в ИСПДн.

В учебном пособии рассмотрены все этапы создания защиты персональных данных: от первичного анализа до ввода в действие системы защиты персональных данных. Такой объем информации позволит специалистам построить эффективную систему защиты в рамках существующих требований.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Уязвимость информационной системы персональных данных – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении ИСПДн, которые могут быть использованы для реализации угрозы безопасности персональных данных.

Характеристика безопасности объекта – требование к объекту, или к условиям его создания и существования, или к информации об объекте и условиях его создания и существования, выполнение которого необходимо для обеспечения защищенности жизненно важных интересов личности, общества или государства.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Содержание

3	Предисловие
	Тема 1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ
5	1.1. Основные понятия и определения
5	1.1.1. Актуальность проблемы защиты персональных данных в информационных системах
8	1.1.2. Основные понятия информационной безопасности
11	1.1.3. Федеральный закон «Об информации, информационных технологиях и о защите информации»
	Тема 2. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
16	2.1. Международное и национальное право в области защиты персональных данных
17	2.1.1. Конвенция «О защите физических лиц при автоматизированной обработке персональных данных»
26	2.1.2. Директива о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных
35	2.1.3. Директива в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи
40	2.1.4. Дополнительный протокол о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации
46	2.2. Федеральное законодательство Российской Федерации в области защиты персональных данных
48	2.2.1. Требования к защите персональных данных при их обработке в информационных системах персональных данных
56	2.2.2. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

- 59 2.2.3. Требования к материальным носителям биометрических персональных данных
- 63 2.3. Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»
- 63 2.3.1. Общие положения закона
- 65 2.3.2. Принципы и условия обработки персональных данных
- 67 2.3.3. Категории персональных данных
- 69 2.3.4. Права субъекта персональных данных
- 70 2.3.5. Обязанности оператора персональных данных
- 75 2.4. Специальные нормативные документы по технической защите сведений конфиденциального характера
- 75 2.4.1. Нормативно-методические документы ФСТЭК РФ
- 83 2.4.2. Нормативно-методические документы ФСБ РФ

3. УГРОЗЫ И УЯЗВИМОСТИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

- 90 3.1. Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах
- 91 3.1.1. Основные принципы моделирования угроз с использованием методических документов ФСТЭК и ФСБ
- 92 3.1.2. Угрозы информационной безопасности
- 95 3.1.3. Общая характеристика уязвимостей информационной системы персональных данных
- 98 3.2. Наиболее часто реализуемые угрозы
- 98 3.2.1. Угрозы утечки информации по техническим каналам
- 101 3.2.2. Угрозы несанкционированного доступа к информации в информационной системе персональных данных
- 112 3.3. Методология формирования модели угроз с использованием Методических рекомендаций ФСБ
- 112 3.3.1. Общие принципы
- 113 3.3.2. Методология формирования модели угроз верхнего уровня

116	3.3.3. Методология формирования детализированной модели угроз
118	3.3.4. Методология формирования модели нарушителя
	4. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
127	4.1. Порядок организации защиты персональных данных
127	4.1.1. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных
128	4.1.2. Оценка обстановки и формирование замысла защиты персональных данных
131	4.1.3. Организационно-распорядительная документация по защите персональных данных
135	4.2. Меры по обеспечению безопасности персональных данных
135	4.2.1. Состав и содержание мер по обеспечению безопасности персональных данных
146	4.2.2. Порядок выбора мер по обеспечению безопасности персональных данных
151	4.3. Построение системы защиты персональных данных
151	4.3.1. Основные этапы при построении системы защиты персональных данных
153	4.3.2. Комплекс организационных и технических мероприятий в рамках СЗПДн
155	4.3.3. Уведомление Роскомнадзора об обработке персональных данных
158	4.4. Подсистемы в составе СЗПДн
158	4.4.1. Общая характеристика подсистем
163	4.4.2. Межсетевые экраны
165	4.5. Аттестация, сертификация и лицензирование в области защиты персональных данных
165	4.5.1. Сертификация средств защиты персональных данных

170	4.5.2. Аттестации ИСПДн по требованиям безопасности информации
173	4.5.3. Лицензирование деятельности по защите персональных данных
179	4.6. Контроль в области защиты персональных данных
179	4.6.1. Регуляторы в области защиты персональных данных
181	4.6.2. Проверки Роскомнадзора
185	4.6.3. Проверки ФСБ
188	4.6.4. Проверки ФСТЭК
193	Глоссарий