

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/diplomnaya-rabota/207189>

Тип работы: Дипломная работа

Предмет: Информационные технологии

ВВЕДЕНИЕ 3

1. Анализ требований к обеспечению защищенности кредитно-финансовой организации от утечек конфиденциальной информации 5

1.1 Обзор законодательной базы обеспечения защиты информации 5

1.2. Общие сведения о DLP-системах 9

1.3 Анализ утечек конфиденциальной информации 23

1.4. Требования к системе обеспечения информационной безопасности кредитно-финансовой организации от утечек конфиденциальной информации 25

2. Анализ актуальных угроз от утечек конфиденциальной информации кредитно-финансовой организации 29

2.1. Общая характеристика кредитно-финансовой организации кредитно-финансовой организации и ее ИТ-инфраструктуры 29

2.2. Анализ обрабатываемой информации в информационных системах Управления ПФР 32

2.3. Построение модели угроз и модели нарушителя 47

3. Организация мероприятий по внедрению DLP-системы в кредитно-финансовой организации 62

3.1. Анализ рынка DLP-систем 62

3.2. Выбор DLP-системы для организации защиты конфиденциальной информации от утечек в кредитно-финансовой организации 67

3.3. Общие подходы к внедрению DLP-систем в кредитно-финансовой организации 70

3.4. Оценка экономической эффективности внедрения DLP 73

ЗАКЛЮЧЕНИЕ 79

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 81

Нормативная база в области защиты персональных данных включает:

□ 152-ФЗ «О Персональных данных» от 27.07.2006;

□ 149 – ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006;

□ Статьи Трудового кодекса, кодекса об административных правонарушениях;

□ Локальные нормативные акты.

Нормативной базой технологии систем информационной безопасности являются: федеральное законодательство, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, а также руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и ФСБ России, регулирующие вопросы безопасности информации. В соответствии с нормативными документами в области защиты информации, каждое предприятие и организация, в которой производится обработка персональных данных, обязано принять ряд организационных и технологических мер по обеспечению защиты информации.

Приведем основные положения законодательных актов в области информационной безопасности.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным

Согласно Федеральному закону от 27 июля 2006г. № 152-ФЗ, оператор в рамках обработки персональных данных должен обеспечивать комплекс необходимых правовых, организационных и технических мер по обеспечению конфиденциальности персональных данных, что достигается путем определения угроз безопасности, оценки эффективности мероприятий по обеспечению безопасности, контроля за принимаемыми мерами по защите информации [8].

Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Постановление № 1119 содержит довольно подробную классификацию информационных систем персональных данных, угроз безопасности таких систем (п. 6), уровней защищенности информационных систем от указанных угроз

Приказ ФСТЭК России № 21 от 18.02.2013 определяет принципы классификации систем персональных данных. Согласно приказу ФСБ от 10.07.2014 № 378 определены четыре уровня защищенности персональных данных.

Каждый из присвоенных уровней защищенности предполагает применение соответствующих мер по обеспечению информационной безопасности.

В зависимости от соотношения типа информационной системы и характерных для нее угроз выделены четыре уровня защищенности персональных данных, необходимых для конкретной информационной системы.

Персональные данные - любая информация, имеющая отношение к определенному или определяемому на основании такой информации физическому лицу, позволяющая его идентифицировать включающая реквизиты:

фамилия, имя, отчество;

дату и место рождения;

контактные данные;

данные об образовании, месте работы;

иные данные (о состоянии здоровья, биометрические данные, реквизиты документов, данные идентификации субъекта в банковских системах и др.)

Субъект персональных данных - физическое лицо, идентифицируемое посредством персональных данных (владелец персональных данных).

1. База данных угроз ФСТЭК. [Электронный ресурс]. Режим доступа: <https://bdu.fstec.ru/threat> (дата доступа: 27.11.2021)
2. Клименко И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И. С. Клименко. - Москва: ИНФРА-М, 2020. - 178с.
3. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2018. - 250 с.
4. Солодяников А. В. Комплексная система защиты объектов информатизации: учебное пособие / А. В. Солодяников. - Санкт-Петербург: Изд-во Санкт-Петербургского государственного экономического университета, 2017. - 91 с.
5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И. С. Клименко. - Москва: ИНФРА-М, 2020. - 178 с.
6. Чекулаева Е. Н., Кубашева Е. С. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола: Поволжский государственный технологический университет, 2020. - 153 с.
7. Алексеев А. П. Многоуровневая защита информации: монография / А. П. Алексеев. - Самара : ПГУТИ, 2017. - 128 с.
8. Благодаров, А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А. В. Благодаров, В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш. - Москва: Горячая линия-Телеком, 2015. - 115 с.
9. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей: методы и средства: учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2017. - 225с.
10. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа : [монография] / Ю. К. Язов, С. В. Соловьев. - Воронеж: Кварта, 2018. - 588 с.
11. Марков А. С. Техническая защита информации: курс лекций: учебное пособие / Марков А.С. - Москва : Изд-во АИСНТ, 2020. - 233с.
12. Королев, Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
13. Михайлова, Е. М. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017. - 342 с.
14. Камалова Г. Г. Юридическая ответственность за нарушение конфиденциальности информации: монография / Камалова Гульфия Гафиятовна. - Саратов : Амирит, 2019. - 160 с.

15. Никифоров, С. Н. Защита информации: защита от внешних вторжений : учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 82 с
16. Белов, Е. Б. Организационно-правовое обеспечение информационной безопасности: учебник / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - Москва: Академия, 2020. - 332с.
17. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. - Новосибирск: НГУЭУ, 2018. - 83 с.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/diplomnaya-rabota/207189>