

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/otchet-po-praktike/97655>

Тип работы: Отчет по практике

Предмет: Информатика

Введение 3

1. Участие в планировании и организации работ по обеспечению защиты объекта 5

1.1. Организация системы безопасности организации 5

1.2. Техническое обеспечение защиты информации 9

2. Организация и технология работы с конфиденциальными документами 12

2.1. Организация функционирования системы конфиденциального документооборота. 12

2.2. Организация работы персонала с конфиденциальной информацией 12

3. Применение программно-аппаратных и технических средств защиты информации 14

Заключение 20

Список использованных источников 21

Введение

Актуальность

Специфика работы современных организаций такова, что в соответствии с технологией работы необходимо осуществление обмена информацией, доступ к которой является ограниченными в соответствии с требованиями законодательства.

Таким образом, для обеспечения нужного уровня защищенности необходимо создать защищённую сетевую инфраструктуру, обеспечивающую защиту от несанкционированного доступа.

Обеспечение защиты персональных данных в настоящее время является актуальной задачей в силу того, что утечка данных, позволяющих идентифицировать личность людей, может привести к негативным последствиям для субъекта персональных данных, что включает: потерю имущества, предоставление несанкционированного доступа к банковским счетам, обнародованию конфиденциальной информации и др. Это связано с тем, что с внедрением систем электронного документооборота становится возможным предоставление доступа к аккаунтам субъекта по предъявлению определенного типа персональной информации.

Политика информационной безопасности должна предусматривать комплекс мероприятий, связанных с обеспечением организационных мер, разработкой документационного обеспечения защиты информации, разработкой регламентов использования программной защиты информации, физической защиты помещений, а также защиты от утечек информации с использованием каналов связи.

Обеспечение защиты персональных данных в настоящее время регламентировано в различных законодательных актах федерального уровня, а также отраслевых документах. Таким образом, при использовании информационных систем, в которых проводится обработка персональных данных необходимо принятие мер по обеспечению их защищенности в соответствии с установленными стандартами.

Цель прохождения практики: анализ архитектуры защиты информации в условиях ГУФСИН России по Пермскому краю.

Задачи работы:

- Анализ нормативных актов, регламентирующих вопросы информационной безопасности;
- Классификация видов угроз безопасности;
- Анализ системы защиты конфиденциальной информации;
- Анализ программной компоненты защиты информации.

Объект исследования: системы информационной безопасности ГУФСИН России по Пермскому краю

Предмет исследования: архитектура защиты информации ГУФСИН России по Пермскому краю.

1. Участие в планировании и организации работ по обеспечению защиты объекта

1.1. Организация системы безопасности организации

Организационные меры защиты включают в себя административные, управленческие меры, определяющие порядок работы систем по обработке данных, использованию ее ресурсов, деятельности обслуживающего персонала, а также технологии по взаимодействию пользователей с системой таким образом, чтобы минимизировать вероятность реализации угроз безопасности персональных данных (либо максимально снизить размер ущерба при их реализации).

В таблице 2 приведено описание перечня документов, регламентирующих организацию защиты информации УФСИН.

Таблица 1 - Документационное обеспечение защиты конфиденциальной информации

Угроза Технология защиты Документационное обеспечение

Вредоносная программа Антивирусное программное обеспечение «Положение об антивирусной защите в подразделениях ООО

Вторжение в ИСПД по информационно-телекоммуникационным сетям Технология VipNet «Аппаратный журнал VipNet Coordinator»

Закладка аппаратная Тестирование аппаратных средств «Акт ввода в эксплуатацию средств вычислительной техники»

Закладка программная Тестирование программных средств «Положение о Фонде Алгоритмов и Программ в подразделениях ООО

Произвольное копирование баз данных Разграничение доступа «Таблицы разграничения доступа к информационным ресурсам в подразделениях ООО,

«Инструкция о резервном копировании информационных ресурсов в подразделениях ООО

Накопление данных пользователями ИСПД Ограничение уровня доступа «Таблицы разграничения доступа», должностные инструкции

Наличие программных ошибок Взаимодействия с разработчиками «Заявка на доработку программного обеспечения»

Ошибки в работе персонала Программные и аппаратные технологии защиты "Руководство пользователя"

Чрезвычайные ситуации Порядок эвакуации носителей информации Порядок эвакуации носителей информации

Компрометация электронной подписи Выпуск новых ключей ЭП, расследование причин «Порядок обращения с ключами ЭП»

Компрометация паролей Принудительная смена пароля, блокировка учетных записей «Инструкция по обращению парольной документации»

Визуальный съём отображаемых данных (при присутствии посторонних лиц в процессе обработки данных пользователем) Блокировка экрана с использованием электронного ключа Порядок доступа в помещения организации

Таким образом, разработка комплекта документационного обеспечения способствует противодействию угрозам конфиденциальности информации при её обработке в автоматизированной информационной системе.

В рамках совершенствования системы организации защиты персональных данных предлагается принятие ряда организационных мер.

1. Документирование учета носителей информации. Пример формы Журнала учета внешних носителей, используемых для работы с персональными данными.

2. Определение приказом рабочих станций, используемых для работы с персональными данными. Станции должны опечатываться специальными защитными знаками, номера которых указываются в данном журнале.

3. Проведение обследования помещений, где обрабатываются персональные данные, с оформлением акта. В соответствии с определенными выше угрозами, в подразделениях организаций необходимо принятие ряда организационных мер, определяемых в локальных документах, перечень которых приведен в таблице 2.

Каждому из типов угроз сопоставлено технологическое решение, подкрепленное документационным обеспечением [3].

Выводы по организации системы защиты информа

Список использованных источников

1. IDS – Snort. О программе. [Электронный ресурс]. Режим доступа: <http://www.netconfig.ru/ready/snort/>
2. Сетевая защита информации. [Электронный ресурс]. Режим доступа: http://icdv.ru/uslugi/sredstva_doverennoj_zagruzki/
3. Гофман М.В. Безопасность сетей ЭВМ : учебное пособие / М.В. Гофман. - Санкт-Петербург: ФГБОУ ВО ПГУПС, 2017. - 241с.
4. Бехроуз А. Криптография и безопасность сетей: учебное пособие / Фороузан А. Бехроуз. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с.
5. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник / Е. Л. Новикова. - Москва : Академия, 2018. - 189 с.
6. Новиков С. Н. Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи / Новиков Сергей Николаевич. - Новосибирск, 2016. - 39 с.
7. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей: [учебный курс] / В.Г. Олифер, Н.А. Олифер. - Москва : Горячая линия - Телеком, 2016. - 643 с.
8. Басыня Е. А. Сетевая информационная безопасность и анонимизация: учебное пособие / Е. А. Басыня. - Новосибирск : Изд-во НГТУ, 2016. - 74с.
9. Лавров Д. Н., Колмаков А. В. Анализ безопасности компьютерных сетей: тесты на проникновение и поиск уязвимостей сетевых протоколов: учебное пособие / Д.Н. Лавров, А.В. Колмаков. - Омск : Изд-во Омского государственного университета, 2016. - 546с.
10. Голиков А.М. Основы проектирования защищенных телекоммуникационных систем [Электронный ресурс]: учебное пособие / А.М. Голиков. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. - 396 с
11. Сафонов В.О. Основы современных операционных систем [Электронный ресурс] : учебное пособие / В.О. Сафонов. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 826 с
12. 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.
13. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва : ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
14. Такатлы Д. А. Защита персональных данных / Д. А. Такатлы. - Петропавловск-Камчатский: Дальневосточный филиал Федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации", 2016. - 92 с.
15. Овчинникова Т. А. Ответственность за нарушение требований законодательства РФ о персональных данных: монография / Т. А. Овчинникова . - Хабаровск : Изд-во ТОГУ, 2018. - 81с.
16. 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.
17. Аникин Д. В. Информационная безопасность и защита информации : учебное пособие / Д.В. Аникин. - Барнаул : Изд-во Алтайского государственного университета, 2018. - 196 с.
18. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. - 334 с.
19. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова. - Ухта : УГТУ, 2016. - 69 с.
20. Ахметов И. В., Карабельская И. В., Губайдуллин И. М., Сафин Р. Р. Моделирование бизнес-процессов: учебное пособие. - Уфа: Уфимский государственный университет экономики и сервиса, 2015. - 67 с.
21. Бабиева Н. А., Раскин Л. И. Проектирование информационных систем : учебно-методическое пособие / Н. А. Бабиева, Л. И. Раскин. - Казань : Медицина, 2014. - 200с.
22. Баранников Н. И., Яскевич О. Г. Современные проблемы проектирования корпоративных информационных систем / Н. И. Баранников, О. Г. Яскевич; ФГБОУ ВПО "Воронежский гос. технический ун-т". - Воронеж: Воронежский государственный технический университет, 2014. - 237 с.
23. Королев Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
24. Михайлова Е. М., Анурьева М. С. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р.

Державина", 2017.

25. 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

26. Никифоров С. Н. Защита информации: учебное пособие / С.Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2017. - 76 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/otchet-po-praktike/97655>