Тип работы: Курсовая работа

Предмет: Информационные технологии

Содержание

Введение

В рамках данной работы проведен анализ технологий обеспечения защиты от сетевых угроз на ресурсы корпоративных сетей. Специфика современных компаний связана с необходимостью использования информационных систем в рамках ведения производственных процессов. Сетевые информационные ресурсы компаний используются как для информирования о свой деятельности, так и для непосредственного взаимодействия с клиентами в рамках осуществления основной деятельности. Таким образом, от стабильности функционирования сетевых информационных ресурсов зависит возможность исполнения компаниями своих функций, работы с документами, проведения платежей. Бесперебойное функционирование информационных ресурсов обеспечивает возможности работы подразделений компаний, выполнения сотрудниками своих обязанностей, обеспечивает возможности взаимодействия с клиентами, с партнерами, в некоторых случаях позволяет обеспечивать проведение платежей.
В компаниях с разветвленной филиальной сетью зачастую используются информационные системы, имеющие распределенную архитектуру, связь между сегментами которой обеспечивается через настройку механизмов обмена данными. В случае проведения атак на серверы, через которые производится обмен информацией, наблюдаются нарушения доступа к информационным ресурсам, невозможность актуализации данных. Таким образом, использование распределенных систем позволяет эффективно распределять вычислительную нагрузку между сегментами ИТ-инфраструктуры, но при этом необходимо обеспечивать защиту систем от внешних атак.
Цель курсовой работы заключается в разработке мер по анализу безопасности использования межсетевых экранов.
Задачи работы:
 анализ специфики организации защиты сетевых ресурсов;
 анализ функционала межсетевых экранов;
 анализ безопасности использования межсетевых экранов с использованием специализированных программных средств.
Объект исследования: технологии обеспечения информационной безопасности.
Предмет исследования: системы защиты от сетевых угроз на информационные ресурсы.

1. Аналитическая часть
1.1 Обзор законодательных актов в области защиты информации

В рамках данной работы проведён анализ законодательных актов в области обеспечения информационной безопасности.
Концепция информационной безопасности России содержит официально принятую систему взглядов на проблемы, связанные с обеспечением защиты информации, включает описание типовых методов и средств, обеспечивающих решение задач по защите информации.
Развитие информационных технологий предполагает возможности для утечек больших массивов данных по определенной тематике, включая данные персонифицированного характера. Используемые в настоящее время носители информации малогабаритны, но при этом позволяют сохранять на них значительные объемы информации. Таким образом, при использовании информации конфиденциального характера необходимо учитывать возможность их несанкционированного копирования и принимать превентивные меры.
Нормативная база технологии защиты информации включает в себя: нормы федерального законодательства, указы Президента Российской Федерации и постановления Правительства РФ, а также регламентирующие документы федеральных структур, регулирующих технологии безопасности информации.
Основные нормативные акты, регулирующие вопросы обеспечения защиты информации, включают в себя:
 Конституцию Российской Федерации;
 Законодательство о персональных данных (152-ФЗ от 27.07.2006);
 Федеральный закон об информации информационных технологиях и о защите информации (149-ФЗ от 27.07.2006);
 Федеральный закон об электронной подписи (63-ФЗ от 06.04.2011);
 Нормативные акты, регламентирующие документы федеральных служб.
Использование межсетевых экранов регламентируется в документах:
 «Положение о системе сертификации средств защиты информации» (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55, вступило в силу 1 августа 2018 г.);
 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утверждены приказом ФСТЭК России от 30 июля 2018 г. № 131, вступили в силу 1 августа 2018 г., применяются при проведении сертификационных испытаний с 1 мая 2019 г.);
 «Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении» (утверждена ФСТЭК России 11 февраля 2019 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.).
Определение термина «защита информации» приводится в статье 16 ФЗ «Об информа¬ции, информационных технологиях и защите информации» (149-ФЗ от 27.07.2006):
Обеспечение информационной безопасности предполагает необходимость проведения правовых, организационных и технических мероприятий, предполагающих решение вопросов в областях:
1) обеспечения защиты информации от несанкционированного доступа, препятствие уничтожению, модифицированию, блокированию, копированию, предоставлению, распространению, а также иных неправомерных действий в отношении защищаемой информации;
2) соблюдения требований к конфиденциальности данных ограниченного доступа;
3) реализации права на доступ к информации».
Обеспечение информационной безопасности предполагает учет всех аспектов, связанных с проведением определения, достижения и поддержания конфиденциальности, целостности, неотказуемости, доступности, аутентичности, подотчетности и достоверности информации и средств ее обработки.
Согласно 149-ФЗ, информация классифицируется на типы:
- общедоступная;
- конфиденциальная;
- информация, относимая к категории «государственная тайна».
Конфиденциальная информация представляет собой информацию, не отнесенную к категории государственной тайны, доступ к которой ограничивается федеральными нормативно-правовыми актами. К категориям конфиденциальной информации относятся:
1) данные для служебного использования;
2) данные, относимые к коммерческой тайне;
3) данные, содержащие персонифицированную информацию;
4) данные, относимые к категории профессиональной тайны.

Каждая из указанных категорий информации подлежит защите согласно правовым нормам, источниками которых являются отраслевые стандарты.
Деятельность по обеспечению защиты информации предполагает также мероприятия по защите интеллектуальной собственности.
С проблемами обеспечения защиты информации имеют тесную связь юридические аспекты, регламентирующие деятельность в области информационных технологий, которую можно раз¬делить по категориям:
1) использование телекоммуникационных технологий;
2) работа с криптографическими системами, включающими системы электронного документооборота;
3) проведение сертификации, лицензирования и аттестации архитектуры информационной безопасности на предприятиях.
Также, к работам по обеспечению защиты информации относятся механизмы по при¬менению мер ответственности за нарушения требований законодательства РФ об информации, информационных технологиях и о защите информации. Данная деятельность регламентируется на государственном уровне.
Таким образом, при обзоре нормативно-правовых актов РФ необходимо от¬дельное рассмотрение направлений, регламентирующих деятельность в области об¬работки и защиты:
1) общедоступных данных;
2) информации, с элементами коммерческой тайны;
3) служебных данных с ограниченным способом распространения;
4) информации, отнесенной к категории профессиональной тайны;
5) персональным данным;
6) государственной тайне;
7) интеллектуальной собственностью;
8) данных о настройках защиты телекоммуникационных систем;
9) данных, использующих криптографические системы;
10) информацию и объекты информатизации, подлежащие лицензирова¬нию, сертификации и аттестации объектов и средств защиты информации;
11) о нарушениях норм законодательства РФ в области информации, информационных технологиях и о защите информации.
В приказе № 17 ФСТЭК РФ определены требования к обеспечению защиты информации, содержащейся в государственных информационных системах. В указанном документе определены требования к определению типов субъектов доступа (пользователям, процессам и иным субъектам доступа) и объектов доступа, которые выступают в качестве объектов защиты (аппаратное обеспечение, объекты файловой системы, запускаемые и

Список использованных источников

1. Межсетевой экран User Gate. Описание. [Электронный ресурс]. Режим доступа: https://www.usergate.com/ru/next-generation-firewall?_openstat=ZGlyZWN0LnlhbmRleC5ydTszNTUzMDkzMjs1ODU5ODgzNzcyO3lhbmRleC5ydTpwcmVtaXVt&yclid=3945
2. Внуков А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — Москва: Издательство Юрайт, 2022. — 161 с.
3. Аникин Д. В. Информационная безопасность и защита информации: учебное пособие / Д.В. Аникин. - Барнаул: Изд-во Алтайского государственного университета, 2018. - 196 с.
4. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с.
5. 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.
6. Запечников С. В. Криптографические методы защиты информации: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с.
7. Бабиева Н. А., Раскин Л. И. Проектирование информационных систем: учебно-методическое пособие / Н. А. Бабиева, Л. И. Раскин. - Казань: Медицина, 2014. – 200с.
8. 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.
9. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР ИНФРА-М, 2018. – 334 с.
10. Белобородова Н. А. Информационная безопасность и защита информации : учебное пособие / Н. А. Белобородова; Минобрнауки России, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования "Ухтинский гос. технический ун-т" (УГТУ). - Ухта : УГТУ, 2016. - 69 с.
11. Белобородова Н. А. Информационная безопасность и защита информации: учебное пособие / Н. А. Белобородова. - Ухта : УГТУ, 2016. - 69 с.
12. 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.
13. 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.
14. Герасименко В.А., Малюк А.А. Основы защиты информации. – СПб.: Питер, 2010. – 320с
15. Горев А. И., Симаков А. А. Обработка и защита информации в компьютерных системах : учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Омск : ОмА МВД России, 2016. - 87 с.
16. Кондратьев А. В. Техническая защита информации. Практика работ по оценке основных каналов утечки : [учебное пособие] / А. В. Кондратьев. - Москва: Горячая линия - Телеком, 2016. - 304 с.
17. Королев Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
18. Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — Москва: Издательство Юрайт, 2022. — 473 с.
19. 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.
20. Михалевич Е.В. Обработка персональных данных: анализ законодательства и судебной практики / Е.В. Михалевич. - Москва : ФГБУ "Редакция "Российской газеты", 2019. - 143 с.
21. 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