УДК 004.56

Аброськина Е.С.

Студент-магистр

2 курс, факультет «Отдел магистратуры»

Поволжский государственный университет телекоммуникаций и информатики

Самара, Россия

ОБСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬТЕРНЫХ СЕТЯХ

Аннотация: *Данная статья посвящена обеспечению информационной безопасности в компьютерных сетях. Здесь раскрывается понятие ЛВС и какие классификации ЛВС существуют на текущий момент. Также рассмотрены виды угроз и проведен обзор методов защиты информации.*

Ключевые слова: *ЛВС, метод, защита информации, угроза, компьютерная сеть, ПО.*

Abroskina E.S.

Student-magistr

2nd year, faculty "Department of magistracy"

Volga State University of Telecommunications and Informatics

Samara, Russia

ENSURING INFORMATION SECURITY IN COMPUTER NETWORKS

Annotation: *This article is devoted to ensuring information security in computer networks. Here the concept of a LAN is revealed and what classifications of LANs exist at the moment. The types of threats are also considered and an overview of information protection methods is carried out.*

Keywords: *LAN, method, information protection, threat, computer network, software.*

В современном мире вопрос защиты информации становится актуальным для многих организаций, т.к. информация является одним из самых ценных ресурсов, и ее роль в обществе продолжает увеличиваться. Автоматизация процессов обработки, хранения и передачи информации привела к возникновению новых проблем, связанных с ее безопасностью. В последнее время сложилась устойчивая тенденция к увеличению количества атак на компьютерные системы и сети. Механизмы и способы взлома постоянно совершенствуются, и существующие средства защиты их полностью «не перекрывают». Все это делает разработку и внедрение новых методов и средств защиты информации в компьютерных сетях весьма актуальными.

Понятие ЛВС

Под локальной вычислительной сетью (ЛВС) понимается компьютерная сеть, которая служит интересам ограниченного количества пользователей, покрывая одно или несколько зданий, например, офисы или помещения институтов.

ЛВС классифицируются по способу администрирования:

- локальные;
- распределенные;
- городские.

В ЛВС компьютеры объединяются при помощи оптоволоконных кабелей или по спутниковой связи. Объединение ПК в сеть дает возможность:

- передавать информацию без съемных носителей;
- совместно работать в программе, установленной на одном компьютере, нескольким пользователям;
- совместно пользоваться устройствами, например, принтером;
- применять одно решение для защиты конфиденциальной информации на нескольких рабочих станциях.

С другими сетями ЛВС соединяется через шлюзы. Она может подключаться к Интернету или быть автономной, во втором случае решить задачу обеспечения безопасности данных проще.

Виды угроз

При решении вопроса об информационной безопасности в первую очередь необходимо определить вид угрозы, чтобы оценить насколько подвержены данные риску.

Существует 2 вида несанкционированного доступа к информации:

1. Прямой - необходим физический доступ к сети;
2. Косвенный - осуществляется без прямого физического доступа к данным.

Список способов неправомерного получения данных достаточно огромен, и угроза для системы может быть создана, но использована единожды.

Перечислим основные способы получения несанкционированного доступа к информации:

- Фото с экрана;
- Применение вредоносных программ;
- Считывание электромагнитных волн мониторов (перехват ван Эйка);
- Применение программных ловушек;
- Запрещенное копирование;
- Проникновение в компьютеры других пользователей, с помощью чужих средств идентификации, для получения информации ограниченного доступа;
- Получение информации с помощью серии разрешенных запросов;
- Хищение носителей данных.

С данными способами хищения информации можно успешно бороться. Как правило, 80% таких случаев связаны с действиями внутренних пользователей.

Получение данных незаконным путем может привести к серьезным последствиям:

- Разглашение и распространение данных. Этому риску подвержены документы, которые относятся к коммерческой тайне или же являются интеллектуальной собственностью. Разглашение сведений, которые относятся к персональным данным, влечет за собой уголовную ответственность;
- Уничтожение по умыслу третьих лиц или из-за поломки оборудования, носителей информации, либо в результате преднамеренного заражения рабочей станции при помощи компьютерных вирусов;
- Намеренное искажение, подмена достоверной информации ложной.

На вопросах безопасности не стоит экономить. По данным опроса «Лаборатории Касперского», за последние 12 месяцев российские компании малого и среднего бизнеса в среднем потратили на обеспечение безопасности корпоративного периметра 4,7 млн. рублей каждая - это практически в 2 раза больше, чем за аналогичный период годом ранее (2,4 млн. рублей).

Меры безопасности

Применение различных методов защиты информации необходимо учитывать на этапе разработки архитектуры сети.

Методы защиты информации делятся на:

- Организационные;
- Программные;

- Технические или аппаратные;
- Аппаратно-программные.

Организационные

К организационным методам информационной безопасности относят:

- Разграничение прав пользователей в работе с массивами информации;
- Контроль за выводом информации на принтер, создание защищенных зон для печати;
- Ограничение доступа в рабочие помещения, введение системы пропусков;
- Контроль за распечатанными экземплярами документов, которые содержат критичную информацию;
- Выделение для обработки ценной информации специальных АРМ без подключения к Интернету;
- Особый порядок учета и хранения съемных носителей информации.

Для ограничения действий пользователей в крупных компаниях необходимо:

- Ввести на предприятии режим коммерческой тайны, составив исчерпывающий перечень конфиденциальных данных;
- Проводить тренинги, посвященные способам защиты информации;
- Включить в трудовые договоры условие об ответственности за разглашение коммерческой тайны или персональных данных.

При возникновении случаев невнимательного отношения к данным, которые находятся в ЛВС, необходимо виновных сотрудников привлекать к уголовной ответственности. Подобные случаи предотвратят в будущем

новые, т.к. политика безопасности должны быть донесена до каждого сотрудника, периодически обновляться и действовать на ежедневной основе. Контроль соблюдения всех правил и норм осуществляется сотрудниками отдела безопасности.

Программные

С каждым годом все больше совершенствуются вредоносные программы, вместе с ними совершенствуются и способы борьбы с ним. В настоящее время вредоносное ПО может длительное время оставаться незамеченным и даже самые хорошие антивирусы не могут его обнаружить. Данные программы недорогие на черном рынке (большинство бесплатные), в свободном доступе лежат для хакеров, а площадь заражения во много раз выросло.

В зависимости от решаемых задач программные методы защиты информации делятся на следующие виды:

- Антивирусы;
- Средства обнаружения вторжения, которые сигнализируют о попытках несанкционированного доступа в ВС;
- Межсетевые экраны;
- Средства криптографической защиты информации;
- Утилиты для контроля съемных носителей;
- Средства идентификации копий документов;
- Средства доверенной загрузки;
- СКУД;
- Решения для аудита данных в информационной системе.

Программные средства защиты данных в России, проходят обязательную сертификацию в ФСБ, что свидетельствует об их надежности.

Для средних и крупных организаций самым лучшим средством защиты данных в сети являются DLP-системы. Это решение, которое позволяет отслеживать данные внутри сети и на выходе из нее. DLP-системы также сертифицируются, кроме того в них определяют степень содержания незадекларированных возможностей. Данная проверка показывает насколько безопасно данное ПО и не содержится ли в нем скрытых функций.

Технические

Технические методы защиты информации очень эффективны, но имеют высокую стоимость. Они устойчивы к внешнему воздействию, защищены от вмешательства в конструкцию, гарантируют ограничение неправомерного доступа в полном объеме.

Технические методы защиты делятся на 2 группы:

1. *Аппаратные* - встраиваются в компьютер или совместимы с ними через определенный интерфейс (USB, Wi-Fi);
2. *Физические* - представляют собой оборудование, которое защищает ЛВС и их элементы от несанкционированного доступа.

Кроме перечисленных методов также широко применимы генераторы акустических помех, которые предотвращают подслушивание, использование мягких прокладок под оборудование, что снижает риски утечки информации по акустическим каналам.

Аппаратно-программные

Аппаратно-программные средства защиты информации включают в себя техническую часть и программный код. К таким средствам относят:

- Специализированные сети хранения (SAN - Storage Area Network);

- Аппаратные средства контроля доступа;
- Ленточные накопители;
- Дисковые хранилища данных.

Выбор аппаратно-программного метода защиты информации должно проходить осознанно, т.к. в отличие от программных средств защиты, его сложнее поменять на новое по мере развития кибертехнологий.

Использованные источники

1. Информационная технология. Методы и средства обеспечения безопасности [Текст]: ГОСТ Р ИСО/МЭК 15408 – 1 - 2008. Введ. 2009-10-01. – М.: Стандартинформ, 2009.

2. Информационная безопасность [Электронный ресурс]: 2018. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/, свободный. – Загл. с экрана.

3. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: 2017. – Режим доступа: https://studref.com/322429/informatika/informatsionnaya_bezopasnost_kompyuternyh_sistem_i_setey, свободный. – Загл. с экрана