Минобрнауки России
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Сыктывкарский государственный университет имени Питирима Сорокина»
Колледж экономики, права и информатики

КУРСОВАЯ РАБОТА

по дисциплине «Эксплуатация объектов сетевой инфраструктуры »
Тема: «Анализ сетевых угроз в корпоративной сети»

Руководитель:
Дуркин А.А
_____
«__»_____2022 г.

Исполнитель:
студент группы 1435а-САО
Булышев М.А
«__»_____2022 г

Сыктывкар 2022

Содержание

В 2017 году вирус затронул компании и госорганы Европы, США, Австралии, России, Украины, Индии, Китая. Среди пострадавших — российские компании «Роснефть» и «Башнефть», международные корпорации Merck, Maersk, TNT Express, Saint-Gobain, Mondelez, Reckitt Benckiser. На Украине пострадало более 300 компаний, включая «Запорожьеоблэнерго», «Днепроэнерго», Киевский метрополитен, украинские мобильные операторы «Киевстар», LifeCell и «Укртелеком», магазин «Ашан», Приватбанк, аэропорт Борисполь. 10% памяти всех компьютеров в стране оказалось стерто. Общая сумма ущерба от деятельности хакеров составила более $10 млрд. Все эти корпорации пострадали от одного вируса Petya из-за несовершенства безопасности.

Эта история, как и многие другие приводят к выводу, что анализ сетевых угроз в корпоративной сети просто необходим в крупных компаниях и побуждают совершенствовать меры безопасности.

Цель этой работы определить актуальность усиления безопасности в корпоративной сети.

Задачи работы:

1. Изучить теоретический материал;
2. На основе статистики определить опасность угроз;

В этой курсовой работе будут использоваться такие методы как:

1. Анализ;
2. Сравнение;
3. Наблюдение;

Введение

1.Основная часть

1.1 Типы угроз

Обеспечение безопасности информации в компьютерных сетях предполагает создание препятствий для любых несанкционированных попыток хищения или модификации передаваемых в сети данных.

Таким образом, защита данных в компьютерных сетях одна из самых острых проблем в современном мире.

Обеспечение безопасности информации в компьютерных сетях предполагает создание препятствий для любых несанкционированных попыток хищения или модификации передаваемых в сети данных.

Для того, чтобы правильно оценить возможный реальный ущерб от потери информации, хранящейся на компьютере или циркулирующей в вычислительной сети, необходимо рассмотреть угрозы, которые при этом могут возникнуть и какие необходимо принимать адекватные меры по их защите.

Под угрозой понимается событие (воздействие), которое в случае своей реализации становится причиной нарушения целостности информации, ее потери или замены.

Можно выделить три типа угроз:

- несанкционированное получение информации злоумышленником (утечка информации);

- постоянное или временное блокирование некоторого сервиса, в результате чего система перестает выполнять свои функции по назначению;

- умышленное или случайное изменение информации, например, удаление файлов или записей в БД.

Угроза раскрытия заключается в том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова «раскрытие» используются термины «кража» или «утечка».

Угроза отказа в обслуживании возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Угроза целостности включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие.

Данным угрозам может быть подвержена вся информация локально вычислительной сети отдела. Но с учетом структуры ВС предприятия и характера информации, циркулирующей на предприятии, можно выделить наиболее опасные угрозы для каждого конкретного потока:

а) Для информации хранящейся на серверах предприятия наиболее опасной является угроза раскрытия, поскольку она составляет коммерческую тайну и необходима для работы всем отделам предприятия.

б) Для информации циркулирующей в отделах 1, 2 и 3 наиболее опасной является угроза отказа в обслуживании, поскольку работа отдела главным образом зависит от обмена информацией с файловым сервером. Таким образом, реализация угрозы отказа в обслуживании может повлиять на работу всех трех отделов.

в) Для информации циркулирующей в отделе бухгалтерии наиболее опасной является угроза целостности (особенно для информации, хранящейся на сервере БД), поскольку изменение этой информации может привести к нарушению работоспособности отдела. Также необходимо отметить, что в данном отделе обрабатывается информация, составляющая коммерческую тайну (бухгалтерская документация, отчеты, документы), поэтому необходимо обеспечить также сохранение ее конфиденциальности.

Кроме того угрозы могут быть преднамеренно создаваемыми (умышленными) и случайными.

Наиболее опасным источником угроз информации для предприятия являются преднамеренные действия злоумышленников.

К умышленным угрозам безопасности ВС предприятия можно отнести:

а) Несоответствующий доступ происходит, когда пользователь, законный или неавторизованный, получает доступ к ресурсу, который пользователю не разрешено использовать. Несоответствующий доступ может происходить просто потому, что права доступа пользователей к ресурсу не назначены должным образом. Однако несоответствующий доступ может также происходить потому, что механизм управления доступом или механизм назначения привилегий обладают недостаточной степенью детализации. В этих случаях единственный способ предоставить пользователю необходимые права доступа или привилегии для выполнения определенной функции состоит в том, чтобы предоставлять пользователю больше доступа, чем необходимо, или больше привилегий, чем необходимо.

Наиболее интересной для злоумышленника является информация, хранящаяся на почтовом сервере (служебная переписка), на сервере БД отдела бухгалтерии (бухгалтерская отчетность), информация на файловом сервере (электронные чертежи, модели), информация хранящаяся на ftp сервере (рабочие архивы и архивы с лицензионным ПО). С точки зрения несанкционированного доступа к сетевым ресурсам наиболее открытым перед данной угрозой является файловый сервер, поскольку доступ к нему имеют практически все работники предприятия.

б) Раскрытие и модификация данных или программного обеспечения ЛВС происходит, когда к данным или программному обеспечению осуществляется доступ, при котором они читаются, изменяются и, возможно, разглашаются некоторому лицу, которое не имеет доступа к данным. Это может производиться кем-либо путем получения доступа к информации, которая не зашифрована, или путем просмотра экрана монитора или распечаток информации. Когда незаметная модификация данных происходит в течение длительного периода времени, измененные данные распространяются по ЛВС, искажая базы данных, электронные таблицы и другие прикладные данные. Это может привести к нарушению целостности почти всей прикладной информации.

Наибольший вред для предприятия принесет модификация оперативной информации на сервере БД, раскрытие и модификация данных

на файловом сервере, модификация программ на всех серверах отдела и рабочих станциях.

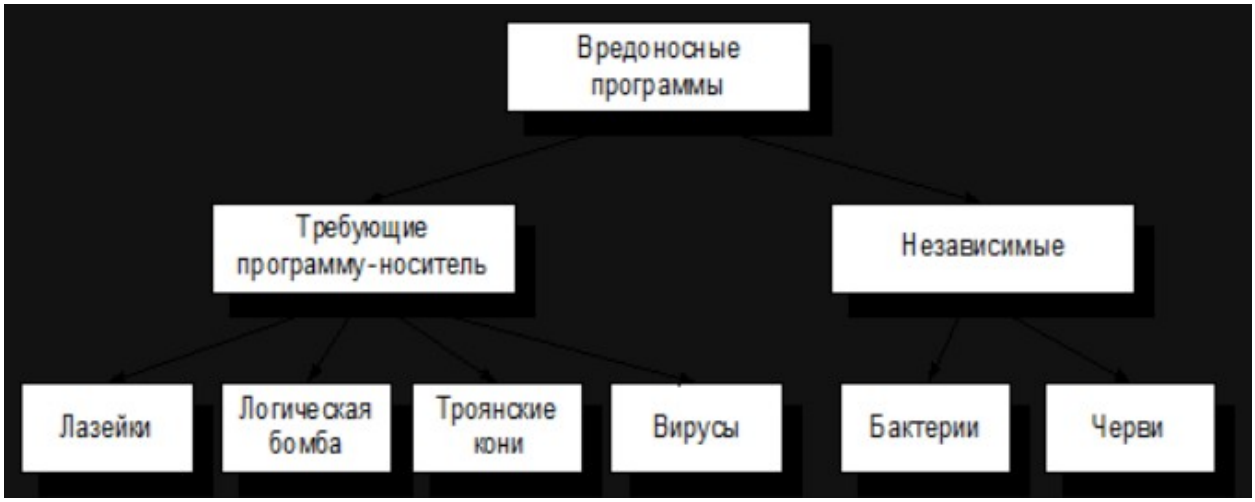
в) Раскрытие, модификация или подмена трафика вычислительной сети

Опасность для предприятия представляет прослушивание каналов передачи данных в отделе бухгалтерии, а также между файловым сервером и отделами 1,2,3. Этот вид угроз может быть осуществлен злоумышленником при непосредственном подключении к соответствующему каналу передачи данных, прослушиванием трафика, злоупотреблении предоставленным подключением к сети с помощью присоединения сетевого анализатора, и т.д.

г) Разработка и распространение вредоносных программ (использование злоумышленником программ для нарушения работы и получения необходимой информации).

Под вредоносными программами понимаются такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации. Классификация вредоносных программ представлена на рисунке 1

(Рис.1) Классификация вредоносных программ.



Проникновение такой программы на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вредоносная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

Результатом работы вредоносной программы может быть:

- относительно безвредное вмешательство в работу компьютера например, злая шутка, когда экран гаснет и выдается сообщение, что ваш жесткий диск отформатирован;

- нанесение реального вреда - когда винчестер действительно форматируется, или стираются важные файлы;

- настоящее преступление - когда с помощью троянских программ злоумышленники крадут конфиденциальную информацию компании.

К программам, требующим программу - носитель, относиться программный код, который не может работать независимо от некоторой реальной прикладной программы, утилиты или системной утилиты.

К независимым программам принадлежат самостоятельные программы, которые могут быть запушены стандартными средствами операционной системы, как любая другая программа.

Самыми опасными и распространенными программами такого вида являются:

- "программы троянцы";

- вирус;

- "червь";

"Программы троянцы" представляет собой полезную или кажущуюся полезной программу или команду процедур, содержащую скрытый код, который после запуска программы - носителя выполняет нежелательные или разрушительные функции. Опасность "программы троянца" заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователям. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне).Наиболее надежным способом защиты от этой угрозы

является создание замкнутой среды исполнения программ. Желательно также, чтобы привилегированные и непривилегированные пользователи работали с разными экземплярами прикладных программ, которые должны храниться и защищаться индивидуально.

Вирус представляет собой программы, которая может “заражать” другие программы путем их модификации. В модифицированный код включается код вируса, в результате чего код вируса может продолжать заражать другие программы.

"Червь" - сетевая программа использует сетевые соединения для распространения из одной системы к другой. Во время работы на отдельном компьютере сетевой “червь” может вести себя как компьютерный вирус или как “бактерия” либо внедрять “троянских коней”, либо выполнять другие разрушительные операции.

Всем этим угрозам могут подвергнуться рабочие станции всех отделов. Наибольшие потери предприятие понесет при попадании таких программ на сервера предприятия, т.к. на них хранится конфиденциальная информация (сервер БД) и информация необходимая для работы всех отделов (файловый сервер). Почтовый сервер наиболее подвержен атакам вредоносных программам, приходящих из Internet, а т.к. с него информация распространяется на все рабочие станции это также может принести огромные потери. Злоумышленник может использовать данные программы для нарушения работы отделов и получения необходимой информации. Для предотвращения действий этих программ необходимо фильтровать весь входящий трафик при помощи межсетевого экрана, кроме того для защиты от таких программ необходимо использовать антивирусные программы.

Всем этим угрозам могут подвергнуться рабочие станции всех отделов. Наибольшие потери предприятие понесет при попадании таких программ на сервера предприятия, т.к. на них хранится конфиденциальная информация (сервер БД) и информация необходимая для работы всех отделов (файловый сервер). Почтовый сервер наиболее подвержен атакам вредоносных программа, приходящих из Internet, а т.к. с него информация распространяется на все рабочие станции это также может принести огромные потери. Злоумышленник может использовать данные программы для нарушения работы отделов и получения необходимой информации. Для предотвращения действий этих программ необходимо фильтровать весь входящий трафик при помощи межсетевого экрана, кроме того для защиты от таких программ необходимо использовать антивирусные программы.

д) кража электронных чертежей, моделей и расчётной документации (наибольшие потери предприятие понесет при краже информации хранящейся на файловом сервере);

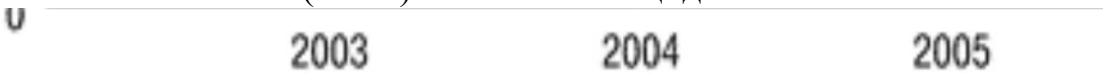
е) разрушение архивной информации или умышленное ее уничтожение

(наибольшие потери предприятие понесет при разрушении или уничтожении информации хранящейся на ftp сервере и файловом сервере).

2. Статистика инцидентов

Возьмем, к примеру, некоторую среднестатистическую корпоративную сеть, содержащую 500 компьютеров с электронной почтой и выходом в Интернет. Предположим, что сотрудники имеют привилегии уровня опытного пользователя, что позволяет им самостоятельно устанавливать программное обеспечение и изменять основные настройки компьютера. При этом считается, что электронная почта идет через корпоративный почтовый сервер, защищенный одним из популярных в нашей стране антивирусов, например AVP или DrWeb, а выход в Интернет осуществляется централизованно через корпоративный прокси-сервер и Firewall. В этом случае статистика инцидентов имеет вид, показанный на рис. 2.

(Рис.2)Статистика инцидентов



Естественно, это усредненная статистка, относящаяся к некоторой мифической сети, так как в любой реальной ЛВС эти цифры могут быть другими, поскольку зависят от множества факторов. Анализ причин инцидентов показывает картину, приведенную на рис. 3.

(Рис.3.) Причины инцидентов

Как видно из диаграммы, основной причиной всевозможных инцидентов являются вредоносные программы различных типов. В эту категорию попадают вирусы, программы категории Malware (шпионские программы, модули отображения рекламы и прочее нежелательное ПО).

Очень часто появление вредоносного ПО напрямую связано с действиями пользователя, например с посещением сайтов или с установкой программ непроизводственного назначения. Анализ процентного состава вредоносного ПО показывает следующую картину (рис. 4).

(Рис.4) Типы вредоносного ПО

Основная доля приходится на Trojan-Downloader, которые выполняют функции троянских загрузчиков вредоносного ПО. При этом следует отметить, что почтовые вирусы и сетевые черви не занимают лидирующих позиций, что в первую очередь связано с тем, что данная статистика получена в ЛВС, в которых применяется комплексная антивирусная защита и сетевые черви блокируются еще на уровне корпоративного почтового сервера.

На диаграмме, представленной на рис. 2, видно, что примерно 25% инцидентов приходится на действия пользователей, причем инцидент может возникнуть в случае умышленных действий (предполагающих наличие у пользователя ЛВС некоего злого умысла и плана для его реализации) или неумышленных. Анализ показывает, что подавляющее число связанных с деятельностью пользователей инцидентов вызвано именно неумышленными действиями. Оставшиеся 5% приходятся на категорию, названную хакерскими атаками, причем под хакерской атакой понимается в том числе и применение средств социальной инженерии.

Случай 1. Многопоточная закачка

Сценарий. Сотрудник К загружает из Интернета утилиту для многопоточного сохранения контента указанных сайтов. Указав несколько сайтов, он запускает утилиту в фоновом режиме. В результате сбоя утилита начинает выдавать 500-700 запросов в секунду в непрерывном цикле, что приводит к ситуации DoS на корпоративном прокси-сервере.

Анализ. В данном случае злой умысел со стороны сотрудника отсутствует, однако анализ ситуации показал, что применение данной утилиты не требуется для решения производственных задач. Кроме того, утилита не проходила никаких тестов со стороны администраторов сети и ее применение не было согласовано с ними, что, собственно, и привело к данной ситуации.

Решение проблемы. В корпоративной политике безопасности вводится запрет на установку программного обеспечения, активно взаимодействующего с Интернетом, без согласования с администраторами и службой безопасности. После этого проводятся технические мероприятия для поиска и удаления подобных программ и блокировки их последующей установки.

3.Примеры инцидентов и их решение

Рассмотрим несколько характерных случаев, наглядно демонстрирующих типичные инциденты, связанные с деятельностью пользователей. Все описанные ниже случаи взяты из практики и с весьма высокой степенью вероятности могут возникнуть в любой корпоративной сети.

Случай 2. Электронная почта

Сценарий. Желая поздравить с Новым годом коллег, сотрудник К составляет базу рассылки из 1500 адресов, после чего создает письмо с Flash-мультфильмом размером в 1,5 Мбайт и запускает рассылку. Подобные операции производят также его коллеги, рассылая поздравительные письма с вложенными картинками, Flash-роликами и звуковыми файлами. В результате создается ситуация DoS на почтовом сервере и блокируется прием-отправка деловой корреспонденции.

Анализ. Это типичный пример нецелевого использования корпоративной электронной почты, обычно подобные проблемы возникают перед праздниками. Наиболее характерно данная ситуация проявляется в больших сетях (более 500 пользователей).

Решение проблемы. Технически решить подобную проблему очень сложно, так как ограничения на объем письма и количество писем в единицу времени не всегда приемлемы и малоэффективны при большом количестве пользователей. Наиболее действенная мера — разработка правил использования корпоративного почтового сервера и доведение этих правил до сведения всех пользователей.

Случай 3. Средства анализа сети

Сценарий. Недавно принятый на работу молодой программист для самообразования загружает из Интернета сканер сетевой безопасности XSpider. Для изучения его работы он выставляет настройки по максимуму и в качестве цели указывает адрес одного из корпоративных серверов. В

Целью этой работы было определение актуальности усиления безопасности в корпоративной сети.

Для того, чтоб достигнуть цели была поставлена и достигнута задача изучить теоретический материал, а так же на основе статистик была определена тенденция роста угроз и то, по какой причине растут угрозы.

На основе всех приведенных данных можно сказать что:
результате средства защиты сервера регистрируют атаку, замедляется время реакции сервера на запросы пользователей.

Анализ. В данном случае злой умысел отсутствует, так как установивший данную программу пользователь сети не имел четкого представления о возможных последствиях.

Решение проблемы. В корпоративной политике безопасности вводится раздел, категорически запрещающий установку и использование на рабочих местах пользователей средств активного и пассивного исследования сети, генераторов сетевых пакетов, сканеров безопасности и иных средств. Согласно данному положению применение подобных инструментов разрешается только администраторам сети и специалистам по защите информации.

Заключение

- В каждой компании обязана быть внутренняя служба безопасности.

- На официальном уровне одним документом должны быть прописаны правила.Без данного документа невозможно как таковое проведение служебных расследований и наказание пользователей за грубые нарушения правил работы в сети. Кроме того, наличие утвержденной политики информационной безопасности сводит к минимуму конфликтные ситуации между пользователями и администраторами сети, поскольку и те и другие действуют в рамках единых нормативных документов.

Кроме того, даже после технологического бума и повсеместной автоматизации «у руля», как и прежде, остается человек. И чаще всего причиной поломок в локальных внутренних сетях и угрозой безопасности является человеческая халатность.

Методом борьбы в таком случае послужит ужесточение контроля и обучение рядового пользователя базовым нормам безопасности.

Библиографический список

1. Болотова.Л.С, Волкова.В.Н., Денисов.А.А / «Теория и системный анализ в управлении организациями» // Справочник, Учебное пособие под ред. В.Н.Волковой и А.А.Емельянова. - 2016 г. -848 с.

2. Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика / «Анализ современных угроз безопасности информации, возникающих при сетевом взаимодействии». / Бабенко.М.В / - 2018 г. - 4 с.

3. Мещеряков Р.В., ШелупановА.А., Белов Е.Б., Лось В.П. Основы информационной безопасности.- М.: Горячая линия-Телеком, 2018. - 350 с

4. Нагиева.А.Ф. Корпоративные сети и проблемы безопасности / А. Ф. Нагиева. — Текст : непосредственный // Молодой ученый. — 2016. — № 29 (133). — С. 34-36.

5. «Обеспечение информационной безопасности информационной советующей системы» / Аверченкова.Е.Э., Гончаров.Д.И., Лысов.Д.А./ - 2016 г. - 17 с.

6. Парламентская Ассамблея Организации Договора о коллективной безопасности /«О проекте Концепции плана действий и инструментария в вопросах противодействия кибервызовам и угрозам» // г. Москва 30.11.2020. - № 13-5.4

7. Разработка рекомендаций по повышению защищённости ЛВС ООО «Авиа ОК»/ Романов.П.А. / -2019 г. - 27 с.

8. «Разработка моделей объекта защиты и угроз нарушения безопасности в информационной системе, базирующейся на технологии виртуализации» / Тулиганова.Л.Р., Павлова.И.А., Машкина.И.В. - 2017 г. - 15 с.

9. «Угрозы безопасности вычислительных комплексов: классификация, источники возникновения и методы противодействия» / Абрамов.Н.С., Фраленко.В.П. / -2015 г. - 46 с.

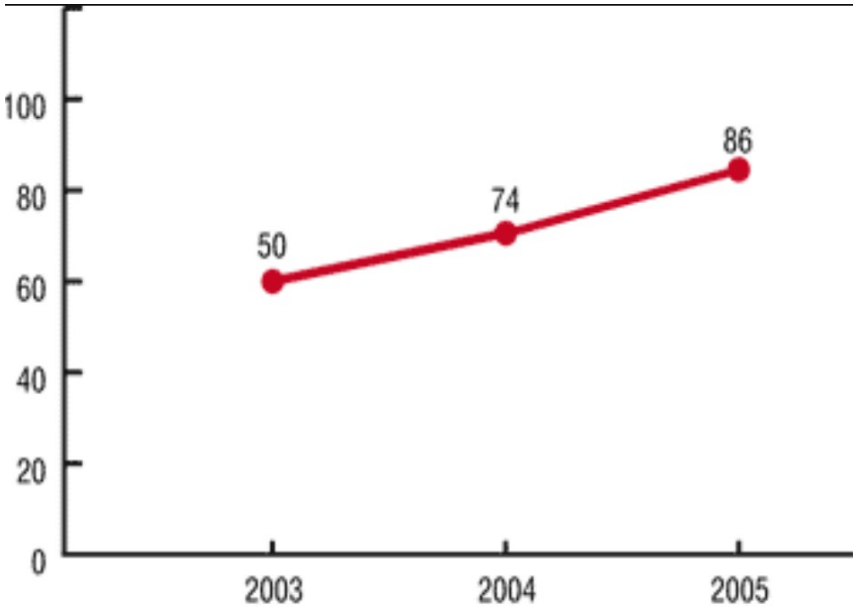
10. «Вирус Petya». [электронный ресурс]. Режим доступа: ru.wikipedia.org›wiki/Petya. (дата обращения: 28.11.2021).

Приложение А

(Рис.1)

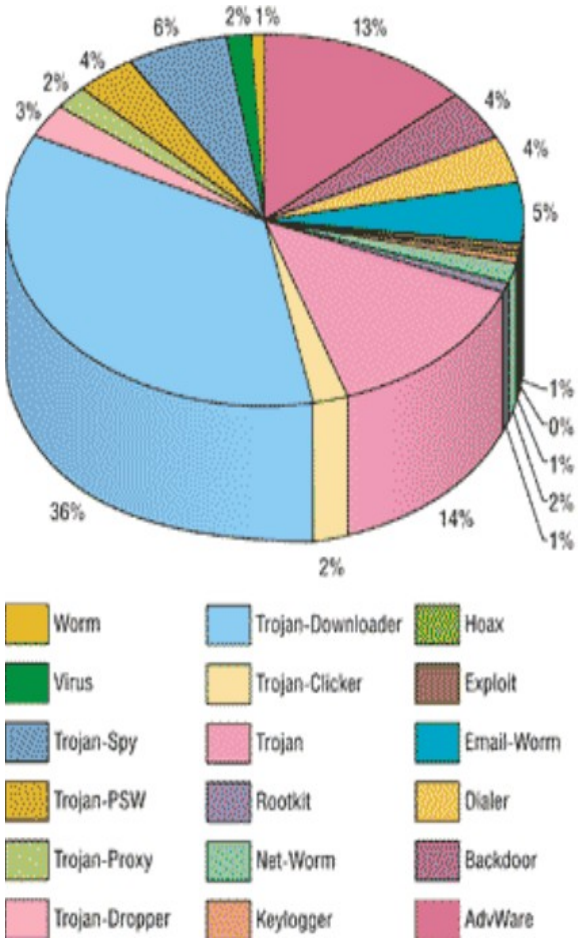

Вредоносные программы
Требующие программу-носитель
Независимые
Лазейки
Логическая бомба
Троянские кони
Вирусы
Бактерии
Черви

(Рис.2)


100
80
60
40
20
0
50
74
86
2003
2004
2005

(Рис.3)

(Рис.4)



AdvWare	2446
Backdoor	813
Dialer	760
Email-Worm	970
Exploit	129
Hoax	81
Keylogger	108
Net-Worm	320
Rootkit	140
Trojan	2512
Trojan-Clicker	405
Trojan-Downloader	6569
Trojan-Dropper	542
Trojan-Proxy	380
Trojan-PSW	698
Trojan-Spy	1169
Virus	286
Worm	153
Объем выборки ITW	18 481

образовательное учреждение высшего образования
«Сыктывкарский государственный университет имени Питирима Сорокина»
Колледж экономики, права и информатики

ОТЗЫВ РУКОВОДИТЕЛЯ КУРСОВОЙ РАБОТЫ

на курсовую работу студента (ки)

_____

_____
(фамилия, имя, отчество)

выполненной на тему

_____

_____

_____

_____

_____

1. Соответствие курсовой работы заявленной теме_____

_____

_____

_____

_____

_____

2. Оценка качества выполнения курсовой работы_____

_____

_____

_____

_____

_____

3. Оценка полноты разработки поставленных вопросов, теоретической и практической значимости курсовой работы _____

_____

_____

_____

_____

_____

4. Оценка курсовой работы _____

Руководитель
курсовой работы _____ _____
(подпись) (Расшифровка подписи)

«____»_____ 20 ____ г.