ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

А.Ж. Анетова[1)], А. Талгат[2)]

1) Старший преподаватель Казахского агротехнического университета им.С.Сейфуллина (КазАТУ), г. Нур-Султан, Казахстан, Aizhan83@mail.ru

2) Старший преподаватель Казахского университета технологии и бизнеса (КазУТБ), г. Нур-Султан, Казахстан, amangul_talgat81@mail.ru

Аннотация: в свете того, что экономика все больше интегрируется в мировую, необходимо соблюдение международных требований конфиденциальности, защиты информационных ресурсов. В данной работе рассматриваются проблемы информационной безопасности, методы и средства ее обеспечения.

Ключевые слова: информационные технологии, информационная безопасность, атаки на операционную систему, на базы данных, сетевые атаки, аппаратно-программные средства защиты информационных ресурсов.

PROBLEMS OF INFORMATION SECURITY. METHODS AND MEANS OF PROTECTING INFORMATION RESOURCES

A.Zh. Anetova[1)], A. Talgat[2)]

1) Senior Lecturer at S. Seifullin Kazakh Agro Technical University (KazATU), Nur-Sultan, Kazakhstan, Aizhan83@mail.ru

2) Senior Lecturer, Kazakh University of Technology and Business (KazUTB), Nur-Sultan, Kazakhstan, amangul_talgat81@mail.ru

Abstract: in light of the fact that the economy is increasingly integrated into the world one, it is necessary to comply with international requirements for confidentiality and protection of information resources. This paper discusses the problems of information security, methods and means of ensuring it.

Key words: information technology, information security, attacks on the operating system, on databases, network attacks, hardware and software for protecting information resources.

Современный мир стал цифровым. В настоящее время наблюдаются следующие тенденции в развитии и использовании современных информационных технологий (ИТ):

- усложнение программных средств компьютерной системы;

- сбор и хранение крупных информационных баз на электронных носителях;

- прямой доступ к ресурсам компьютерной системы большого числа пользователей различной категории и с различными правами доступа в системе;

- объединение в общий информационный массив различных методов доступа; увеличение стоимости ресурсов компьютерных систем;

- использование большинством государственных и частных организаций специальных антивирусных программ в качестве средств безопасности;

- широкое использование Интернет и пр.

Но ситуация сегодня такова, что каждую минуту компьютерная информация может подвергнуться (или подверглась) опасности.

Самое удивительное, что большинство из тех, кто столкнулся с подобными неприятностями, были далеко не зелеными новичками, только вчера севшими за компьютер и потому слабо знакомыми с его основами. Бизнесмены, трейдеры, студенты и даже веб-дизайнеры, все они находятся в так называемой «зоне риска», поскольку обладают по-настоящему ценной для них информацией, но в большинстве своем - сквозь пальцы смотрят на вопросы компьютерной безопасности [1].

Возможные причины возникающих опасностей:

Операционная система Windows, которой вы пользуетесь, имеет массу уязвимостей и программных «дыр» (иначе компания-производитель не выпускала бы бесконечные обновления и «заплатки»).

Жесткий диск - сложное и невероятно хрупкое электронно-механическое устройство, требующее особого надзора и обращения, иначе оно может отказать.

Информационный поток все время увеличивается. Нам приходится хранить и обрабатывать все больше информации на компьютере. Особенно со мной согласятся интернет-предприниматели.

Основная проблема сегодня - как надежно защитить эту информацию?

В настоящее время информационная безопасность является одной из важнейших проблем современного общества.

Под информационной безопасностью (ИБ) следует понимать защиту интересов субъектов информационных отношений. Основные составляющие защиты информации - обеспечение ее конфиденциальности, целостности, доступности. Главные проблемы современных предприятий в контексте ИБ - это хакерские атаки, различные модификации вредоносного программного обеспечения (ПО), другие внешние угрозы. Высокую обеспокоенность вызывают внутренние угрозы (утеря конфиденциальной информации компанией). Внешние угрозы становятся менее проблемными, качество «защитного» ПО повышается, и практически все компании уже научились профессионально его использовать; во-вторых, информация, как таковая, давно стала ключевым активом предприятия, без

которого его деятельность немыслима. В настоящее время наблюдается тенденция сознательного взлома компьютерных систем с целью хищения или повреждения информации [2].

Рассмотрим методы взлома компьютерных систем. Соблюдение адекватной политики безопасности является значительно более трудной задачей для данного уровня, т.к. внутренняя структура современных операционных систем чрезвычайно сложна. От архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки, зависит успех реализации алгоритма хакерской атаки. Задача хакера - найти слабое место в конкретной системе защиты, а не организация эффективной атаки на операционные системы только с помощью сложнейших средств, основанных на самых последних достижениях науки и техники. Чем проще алгоритм атаки, тем больше вероятность ее завершения без ошибок и сбоев.

Важно заметить, что устранить полностью угрозу взлома компьютерной системы на уровне ОС невозможно вне зависимости от предпринятых мер. Поэтому политика обеспечения безопасности должна проводиться так, чтобы, даже преодолев защиту, создаваемую средствами операционной системы, хакер не смог нанести серьезного ущерба.

Защищать операционную систему гораздо сложнее в отличие от систем управления базами данных (СУБД), но чтобы получить доступ к файлам СУБД, большинство хакеров делают это с помощью средств ОС, при этом необходимо взломать защиту компьютерной системы на уровне ОС.

Существуют два специфических сценария атаки на СУБД, для защиты от которых требуется применять специальные методы.

В первом случае результаты арифметических операций над числовыми полями СУБД округляются в меньшую сторону, а разница суммируется в некоторой другой записи СУБД (как правило, эта запись содержит личный счет хакера в банке, а округляемые числовые поля относятся к счетам других клиентов банка.

Во втором случае хакер получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея хакерской атаки на СУБД - так хитро сформулировать запрос, чтобы множество записей, для которого собирается статистика, состояло только из одной записи.

Сетевое программное обеспечение (СПО) является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаще всего не защищен, и всякий, кто может иметь доступ к этому каналу, соответственно, может перехватывать сообщения и отправлять свои собственные [3].

На уровне СПО возможны следующие хакерские атаки: сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а,

следовательно, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);

создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);

отказ в обслуживании (хакер отправляет в сеть сообщения специального вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

С проникновением компьютеров в различные сферы жизни возникла принципиально новая отрасль - информационная индустрия. Объем циркулирующей в обществе информации удваивается примерно каждые пять лет. Человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит само благополучие и даже выживание человечества в его нынешнем качестве.

В последние годы в отечественной и зарубежной печати большое внимание уделяется вопросам защиты информации, накапливаемой, хранимой и обрабатываемой как в отдельных ЭВМ, так и в построенных на их основе вычислительных системах. При этом под защитой информации понимается создание в ЭВМ и вычислительных системах организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации [4,5] .

Использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных предприятий. Безопасность информации - это один из основных показателей качества информационной системы.

Вероятность вирусной атаки значительно возрастает при объединении компьютеров в сеть и становится неизбежной при подключении к информационно-вычислительным сетям общего пользования.

Использование антиспамовых фильтров помогает защититься и от некоторых почтовых червей. Самое очевидное применение - это при получении первого зараженного письма отметить его как нежелательное, и в дальнейшем все другие зараженные письма будут заблокированы фильтром.

Все вышеперечисленные средства так или иначе могут помочь в борьбе с вирусами, но ни одно из них полностью проблему не решает. Далеко не все вирусы распространяются путем атак на сетевые службы и могут быть заблокированы брандмауэрами. Многие вредоносные программы не имеют никакого отношения к электронной почте, а, значит, антиспамовые фильтры против них бессильны. Поэтому самыми эффективными средствами защиты от вирусов были и остаются

антивирусные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Для того, чтобы построить действительно надежную антивирусную защиту, использовать антивирусы нужно обязательно [6] .

Применительно к обеспечению безопасности компьютерной системы идентификация пользователя означает подтверждение того, что предъявленное имя соответствует имени данного субъекта. Преимущества программных средств информационной безопасности:

- гибкость (адаптация к различным условиям применения); простота применения и тиражирования;

- неограниченные возможности развития программных средств.

Недостатки программных средств информационной защиты: низкая производительность; многие программные средства не встроены в компьютерную систему; значительное снижение эффективности всей компьютерной системы в связи с потреблением ее ресурсов защитными программами.

Список использованных источников:

1. Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства для защиты объектов и информации. - СПб.: Лань, 2000. - С. 70-73.
2. Баранов В.М. и др. Защита информации в системах и средствах информатизации и связи: Учеб. пособие. - СПб.: 2006. - С. 125-127.
3. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. - М.: Юрид. лит., 2008. - С. 170-172.
4. Безруков Н.Н. Компьютерная вирусология: Справ. руководство. - Киев: УРЕ,2001. - С. 152-154
5. Старкова А.Ю., Пустобаева М.А., Карлов Д.Н. Нейронные сети в шифровании данных // Современные электротехнические и информационные комплексы и системы. Материалы I Международной научно-практической конференции студентов, аспирантов и преподавателей. 2019. - С. 160-163.
6. Хатч Б., Ли Д., Курц Д. Секреты хакеров. - М.-СПб.-К.: Вильямс, 2002. – С. 75-77.