УДК 004

Бедняк С.Г., кандидат педагогических наук, доцент
Заместитель заведующего кафедрой «Информационные системы и технологии»
Поволжский Государственный Университет Телекоммуникаций и Информатики
Россия, г. Самара
Бозоров К.А., Соловьева П.С.
студенты 3 курса,
факультет «Информационные системы и технологии»
Поволжский Государственный Университет Телекоммуникации и Информатики
Россия, г. Самара

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация:*В настоящее время все больше людей осознают важность безопасности информации. Вопрос о защите информации встает не только на государственном уровне, промышленном, но и на организационном и частном.Принципиальная особенность современной ситуации заключается в том, что важнейшей задачей сегодня становится защита информации.*

Ключевые слова: *Информация, безопасность, данные, защита.*

Annotation: *At present, more and more people are realizing the importance of information security. The issue of information protection rises not only at the state level, industrial, but also organizational and private. A fundamental feature of the current situation is that the most important task today is the protection of information.*

Key words:*Information, security, data, protection.*

С самим появлением человечества появилась необходимость передачи информации нужным людям так, чтобы эта информация она не становилась известной посторонним. Сначала для передачи информации использовались устная речь и жестикуляция. Но с появлением письменности возник вопрос озасекреченности сообщений. Так возникло искусство криптографии, предназначенное для тайной передачи написанных сообщений.

Были придуманы способы передачи сообщений, слова которых были разбросаны в большом тексте на отстраненную тему: технологии письма симпатическими чернилами, исчезающими спустя время; запись сообщения с помощью шифров.

Развитие криптографии в XX веке было стремительным, но неравномерным. Анализ истории ее развития как специфической области человеческой деятельности выделяет три основных периода. Начальный, имевший дело лишь с ручными шифрами, начавшийся в древности, закончился лишь в конце тридцатых годов XX века. Следующий период отмечен созданием и широким внедрением в практику сначала механических, потом электромеханических и, наконец, электронных устройств шифрования, созданием сетей засекреченной связи. Его началом можно считать применение телеграфных шифровальных машин, использующих длинный одноразовый ключ. Длится он по наши дни. С развитием разветвленных коммерческих сетей связи, электронной почты и глобальных информационных систем самыми главными стали проблемы распределения секретных ключей и подтверждения авторства. К ним теперь привлечено внимание широкого круга криптологов. Началом третьего периода развития криптологии обычно считают 1976 год, когда американские математики Диффи и Хеллман предложили принципиально новый вид организации засекреченной связи без предварительного снабжения абонентов секретными ключами, так называемое шифрование с

открытым ключом. Новый период развития криптографии характеризуется появлением полностью автоматизированных систем шифрованной связи, в которых каждый пользователь имеет свой индивидуальный пароль для подтверждения подлинности, хранит его.

В настоящее время все больше людей осознают важность безопасности информации. Вопрос о защите информации встает не только на государственном уровне, промышленном, но и на организационном и частном.

Принципиальная особенность современной ситуации заключается в том, что важнейшей задачей сегодня становится защита информации в компьютерных сетях.

Сейчас отсутствует какая-либо универсальная методика, позволяющая четко соотносить ту или иную информацию к категории коммерческой тайны. Можно только посоветовать исходить из принципа экономической выгоды и безопасности предприятия - чрезмерная "засекреченность" приводит к необоснованному подорожанию необходимых мер по защите информации и не способствует развитию бизнеса, когда как широкая открытость может привести к большим финансовым потерям или разглашению тайны.

Выполнение процедур шифрования и дешифровки, в любой системе информационного процесса, замедляет передачу данных и уменьшает их доступность, так как пользователь будет слишком долго ждать свои «надежно защищенные» данные, а это недопустимо в некоторых современных компьютерных системах. Поэтому система безопасности должна в первую очередь гарантировать доступность и целостность информации, а затем уже (если необходимо) ее конфиденциальность.

Широкое внедрение компьютеров во все виды деятельности, постоянное наращивание их вычислительной мощности, использование компьютерных сетей различного масштаба привели к тому, что угрозы

потери конфиденциальной информации в системах обработки данных стали неотъемлемой частью практически любой деятельности.

Информационная безопасность компьютерных систем достигается обеспечением конфиденциальности, целостности и достоверности обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

На сегодняшний день сформулировано три базовых принципа, которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере информации, а также зашита от неавторизованного создания или уничтожения данных;целостность обеспечивает гарантии точности и надежности информации и предоставляющих ее информационных систем, предотвращает возможность несанкционированных изменений.
- конфиденциальность информации; конфиденциальность обеспечивает необходимый уровень секретности в каждой точке обработки данных и предотвращает их несанкционированное раскрытие.
- доступность; доступность обеспечивает уполномоченным лицам надежный и своевременный доступ к данным и ресурсам. На доступность системы может повлиять сбой аппаратного или программного обеспечения.

Информационная безопасность - это прежде всего защита сети от различного вида атак. Существует ряд простых средств, с помощью которых можно остановить попытки проникновения в сеть, к ним относятся:

1. Оперативная установка исправлений для программ, работающих в интернете.
2. Антивирусные программы по обнаружению различного рода взломов и вирусов незаменимы для повышения безопасности любой сети. Они наблюдают за работой компьютеров и выявляют на них вредоносные программы.

3. Следует использовать наиболее надёжные пароли, менять их как можно чаще и чтобы их длина была максимальной. Это может предотвратить кражу секретной и не секретной информации.
4. Соединения с удаленными машинами (компьютерами) должны быть защищены с помощью паролей, чтобы избежать проникновения в сеть с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей.
5. При установке новой операционной системы обычно разрешаются все сетевые средства, что является не безопасным. Кроме вышеперечисленных средств защиты информации, существует еще множество способов предотвращения взломов и краж информации. Для избегания неприятных ситуаций необходимо изучать рекомендации по безопасности и придерживаться необходимых средств защиты.

Важным моментом при использовании системы защиты информации является обеспечение потенциального невмешательства иных присутствующих в системе программ в процесс обработки информации компьютерной системой, работу системы защиты информации.С помощью посторонних программ, присутствующих в компьютерной системе, злоумышленник может реализовать опосредованный несанкционированный доступ, то есть реализованный не напрямую, а путем запуска в систему постороннего программного обеспечения, так называемые вирусы.

Использованные источники:

1. Анисимова И.Н., Стельмашонок Е.В. Защита информации. Учебное пособие. - 2002.
2. Нечаев В.И. Элементы криптографии. Основы теории защиты информации.: Учеб.пособие для ун-тов и пед.вузов. - М.: Высшая школа, 1999. - 109 с.

3. Защита информации в компьютерных системах и сетях./ Романец Ю.В., Тимофеев И.А., Шаньгин В.Ф. - М.: Радио и связь, 1999. - 328 с.
4. Мельников В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электрониинформ, 1997.