ИНФОРМАЦИОННАЯ УГРОЗЫ

Современный мир представляет собой информационное общество: компьютеры контролируют работу атомных реакторов, распределяют электроэнергию, управляют самолётами и космическими кораблями, определяют надёжность систем обороны страны и банковских систем, т.е. используются в областях общественной жизни, обеспечивающих благополучие и даже жизнь множества людей.

Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

Информационная безопасность – совокупность мер по защите информационной среды общества и человека

О важности этой проблемы свидетельствуют многочисленные факты. Более 80% компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе, информационные технологии все еще остаются сильно уязвимыми для посторонних воздействий. И касается это не только бизнес-процессов, но и личной жизни.

- Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности? (вирусы, черви, трояны, хакеры, спам, мошенничество, несоблюдение закона об авторском праве).

Перечислим некоторые виды компьютерных преступлений, когда компьютер является инструментом для совершения преступления, а объектом преступления является информация:

1. Несанкционированный (неправомерный) доступ к информации. Лицо получает доступ к секретной информации, например, путём подбора шифра (пароля).

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных. Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

2. Нарушение работоспособности компьютерной системы. В результате преднамеренных действий ресурсы вычислительной системы становятся недоступными, или снижается её работоспособностью. Примером такого рода преступлений является создание и распространение компьютерных вирусов.

Вирус - это программа, которая может проникнуть в компьютер различными путями и вызвать эффекты, начиная от просто раздражающих восприятие до очень разрушительных. Вирусы могут проникать в компьютеры через электронную почту, Интернет, различные виды дисков и т.д., и имеют следующие характеристики:

- они способны размножаться, заражая другие файлы и программы;
- когда они активны, то способны выполнять раздражающие или разрушительные действия на Вашем компьютере.

3. Подделка (искажение или изменение), т.е. нарушение целостности компьютерной информации. Эта деятельность является разновидностью неправомерного доступа к информации. К подобного рода действиям можно отнести подтасовку результатов голосования на выборах, референдумах и т.д. путем внесения изменений в итоговые протоколы.

Киберпреступники изобретают все новые и новые способы обмана пользователей. Интернет-мошенники постоянно придумывают что-то новое, но при этом выбирают самые легкие и простые пути для своих махинаций. Активным интернет-пользователям ежедневно приходят фальшивые письма с предложениями от известных компаний, в браузере всплывают зараженные баннеры, приходят ссылки на поддельные сайты, попадаются файлы, содержащие вредоносные программы. Угроз возникает много, и главный совет – всегда быть настороже и заранее обезопасить свои действия.

Простые домашние пользователи – самый «лакомый» кусок для интернет-мошенников. Основная опасность – финансовая. Киберпреступники могут украсть данные кредитных карт, получить доступ к банковской информации, электронным кошелькам, личным данным или «взять компьютер в заложники», чтобы вынудить отправить SMS с заоблачной стоимостью. На второе место можно поставить угрозу заражения. В этом случае домашний компьютер становится источником рассылки спама и вирусов, участвует в попытках взлома или DDoS-атаках, а его владелец становится невольным соучастником этих киберпреступлений.

К информационным угрозам стоит причислить и телефонных мошенников, которые разными путями (звонки, смс и т.п.) пытаются завладеть финансовыми средствами абонентов.

Надо помнить, что информация, которую мы получаем через интернет и другие источники СМИ, не всегда правдива и может быть направлена на снижение патриотизма, разрушение личности и т.д.

Меры обеспечения информационной безопасности.

Эти меры применяются в основном на этапе эксплуатации информационной системы.

Разработчики системы, предназначенной для обработки важной информации, должны предусмотреть средства защиты уже на этапе её создания. Существует даже специальный термин «защищенная система» - это информационная система, обеспечивающая безопасность обрабатываемой информации и поддерживающая свою работоспособность в условиях воздействия на неё заданного множества угроз (нарушение целостности информации, несанкционированный доступ, попытки нарушения работоспособности).

Средства защиты современных информационных систем должны учитывать современные формы представления информации (гипертекст, мультимедиа и т.д.). Развитие локальных сетей Internet диктует необходимость эффективной защиты при удаленном доступе к информации. Необходимо осуществлять защиту от автоматических средств нападения: компьютерных вирусов, автоматизированных средств взлома.

Наряду с программно-техническими средствами защиты информации действуют правовые, юридические меры защиты. Перейдите по ссылке познакомьтесь с мерами обеспечения информационной безопасности.

К защите информации также относится и осуществление авторских и имущественных прав на интеллектуальную собственность, каковым является программное обеспечение.