Типы компьютерных угроз

Григорян Т.Н.

Электронное пособие для уроков информатики
ЦО №1434

Общее понятие о

Технических компьютерных

- Угрозах
 Объектом защиты информационной безопасности от технических компьютерных угроз (ТКУ) являются компьютерные системы и сети. Путем реализации ТКУ можно также получать данные непосредственно о пользователях (людях и программах) компьютерных систем и сетей, о режимах их работы, об их интересах и т.п.
 - Таким образом, <u>ТКУ добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей.</u>

Т. к. сеть в данном случае выступает не более чем как канал связи.

Типы информации для ТКУ

Классификация компьютерных угроз

Алгоритмические компьютерные угрозы

Алгоритмические компьютерные угрозы

 добывание данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и некоторых возможностей компьютерных систем и сетей.

Семантические компьютерные угрозы

Семантические компьютерные угрозы

 добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей.

Вирусные компьютерные угрозы

Вирусные компьютерные угрозы

 добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами.

Разграничительные компьютерные угрозы

Разграничительные компьютерные угрозы

- добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе преодоления средств разграничения доступа, а также реализация несанкционированного доступа при физическом доступе к компьютеру или компьютерным носителям информации.

Сетевые компьютерные угрозы

Сетевые компьютерные угрозы

добывание данных из компьютерных сетей, путем анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации, а также блокирование доступа к ним, модификация, перехват управления либо маскирование своих действий.

Потоковые компьютерные угрозы

Потоковые компьютерные угрозы

 добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров.

Аппаратные компьютерные угрозы

Аппаратные компьютерные угрозы

добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими типами ТКУ.

Форматные компьютерные угрозы

Форматные компьютерные угрозы

добывание информации и сведений путем "вертикальной" обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем в информацию для последующего ее представления пользователям.

Пользовательские компьютерные угрозы

Пользовательские компьютерные угрозы

добывание информации о
пользователях, их деятельности и
интересах на основе определения их
сетевых адресов, местоположения,
организационной принадлежности,
анализа их сообщений и информационных
ресурсов.

Заключение

Объектами защиты от технических компьютерных угроз являются: компьютерные системы (сети) и характеристики их пользователей и программноаппаратных средств. Выделено 9 типов угроз: семантических, алгоритмических, вирусных, разграничительных, сетевых, потоковых, аппаратных, форматных и пользовательских. Необходимо особо отметить, что все эти 9 типов компьютерных угроз просто необходимо учитывать при обеспечении безопасности информации в системах информационных инфраструктур.