
Несанкционированный доступ к информации
Внедрение компьютерного вируса
Компьютерная преступность
Подделка выходной информации
Несанкционированное копирование конфиденциальной информации
НАКАЗАНИЕ

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ

может осуществляться с целью её хищения (копирование на свой носитель и последующее блокирование доступа к информации) или же ради развлечения или последующего использования данной информации. Существуют множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, хищением носителей информации; установкой аппаратуры записи и т. д.

НАЗАД

ВНЕДРЕНИЕ КОМПЬЮТЕРНОГО ВИРУСА

процесс внедрения вредоносной программы с целью нарушения работы ПК. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Вирус может проявлять себя в разных формах. Это могут быть замедления в выполнении программ; увеличение объёма программных файлов и наконец, эти проявления могут привести к стиранию файлов и уничтожению программного обеспечения.

НАЗАД

ПОДДЕЛКА ВЫХОДНОЙ ИНФОРМАЦИИ

подделка информации может преследовать различные цели. Итогом подделки является то, что конечному потребителю информации будут предоставлены недостоверные данные. Примером могут служить подтасовка результатов выборов или же хищение различного вида товаров, путем ввода в программу фальшивых данных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

НАЗАД

Несанкционированное копирование конфиденциальной информации

в процессе работы каждой компании неизбежны случаи утечки конфиденциальной информации. Несмотря на то, что защитные системы, отвечающие за хранение и доступ к внутренней информации, постоянно совершенствуются, проблема продолжает существовать. Организации несут огромные потери из-за несанкционированного распространения конфиденциальной информации. Несанкционированное копирование может осуществляться посредством изъятия средств компьютерной техники; перехвата информации; несанкционированного доступа к технике, а также манипуляции данными и управляющими командами.

НАЗАД

НАКАЗАНИЕ

По УК РФ преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации(ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), [нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей] (ст. 274 УК РФ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) совершаются только путём действий, в то время как [нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей] (ст. 274 УК РФ) — путём как действий, так и бездействием.

НАЗАД