На сегодняшний день этим уже пользуются спецслужбы и органы охраны правопорядка, посольства таможенные структуры, крупные компании (делая рыночные исследования, участвуя в информационной войне с конкурентами и оценивая кандидатуры работников при приёме на работу) и обычные граждане желающие узнать больше о других и использовать эту информацию либо в своих целях. Информация, которую можно получить таким способом, бывает порой более содержательной и полезной чем данные, содержащиеся в государственных базах данных.

Проблема конфиденциальности продолжает существовать, так как с эволюцией средств хранения и передачи данных, носителей масс-медиа, с зарождением сети Интернет правоприменительная практика в области конфиденциальности информации отступает перед стремительным ростом технологий. Правоохранительные органы на сегодняшний день не располагают достаточной подготовкой кадров, для расследования компьютерных преступлений в области нарушения конфиденциальности, а население делает всё меньше различий между конфиденциальной и общедоступной информацией, что делает эти преступления невидимыми. Необходимо повышать квалификацию для правоприменения существующих законов и соглашений, и информировать население об опасности разглашения конфиденциальной информации.

КЛАССИФИКАЦИЯ СПОСОБОВ НАНЕСЕНИЯ АТАК ДЛЯ ВЫБОРА СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Лидия СИВКО, Александр ДОРОХОВ
Харьковский Национальный Экономический Университет (Украина)

Currently there are many methods of application attacks at the systems technical data protection in modern society. This led to the need for research to the classification of these methods. The obtained results of the work listed below.

Развитие и внедрения в Украине европейских и международных стандартов информационной безопасности, актуализация проблем противодействия компьютерной преступности создали благоприятные условия для стремительного развития средств зхащиты от угроз нарушения режима безопасности.

Выбор средств защиты зависит от того, какими возможными способами злоумышленник будет пытаться совершить информационную атаку. Атака на информацию – это преднамеренное нарушение набора правил, установленных собственниками информационного объекта или уполномоченного им лица при хранении, поддержке или предоставлении доступа к данному информационному объекту.

Целью исследования является анализ вероятных способов совершения атак (ВССА) системы технической защиты информации (СТЗИ) на основе рассмотрения уже существующих неоднозначных классификаций. Важность определения более четкой классификации данных способов обусловлена необходимостью учета данных способов при осуществлении технической защиты в учреждении, использующем в своей деятельности государственную тайну.

Для СТЗИ, не составляющей государственной тайны, ВССА непосредственно влияют на объем средств, выделяемых на создание и обеспечение функционирования такой системы, что также немаловажно в условиях современной рыночной экономики.

Класиификация способов совершения атак на информацию представляет собой разностороннюю проблему и, в значительной, степени зависит от формы хранения, обработки и передачи информации, а также от тех целей, которые преследует вероятный нарушитель.

Обобщенные пути несанкционированного воздействия на информацию перечислены в государственном стандарте ГСТУ 3396.0-96 (Техническая защита информации Основные положения). Согласно этому документу атаки могут осуществляться [2] техническими каналами (оптические, радио и т.п.), каналами специального воздействия (через формирование полей и сигналов с целью нарушения целостности информации), несанкционированным доступом (маскировка под зарегистрированного пользователя, внедрение компьютерных вирусов).

Однако опыт использования стандарта ГСТУ 3396.0-96 в практической деятельности позволяет сделать выводы относительно неоптимальности вышеупомянутых положений.

Существуют и другие научно обоснованные классификации. Большинство специалистов в области ТЗИ признают существование технических каналов утечки информации (ТКУИ), как одного из основных источников несанкционированной утечки информации.

Однако следует отметить, что однозначное и общепринятое определение термина ТКУИ на сегодня отсутствует. В данном исследовании используется собственное формализованное определение, сочетающее в себе оба подхода: технический канал утечки информации – это совокупность носителя информации, среды распространения информационного сигнала, помех и шумов, мешающих передаче сигнала и средства технической разведки.

Существует еще один довольно распространенный подход, сторонники которого считают, что ТЗИ является одним из способов несанкционированного доступа к информации [1]. Особого внимания заслуживает предположение о том, что каждый вид потенциальной угрозы осуществляется по определенной совокупности потенциальных каналов несанкционированного доступа (по мнению западных специалистов, такие угрозы занимают приоритетное место), или потенциальных каналов несанкционированного воздействия в отношении защищаемой информации [1].

Следует отметить [1], что в некоторых случаях злоумышленник, которому не удается получить информацию по техническим каналам, может прибегнуть к ее уничтожению.

Все изложенное выше позволяет с полным основанием выделить два вида возможных способов совершения атак на информацию: атаки, которые реализуются путем несанкционированного доступа (подвидом таковых являются атаки, которые реализуются путем использования технических каналов утечки информации) и атаки, которые реализуются путем несанкционированного воздействия (подвидом таких являются атаки реализующиеся путем использования технических каналов несанкционированного воздействия на информацию).

Ниже приведен перечень ВССА на информацию в электронном виде, которые реализуются путем использования каналов несанкционированного доступа:

- похищение данных всей автоматизированной системы (АС) или ее компонентов;
- похищение магнитных, оптических и электронных носителей информации;
- подмена отдельных компонентов АС на аналогичные;
- атаки, которые реализуются путем использования технических каналов утечки информации (получения и извлечения информации за счет использования побочных электромагнитных излучений и наводок, с использованием компьютерной сети – так называемые "дистанционные атаки", с экрана монитора путем подсматривания, с использованием закладных устройств, получение информационных сигналов из сети электропитания, с цепей заземления и т.д.).

Перечень же ВССА на информацию в электронном виде, которые реализуются путем использования каналов несанкционированного воздействия слежующий:

- физическое уничтожение АС, или ее составляющих (например, организация пожара или другогочрезвычайного события в помещении, где находится такая АС);
- уничтожение магнитных, оптических и электронных носителей;
- уничтожение источников питания АС;
- умышленное силовое воздействие сетями питания;
- уничтожение проводных коммуникаций и коммуникационного оборудования компьютерных сетей;
- атаки, которые реализуются путем использования технических каналов несанкционированного воздействия на информацию (вирусное воздействие, влияние путем использования деструктивных программных средств).

В результате проведения исследования нами предлагается использовать вышеописанную классификацию, которая может стать системообразующей в процессе исследования всей совокупности вероятных способов совершения атак на информацию, и следовательно, может быть использована в процессе построения систем ТЗИ, предназначенных для защиты открытой информации и информации с

ограниченным доступом на общегосударственном уровне и на уровне отдельных учреждений, предприятий, организаций, при формирования концепции противодействия компьютерной преступности.

Литература

1. В. Хорошко, А.Чекатов. Методы и средства защиты информации. – М.: ЮНИОР, 2010. – 501 с.
2. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. – К.: Держстандарт України, 1996. – 20 с.

ЭКЗИСТЕНЦИАЛЬНЫЙ АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Денис САЛТЫКОВ,
Молдавская Экономическая Академия

This article presents an existential view of information security problem. Also, here will be specified a great goal of information technologies and very special level of responsibility of security experts.

Новые условия человеческого существования

Стремительное развитие информационных технологий поставило общество на совершенно новый уровень. Само существование человека отныне приобретает принципиально иной характер, так как становится всё более обусловленным процессами информатизации. Стоит отметить тот факт, что тенденция проникновения информационных технологий во все области человеческой жизни – от быта до наивысших уровней управления – ставит специалистов перед высокой ответственностью.

Процесс информатизации явился главным этапом становления так называемого постиндустриального или информационного общества, когда информация становится главной ценностью, вытесняя материальные товары и средства их производства. В процессе развития информационных технологий сократилось множество рабочих мест в силу их неактуальности, но процесс породил и немалое количество совершенно новых специфических задач, которые в свою очередь породили новый спрос на рынке рабочей силы. Двумя основными секторами, обеспечившими этот спрос, явились наука и бизнес-сектор. Специалисты в области информационных технологий стали занимать в указанных областях ключевые посты, а также были сформированы многочисленные соответствующие отделы, которые стали играть одну из главных ролей в деятельности научных и коммерческих учреждений.