Пушина Е.Г., Калугин Р.Ю.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Персональные компьютеры, системы управления и сети на их основе, быстро входят во все области человеческой деятельности. Среди них необходимо выделить, такие сферы применения как военная, банковская, посредническая, научные исследования в образовательной деятельности и др.

Вполне очевидно, что усложнение методов и средств машинной обработки, повсеместное использование глобальной сети Интернет, приводят к тому, что информация становится все более уязвимой. Этому способствуют такие факторы, как постоянно возрастающие объемы обрабатываемых данных в службах материально-технического обеспечения, расширение круга пользователей, имеющих доступ к ресурсам, недостаточный уровень защиты аппаратных и программных средств от несанкционированного доступа. Учитывая эти факты, защита информации в процессе ее сбора, хранения, обработки и передачи приобретает исключительно важное значение в военной области. Для успешного выбора способов и средств защиты информации от возможного несанкционированного доступа необходимо классифицировать существующие угрозы информационной безопасности, которые по воздействию на объекты информационной безопасности делятся на: непреднамеренные и преднамеренные [1].

Непреднамеренные угрозы связаны главным образом со стихийными бедствиями, сбоями и отказами технических средств обработки и передачи информации (ТСПИ). Реализация этого класса угроз приводит, как правило, к нарушению достоверности и сохранности информации, реже – к нарушению конфиденциальности.

Угроза второго класса носит преднамеренный характер и связана с несанкционированным доступом к информации, хищения информации из библиотек, банков и баз данных, внедрением электронных устройств перехвата информации в технические средства и помещения (объекты) вычислительной техники (ВТ). Реализация этих угроз приводит к нарушению основных свойств информации: достоверности, сохранности и конфиденциальности. В результате воздействия угроз ухудшается функционирование аппаратных средств и характеристики обрабатываемой информации, что в конечном итоге приводит к ухудшению качества функционирования электронно-вычислительной техники, сети и снижения эффективности решаемых задач в области материально-технического обеспечения войск.

Для обеспечения безопасности информации на объекте вычислительной техники создается система защиты, которая включает в себя организационные меры и технические средства защиты.

К организационным мерам относятся мероприятия, связанные по выполнению требований руководящих документов по обеспечению безопасности информации и установлением ответственных должностных лиц органов управления за обеспечение безопасности обрабатываемой информации.

Объектами ВТ является помещения управления, отделов и служб воинской части, где устанавливаются персональные ЭВМ, автоматизированные рабочие места (АРМ) начальников служб и другие технические средства обработки и передачи информации. Сбор, хранение и обработка информации на объекте вычислительной техники разрешается только после завершения работ по созданию системы защиты, проверки ее функционирования комиссией, назначенной командиром воинской части. Ответственность за организацию выполнения требований по обеспечению безопасности информации, обрабатываемой с использованием персональных ЭВМ и сетей на их основе возлагается на начальников отделов и служб воинской части.

Каждая персональная ЭВМ должна быть проконтролирована и для каждой ЭВМ должны выполняться требования предприятия на ее эксплуатацию в соответствии с присвоенной категорией. Все персональные ЭВМ иностранного или совместно Российско-иностранного производства при вводе в эксплуатацию проходят специальные исследования и лабораторную поверку на наличие возможного внедрения специальных устройств перехвата. Использование, в составе персональных ЭВМ, обрабатывающих служебную информацию периферийных устройств не предусмотренной комплектацией данной ЭВМ, не прошедших специальных исследований, запрещается [2].

Размещение и установка персональных ЭВМ в помещениях отделов и служб воинской части должна исключить возможность их бесконтрольного использования и просмотра сведений лицами, не имеющими на это права.

Для непосредственного выполнения мероприятий по обеспечению безопасности информации распоряжением командира воинской части назначаются должностные лица, ответственные за эксплуатацию персональных ЭВМ и ТСПИ. Обеспечение безопасности информации от санкционированного доступа осуществляется в соответствии с законами РФ. Наиболее общим законом РФ является Конституция РФ. Главы 23, 29, 41 в той или иной мере затрагивают вопросы информационной безопасности [3].

Действующий Уголовный кодекс РФ предусматривает наказание за преступление, связанное с нарушением конфиденциальности информации. Глава 28 «Преступление в сфере компьютерной информации» содержит статьи 272, 273, 274 посвященные преступлениям, связанным соответственно с неправомерным доступом к компьютерной информации, нарушением правил эксплуатации ЭВМ.

Особенностью обучения информационной безопасности является то, что недостаточно только изучить организационные и технические средства защиты информации, необходимо прививать курсантам нравственность и воспитывать чувство ответственности за использование информации, которая может причинить ущерб не только личности обучающегося, но и всему образовательному процессу в целом.

Список использованной литературы

1. Конституция Российской Федерации.

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ. Об информации, информационных технологиях и о защите информации.
3. Уголовный кодекс Российской Федерации.

Сведения об авторах:

1. Пушина Е.Г., преподаватель кафедры ВВИМО
2. Калугин Р.Ю., курсант ВВИМО