Кашкин Евгений Владимирович
канд. техн. наук, доцент
Дебунов Андрей Александрович
аспирант
Меркулов Алексей Андреевич
аспирант
ФГБОУ ВО «Московский технологический университет»
г. Москва

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *основным приоритетным направлением работы с информацией на сегодняшний день является информационная безопасность. Важность защиты информационных каналов, обеспечения хранения и обработки информации в защищенном режиме является неотъемлемой частью современных информационных технологий. В работе рассматриваются основные направления защиты информации. Обозначаются ключевые места при формировании политики безопасности информационной системы.*

Ключевые слова: *информационная безопасность, информация, информационные технологии, информационные ресурсы.*

В том или ином виде информация всегда являлась для человека большой ценностью. Умышленно искаженная информация называется дезинформацией. В наши дни информация представляет собой один из важнейших ресурсов и является одной из движущих сил прогресса человеческого общества, где основополагающим свойством данного понятия остаётся ценность, определяющаяся степенью полезности информации для владельца или получателя.

В современном мире практически не осталось сфер человеческой и общественной деятельности, где не применялись бы информационные технологии, являющиеся средством повышения эффективности и производительности работы человека. Увеличение охватываемых информационными технологиями отраслей

деятельности повлекло за собой развитие такой отрасли наук, как информационная безопасность. С развитием информационных систем и технологий, которые полностью внедрились в инфраструктуру общества, государства и бизнеса, информация стала более важным ресурсом, по сравнению с материальными и энергетическими элементами экономического потенциала и появилось понятие «информационные ресурсы», определяющееся как отдельные документы или массивы документов в информационных системах. Информационные ресурсы представляют собой собственность, которая находится в ведении органов и организаций и подлежит учету и защите. Информация требует защиты по той причине, что её можно превратить в наличность, кому-нибудь продав, или уничтожить, что нанесёт вред её обладателю, так как в первую очередь ценность информации определяется приносимыми доходами. Обеспечение точности и безопасности информации на сегодняшний день является важнейшей проблемой информатизации общества. Как следствие ценности информации, в современных условиях информационного общества широко распространены действия, направленные на получение защищенной информации различными способами, вплоть до шпионажа, например, с использованием современных технических средств информационной разведки. Информация, доступ к которой ограничен в соответствии с законодательством, называет конфиденциальной. Деятельность злоумышленника может быть направлена на завладение информацией, её уничтожение, либо модификацию [1–4].

Если конфиденциальной информацией завладеет злоумышленник, то речь идёт об утечке информации. Чтобы этого избежать, необходимо принять меры по защите информации от утечки. Утечка информации может быть связана с хищением носителя или ЭВМ, что быстро обнаруживается, но может быть совершена негласно, например, с применением технических средств, что нанесёт владельцу больший ущерб, следственно, утечка информации бывает разной по последствиям. Такое понятие, как модификация информации, всегда считается неявным для владельца, но проявляться может по-разному. Если взять в качестве примера какой-либо финансовый документ, то злоумышленник может нанести

вред владельцу информации, изменив номер счета, куда направляются материальные средства, либо размер суммы, которая подлежит перечислению на указанный счет. Злоумышленник может изъять части сообщения из канала связи, либо изменить порядок следования частей сообщения в сетях с коммутацией пакетов, данная модификация нанесёт не малый вред получателю информации. Аналогично, если у злоумышленника есть возможность послать фальсифицированное сообщение банку с указанием перечислить денежные средства, такая модификация информации может нанести владельцу прямой материальный ущерб. Уничтожение информации может повлечь за собой, например, крах вычислительной системы, если не было осуществлено резервное копирование информации, иначе злоумышленник может временно вывести систему из строя, если профилактические меры по резервному копированию данных были приняты.

Список литературы

1. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности / П.Ю. Филяк, В.М. Шварев // Информация и безопасность. – 2015. – Т. 18. – №4. – С. 580–583.

2. Информационный стресс – фактор, снижающий качество систем управления безопасностью / С.А. Рыбин, Б.В. Чувыкин // Труды международного симпозиума Надежность и качество. – 2008. – Т. 2. – С. 172–175.

3. Математическая модель для обработки данных с тепловых датчиков для управления системой задвижек тепловых контуров зданий специального назначения / Е.В. Кашкин, Т.Ю. Морозова // Естественные и технические науки. – 2013. – №6 (68). – С. 289–292.

4. Разработка методов и средств планирования и управления производственными процессами и их результатами / М.А. Назаренко, Е.В. Кашкин, И.А. Маркова, В.И. Селиванов, И.В. Макарова // Международный журнал экспериментального образования. – 2016. – №11–1. – С. 114–115.