

УДК 343.985

*И. Г. Кузьма,
курсант 3-го курса факультета милиции
Могилевского института МВД
Научный руководитель: А. С. Апекунов,
преподаватель кафедры
оперативно-розыскной деятельности факультета милиции
Могилевского института МВД*

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Информация бывает как общедоступного, так и ограниченного доступа (конфиденциальная информация). Особенность информации ограниченного доступа заключается в том, что такой информацией может пользоваться только определенный круг лиц, так как пользование такой информацией другими лицами может нанести какой-либо вред владельцу такой информации.

Информация как объект защиты информации имеет свои особенности. В первую очередь информация не материальна, ее нельзя измерить, потрогать. Информация хранится на материальном носителе и может передаваться по различным каналам связи.

Технические средства защиты информации — различные по типу устройства (механические, электромеханические, электронные и др.), которые на уровне оборудования решают задачи информационной защиты. В целях предотвращения использования информации, которая подлежит конфиденциальности, она подвергается определенной защите. Защита информации препятствует несанкционированному доступу к такой информации, тем самым обеспечивая ее сохранность.

Существуют четыре вида защиты конфиденциальной информации: правовой, физический, криптографический, технический. У каждого вида защиты информации своя специфика. Правовая защита информации заключается в том, что создаются нормативно-правовые акты в данном направлении. Криптографическая защита основывается на том, что специальные средства осуществляют криптографическое преобразование защищаемой информации. Физические средства защиты представляют собой ограничение физического доступа к защищаемым данным. Примером физического средства защиты может служить обычный замок. Технические средства защиты заключаются в использовании различных аппаратных устройств [1]. защите информации в настоящее время уделяется

больше внимание со стороны государства, так как утечка определенной информации может нанести вред не только личной жизни физических лиц, нарушив их законные права, но и суверенитету Республики Беларусь.

Благодаря техническим средствам обеспечивается защита помещения, в котором хранится защищаемая информация, от возможности утечки по техническим каналам, а также проникновения в него посторонних лиц. В зависимости от степени защищаемого объекта применяются различные технические средства: начиная от дверей, препятствующих несанкционированному доступу, заканчивая более сложными техническими средствами [2].

В законодательстве Республики Беларусь также имеется отражение правовой защиты информации. Так, согласно ст. 29 Закона Республики Беларусь «Об информации, информатизации и защите информации», к техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации [3].

Одна из IT-платформ совмещает в целом физические, аппаратные, программные средства защиты, называя все эти средства техническими средствами защиты информации [4]. С этим нельзя не согласиться, так как использование физических, аппаратных и программных средств защиты увеличивает уровень защищенности информации, тем самым повышая у ее обладателя уверенность в ее сохранности. К примеру, для защиты какой-либо информации, хранящейся на компьютере, было установлено программное обеспечение, которое исключает доступ к посторонним лицам, но при этом помещение, в котором находится компьютер, не было защищено физически. Ничего не мешает злоумышленнику проникнуть в такое помещение и изъять жесткий диск, на котором хранится информация. Поэтому рекомендуется совмещать все средства защиты. К физическим средствам защиты относятся установление решеток на окна, исключающих проникновение снаружи; установление сигнализаций, камер видеонаблюдения, замков; установление ударопрочных пленок на окна. К программным средствам защиты относят программное обеспечение, которое устанавливается непосредственно на компьютер или сервер; антивирусные программы, которые изолируют или удаляют вредоносные программы; системы аккаунтов и паролей; DLP-системы, которые предотвращают утечку информации, например, мешают сотруднику скопировать секретную базу данных на флешку. К аппаратным средствам защиты относят генераторы шума; аппаратные регистры паролей (к примеру, специальная флешка, которую необходимо вставить в компьютер для использования информации); аппаратные модули доверенной загрузки, которые не позволяют загрузить на компьютер посторонние программы.

Таким образом, комплексное использование средств защиты информации позволит обеспечить безопасность данных от несанкционированного доступа посторонних лиц.

1. Виды защиты конфиденциальной информации [Электронный ресурс] // «СОЛАР СЕКЬЮРИТИ» — системы и средства информационной безопасности и защиты данных. URL: https://rt-solar.ru/products/solar_dozor/blog/2090/ (дата обращения: 04.04.2023). [Перейти к источнику](#) [Вернуться к статье](#)

2. Программная и аппаратная защита информации [Электронный ресурс] // Специальная техника и технологии. URL: <http://detektor.ru/prod/common/protect/> (дата обращения: 04.04.2023). [Перейти к источнику](#) [Вернуться к статье](#)

3. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-3 : в ред. от 10.10.2022 г. № 209-3. Доступ из информ.-поисковой системы «ЭТАЛОН». [Вернуться к статье](#)

4. Методы и средства защиты информации: коммерческой тайны и персональных данных [Электронный ресурс] // Средства информационной безопасности. URL: <https://mcs.mail.ru/blog/metody-i-sredstva-zashchity-informacii-personalnyh-dannyh> (дата обращения: 04.04.2023). [Перейти к источнику](#) [Вернуться к статье](#)