УДК 004.056.53

М. С. Шлыков
заместитель начальника
Могилевского института МВД Республики Беларусь
по организации службы
Е. А. Лаппо
доцент кафедры оперативно-розыскной деятельности
факультета милиции
Могилевского института МВД Республики Беларусь,
кандидат юридических наук, доцент

НЕКОТОРЫЕ ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ (ОБЪЕКТОВ)

Цифровизация современного общества свидетельствует о наличии потенциальных и действующих угроз в информационной сфере, с учетом которых информационную безопасность можно определить как способность информационной системы (объекта) противостоять негативным дестабилизирующим факторам. Воздействие указанных факторов на информационную систему (объект) различно и не может быть выражено в конкретных количественных значениях ввиду его основных свойств, таких как: технические свойства объекта, структура, программное обеспечение, наличие защитных барьеров и т. п. В каждый конкретный момент времени объект информатизации характеризуется некоторым состоянием защищенности от внутренних и внешних факторов воздействия на него.

Как известно из литературных источников по рассматриваемому вопросу, информационная безопасность включает:

- состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;
- состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;
- состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;
- экономическую составляющую;
- финансовую составляющую [1, с. 7].

Изложенное свидетельствует, что действие негативных факторов на защищаемую информационную систему (объект) заключается в дестабилизации ее функций и нарушении нормального режима функционирования. Такое воздействие, как правило, носит необратимый характер и обусловлено сложным комплексом происходящих процессов, развивающихся в результате целенаправленного воздействия.

В указанных условиях для обеспечения информационной безопасности уполномоченным на то субъектам требуется на постоянной основе проводить комплекс мероприятий, направленных на защиту информационной системы (объекта), обеспечение целостности, доступности, достоверности информации, бессбойной работы технического оборудования, используемого для ввода, хранения, обработки и передачи данных потребителям информации.

Представляется обоснованной изложенная в различных литературных источниках обобщенная позиция исследователей о том, что основной целью воздействия на информационную систему как объект, подлежащий защите, является получение доступа к информации, нарушение ее конфиденциальности, целостности и доступности. Предпринимаемые меры воздействия на защищаемый объект могут быть обусловлены рядом естественных и искусственных факторов, носящих, в свою очередь, как активный, так и пассивный характер.

Показатель устойчивости информационной системы (объекта) должен определяться на всех этапах ее жизненного цикла. При этом необходим выбор обоснованных критериев определения такого состояния либо исходя из некоторой совокупности типичных факторов, либо из неопределенного множества. В последнем случае должна решаться задача по определению состояний информационной системы (объекта), при которых обеспечивается ее нормальное функционирование. Таким образом, определяющим критерием в рассматриваемом случае будет являться значение отношения фактически выполняемых задач к их теоретически рассчитанному максимуму при наличии неопределенного количества негативных факторов. Показатель защищенности информационной системы объекта невозможно определить в полной мере, так как он не поддается количественной оценке в каких-либо достоверных общепринятых показателях, поскольку он фактически проявляется лишь в случае возникновения негативных последствий (инцидентов, технических неисправностей оборудования, целенаправленных воздействий и т. п.).

Представляется, что учет указанных факторов способен оказать положительное влияние на разработку моделей безопасности информационной системы (объекта) в части организации построения ее структуры, наличия основных и дополнительных элементов, механизмов и средств технической защиты

информации, определения политики безопасности как составной части защищаемой информационной системы (объекта), разработки алгоритма, регламентирующего процессы обеспечения доступа, обработки и сохранности информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы (объекта).

Список основных источников

1. Деятельность органов внутренних дел по пресечению угроз кибербезопасности : учеб.-метод. пособие / А. Н. Александров [и др.]. Белгород : Белгород. юрид. ин-т МВД России им. И. Д. Путилина, 2024. 104 с. Вернуться к статье