***Политика информационной безопасности (ПИБ)***организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, *документированных управленческих решений*, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

***Информационная (информационно-вычислительная) система***– организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

***Информационные процессы***– процессы сбора, накопления, хранения,

обработки (переработки), передачи и использования информации.

***Информационные ресурсы***– отдельные документы или массивы документов в информационных системах.

***Объект*** *–* пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

***Субъект*** *–* активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

***Доступ*** *–* специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

***Атака*** – попытка несанкционированного преодоления защиты системы.

***Несанкционированный доступ (НСД)*** *–* доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

***Защита информации***— организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

***Безопасность информации***— защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

***Безопасность любого ресурса информационной системы***складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности, также могут быть включены другие, такие как аутентичность, подотчетность, надежность; или иначе: *информационная безопасность –* все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки:

***конфиденциальность*** компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия;

***целостность*** компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права; целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени;

***доступность*** компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Для создания эффективной системы информационной безопасности организации или учреждения целесообразно разработать:

* **• *концепцию***
* **• *стандарты***
* **• *процедуры***
* **• *инструкции*,**
* **• *план мероприятий***

***Фактор*, *воздействующий на ИВС***, – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты

***Естественные угрозы***— это угрозы, вызванные воздействиями на информационнуюсистему и ее компоненты объективных физических процессов техногенного характера илистихийных природных явлений, независящих от человека.

***Искусственные угрозы***— это угрозы, вызванные деятельностью человека. Срединих, исходя из мотивации действий, можно выделить:

* • *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками впроектировании информационной системы и ее элементов, ошибками в действияхперсонала и т.п.;
* • *преднамеренные* (умышленные) угрозы, связанные с корыстными, идейными илииными устремлениями людей (злоумышленников).

***Фактор*, *воздействующий на ИВС***, – это явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение данных, блокировка доступа к ним, повреждение или уничтожение системы защиты.