Тип работы: Реферат

Предмет: Информатика

Содержание

Введение

Информация помогает найти партнеров и помогает четко сформулировать позицию по отношению к ним. Защита информации - это комплекс мер, направленных на обеспечение информационной безопасности. Информационная безопасность означает защиту информации и вспомогательной инфраструктуры от случайных или преднамеренных воздействий, естественных или искусственных, которые могут нанести неприемлемый ущерб участникам информационных отношений, включая владельцев и пользователей информации и вспомогательной инфраструктуры.
Вопросы безопасности являются важной частью концепции внедрения новых информационных технологий во все сферы жизни общества. Информационная безопасность является важным аспектом ведения бизнеса в условиях агрессивной рыночной экономики.
В современном деловом мире происходит процесс перехода от материальных активов к информационным. По мере развития организации ее информационная система становится все более сложной, основная цель которой заключается в максимальном повышении эффективности ее деятельности в условиях постоянно меняющейся конкурентной среды.

1.Теоретические аспекты защиты информации в организации

Под защитой информации обычно понимается использование различных средств и методов, принятие мер и осуществление мер, направленных на систематическое обеспечение надежности передаваемой, хранимой и обрабатываемой информации.
Можно выделить несколько основных задач, решение которых в информационных системах и телекоммуникационных сетях обеспечивает защиту информации, а именно:
организация доступа к информации только для уполномоченных лиц;
подтверждение достоверности информации;
защита от перехвата информации при ее передаче по каналам связи;
защита от искажения и ввода ложной информации [5].

Защита информации означает:
обеспечение физической целостности информации, т. е. предотвращение любого искажения или уничтожения информационных элементов;
предотвращение замены (модификации) информационных элементов при сохранении их целостности;
предотвращение получения несанкционированной информации неавторизованными лицами или процессами;
гарантировать, что ресурсы, переданные (проданные) владельцем информации, будут использоваться только в соответствии с условиями, согласованными сторонами.
Угроза информационной безопасности - это совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации, как в результате несанкционированного, так и непреднамеренного воздействия на нее [1].
Основными формами нарушения (угроз), которые возможны при наличии уязвимостей в отношении основных свойств информации, являются:
раскрытие (конфиденциальной) информации – несанкционированное раскрытие защищенной информации потребителям, которые не имеют права на доступ к такой информации;
несанкционированный доступ - получение охраняемой информации заинтересованным лицом с нарушением установленных юридических документов или владельцем, владельцем информации прав или правил доступа к охраняемой информации;[2]
непреднамеренные или несанкционированные последствия, влекущие за собой изменение, искажение (модификацию), искажение информации. копирование, уничтожение и т. д.
блокирование доступа в защищенную зону доступа непреднамеренным или несанкционированным воздействием;
разрушение или отказ носителя в результате непреднамеренных или несанкционированных воздействий.
Причины этих угроз следующие:
1)непреднамеренное или несанкционированное воздействие информации (НПД):
ошибка в информации пользователя,
технический сбой и сбой программного обеспечения информационных систем,
природные явления или другие действия, не направленные на изменение информации, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к потере, уничтожению или выходу из строя носителя информации.
2) аппаратные сбои:
неисправности проводки;
сбои в работе дисковых систем;
сбои в системах резервного копирования;
сбои серверов, рабочих станций, сетевых адаптеров и т. д
3)потеря информации из-за неправильной работы

Список литературы:

1. Аверченков, В. И. Аудит информационной безопасности органов исполнительной власти. Учебное пособие / В.И. Аверченков. - М.: Флинта, 2020. - 297 с.
2. Аверченков, В. И. Аудит информационной безопасности. Учебное пособие / В.И. Аверченков. - М.: Флинта, 2021. - 679 с.
3. Александр, Шилов und Владимир Мищенко Информационная безопасность финансового учреждения / Александр Шилов und Владимир Мищенко. - М.: LAP Lambert Academic Publishing, 2021. - 164 с.
4. Артемов, А. Информационная безопасность. Курс лекций / А. Артемов. - Москва: РГГУ, 2018. - 788 с.
5. Астахова, Людмила Герменевтика в информационной безопасности / Людмила Астахова. - М.: LAP Lambert Academic Publishing, 2020. - 296 с.
6. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: моногр. . - Москва: Мир, 2020. - 552 с.
7. Афанасьев, Алексей Алексеевич Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ / Афанасьев Алексей Алексеевич. - М.: Горячая линия - Телеком, 2020. - 438 с.
8. Бабаш, А. В. Информационная безопасность (+ CD-ROM) / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2021. - 136 с.