Тип работы: Научно-исследовательская работа

Предмет: Информационные технологии

-

Аннотация: Основной целью представленной работы является изучение вопроса, касающегося классификации угроз и средств защиты информации в современных системах информационной безопасности. В процессе написания работы автором использовались теоретические методы исследования. Для более детального и достоверного раскрытия темы использовались отечественные и зарубежные научные источники.
Ключевые слова: информационная безопасность, защита информации, угроза, информационные технологии.
Keywords: information security, information protection, threat, information technology.

Безопасность данных - это состояние защищенности данных, при котором обеспечены целостность, конфиденциальность и доступность [3, с.42]. Информационная безопасность выступает одной из главных проблем современного общества и обусловлена увеличением значимости информации в основных бизнес процессах.
Проблемы защиты информации в настоящее время связаны с дестабилизирующим воздействием внешних и внутренних угроз, возникающих в компании и влияющих на ее функционирование. В свою очередь, понятие проблема безопасности данных взаимосвязано с понятием угроза безопасности.
Это привело к тому, что в деятельности предприятий все больше возникает проблем, оказывающих негативное влияние на систему управления, а также технологическую поддержку в вопросах хранения и обработки данных.
Поэтому методы и инструменты для обеспечения комплексной системы защиты на предприятии должны выполнять мониторинг угроз на уровне информационного, аппаратного и программного обеспечения.
Развитие компьютерных технологий, аппаратного и программного обеспечения расширило круг проблем защиты информационных потоков, циркулирующих в компьютерных сетях от несанкционированного доступа. Основной проблемой является необходимость обеспечения требуемого уровня защиты, при котором необходимо учитывать, что информация, передаваемая по компьютерной сети, может быть получена злоумышленником и передана по каналам связи.
Проблемы информационной безопасности разделяют на три основных вида [5, с.68]:
• перехват данных, связанный с нарушением конфиденциальности информации;
• модификация или изменение данных, связанных с изменением исходного сообщения или полной его подмены с последующей пересылкой адресату;
• нарушение авторства информации, то есть передача информации не от имени автора, а от имени злоумышленника.
Для того чтобы осуществить перехват конфиденциальной информации, злоумышленником используются вирусы, кейлоггеры, троянские программы, вредоносное и шпионское программное обеспечение. Проблемы защиты сети связаны с тем, что не каждая антивирусная программа может своевременно выявить возникшие угрозы в сети и это создает возможность для злоумышленника использовать сеть для достижения поставленных целей.
Однако возможность перехвата информации не всегда создает возможности получения доступа к защищенным данным, с последующей модификацией. В качестве примера перехвата информации может выступать анализ сетевого трафика в сети. В данном случае злоумышленник получает информацию о сети предприятия, но возможность искажать данную информации не имеет. Проблемы безопасности данных также связаны с развитием глобальной сети.
Интернет, которая пользуется популярностью среди различных категорий пользователей. Усиление глобализации, а вместе с тем и информатизации
создает возможности для злоумышленника с любой точки мира создавать угрозы безопасности для компьютерной сети.

К основным задачам информационной безопасности данных относятся:
• обеспечение конфиденциальности, целостности и структурированности информации;
• организация своевременного выявления и предотвращения внешних и внутренних угроз;
• внедрение организационных, инженерно-технических, аппаратно-программных методов, позволяющих усилить защиту данных;
• разработка и совершенствование политики безопасности с учетом современных тенденций развития аппаратного и программного обеспечения.

1. Vekhov V.B., Pastukhov P.S. Crimes in the information community: improving investigations based on the provisions of electronic criminalistics // ex-jure. 2018.
2. Marinkin D.N. Problems of information security and cryptography of the modern blockchain user // Problems of law enforcement. 2019.
3. Malanichev D.M., Mochalov V.V., Huseynov D. A. The use of noise-like signals to ensure information security. Annual International Scientific and Technical Conference of Security Systems. 2019.
4. Plenkin A. P. Using a quantum key to protect a telecommunications network // Technical sciences - from theory to practice. 2019.
5. Filyak P.Yu., Fedirko S.N., Kostina E. A. Ensuring information security using graph databases and graph systems of knowledge representation and management. Information and security. 2018