Молдавский Государственный Университет

Факультет Математики и Информатики

Департамент Информатики

**Лабораторная работа**

**Необходимость создания безопасных АИС.**

Выполнен студентом II курса

специальности Informatică (Științe ale Educației)

**Михайлов Пётр**

Преподаватель

**Анатолий Гладей**

Кишинёв, 2025

**Введение**

В современном мире автоматизированные информационные системы (АИС) играют важнейшую роль в различных сферах деятельности: от финансовых организаций и государственных структур до медицинских учреждений и промышленных предприятий. Однако с ростом цифровизации и глобальной взаимосвязанности возрастает и число киберугроз, которые могут нанести значительный ущерб как отдельным пользователям, так и целым организациям. Именно поэтому создание безопасных АИС становится необходимым условием для стабильного функционирования современной экономики и общества.

**Основные угрозы безопасности АИС**

Основной причиной необходимости защиты АИС является наличие множества угроз. Во-первых, кибератаки и взломы становятся все более изощренными, включая фишинг, вредоносное ПО и атаки «отказ в обслуживании» (DDoS), которые могут привести к утечке данных, финансовым потерям и сбоям в работе систем. Во-вторых, инсайдерские угрозы также представляют значительную опасность, поскольку ошибки или злонамеренные действия сотрудников могут стать причиной компрометации данных или нарушения работы системы. В-третьих, вирусы и вредоносное ПО способны повредить или уничтожить данные, что приведет к потере ценной информации. В-четвертых, отсутствие должных мер аутентификации и шифрования делает систему уязвимой перед несанкционированным доступом злоумышленников. Наконец, уязвимости в программном обеспечении требуют регулярных обновлений и исправления ошибок, чтобы предотвратить возможные атаки.

Кроме того, с развитием технологий появляются новые формы атак. Например, атаки на цепочки поставок (supply chain attacks) позволяют злоумышленникам внедрять вредоносный код еще на этапе разработки программного обеспечения. Также киберпреступники все чаще используют методы социальной инженерии, манипулируя людьми для получения доступа к конфиденциальной информации. Все эти факторы делают кибербезопасность АИС критически важной задачей.

**Принципы защиты АИС**

Для минимизации рисков и обеспечения защиты информации при разработке и эксплуатации АИС необходимо следовать ряду ключевых принципов. Конфиденциальность является основой безопасности, так как данные должны быть доступны только тем пользователям, которые имеют соответствующие права. Целостность информации должна обеспечиваться механизмами защиты от несанкционированного изменения данных. Доступность системы играет важную роль в бесперебойной работе организаций и предотвращении атак, направленных на дестабилизацию работы.

Для усиления безопасности важно внедрять многофакторную аутентификацию, что поможет снизить вероятность взлома учетных записей. Современные криптографические алгоритмы обеспечивают защиту данных от перехвата и расшифровки злоумышленниками. Регулярное обновление программного обеспечения и исправление выявленных уязвимостей позволяют устранить потенциальные угрозы и поддерживать высокий уровень защиты системы. Важным элементом защиты также является мониторинг активности пользователей, анализ логов и своевременное выявление аномального поведения.

**Будущее кибербезопасности АИС**

Помимо технических аспектов защиты, важную роль играет обучение сотрудников и пользователей безопасному поведению в сети. Многие успешные кибератаки происходят из-за человеческого фактора – слабых паролей, использования незащищенных устройств и открытия вредоносных ссылок. Организации должны регулярно проводить тренинги по кибербезопасности, чтобы повышать осведомленность своих сотрудников и минимизировать вероятность успешных атак. Кроме того, создание резервных копий данных и их хранение в защищенных местах позволяет восстановить информацию в случае повреждения или утраты.

Будущее безопасности АИС связано с развитием искусственного интеллекта и машинного обучения. Современные системы анализа данных способны обнаруживать подозрительную активность и реагировать на угрозы в режиме реального времени, что значительно повышает уровень защиты. Интеграция таких технологий с традиционными методами кибербезопасности позволит создавать более надежные системы, способные адаптироваться к новым видам атак и угроз. Также важно учитывать правовые аспекты защиты информации. Государства разрабатывают законодательные акты и регуляторные нормы, направленные на обеспечение информационной безопасности, например, такие как GDPR в Европе или Федеральный закон о защите персональных данных в России. Соблюдение этих стандартов способствует не только защите данных, но и укреплению доверия пользователей к цифровым системам.

Кроме того, развитие квантовых технологий ставит перед специалистами новые задачи. Квантовые компьютеры в перспективе могут угрожать традиционным криптографическим алгоритмам, что потребует внедрения новых методов защиты данных. Уже сейчас ведутся исследования в области постквантовой криптографии, которая обеспечит безопасность информации даже в условиях использования квантовых вычислений.

**Заключение**

Создание безопасных автоматизированных информационных систем является необходимым условием для стабильного функционирования организаций и защиты данных пользователей. В условиях постоянного развития технологий и появления новых угроз важно уделять внимание комплексным мерам безопасности, включая защиту от кибератак, контроль доступа, шифрование данных и регулярное обновление программного обеспечения. Только интегрированный подход к кибербезопасности позволит минимизировать риски и обеспечить надежную защиту информации в цифровую эпоху.

Помимо технических аспектов, большое значение имеет обучение пользователей и внедрение современных технологий, таких как искусственный интеллект, что в будущем позволит создавать более устойчивые и защищенные системы. Также важно учитывать развитие законодательных инициатив в сфере информационной безопасности, поскольку регулирование киберпространства становится ключевым элементом защиты данных на международном уровне. Комплексный подход к кибербезопасности поможет создать надежные и устойчивые АИС, соответствующие современным вызовам и требованиям. Внедрение новых технологий, таких как квантовая криптография и усовершенствованные системы анализа данных, позволит повысить уровень защиты и адаптироваться к угрозам будущего.