УДК 00.004.03

Кудяков Марат Ильдарович

Магистрант, Лениногорского филиала Казанского национального исследовательского технического университета имени А. Н. Туполева.

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫЗ СИСТЕМ

Аннотация. В современном мире, где информационные угрозы становятся все более частым явлением, защита автоматизированных систем становится ключевым фактором обеспечения безопасности производства и сохранности конфиденциальной информации. В данной статье рассматривается методы обеспечения безопасности автоматизированных систем в условиях их защищенного исполнения, современные подходы к распределению ресурсов и изоляции критических компонентов системы в виде физического, программного и организационного характера, их классификация и способы оценивания. Также были определены методики повышения достоверности получаемой информации, которая является важнейшим фактором принятия обоснованных решений в различных сферах.

Annotation. In the modern world, where information threats are becoming more and more common, the protection of automated systems is becoming a key factor in ensuring production safety and the safety of confidential information. This article examines methods for ensuring the safety of automated systems in the conditions of their secure execution, modern approaches to the distribution of resources and isolation of critical components of the system in the form of physical, software and organizational nature, their classification and evaluation methods. Methods for increasing the reliability of the information received, which is the most important factor in making informed decisions in various areas, were also identified.

Ключевые слова: автоматизированные системы, угрозы, методы защиты, информация, аттестация систем.

Keywords: automated systems, threats, protection methods, information, system certification.

Современные автоматизированные системы (АС) играют ключевую роль в функционировании различных отраслей экономики, включая финансовый сектор, здравоохранение, транспорт и многие другие. С ростом зависимости от технологий и автоматизации возрастает и угроза кибератак, что делает защиту информации и систем жизненно важной задачей. В условиях быстро меняющегося технологического ландшафта и растущих требований к безопасности становится очевидной актуальность разработки и внедрения эффективных методов защиты автоматизированных систем.

В данной работе рассматриваются современные методы защиты автоматизированных систем и их безопасного исполнения (АСЗИ). Основное внимание уделено анализу ключевых подходов к повышению надежности информации, что является основополагающим аспектом в обеспечении безопасности данных. Также будет освещена важность аттестации и сертификации систем, поскольку эти процессы играют решающую роль в подтверждении соответствия систем установленным стандартам безопасности и обеспечении доверия пользователей.

Работа включает несколько ключевых тем, которые помогут лучше понять предметную область. В первой части будет представлено введение в методы защиты автоматизированных систем, где будут рассмотрены основные понятия и принципы, лежащие в основе защиты информации. Далее будет проведена классификация методов защиты, которая позволит систематизировать существующие подходы и выделить наиболее эффективные из них.

Одной из центральных тем работы станет обсуждение методов повышения надежности информации. В условиях, когда данные становятся основным активом организаций, обеспечение их целостности и надежности становится критически важным. В этой части работы будут рассмотрены как технические, так и организационные меры, направленные на защиту информации от несанкционированного доступа и искажения.

Также важное место в исследовании займет сертификация и аттестация автоматизированных систем. Эти процессы не только подтверждают соответствие систем требованиям безопасности, но и способствуют повышению уровня доверия со стороны пользователей и клиентов. В рамках работы будет проанализирован процесс сертификации, его этапы и значение для обеспечения безопасности.

Также будут подробно рассмотрены физические меры защиты автоматизированных систем, программные меры защиты и организационные меры безопасности. Физические меры включают защиту оборудования и инфраструктуры, программные меры охватывают использование антивирусных программ, межсетевых экранов и других средств защиты, а организационные меры касаются разработки политик безопасности и обучения персонала.

Таким образом, данная работа направлена на углубление знаний об инструментах и методах обеспечения информационной безопасности, используемых для обеспечения безопасности автоматизированных систем. Методы защиты автоматизированных систем (АС) должны обеспечивать высокий уровень безопасности и устойчивости к внешним и внутренним угрозам. Важно, чтобы они были многоуровневыми и комплексными, охватывающими различные аспекты информационной безопасности.

Аутентификация пользователей является одним из основополагающих методов защиты системы. Этот процесс подразумевает проверку личности пользователя с использованием различных средств, таких как пароли и биометрические данные. Использование многофакторной аутентификации значительно усиливает защиту, снижая вероятность несанкционированного доступа [3].

Регулирование доступа к информации и ресурсам системы имеет решающее значение. Необходимо внедрять политики, определяющие права доступа для различных категорий пользователей. Это не только защищает данные, но и гарантирует, что только уполномоченные лица могут выполнять определенные действия в системе.

Шифрование данных является важным инструментом защиты информации от несанкционированного доступа при передаче и хранении. Современные алгоритмы шифрования обеспечивают высокий уровень защиты, соответствующий требованиям законодательства и стандартам безопасности.

Сегментация сети — метод, который помогает повысить безопасность AS. Разделение сети на более мелкие сегменты помогает ограничить распространение угроз и изолировать критически важные данные. Это означает, что в случае возникновения инцидента безопасность оставшихся сегментов не будет скомпрометирована.

Сертификация и аттестация автоматизированных систем являются обязательными. Эти процессы не только помогают оценить текущий уровень безопасности, но и выявляют уязвимости, которые необходимо устранить. Сертификация позволяет проверить, что системы соответствуют требованиям и стандартам, что значительно повышает доверие пользователей к АС.

Совокупность технических и административных мер безопасности формирует комплексную и эффективную стратегию защиты. Технические меры, такие как внедрение систем обнаружения вторжений и средств контроля сетевого трафика, активно работают в тандеме с административными мерами, включая обучение персонала и разработку политик безопасности.

Таким образом, объединение всех этих методов в единую стратегию позволяет существенно повысить уровень защиты автоматизированных систем, сделав их более устойчивыми к различным угрозам и атакам. Важно помнить, что в динамично меняющейся среде, вызванной развитием технологий и угрозами, необходимость обновления этих методов становится особенно актуальной.

Современные методы защиты автоматизированных систем (АС) базируются на их классификации, которая играет важную роль в определении подхода к обеспечению информационной безопасности. Классификация АС подразумевает разделение на группы в зависимости от уровней защищенности и условий эксплуатации. Согласно утвержденному документу, выделяется девять

классов автоматизированных систем. Например, к классам 1А–1D относятся системы, доступные нескольким пользователям, где значимость обрабатываемых данных различается [7]. Второй класс системы с равными правами доступа пользователей охватывает категории 2А и 2Б, что позволяет формировать соответствующие механизмы защиты.

Методы защиты информации могут включать как аппаратные и программные решения, так и организационные меры. Системы защиты информации (СЗИ) противодействуют несанкционированному доступу и обеспечивают сохранность данных [2]. Использование методов предотвращения потери данных и контроля физического доступа к оборудованию является важной частью комплексной безопасности систем, обеспечивая дополнительные уровни защиты при эксплуатации АС [5].

Следует отметить, что реализация методов защиты требует регулярного проведения аудитов. Оценка эффективности существующих мер и выявление недостатков позволяют проводить необходимые улучшения и адаптацию защитных механизмов к изменяющимся условиям угроз. Участие квалифицированного персонала и периодическое повышение уровня его знаний также способствуют успешному внедрению и поддержанию системы безопасности [2].

Современные стандарты безопасности определяют требования к различным классам АС, что имеет решающее значение для обеспечения их надежной работы и защиты от возможных угроз. Также существует необходимость в интеграции различных подходов к защите, включающих как технические, так и организационные меры, что позволяет достичь более высокого уровня безопасности данных в автоматизированных системах любого типа [4].

В заключение следует отметить, что понимание классификации методов защиты и их дальнейшая реализация в автоматизированных системах занимают важное место в области обеспечения информационной безопасности. Успешная

эксплуатация АС возможна только при комплексном учете всех перечисленных факторов, а также постоянном совершенствовании используемых методов [8].

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 19791-2008

2. Классификация методов защиты информации и их применение в сфере информационной безопасности автоматизированных систем / А.Ю. Нестеров, Г.Г. Палтаджян, В.М. Кравченко, К.Е. Шукалович / Вестник науки и образования. 2024. №1 (144)-1.

3. Курочкин Ю.А. Надежность и диагностирование цифровых устройств и систем. – М.: Энергоатомиздат, 1993. – 240 с.

4. Меры по обеспечению безопасности и защиты информации для сложных информационных систем / Л. Г. Осовецкий, А. В. Суханов, В. В. Ефимов / Системы управления, связи и безопасности. 2017. №1.

5. Милосердов П.С. "Электронное учебное пособие «Программно-аппаратные средства защиты»" // Гаудеамус. 2014. №2 (24), 183-184 с.

6. Надежность АСУ. Учеб. пособие для ВУЗов / Под ред. Я.А. Хетагурова. – М.: Высшая школа, 1979. – 287 с.

7. Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации" от 30.03.1992 // Федеральная служба по техническому и экспортному контролю

8. Северцев Н.А. Надежность систем в эксплуатации и отработке. Учебник для ВУЗов. – М.: Энергоатомиздат, 1989. – 140 с

List of references

1. GOST R ISO/MEQ TOO 19791-2008

2. Classification of information protection methods and their application in the field of information security of automated systems / A.Yu. Nesterov, G.G. Paltajyan, V.M. Kravchenko, K.E. Shukalovich / Vestnik nauki i obrazovanie. 2024. №1 (144)-1.

3. Kurochkin, Yu.A. Reliability and diagnostics of the digital devices and systems. - Moscow: Energoatomizdat, 1993. - 240 c.

4. Measures to ensure security and information protection for complex information systems / L. G. Osovetsky, A. V. Sukhanov, V. V. Efimov // Systems of management, communication and security. 2017. №1.

5. Miloserdov, P.S. ‘Electronic tutorial «Software and hardware means of protection» / / Gaudeamus. 2014. №2 (24), 183-184 c.

6. Reliability of ACS. Textbook for universities // Edited by Y.A. Khetagurov. - Moscow: Higher School, 1979. - 287 c.

7. Guiding document ‘Automated systems. Protection against unauthorised access to information. Classification of automated systems and information protection requirements’ dated 30.03.1992 // Federal Service for Technical and Export Control.

8. Severtsev N.A. Reliability of systems in operation and development. Textbook for higher educational establishments. - Moscow: Energoatomizdat, 1989. - 140 c