УДК 004.777

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

Габриелева Е. Г.

гр. 274003

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Шаронова Е. И. – ведущий инженер-программист ОСТО ЦИИР

Аннотация. В настоящее время защита информации в автоматизированных системах обработки информации является критически важной, так как множество данных хранится и обрабатывается в электронной форме, и их утечка или

компрометация может иметь серьёзные последствия. В данной статье рассматриваются основные угрозы кибербезопасности, методы по их преодолению и защите информации.

Ключевые слова: защита информации, автоматизированные системы обработки информации, шифрование

Введение. В современном мире защита информации в автоматизированных системах обработки информации (АСОИ) является важным вопросом, так как АСОИ содержат большое количество конфиденциальных данных. Преимущества таких автоматизированных систем включают увеличение эффективности работы: автоматизация позволяет выполнять задачи быстрее и точнее, по сравнению с ручным вводом и обработкой информации. Автоматизация помогает устранять ошибки, связанные с человеческим фактором, такие как опечатки или неверное внесение данных, что улучшает качество и надёжность информации. Данная система также позволяет снизить затраты на ручную обработку данных и на документооборот. В целом, автоматизированные системы обработки информации помогают улучшить эффективность и надёжность работы, ускорить процессы и снизить риски ошибок, они способствуют улучшению принятия решений и координации работы в организации [1].

Однако наряду с вышеперечисленными преимуществами существует перечень проблем, возникающих в связи с увеличением объёмов информации и возрастающими угрозами в сфере кибербезопасности. Именно поэтому обеспечение надёжной защиты информации становится жизненно важным и особенно актуальным.

Основная часть. Все угрозы в автоматизированных системах обработки информации, как показано на рисунке 1, делятся на непреднамеренные и преднамеренные. Первые чаще всего связаны с факторами внешней среды, а вторые – с незаконными действиями злоумышленников. Преднамеренные угрозы являются куда более опасными, чем непреднамеренные, так как данные могут быть не только уничтожены, но ещё и захвачены злоумышленниками.

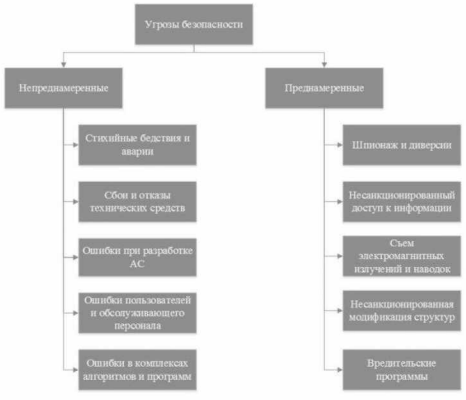

Рисунок 1 – Угрозы кибербезопасности

Далее подробнее рассмотрим самые распространённые угрозы кибербезопасности:

1. Атака на конфиденциальность: нападающие могут пытаться получить несанкционированный доступ к конфиденциальным данным;

2. Атаки на целостность: злоумышленники могут изменять или подделывать данные в автоматизированных системах;

3. Атака на доступность: целью таких атак является нарушение функционирования автоматизированных систем, чтобы лишить их пользователей доступа к сервисам или ресурсам;

4. Вирусы и вредоносные программы: атакующие могут внедрять вирусы и другие вредоносные программы в автоматизированные системы для получения контроля над ними или для нанесения вреда.;

5. Атака типа «отказ в обслуживании» (DDoS): злоумышленники могут использовать бот-сети, чтобы создать огромное количество запросов на сервер, перегружая его и вызывая отказ в обслуживании для легитимных пользователей, что может привести к временной недоступности системы или сервиса;

6. Сетевая атака: взломщики могут попытаться получить доступ в автоматизированные системы через сетевые уязвимости. Это может включать перехват данных, подделку пакетов или взлом сетевых устройств [2].

Все виды перечисленных угроз влекут за собой потерю или утечку данных, финансовые потери или нарушение работы систем. Это может нанести серьёзный ущерб бизнесу или привести к неправильным решениям, основанным на искажённых данных. Поэтому необходимо принимать ряд мер по защите автоматизированных систем.

Выстраивая систему защиты информации в автоматизированных информационных системах корпорации, IT-специалист может использовать различные методы, одновременное применение которых позволяет решать поставленные задачи. Они делятся на следующие подгруппы:

1. Защита данных от утраты в результате аварий или сбоя оборудования;

2. Контроль возможности физического доступа к аппаратуре, панелям управления и сетям, в результате которого возможно повреждение оборудования, хищение информации, намеренное создание аварийных или нештатных ситуаций, установка закладных устройств, позволяющих считывать звуковые и электромагнитные волны;

3. Аутентификация пользователей, программ, съёмных носителей информации;

4. Криптография: использование шифрования данных и цифровых подписей для обеспечения целостности и подлинности данных;

5. Защита сетей и связанных с ними ресурсов от несанкционированного доступа, что включает в себя использование сетевых файерволов, шифрования сетевого трафика, обнаружение вторжений;

6. Аудит и контроль: регулярное проведение аудитов системы для выявления возможных уязвимостей и слабых мест, а также постоянный контроль и мониторинг доступа к информации и действий пользователей;

7. Резервное копирование и восстановление в случае потери или повреждения [3].

Все эти меры должны быть комбинированы и подстроены под конкретные требования и характеристики автоматизированной системы обработки информации для наилучшего обеспечения защиты информации.

Рассмотрим один из надёжных способов защиты информации – её шифрование. Шифрование данных – это преобразование информации, делающее её нечитаемой для посторонних. Существует два основных вида шифрования: симметричное и асимметричное.

Симметричное шифрование для шифрования и дешифрования данных использует один и тот же криптографический ключ. Такой метод прост в работе и понимании, техническая нагрузка на оборудование невелика, и таким образом обеспечивается высокая скорость и надёжность шифрования. К недостаткам

относится сложность обмена ключами: при успешном перехвате ключа злоумышленник получит неограниченный доступ к зашифрованной информации. Advanced Encryption Standard (AES) – это симметричный алгоритм шифрования, использующий ключевое преобразование для защиты данных. Он обеспечивает высокую степень безопасности и эффективность.

Асимметричное шифрование – это метод шифрования данных, предполагающий использование двух ключей: открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и проверки электронной подписи. Закрытый (приватный) ключ применяется для подписания и расшифровки данных, зашифрованных открытым ключом. RSA (алгоритм шифрования с открытым ключом) - это асимметричный алгоритм, который широко используется для шифрования обмена ключей и цифровой подписи [4].

Вне зависимости от выбранного вида шифрования, ни один из них не является гарантом стопроцентной безопасности. Поэтому нужно помнить, что любой подход нужно комбинировать с другими средствами информационной защиты.

Заключение. Данная статья поможет читателям понять, какие меры необходимы для обеспечения безопасности информации в АСОИ, и научит применять соответствующие методы по её защите.

Список литературы

1. Сергеев, М. К. Автоматизированные системы обработки информации и управления // Актуальные исследования. – 2023. – №24 (154). – Ч.I. С. 58–63.

2. . Иванов, К. К. Угрозы безопасности информации в автоматизированных системах / К. К. Иванов, Р. Н. Юрченко, А. С. Ярмонов. — Текст: непосредственный // Молодой ученый. – 2016. – №29 (133). – С. 20–22.

3. Сайт компании Smart-Soft [Электронный ресурс] / Защита информации в автоматизированных системах. – 2020. – Режим доступа: https://www.smart-soft.ru/blog. – Дата доступа: 13.10.2023.

4. Сайт компании Индид [Электронный ресурс] / Шифрование. – 2022. – Режим доступа: https://indeed-company.ru/blog/shifrovanie/. – Дата доступа: 13.10.2023.

UDC 004.777

INFORMATION SECURITY IN AUTOMATED INFORMATION PROCESSING SYSTEMS

Gabrieleva E. G.

gr.274003

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Sharonova E. I. – Senior Engineer-Programmer at OSTO CIIR

Annotation. Currently, information security in automated information processing systems is critically important, as a vast amount of data is stored and processed in electronic form, and their leakage or compromise can have serious consequences. This article examines the main cyber threats, methods to overcome them, and information security measures.

Keywords: information security, automated information processing systems, encryption