УДК 0.004.056.52

*Е. Д. Колосов, А. С. Ткачев, А. О. Леухин, А. В. Кауров**

ВЛИЯНИЕ СИСТЕМНОГО АНАЛИЗА НА ЗАЩИТУ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

В современном мире становится все больше различных систем, сильно влияющих на жизнь людей. В данном случае под системой может пониматься как предприятие в целом, так и какое-либо программное обеспечение. Системы выполняют различные задачи и, как правило, могут быть очень сложными и состоять из множества других подсистем. Отсюда можно сделать вывод, что система – это совокупность взаимосвязанных компонентов (подсистемы, отношения между компонентами), взаимодействующих между собой для выполнения поставленных задач.

Системы могут быть как обычными, так и критически важными. К таким системам можно отнести:

– банковские системы;

– системы телекоммуникации;

– системы управления воздушным и наземным транспортом;

– системы обработки и хранения секретной и конфиденциальной информации.

На самом деле подобных критически важных систем гораздо больше. Объединяет их то, что «для нормального и безопасного функционирования этих систем необходимо поддерживать их безопасность и целостность» [1].

Защита информации в таких системах является одной из важнейших задач.

Перед тем, как приступать к обеспечению защиты информации в системе, предлагается использовать такой инструмент, как системный анализ. Под системным анализом понимается совокупность методологических средств, используемых для подготовки и обоснования решений проблем, связанных с функционированием сложных систем.

* Работа выполнена под руководством доктора технических наук, профессора ФГБОУ ВО «ТГТУ» В. В. Алексеева.

Цель системного анализа состоит в том, чтобы выявить первопричину нежелательных событий, возникающих во время работы системы. Кроме того, необходимо будет разрабатывать ряд мероприятий, которые либо уменьшают вероятность появления этих событий, либо полностью исправляют возникшую проблему.

Системный анализ можно применять в двух случаях:

1. На этапе проектирования системы;

2. В функционирующей системе.

В первом случае анализ выполняется до наступления нежелательных событий, т.е. происходит прогнозирование возможных проблем. Такой анализ называется априорным.

Во втором случае анализ выполняется, как правило, после наступления нежелательных событий и называется апостериорным. Одной из целей данного анализа является разработка рекомендаций по избеганию подобных проблем в будущем.

В обоих случаях системный анализ включает ряд основных шагов по устранению проблемы:

1. Определение проблемы. Это включает в себя определение масштаба проблемы и выявление проблемных областей. Очень важно собрать всю необходимую информацию о данной проблеме для ее полного понимания;

2. Анализ проблемы. Данный шаг подразумевает анализ всех данных для выявления первопричины проблемы;

3. Разработка потенциального решения. На данном этапе происходит разработка и разбор всех возможных решений проблемы. Определяются их плюсы и минусы;

4. Оценка потенциального решения. Здесь происходит оценка каждого решения. Могут учитываться различные факторы, такие как стоимость, сложность реализации, влияние на другие компоненты системы и многие другие;

5. Реализация решения. Финальный шаг, который включает в себя внедрение выбранного решения и мониторинг его эффективности в течение определенного времени;

6. Составление документации. Необязательный шаг, который подразумевает документирование проблемы и ее решения. Пишутся рекомендации по избеганию подобных проблем в будущем.

Следуя этим шагам, можно обеспечить правильное функционирование системы.

Какие-либо шаги при проведении системного анализа могут добавляться или изменяться. Все зависит от самой системы.

При выполнении системного анализа одной из главных задач является реализация безопасности и целостности системы. В первую очередь, необходимо оценить риски и определить уязвимости системы.

Применение системного анализа позволяет определить факторы, влияющие на производительность и надежность системы, а также выявить угрозы безопасности и возможные пути их решения. Для этого необходимо провести анализ данных, проанализировать существующие угрозы и уязвимости, а также разработать стратегию повышения безопасности системы. Следует понимать, что нарушение информационной безопасности системы может привести к потере данных, нарушению репутации, а также к финансовым потерям.

Как видно, системный анализ помогает определить множество проблем в системе, включая проблемы, связанные с защитой информации.

После применения системного анализа можно приступать к поиску средств защиты информации (СЗИ). Сейчас существуют различные СЗИ. Например, аппаратные и программные средства, физические меры, организованные мероприятия, законодательные меры. Средства защиты делятся на технические и нетехнические.

К аппаратным методам защиты можно отнести электронные, электронно-механические и электронно-оптические устройства. Таких средств сейчас создано довольно много. Наиболее распространенными считаются следующие виды защиты:

– специальные реестры для хранения реквизитов защиты паролей, идентифицирующих кодов и т.п.;

– генераторы кодов, предназначенных для автоматического генерирования идентифицирующего кода устройства;

– устройства измерения индивидуальных характеристик человека (голоса, отпечаток) с целью его идентификации;

– специальные биты секретности, значение которых определяет уровень секретности информации, хранимой техническим устройством, которому принадлежат данные биты;

– схемы прерывания передачи информации в линии связи с целью периодической проверки адреса передачи данных.

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации.

Шифрование информации заключается в том, что информация преобразуется в такой вид, при котором нельзя определить ее содержание.

Основные направления работ по рассматриваемому аспекту защиты можно сформулировать таким образом:

– выбор рациональных систем шифрования для надежного закрытия информации;

– обоснование путей реализации систем шифрования в автоматизированных системах;

– разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем;

– оценка эффективности криптографической защиты.

К программным методам защиты можно отнести особые программы, выполняющие функции защиты данных, например, от вредоносных программ. Чаще всего используют именно программные средства защиты, так как они являются более универсальными и простыми в использовании.

Резервное копирование также является одним из основных СЗИ. Оно предназначено для хранения копий данных или программ на каком-либо носителе. Резервное копирование необходимо для восстановления программ или данных в оптимальное состояние после повреждений в результате сбоя или хакерских атак.

К организационным мерам можно отнести обучение пользователей. Пользователи должны быть обучены, как правильно работать с информацией, как обнаруживать и сообщать об угрозах безопасности и какие меры безопасности следует принимать при работе с конфиденциальной информацией.

В заключение можно сказать, что каким бы превосходным не оказался системный анализ, какие СЗИ не использовались бы, полной гарантии безопасности информации быть не может, но при этом сильно увеличится уровень готовности системы к различным проблемам.

Список литературы

1. Прокофьев, О. В. Защита информации и информационная безопасность / О. В. Прокофьев. – 2019. – 240 с.

Межвидовый центр подготовки и боевого применения войск РЭБ
(*учебный и испытательный*)