***Веденеев Илья Александрович***

*студент 5 курса института энергетики и автоматизированных систем,*

*ФГБОУ ВО «МГТУ им. Г.И. Носова»,*

*г. Магнитогорск*

*Научный руководитель* ***Мазнин Дмитрий Николаевич,***

*старший преподаватель кафедры информационной безопасности,*

*ФГБОУ ВО «МГТУ им. Г.И. Носова»,*

*г. Магнитогорск*

# ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

**Аннотация.** В статье рассматривается защита информации в автоматизированной системе управления. Для получения наиболее высоких результатов своей деятельности предприятия переходят на автоматизацию технологических процессов. Защита автоматизированной системы управления технологическим процессом - это процесс, целью которого является обеспечение информационной безопасности технологических процессов.

**Ключевые слова:** автоматизированные системы, защита, технологический процесс, управление.

Защита автоматизированной системы управления технологическим процессом (АСУТП) – это процесс, целью которого является обеспечение информационной безопасности (ИБ) технологических процессов, т.е. ограждение их от любой угрозы информационного характера, мешающей им проходить в установленном порядке.

Необходимость обеспечения ИБ АСУТП устанавливает Приказ №31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах

управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [10], который устанавливает требования к обеспечению защиты информации, обработка которой осуществляется АСУТП на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

В рамках Приказа определяется многоуровневая структура АСУТП, приведенная на рисунке 1. Данная структура АСУТП включает 3 основных уровня. В качестве объектов защиты АСУТП выделяются:

- критически важная информация;
- программно-технический комплекс.

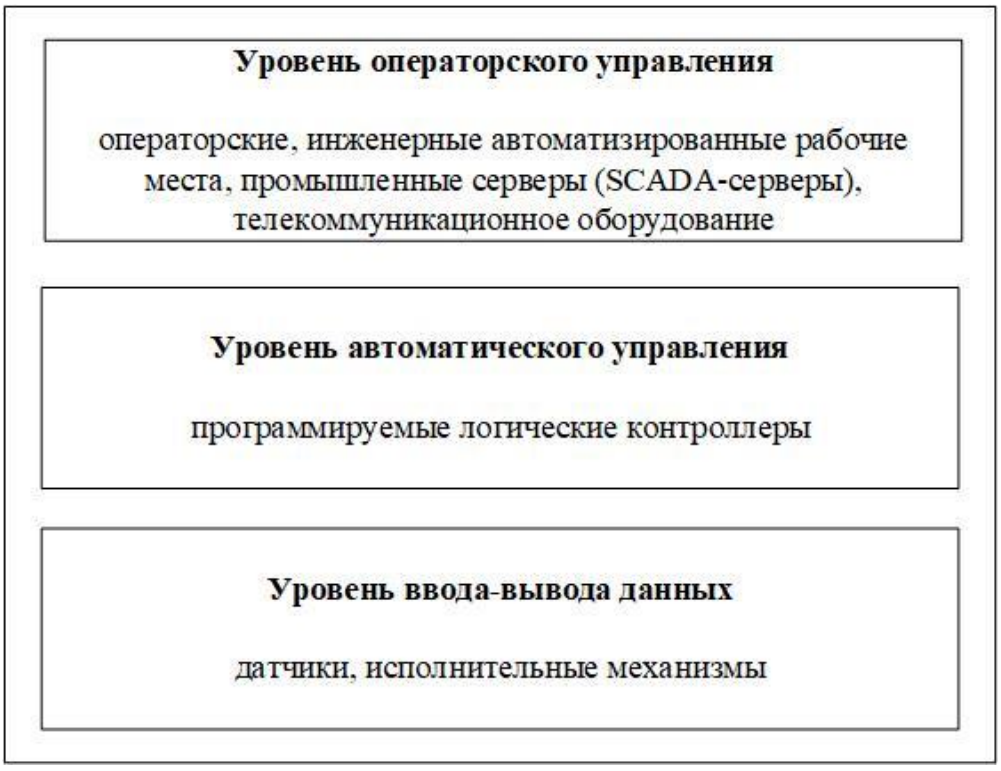


Рисунок 1 - Структура АСУТП

В соответствии с Приказом защита информации, обрабатываемой в АСУТП, является составной частью работ по ее созданию и эксплуатации и обеспечивается на всем пути ее создания и в ходе эксплуатации путем применения организационных и технических мер защиты информации. При этом они должны:

- обеспечивать конфиденциальность, доступность и целостность информации;
- соотноситься с мерами обеспечения безопасности АСУТП [2,11].

Помимо этого, используемые меры защиты не должны негативно сказываться на штатном режиме функционирования АСУТП.

Выделяется 5 основных этапов обеспечения защиты информации в АСУТП (рисунок 2).

На этапе формирования требований проводится классификация АСУТП и определение класса защищенности: К 1 (высокий), К 2 (средний) или К 3 (низкий).

Для определения класса защищенности определится уровень значимости (УЗ) обрабатываемой в АСУТП информации в зависимости от степени возможного ущерба от нарушения конфиденциальности, целостности или доступности.


Рисунок 2 - Этапы обеспечения защиты информации в АСУТП

В случае, если в АСУТП обрабатывается информация двух и более видов, то УЗ определяется отдельно для каждого вида. Итоговый УЗ определяется по наивысшему значению из них или может быть установлен отдельно для каждого из уровней АСУТП.

Определение угроз безопасности информации (УБИ) осуществляется на каждом из уровней АСУТП и должно включать:

- оценку возможностей нарушителей;
- анализ уязвимостей АСУТП

- анализ сценариев реализации УБИ;
- анализ последствий от нарушения свойств безопасности.

В качестве исходных данных при определении УБИ используется банк данных УБИ.

Требования к системе защиты АСУТП определяются в зависимости от класса защищенности и актуальных УБИ, включенных в модель угроз безопасности информации [1,3,7].

На этапе разработки системы защиты осуществляется выбор средств защиты информации (СЗИ), сертифицированных ФСТЭК, и определяются необходимые меры защиты с учетом особенностей функционирования ПО и технических средств АСУ ТП.

Ввод системы защиты информации в эксплуатацию состоит из следующих мероприятий:

- настройка ПО АСУТП;
- разработку документов, определяющих правила и процедуры, реализуемые для защиты информации;
- внедрение организационных мер защиты информации;
- установку и настройку СЗИ;
- проведение предварительных испытаний, опытной эксплуатации и приемочных испытаний системы;
- опытную эксплуатацию системы защиты автоматизированной системы управления;
- анализ уязвимостей АСУТП;
- приемочные испытания системы защиты автоматизированной системы управления.

Этапы обеспечения защиты информации в ходе эксплуатации системы защиты и при выводе ее из действия предусматривают проведение определенных процедур управления ИБ, таких как:

- планирование мероприятий по обеспечению защиты в АСУТП;
- обеспечение действий в нештатных ситуациях;
- обучение персонала;
- анализ УБИ и рисков от их реализации;
- выявление инцидентов и реагирование на них;
- контроль за обеспечением УЗ;
- управление системой защиты и конфигурацией АСУТП;
- архивирование информации, уничтожение данных и остаточной информации при выводе АСУТП из эксплуатации.

*СПИСОК ЛИТЕРАТУРЫ*

*1. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия //Актуальные проблемы современной науки, техники и образования. – 2017. – Т. 1. – С. 217-220.*

*2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. DLP система: защита от утечки информации. Анализ поиска WORDSEARCH //Актуальные проблемы современной науки, техники и образования. – 2016. - Т. 1. - № 1. – С. 187-191.*

*3. Коновалов М.В., Михайлова У.В., Хусаинов А.А., Санарбаев Р.Ж. Алгоритмы шифрования данных //Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2. - № 71. – С. 159-161.*

*4. Лукьянов Г.И., Михайлова У.В. Эффективность применения СЗИ от утечки по акустическим каналам //Вестник УрФО. Безопасность в информационной сфере. – 2014. - № 4 (14). – С. 14-18.*

*5. Лукьянов Г.И., Михайлова У.В., Баранкова И.И., Коновалов М.В. Защита информации по виброакустическим каналам с использованием СЗИ «СОНАТА» // Актуальные проблемы современной науки, техники и образования. – 2015. – Т. 2. – № 1. – С. 186-188.*

*6. Михайлова У.В., Аименева А.А., Полехина А.В. Технические средства защиты информации //Актуальные проблемы современной науки, техники и образования. – 2012. – Т. 2. – № 70. – С. 27-30.*

*7. Михайлова У.В., Поступная А.П., Хасанова Е.Р. Защита информации по виброакустическим каналам // Актуальные проблемы современной науки, техники и образования. – 2012. – Т. 2. – № 70. – С. 31-33.*

*8. Михайлова У.В., Ершов В.А. Способы организации и методы противодействия DOS/DDOS – атакам //Безопасность информационного пространства: сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. – Челябинск: ЮрГУ. – 2015. – С. 73-79.*

*9. Михайлова У.В., Лукьянов Г.И. Эффективность применения СЗИ от утечки по акустическим каналам //Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 4 (14). – С. 14-18.*

*10. Михайлова У.В., Хусаинов А.А. Особенности и проблемы, возникающие при разработке моделей угроз информационной безопасности //Безопасность информационного пространства: сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. – Курган: КГУ. – 2016. – С. 72-75.*

*11. Mikhailova U.V., Saigushev N.Ya., Vedeneeva O.A., Tsaran A.A. Information systems at enterprise. Design of secure network of enterprise // Journal of Physics: Conference Series. – 2018. – Т. 1015. pp. 042054.*