А.А. Бабенко, Д.А. Магомедов

ОЦЕНКА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

(Волгоградский государственный университет)

Аннотация: В данной работе проведен анализ автоматизированных систем управления технологическим процессом, определены угрозы информационной безопасности АСУ ТП, а также проанализированы основные средства защиты информационной безопасности АСУ ТП. Рассмотрены основные методы оценки риска информационной безопасности для определения наилучшего.

Ключевые слова: автоматизированная система управления технологическим процессом, риск, оценка риска, безопасность.

В настоящее время в любом производстве используются автоматизированные системы управления технологическим процессом. Автоматизированная система управления технологическим процессом (АСУ ТП) — это совокупность технических и программных средств, предназначенные для автоматизации управления технологическим оборудованием на промышленных предприятиях. На рисунке 1 представлена общая функциональная схема АСУ ТП. Применение современных АСУ ТП, с одной стороны, повышает эффективность решения различных задач по управлению технологическими процессами, но с другой стороны приводит к существенному увеличению риска нарушения существующей системы информационной безопасности.

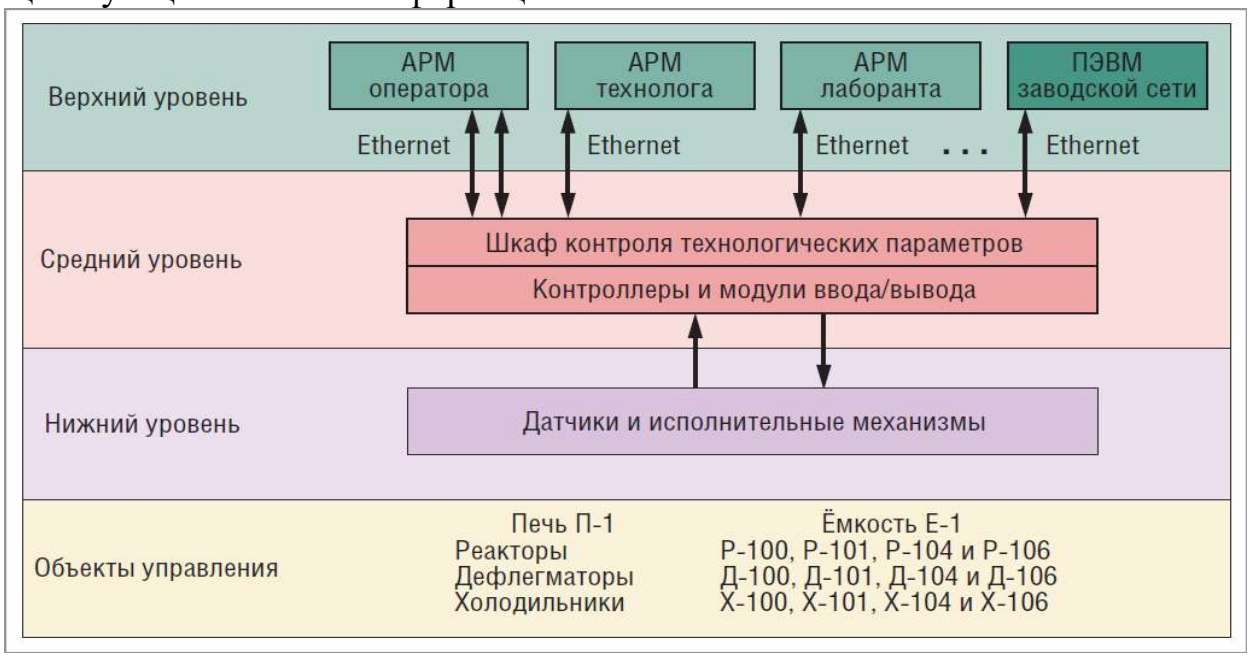

Рис. 1. Общая функциональная схема АСУ ТП

Исходя из цели воздействия на АСУ ТП, выделяют три основных типа угроз информационной безопасности в автоматизированных системах управления технологическим процессом (АСУ ТП):

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение работоспособности АСУ ТП (отказ в обслуживании).

Проведенный анализ автоматизированных систем управления технологическим процессом и мнений экспертов показывает, что с позиции построения СЗИ и возможных рисков нарушения безопасности информации в любом АСУ ТП можно выделить следующие основные компоненты:

- Техническое обеспечение (вычислительные и управляющие устройства, средства получения информации);
- Программное обеспечение (комплекс программ, необходимых для реализации функций АСУ ТП и обеспечения заданного функционирования комплекса технических средств);
- Информационное обеспечение (информация, анализирующая состояние системы управления, системы классификации и кодирования технологической и технико-экономической информации, массивы данных и документы, необходимых для выполнения АСУ ТП);
- Организационное обеспечение (комплекс описаний функциональных, технических и организационных структур, инструкции для оперативного персонала);
- Оперативный персонал (операторы, осуществляющие контроль за управлением системы);
- Эксплуатационный персонал (персонал, обеспечивающий эксплуатацию системы)

Также каждый из этих компонентов можно разделить на множество составляющих элементов, которые могут подвергаться угрозам информационной безопасности.

Угрозами безопасности АСУТП являются:

- внешний несанкционированный доступ для выведения АСУТП и управляемых объектов из строя;
- внешнее несанкционированное управление технологическими объектами с определенными целями;
- блокирование управления АСУТП и управляемыми объектами;
- несанкционированное обновление программного обеспечения для изменения режимов работы технологических объектов.

На рисунке 2 представлено дерево угроз АСУ ТП.

Проведенный анализ угроз информационной безопасности АСУТП показал, что наиболее вероятными источниками угроз безопасности АСУТП выступает персонал предприятия. нелояльные структуры (конкуренты, иностранные спецслужбы и пр.) и криминал (хакеры, кибертеррористы и пр.).

Рис. 2. Дерево угроз АСУ ТП

Для снижения риска информационной безопасности АСУ ТП возможно использование средств защиты информации (СЗИ) которые указаны в государственном сертифицированном реестре средств защиты информации. Также в качестве технических мер повышения защищенности АСУТП и снижения риска информационной безопасности можно предложить следующие мероприятия:

- использование межсетевого экрана между уровнями корпоративной системы и АСУТП;
- антивирусная защита;
- защита удаленного доступа;
- автоматизированный инструментальный анализ защищенности АСУ ТП;
- обнаружение вторжений (IDS/IPS);
- централизованное управление конфигурациями устройств.
- сбор и анализ событий безопасности;

Оценка риска показывает насколько опасна та или иная угроза и позволяет на ранней стадии выявить необходимость в применении дополнительных мер по обеспечению безопасности АСУ ТП. Для сравнения рассмотрим несколько методов оценки риска информационной безопасности АСУ ТП: Мозговой штурм, метод Дельфи и Трехфакторная модель оценки рисков.

Метод мозгового штурма представляет собой обсуждение проблемы группой специалистов в доброжелательной манере, целью которого является идентификация возможных видов отказов и соответствующих опасностей, риска, критериев принятия решений и/или способов обработки риска. Термин "мозговой штурм" часто используют более широко для обозначения любого обсуждения в группе. Однако в процессе классического мозгового штурма применяют специальные методы, когда утверждения одних участников обсуждения способствуют возникновению у остальных участников мозгового штурма новых оригинальных идей.

Метод Дельфи предназначен для получения обобщенного мнения группы экспертов. Хотя данный термин в настоящее время часто используют более широко во всех формах мозгового штурма, существенной особенностью метода Дельфи является то, что эксперты выражают свое мнение индивидуально и анонимно, при этом имея возможность узнать мнения других экспертов.

Помимо этих методов разработана также трехфакторная модель, смысл которой заключается в использовании трех факторов для оценки риска и как интегрального показателя эффективности деятельности предприятия.

В сфере информационной безопасности широкое применение нашла следующая трехфакторная модель:

$$|\boldsymbol{Z}| = \sum_{\boldsymbol{n=1}}^{\infty} \mathbf{AnXnYn}$$

Где, A1…An - весовые коэффициенты, характеризующие вероятность реализации угроз АСУ ТП; X1…Xn - степень воздействия угрозы; Y1…Yn – вес угрозы; Z - значение оценки риска.

Вероятность реализации угроз принимает значения от 1 до 4, где 1 – угроза существует, но не встречалась в рассматриваемой сфере, 2 – угроза возникает в рассматриваемой сфере 2–3 раза в год, 3 – угроза была реализована в рассматриваемой системе, 4 – угроза возникает 2–3 раза в год в рассматриваемой сфере.

Степень воздействия угрозы может быть высокой(9), средней(6) и низкой(3).

Вес угрозы рассчитывается по формуле: $Y = \frac{An}{100} * \frac{Xn}{100}$

где, Y – вес угрозы, An – степень воздействия угрозы, Xn – вероятность реализации угроз АСУ ТП

Для проведения сравнительного анализа методов оценки риска информационной безопасности АСУ ТП были выбраны следующие критерии:

- Ресурсы и возможности
- Неопределенность
- Сложность
- Возможность получения количественных выходных данных

Таблица 1. Сравнительный анализ методов оценки риска информационной безопасности АСУ ТП

Критерии / Методы оценки рисков	Ресурсы и возможности	Неопределенность	Сложность	Возможность получения количественных выходных данных
Мозговой штурм	Низкие	Низкая	Средняя	Нет
Метод Дельфи	Средние	Средняя	Высокая	Да
Трехфакторная модель	Средние	Средняя	Средняя	Да

Таким образом, при анализе методов оценки риска информационной безопасности АСУ ТП нами была выбрана трехфакторная модель как наилучший метод для оценки риска.

По мнению авторов, наиболее эффективным методом для осуществления информационной безопасности АСУТП является построение комплексной системы защиты АСУТП, которая должна реализовывать следующие функции:

- управление и контроль доступом субъектов к объектам защиты;
- защиту машинных носителей информации;
- целостность и конфиденциальность программной среды;
- антивирусную защиту;
- регистрацию событий и расследование инцидентов ИБ;
- межсетевое экранирование;
- обнаружение/противодействие вторжениям/атакам различной природы;
- мониторинг/анализ защищенности информационных систем;
- обеспечение безопасной разработки прикладного ПО;
- управление обновлениями программного обеспечения;
- обеспечение доступности технических средств и информации;

Это позволит добиться следующих результатов:

- снизить риски отказа или внештатного функционирования систем АСУТП и контролируемых/управляемых объектов;
- обеспечить соответствие требованиям законодательства России и нормативным требованиям ФСТЭК России по защите АСУТП;
- создать эффективную систему выявления и подавления современных целенаправленных атак;
- Даст возможность оперативного консолидированного мониторинга и расследования атак и инцидентов, в том числе в реальном времени.

Исходя из вышеизложенного, для снижения риска информационной безопасности АСУТП необходимо проведение мероприятий на системном уровне.

Построение защищенной АСУТП на базе требований ФСТЭК России, введение дополнительных мер и средств защиты, проведение обучения персонала и т д, то есть провести намеренную работу по снижению риска.

Литература

1. Цапко Г.П., Вериго А.А., Каташев А.С. Анализ рисков безопасности автоматизированных систем управления технологическими процессами // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №5 (2016)

2. Астапчук В.А. Архитектура корпоративных информационных систем / В.А. Астапчук, П.В. Терещенко. – Новосибирск: НГТУ, 2015 - 75 с.

3. Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014 - 192 с.

4. Дятлов С.А. Информационно-сетевая регулирование: Монография / С.А. Дятлов, В.П. Марьяненко, Т.А. Селищева - М.: НИЦ ИНФРА-М, 2016 - 414 с.

5. Комплексная безопасность бизнеса в условиях экономической нестабильности: материалы науч.-практ. конф. / отв. ред. Е.В. Стельмашонок, С.Н. Максимов. – СПб.: Изд-во СПбГЭУ, 2014 – 151 с.

6. Малюк А.А. Теория защиты информации. - М.: Гор. линия-Телеком, 2012 – 184 с.

7. Прокопенко А.В. Синтез систем реального времени с гарантированной доступностью программно-информационных ресурсов: монография / А.В. Прокопенко, М.А. Русаков, Р.Ю. Царев. - Красноярск: Сиб. федер. ун-т, 2013-92 с.

А.А. Батаргалиев, К.Е. Климентьев, В.И. Соловьева

НАУЧНЫЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ВОПРОСАМ ЗАЩИТЫ ИНФОРМАЦИИ

(Самарский университет)

Введение. Преподаватели кафедры ИСТ Самарского университета принимают участие в подготовке бакалавров, магистров и специалистов на разных специальностях ВУЗа, включая, например, 09.03.01 – Информатика и вычислительная техника и 10.05.03 – Информационная безопасность автоматизированных систем. Методическая поддержка курсов, посвященных вопросам защиты информации (см., например, работы [1,2,3,4]), требует проведения ряда предварительных исследований, имеющих самостоятельную научную и техническую ценность. Эти исследования, преимущественно, затрагивают ряд вопросов, связанных с «классической» криптографией, то есть, не актуальной с точки зрения практического применения, но содержащей ряд теоретических положений, знание которых важно при изучении «современной» криптографии.