Тип работы: Магистерская работа

Предмет: Информатика основы

Введение

Специальные предприятия, использующие в своей деятельности автоматизированные системы управления технологическими процессами, являются субъектами критической информационной инфраструктуры.

В настоящее время, к сожалению, возрастает количество случаев попыток взлома промышленных информационных систем с целью выведения их из строя, нанесения предприятию максимального ущерба. Серьезной угрозой для специальных предприятий является целенаправленная деструктивная деятельность экстремистских, террористических, враждебно настроенных формирований и организаций. Соответственно, возникает реакция предприятий, выражающаяся в проведении соответствующих мероприятий для защиты своего производства.

Для нормальной работы всего комплекса автоматизированной системы управления технологическими процессами (АСУ ТП) на любом предприятии, необходимо обеспечение его информационной безопасности. Особенно это относится к предприятиям, отнесенным к критической информационной инфраструктуре. Это предприятия:

- здравоохранения;
- банковской сферы;
- топливно-энергетического комплекса;
- атомной промышленности;
- военно-промышленного комплекса;
- ракетно-космической отрасли;
- горнодобывающей промышленности;
- металлургии и химической промышленности;
- науки;
- транспорта;
- связи.

На таких предприятиях защита АСУ ТП особенно критична, так как в случае выхода систем АСУ ТП из строя возможно возникновение экологических, гуманитарных катастроф, иногда с человеческими жертвами, тяжелые экономические последствия.

Актуальность настоящей работы обусловлена несколькими факторами:

 большими рисками в случае успешных деструктивных действий злоумышленников;
 сложностью изоляции АСУ ТП от инфоструктуры предприятия;
 доступностью злоумышленникам основных открытых протоколов и технологий применяемых в АСУ ТП;
 появлением новых видов оборудования и программного обеспечения в составе АСУ ТП, большинство из которых западного производства;
 непрерывным развитием предприятий и организаций, повышением сложности технологических процессов.
Основной задачей является обеспечение высокого уровня готовности автоматизированных систем управления технологическими процессами на специальных предприятиях к бесперебойному функционированию в условиях деструктивных воздействий, в том числе, информационно-технических.
Одним из подходов к достижению решения этой задачи является оценка информационных рисков АСУ ТП. Оценив риски, можно принять упреждающие меры к их минимизации.
Целью настоящей работы является разработка методики оценки информационных рисков АСУ ТП на специальных предприятиях.
В ходе работы для достижения этой цели необходимо решить ряд задач.
Задачи работы:
 исследовать функции и структуру современной АСУ ТП;
 определить основные типы угроз информационной безопасности АСУ ТП специальных предприятий;
 изучить методы защиты АСУ ТП;
 провести сравнительный анализ существующих методик оценки рисков;
 сформировать необходимые модели и алгоритмы.

Объект работы: информационная безопасность автоматизированной системы управления технологическими процессами специальных предприятий.
Предмет работы: методика оценки информационных рисков АСУ ТП на специальных предприятиях.

Глава 1. Специфика построения АСУ ТП и информационная безопасность.

1.1 Автоматизация и автоматика

Существует различные направления организации управления технологическими процессами, которые призваны увеличить производительность труда, качество выпускаемой продукции и, в конечном итоге, решение задач предприятия по получению максимальной прибыли в процессе основной деятельности.
Системы управления технологическими процессами делятся на два класса : автоматические и автоматизированные.
Системы автоматического управления благополучно работают без участия человека в контуре управления. Обычно состоят из объекта управления и управляемого устройства. Существуют замкнутые и разомкнутые системы автоматического управления. В замкнутых системах существуют каналы обратной связи, которые обеспечивают регулирование управляющего воздействия в зависимости от управляемой величины. В

разомкнутых системах управление осуществляется без контроля состояния управляемого объекта.
Схемы систем автоматического управления представлены на рисунках 1 и 2.
а)
X Y

б)
X □X Y

Рис. 1. Функциональные схемы САУ: а – разомкнутой; б – замкнутой

Рис.2 Система автоматического управления

Основная особенность САУ заключается в том, что в них происходит очень быстрый анализ сигналов обратной связи перед формированием сигналов управления. Объем информации – очень большой. Человек просто не успеет на нее реагировать. Соответственно, в такой ситуации человек не может быстро принимать адекватные решения, т.е. он физически не способен заменить САУ. Примером могут служить системы автоматического управления, установленные на технологических установках газодобывающих предприятий. Система является замкнутой, где объектом управления является технологическая установка, которая формирует обратную связь, отправляя сигналы на исполнительные механизмы на газовых скважинах.
Другим классом систем управления являются автоматизированные системы управления. В этом случае в принятии управленческих решений принимает участие человек. Необходимо понимать, что человек по скорости восприятия и обработки информации значительно уступает автоматике. Поэтому человек может участвовать только в некоторых процессах, требующих его непосредственного решения. В рамках АСУ ТП для управления системы пользователем используется преобразующий интерфейс для снижения объемов информации, демонстрирующий показатели технологического процесса. Человек может оказать влияние на объект управления, но не прямое, а косвенное. Такое воздействие отличается тем, что результат воздействия и сигналы, поступающие по каналам обратной связи могут не совпадать. Операторы должны проверять результаты своих действий вручную.

Рис. 3 Автоматизированное управление АСУ ТП

1.1.1 Уровни управления

Каждый из этих уровней характеризуется своими возможностями и решаемыми задачами.
Самым нижним является уровень контрольно-измерительных приборов и автоматики. Этот уровень состоит из датчиков и исполнительных механизмов, которые взаимодействуют непосредственно с объектом управления. Это оборудование используется для измерения характеристик объекта и их изменения по

определенным правилам.
На среднем уровне расположены программируемые логические контроллеры (ПЛК) и устройства связи с объектом (УСО). В ПЛК и УСО встроены алгоритмы, по которым формируются управляющие воздействия на механизмы нижнего уровня и происходит анализ информации от датчиков.
Система сбора данных и оперативно-диспетчерского управления (SCADA), или распределенная система управления (DSC) находится на верхнем уровне. Описание уровней управления АСУ ТП представлено на рисунке 4.

Рис. 4 Уровни управления АСУ ТП

На верхнем уровне оператор может получать информацию с датчиков или непосредственно управлять исполнительными механизмами. Взаимодействие оператора с нижним уровнем происходит через средний.

1.1.2 Функции АСУ ТП

АСУ ТП выполняет, по крайней мере, три основные функции:
- управляющую;
- противоаварийную;
- информационную.

Список использованной литературы

1. Агеев, С.А. Оценка рисков сетевой компьютерной безопасности на основе нечеткого логического вывода / С.А. Агеев, И.Б. Саенко // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». - Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. - Том 3. - С. 28-30.
2. Ажмухамедов, И.М. Управление рисками информационной безопасности в условиях неопределенности / И.М. Ажмухамедов, О.Н. Выборнова, Ю.М. Брумштейн // Проблемы информационной безопасности. Компьютерные системы. - 2016. - № 1. - С. 7-14.
3. Ажмухамедов, И.М. Анализ рисков информационной безопасности / И.М. Ажмухамедов, О.Н. Выборнова, О.М. Князева: Учебное пособие. - Астрахань: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный технический университет», 2015. - 104 с.
4. Аникин, И.В. Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками / И.В. Аникин, Л.Ю. Емалетдинова, А.П. Кирпичников // Вестник технологического университета. - 2015. - Том 18, № 7. - С. 247-250.
5. Аникин, И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях / И.В. Аникин // Инфокоммуникационные технологии. - 2015. - Том 13, № 2. - С. 215-221.
6. Аникин, И.В. Методология количественной оценки и управления рисками информационной безопасности / И.В. Аникин, Л.Ю. Емалетдинова // Информация и безопасность. - 2016. - Том 19, № 4. - С. 539-542.

7. Александровская, Л.Н. Безопасность и надежность технических систем / Л.Н. Александровская, И.З. Аронов, В.И. Круглов, А.Г. Кузнецов, Н.Н. Патраков, А.М. Шолом: Учебное пособие. - М.: Логос, 2004. - 376 с.
8. Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. - 2015. - № 1(9). - С. 73-79.
9. Баранова, Е.К. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 / Е.К. Баранова, А.С. Забродоцкий // Образовательные ресурсы и технологии. - 2015. - № 3(11). - С. 73-80.
10. Барабанов, А.В. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении /
А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Системы высокой доступности. - 2018. - Том 14, № 3. - С. 12-17.
11. Буйневич, М.В. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации / М.В. Буйневич, В.В. Покусов, К.Е. Израилов // Информатизация и связь. - 2021. - № 4. - С. 66-73.
12. Буйневич, М.В. Аналитическое моделирование работы программного кода с уязвимостями / М.В. Буйневич, К.Е. Израилов // Вопросы кибербезопасности. - 2020. - № 3(37). - С. 2-12.
13. Булдакова, Т.И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели / Т.И. Булдакова, Д.А. Миков // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. - 2013. - № 11. - С. 295-310.
14. Глухов, А.П. Оценка чувствительности ресурсов и рисков применения систем критических приложений к влияющим факторам / А.П. Глухов, Н.Н. Котяшев, А.В. Купцов // Стратегическая стабильность. - 2007. - № 1(38). - С. 39-44.
15. Козунова, С.С. Формализованное описание процедуры управления рисками информационной системы / С.С. Козунова, А.Г. Кравец // Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика. - 2018. - № 2. - С. 61-70.
16. Милославская, Н.Г. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю Сенаторов, А.И. Толстой: Учебное пособие для вузов. 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 130 с.
17. Еремеев, М.А. Продукционное представление знаний для моделирования источников атак в сети / М.А. Еремеев, А.Г. Ломако, В.М. Моргунов, Н.В. Свергун // CDE'17: The 2017 Symposium on Cybersecurity of the Digital Economy. - Иннополис: Издательский Дом "Афина" (Санкт-Петербург), 19-20 сентября, 2017. - С. 167-180.
18. Новохрестов, А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады ТУСУРа. - 2016. - Том 19, № 3. - С. 111-114.
19. Платонов, В.В. Методы выбора свойств для систем обнаружения сетевых атак / В.В. Платонов // Методы и технические средства обеспечения безопасности информации. - 2016. - № 25. - С. 24-25.
20. Zegzhda, D.P. Approach to APCS Protection from Cyber Threats /
D. P. Zegzhda, T.V. Stepanova // Automatic Control and Computer Sciences. - 2015. - no. 49(8). - pp. 659-664.
21. Зегжда, Д.П. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации / Д.П. Зегжда, Ю.С. Васильев, М.А. Полтавцева, И.Ф. Кефели, А.И. Боровков // Вопросы кибербезопасности. - 2018. - № 2(26). - С. 2-15.
22. Зегжда, П.Д. Систематизация киберфизических систем и оценка из безопасности / П.Д. Зегжда, М.А. Полтавцева, Д.С. Лаврова // Проблемы информационной безопасности. Компьютерные системы. - 2017. - № 2. - С. 127-138.
23. Зегжда, П.Д. Информационная безопасность киберпространства в эпоху Industry 4.0 / П.Д. Зегжда // Методы и технические средства обеспечения безопасности информации. - 2017. - № 26. - С. 3-5.
24. Кононов, А.А. Оценка рисков в иерархических структурах критически важных объектов / А.А. Кононов, К.В. Черныш, Д.С. Гуревич,
А.К. Поликарпов // Труды института системного анализа российской академии наук. - 2010. - Том 52. - С. 5-15.
25. Кононов, А.А. О методологии критериального моделирования безопасности больших систем, критически важных объектов и критических инфраструктур / А.А. Кононов, П.И. Кулаков, А.К. Поликарпов // Проблемы управления безопасностью сложных систем.
Труды XXIV Международной научной конференции. - Москва, 21 декабря, 2016. - С. 276-279.
26. Котенко, И.В. Метрика безопасности для оценки уровня защищенности компьютерных сетей на основе

построения графов атак / И.В. Котенко, М.В. Степашкин // Защита информации. INSIDE. - 2006. - № 3. - С. 2-11.
27. Комашинский, Н.А. Проблемы обнаружения целенаправленных атак (APT)
на критически важные информационные системы / Н.А. Комашинский, И.В. Котенко // АПИНО 2018: Актуальные проблемы
инфотелекоммуникаций в науке и образовании, VII Международная научнотехническая и научно-методическая конференция. - Санкт- Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (Санкт-Петербург), 28 февраля-1 марта, 2018. - Том 1. - С. 483-485.
28. Лившиц, И.И. Подходы к управлению киберрисками в нефтегазовых проектах / И.И. Лившиц // Менеджмент качества. - 2018. - № 4. - С. 272¬277.
29. Лившиц, И.И. Разработка системы управления ИБ для критичного объекта ТЭК / И.И. Лившиц, В.В. Маликов // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». - Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. - Том 3. - С. 161-165.
30. Паращук, И.Б. Информационная безопасность телекоммуникационной компоненты киберфизических систем / И.Б. Паращук // Региональная информатика и информационная безопасность. - Санкт-Петербург: Санкт- Петербургское Общество информатики, вычислительной техники, систем связи и управления, 1-3 ноября, 2017. - С. 150-152.
31. Жмуров, В.Д. Некоторые подходы к анализу надежности программного обеспечения автоматизированных систем управления сетями связи /
В.Д. Жмуров, И.Б. Паращук, Л.В. Саяркин // АПИНО 2018: Актуальные проблемы инфотелекоммуникаций в науке и образовании, VII Международная научнотехническая и научно-методическая конференция.
- Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (Санкт-Петербург), 28 февраля-1 марта, 2018. - Том 4. - С. 234-239.
32. Черешкин, Д.С. Проблемы обеспечения кибербезопасности критически важных объектов национальной инфраструктуры / Д.С. Черешкин // СИБ - 2014: Международная научно-практическая конференция «Современные проблемы и задачи обеспечения информационной безопасности». - Москва, 3 апреля, 2014. - С. 233-241.
33. Черныш, К.В. Индикативная оценка рисков на критериальных моделях критически важных объектов и критических инфраструктур / К.В. Черныш, А.А. Кононов // XI Всероссийской конференции «Методологические проблемы управления макросистемами». - Апатиты: КНЦ РАН, 26 марта-3 апреля, 2016. - С. 86-89.
34. Чертовской, В.Д. Методология математического описания и моделирования адаптивной автоматизированной системы управления производством / В.Д. Чертовской // Информационные технологии. - 2018.
- Том 24, № 2. - С. 81-86.
35. Пищик, Б.Н. Безопасность АСУ ТП / Б.Н. Пищик // Вычислительные технологии. - 2013. - Том 18. - С. 170-175.