2. Беляев Н. Н. Защита атмосферы от загрязнения при эмиссии опасного вещества из движущегося железнодорожного вагона / Н. Н. Беляев, А. В. Берлов, П. С. Кириченко // Строительство, материаловедение, машиностроение: сб. науч. тр. / под общ. ред. В. И. Большакова.– Днепропетровск : ПГАСА, 2016. – Вып. 87. – С. 13–18.

3. Berlov O. V. Atmosphere protection in case of emergency during transportation of dangerous cargo / O. V. Berlov // Наука та прогрес транспорту. Вісн. Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна. – Дніпропетровськ : Дніпропетр. нац. ун-т залізн. трансп. ім. акад. В. Лазаряна, 2016. – Вип. 1 (61). – С. 48–54.

Бондаренко К. О.

Студент ХНАДУ

КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Практически каждый день мы слышим о вмешательстве третьих лиц, в различных областях нашей жизнедеятельности. Поэтому, на сегодняшний день одним из важных вопросов при проектировании и функционировании технологических процессов является безопасность систем.

Влияние на безопасность технологического процесса может оказывать, как организационное управление, так и выбор аппаратных и программных средств, поэтому влияние на процесс может оказать, как ошибка оператора или неисправность одного из элементов системы, но и ошибки программного обеспечения, как в случае случайного заражения, так и целенаправленного действия [1-2].

Целью статьи является повышение безопасности автоматизированных систем управления за счет определения критериев ее оценки.

Критерии оценки безопасности определяются уязвимостями АСУ ТП, которые в свою очередь можно разделить на ошибки в организации управления, ошибки в проектировании и использовании аппаратных, программных и сетевых средств.

Уязвимости АСУ ТП обусловленные ошибками в организации управления [3]:

- не отвечающая требованиям политика безопасности для АСУ ТП;

- отсутствие инструкций безопасности АСУ ТП;

- не отвечающая требованиям архитектура и дизайн системы безопасности;

- не было разработано специализированных или документированных процедур в рамках политики безопасности для АСУ ТП;

- отсутствие или недостаточность руководящих документов по особенностям работы с оборудованием в рамках АСУ ТП;

- отсутствие механизма административных действий в области безопасности;

- отсутствие на АСУ ТП специфицированной конфигурации по управлению изменениями.

Уязвимости аппаратной части АСУ ТП [3]:

- не поддерживаются обновления безопасности;

- проведение обновления для операционных систем и приложений без исчерпывающего тестирования;

- использование стандартных конфигураций;

- критические конфигурации не хранятся или не подвергаются резервному копированию.

- незащищённость данных на портативных устройствах;

- отсутствие адекватной политики в области парольной защиты;

- пароли не используются;

- применение не отвечающих требованиям средств управления доступом;

- не отвечающее требованиям тестирование изменений в области безопасности;

- не соответствующая требованиям физическая защита критически важных систем;

- посторонние лица среди персонала имеют физический доступ к оборудованию;

- небезопасный доступ к компонентам АСУ ТП;

- радиочастотные или электромагнитные импульсы;

- отсутствие резервного питания;

- отсутствие дублирующих устройств для критически важных компонентов.

Программные уязвимости АСУ ТП [3]:

- переполнение буфера;

- установленные возможности для обеспечения безопасности не включены по умолчанию;

- неправильное реагирование на неопределённые, плохо определённые или неправильные условия;

- технология связывания и внедрения объектов в другие документы OLE для управления процессами основывается на использовании удалённого вызова процедур и технологию распределённой компонентной объектной модели DCOM;

- использование небезопасных индустриальных протоколов АСУ ТП;

- использование незашифрованных данных в рамках протокола;

- функционирование ненужных служб;

- не соответствующие требованиям механизмы аутентификации и контроля доступа в программном обеспечении для конфигурирования и программирования;

- ведение системных журналов (т.н. “логирование”) не осуществляется;

- инциденты не определяются;

- не установлено программное обеспечение по защите от вредоносных программ;

- программное обеспечение по защите от вредоносного ПО устарело или имеет устаревшие сигнатуры вирусов (уязвимостей, атак).

Сетевые уязвимости [3]:

- слабая архитектура безопасности сети;

- не реализована система контроля информационных потоков;

- неправильно настроенное оборудование для обеспечения безопасности;

- настройки сетевого оборудования не хранятся и не подвергаются резервному копированию;

- пароли не шифруются на этапе передачи;

- пароли существуют неопределённый срок на сетевых устройствах;

- применяется не удовлетворяющая стандартам система контроля доступа;

- не удовлетворяющая стандартам физическая защита сетевого оборудования;

- небезопасные физические порты;

- неуполномоченные сотрудники имеют доступ к оборудованию и сетевым соединениям;

- отсутствие дублирующих устройств у критически важных сетевых компонентов.

Большинство из описанных уязвимостей сложно оценить и описать четкими значениями, поэтому для принятия решений оценки безопасности предлагается использовать математический аппарат нечеткой логики, позволяющий количественно определить безопасность системы [4-6].

Таким образом, в данной статье были предложены критерии оценки безопасности технологических процессов, которые позволят уменьшить влияние уязвимостей на производство.

Литература:

1. Goldenberg N., Wool A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems // International Journal of Critical Infrastructure Protection. 2013. Vol. 6. Issue 2. P. 63–75.

2. Rafael Ramos Regis Barbosa, Sadre R., Pras A. Flow whitelisting in SCADA networks // International Journal of Critical Infrastructure Protection. 2013. Vol. 6. Issue 3–4 P. 150 –158.

3. Stouffer K., Falco J., Scarfone K. Guide to Industrial Control Systems (ICS) Security. [Электронный ресурс].National Instituteof Standards and Technology Gaithersburg. Gaithersburg, Maryland, USA. 2011. URL: https://csrc.nist.gov/publications/detail/sp/800-82/archive/2011-06-09

4. Брежнев О. В. Методология обеспечения безопасности критических инфраструктур в условиях неопределённости: концепция и принципы/ Брежнев О. В., Харченко В. С. // Радіоелектронні і комп'ютерні системи. – Харків: НАКУ «ХАИ». – 2015. – №1(71). – С.25–32.

5. Крючковский В.В. Введение в нормативную теорию принятия решений. Методы и модели:монография / В. В. Крючковский, Э. Г. Петров, Н. А. Соколова, В. Е. Ходаков; под ред. Э. Г. Петрова.- Херсон: Гринь Д. С., 2013. -284 с.

6. Нефёдов Л. И. Математическая модель выбора программного обеспечения с учетом нечеткой информации / Л. И. Нефёдов, Ю. А. Петренко, А. С. Кононыхин // Вісник Національного технічного університету «ХПІ». – 2014. – №17. – С.13–17.