Предложенная архитектура позволяет разработать систему управления рисками информационной безопасности в ГИС, которая поможет эксперту провести оценку рисков ИБ для активов ГИС и минимизировать последствия от них, определив контрмеры и состав системы защиты информации, минимизирующий вероятность реализации существующих угроз ИБ.

Литература

1. Жуйкова С.А., Курина А.Д., Бабенко А.А. Модель оценки рисков на различных этапах жизненного цикла информационной системы. – Актуальные вопросы информационной безопасности регионов в условиях перехода России к цифровой экономике. материалы VII Всероссийской научно-практической конференции. Волгоградский государственный университет. 2018. С. 233-238.

2. Бабенко А.А., Козунова С.С. Модель определения состава системы защиты информации в государственной информационной системе. – Информационные системы и технологии. 2021. № 2 (124). С. 92-101.

3. Бабенко А.А. Экспертный метод определения состава системы технической защиты информации в государственных информационных системах. – Перспективные информационные технологии (ПИТ 2021). Труды Международной научно-технической конференции. под ред. С.А. Прохорова. Самара, 2021. С. 136-139.

4. Бабенко А.А., Магомедов Д.А. Оценка риска информационной безопасности автоматизированной системы управления технологическим процессом. – Перспективные информационные технологии (ПИТ 2021). Труды Международной научно-технической конференции. под ред. С.А. Прохорова. Самара, 2021. С. 140-145.

5. Бабенко А.А. Жарков Г.В. Программа определение состава системы технической защиты информации в государственных системах: св-во о гос. рег. прогр. для ЭВМ 2020615502 Российская Федерация. Зарегист. 25.05.2020.

А.А. Бабенко, А.А. Вдовкин

АЛГОРИТМ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НЕФТЕГАЗОВОЙ ОТРАСЛИ

(Волгоградский государственный университет)

Защита объектов нефтехимического и нефтегазового производства является актуальной проблемой. Остро стоит необходимость решения технических и программных вопросов безопасности технологических процессов. Современные бизнес системы во многом базируются на информационной сфере, что требует поддержания определенного уровня информационной безопасности включающей в себя программно-аппаратные, технические и организационные меры защиты на всех уровнях управления [1, 2].

Существуют следующие методы оценки рисков информационной безопасности предприятий: CRAMM, FRAP, RiskWatch, OCTAVE. В работе используется метод CRAMM, включающий в себя более трех тысяч различных контрмер, собранных в логические группы. Опираясь на приказ для обеспечения безопасности ФСТЭК России от 14 марта 2014 г. N 31 и ФЗ от 26 июля 2017 г. N 187-ФЗ ФСТЭК России для обеспечения безопасности инфраструктуры нами разработан алгоритм оценки риска информационной безопасности автоматизированной системы управления технологическими процессами (АСУ ТП) нефтегазовой отрасли.

Для проведения экспериментальных исследований выбрана АСУ ТП компрессорного цеха – система автоматизированного управления газоперекачивающего агрегата (ГПА), являющаяся подсистемой системы компрессорного цеха. Система автоматизированного управления газоперекачивающего агрегата направлена на автоматическое управление, стабилизацию и регулирование работы ГПА.

Выделяют следующие информационные функции САУ ГПА:

1. Удаленное представление режимных параметров агрегата в цифровой и графической форме;
2. Обмен информацией с системами управления верхнего уровня;
3. Учёт наработки ГПА, количества пусков и остановов;
4. Предупредительная и аварийная сигнализация;
5. Расчёт ряда косвенных параметров.

В состав САУ ГПА входят следующие программно-технические средства (ПТС):

1) основные программно-технические средства САУ ГПА, включающие блок управления и регулирования и вторичные преобразователи;
2) автоматизированное рабочее место оператора ГПА;
3) панель резервного управления и индикации;
4) блок экстренного останова, и.т.д.

Программное обеспечение автоматизированного рабочего места:

1. SCADA – система Wonderware InTouch HMI;
2. Интернет (Интранет) клиенты Wonderware InTouch HMI;
3. система SMLogix;
4. инструментальный программный комплекс промышленной автоматизации CODESYS.

На основе математической модели, представленной в [3], нами определена степень риска уязвимостей компонентов автоматизированной системы управления по оценке CVSS второй и третьей версии. Обозначено, что большая часть совокупности уязвимостей АСУ ТП находятся в высокой и критической степени риска [4].

Анализ полученных результатов оценки степени риска программно-технического, организационного обеспечения автоматизированной системы управления по вышеуказанному методу, позволил выявить компоненты АСУ ТП с высоким уровнем угроз.

Далее, в соответствии с методикой:

1. выбраны из БДУ ИБ ФСТЭК России и из международных банков данных актуальные для нашей системы угрозы;
2. определены значения параметров угроз ИБ АСУ ТП;
3. вычислены оценки рисков ИБ АСУ ТП;
4. проведено сравнение полученных оценок уязвимостей с оценкой уязвимостей из БДУ ИБ ФСТЭК России.

Выбранные из ЬДУ ИБ ФСТЭК России, актуальные для нашей системы угрозы представлены в таблице 1.

Таблица 1. Потенциальные уязвимости ИБ АСУ ТП

Название	Описание
BDU:2021-03149	Потенциальная уязвимость библиотеки CODESYS Control V2 Linux SysFile программного комплекса промышленной автоматизации CODESYS.
BDU:2021-02335	Потенциальная уязвимость микропрограммного обеспечения МЭ Cisco Adaptive Security Appliance Software (ASA) и Cisco Firepower Threat Defense (FTD) связана с копированием буфера без проверки размера входных данных. Воздействие посредством уязвимости может позволить нарушителю, действующему удаленно, оказать влияние на конфиденциальность и доступность защищаемой информации.
BDU:2021-04331	Потенциальная уязвимость микропрограммного обеспечения программируемого логического контроллера Schneider Electric Modicon M340, Modicon Quantum, Modicon Premium, обоснованная раскрытием информации, способствует несанкционированному доступу к защищаемой информации.

Оценки уязвимостей из банка данных безопасности информации ФСТЭК России и вычисленные с помощью разработанной программы представлены в таблице 2.

Таблица 2. Оценки уязвимостей

Название уязвимости (номер в банке данных ФСТЭК)	Базовая оценка CVSS 2.0		Базовая оценка CVSS 3.0		Оценка программы	
	Оценка	Уровень опасности	Оценка	Уровень опасности	Оценка	Уровень опасности
BDU:2021-03149	4,6	Средний	5,3	Средний	5,1	Средний
BDU:2021-	7,5	Высокий	8,2	Высокий	8,2	Высокий

02335						
BDU:2021-04331	7,8	Высокий	7,5	Высокий	7,8	Высокий

В статье экспериментально проверен способ оценки уровня значимости угроз. В качестве эталона брались уже сформированные экспертами оценки из банка данных угроз ФСТЭК. В дальнейшем предполагается дополнить программу модулем по определению контрмер для снижения уровня выявленных рисков АСУ ТП.

Литература

1. 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: Приказ ФСТЭК РФ №31 от 14 марта 2014 г. URL: https://fstec.ru/component/attachments/download/714 (дата обращения 7.04.2022).

2. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // Собрание законодательства РФ. 2017. № 31 (Часть I). Ст. 4736.

3. Кирсанов, С.В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли / С.В. Кирсанов // Доклады ТУСУРа. – 2013. – № 2(28). – С. 112–115.

4. Бабенко А.А., Магомедов Д.А. Оценка риска информационной безопасности автоматизированной системы управления технологическим процессом. – Перспективные информационные технологии (ПИТ 2021). Труды Международной научно-технической конференции. под ред. С.А. Прохорова. Самара, 2021. С. 140-145.

Д. П. Баландин, М. Д. Лимов, М. Н. Осипов

ПРИМЕНЕНИЕ СПЕКЛ-СТРУКТУР ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ФАЛЬСИФИКАЦИИ

(Самарский университет)

В повседневной жизни человек постоянно встречается с объектами, имеющими различные элементы защиты их подлинности. Это могут быть документы, изделия, упаковки. Поэтому, при каждом столкновении с ними, может возникнуть вопрос об их подлинности. Для недопустимости фальсификации, или как минимум ее затруднения объект защиты обеспечивают комплексом опреде-