Интеллектуальная система оценки рисков информационной безопасности АСУ ТП объекта нефтедобычи

А.В. Слинин
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: nags.09@yandex.ru

В.И. Васильев
Факультет информатики и робототехники
Уфимский государственный авиационный технический университет
Уфа, Россия
e-mail: vasilyev@ugatu.ac.ru

Аннотация[1]

В последние несколько лет наблюдается резкий рост актуальности проблемы обеспечения кибербезопасности объектов критической информационной инфраструктуры. В данной статье предложен подход к оценке рисков информационной безопасности объекта критической информационной инфраструктуры на основе нечеткой нейронной сети.

Ключевые слова: кибербезопасность; критическая информационная инфраструктура; оценка рисков; автоматизированная система управления; нечеткая нейронная сеть; объект нефтедобычи; моделирование.

Введение

В современном мире объекты критической информационной инфраструктуры (КИИ) постоянно подвергаются кибератакам со стороны злоумышленников. Исходя из этого, наблюдается стабильный рост числа инцидентов информационной безопасности (ИБ). Для повышения устойчивости функционирования объектов КИИ целесообразно реализовать комплекс мероприятий по обеспечению ИБ [1].

В соответствии с Федеральным законом N 187 «О безопасности критической информационной инфраструктуры Российской Федерации», [2] к *субъектам КИИ* относятся государственные органы, государственные учреждения, российские юридические лица, индивидуальные предприниматели, которым принадлежат и которые обеспечивают функционирование *объектов КИИ* - информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, функционирующих в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности (рис. 1).

В качестве объекта защиты выбрана автоматизированная система управления технологическими процессами первичного пункта сбора нефти (АСУ ТП ППСН), которая является объектом КИИ.

Первичный пункт сбора нефти (ППСН) является частью промышленной системы, которая осуществляет сбор нефти на месторождениях. С целью автоматизации управления технологическими процессами на ППСН, а также для мониторинга работы оборудования ППСН, применяются АСУ ТП.

Главное отличие АСУ ТП от корпоративных информационных систем (КИС), заключается в том, что в КИС, как правило, основной защищаемый ресурс – информация, а основная цель – обеспечение ее конфиденциальности. В АСУ ТП же защищаемым ресурсом, в первую очередь, является сам технологический процесс, и основная цель – обеспечить его непрерывность и целостность. Масштабы последствий от реализации угроз в АСУ ТП могут привести не только к финансовому, но и к серьезному ущербу окружающей среде, а также жизни и здоровью людей [3].

Для того, чтобы обеспечить защиту АСУ ТП, необходимо произвести моделирование объекта защиты, выделить активы, идентифицировать угрозы и уязвимости, оценить риски информационной безопасности. Затем, на основании полученных результатов, выбрать и применить контрмеры, необходимые для нейтрализации угроз.

Труды Седьмой всероссийской научной конференции "Информационные технологии интеллектуальной поддержки принятия решений", 28-30 мая, Уфа-Ставрополь, Ханты-Мансийск, Россия, 2019

Рис. 1. Субъекты и объекты КИИ

Моделирование АСУ ТП как объекта защиты производится на основе документа ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» [4].

Моделирование АСУ ТП ППСН

Согласно стандарту ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 [4], моделирование АСУ ТП как объекта защиты включает в себя разработку 4 моделей:

1. Базовая модель.
2. Объектная модель.
3. Базовая архитектура.
4. Зональная модель.

Базовая модель (рис. 2) характеризует АСУ ТП, представляя ее в виде логических уровней, каждый из которых соответствует определенному виду деятельности.

На основе Базовой модели на следующем этапе строится *Объектная модель*, которая отражает основные объекты АСУ ТП, взаимодействие с сетями и подразделениями, которые участвуют в технологических процессах и присутствуют на различных уровнях иерархии.

Следующим шагом в процессе моделирования АСУ ТП является построение модели *Базовой архитектуры*, которая отражает все основные элементы АСУ ТП, в том числе телекоммуникационное оборудование и линии связи, строится на основе Объектной модели.

Заключительным этапом моделирования является построение *Зональной модели* (рис. 3), которая разделяет объект защиты на отдельные зоны – группы логических или физических объектов в пределах предприятия, объединенные по общим характеристикам (требования безопасности, критичность для ТП и т.д.).

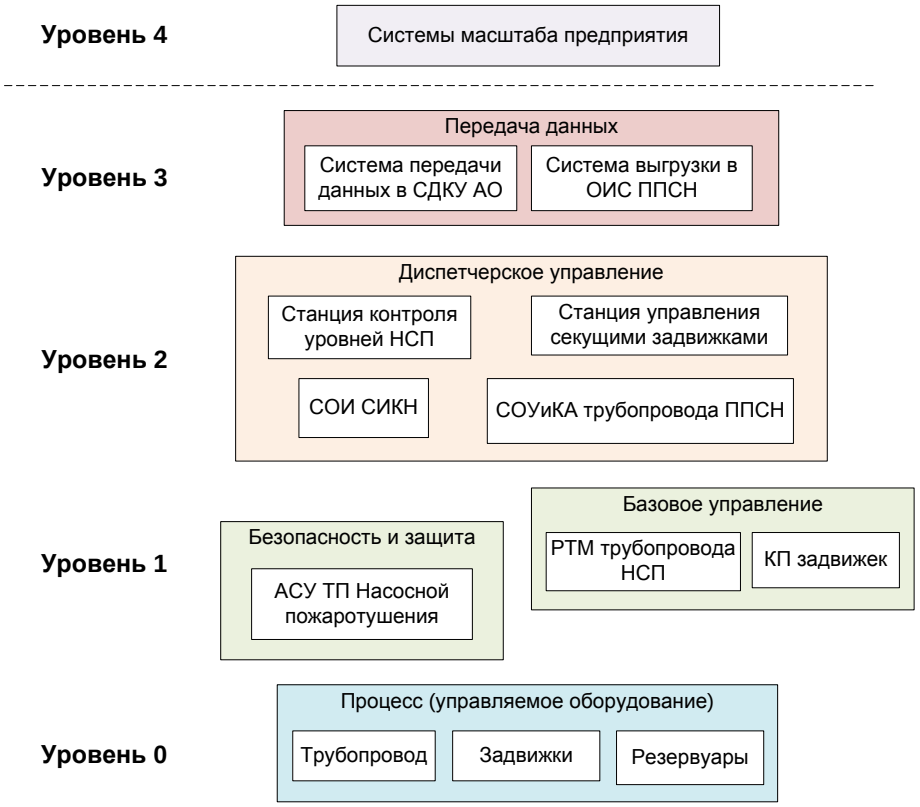

Рис. 2. Базовая модель

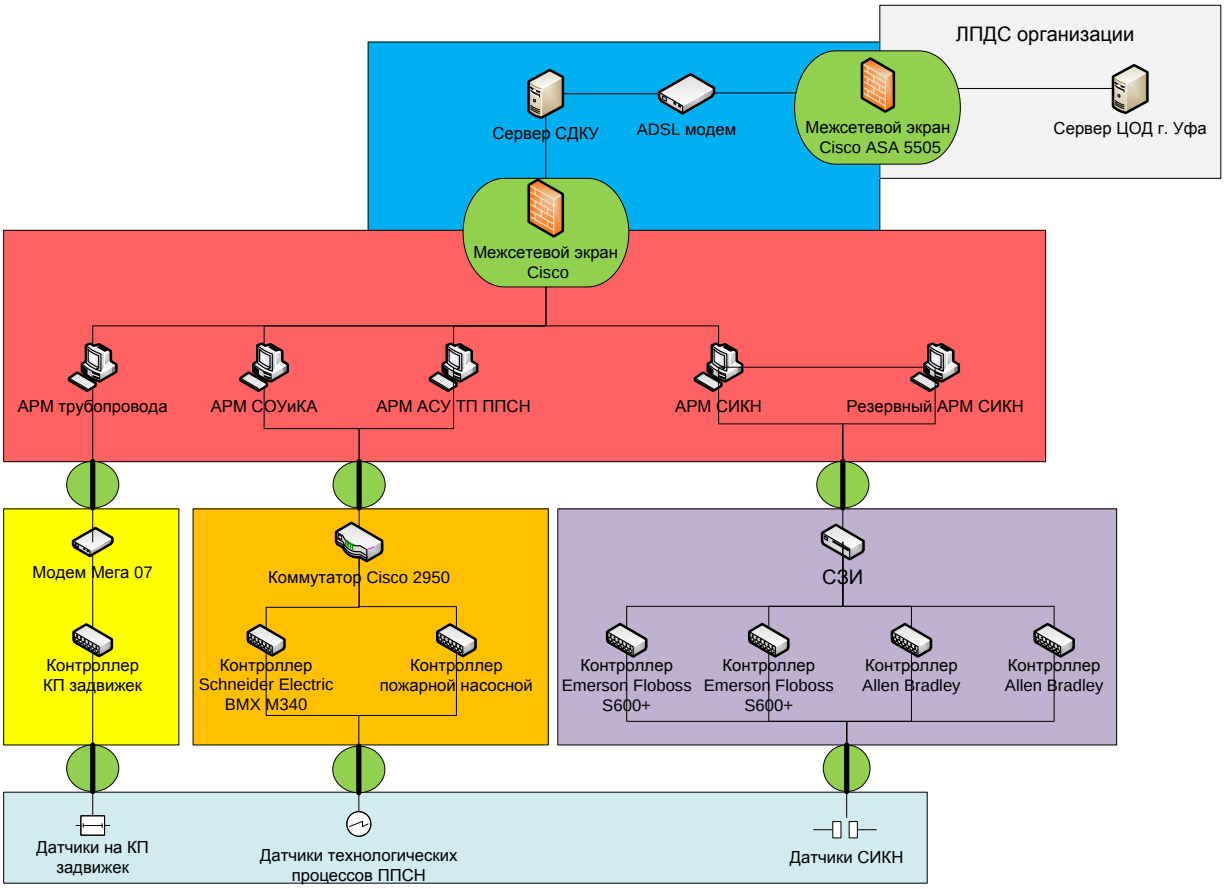

Рис. 3. Зональная модель

Как видно на рис. 3, объект защиты разделен на 7 зон безопасности: зона датчиков, зона управления задвижками, зона управления технологическими процессами ППСН, зона управления система измерения количества нефти (СИКН), зона критических устройств управления, зона сервера система диспетчерского контроля и управления (СДКУ), зона линейная производственно-диспетчерская станция (ЛПДС) организации.

Для сервера СДКУ выделена отдельная зона безопасности, т.к. в целях эффективности такой сервер должен иметь доступ к критическим устройствам управления, которые являются источниками получаемых данных. Однако, по мере производственной необходимости может требоваться представление этих данных диспетчерам и персоналу по оптимизации производственного процесса, поэтому необходим более свободный доступ к устройству.

На основании полученной Зональной модели на следующей стадии осуществляется детальная оценка рисков ИБ в выбранной зоне [5].

Для оценки рисков выбрана зона критических устройств управления, т.к. она обладает свойством наибольшей критичности для технологического процесса, и, соответственно, наиболее строгими требованиями к обеспечению безопасности.

Оценка рисков будет производиться при помощи интеллектуальной системы поддержки принятия решений (ИСППР), разработанной на основе нечеткой нейронной сети (НС).

Разработка интеллектуальной системы поддержки принятия решений при оценке рисков ИБ на основе нечеткой нейронной сети

Построение нечеткой нейронной сети производится в программном пакете MATLAB с помощью специального графического редактора адаптивных нейронных сетей ANFIS. Редактор ANFIS позволяет создавать конкретную модель адаптивной системы нейро-нечеткого вывода, выполнять ее обучение, визуализировать структуру, изменять и настраивать ее параметры, а также использовать настроенную сеть для получения результатов нечеткого вывода [6].

Структура нечеткой нейронной сети представлена на рисунке 4.

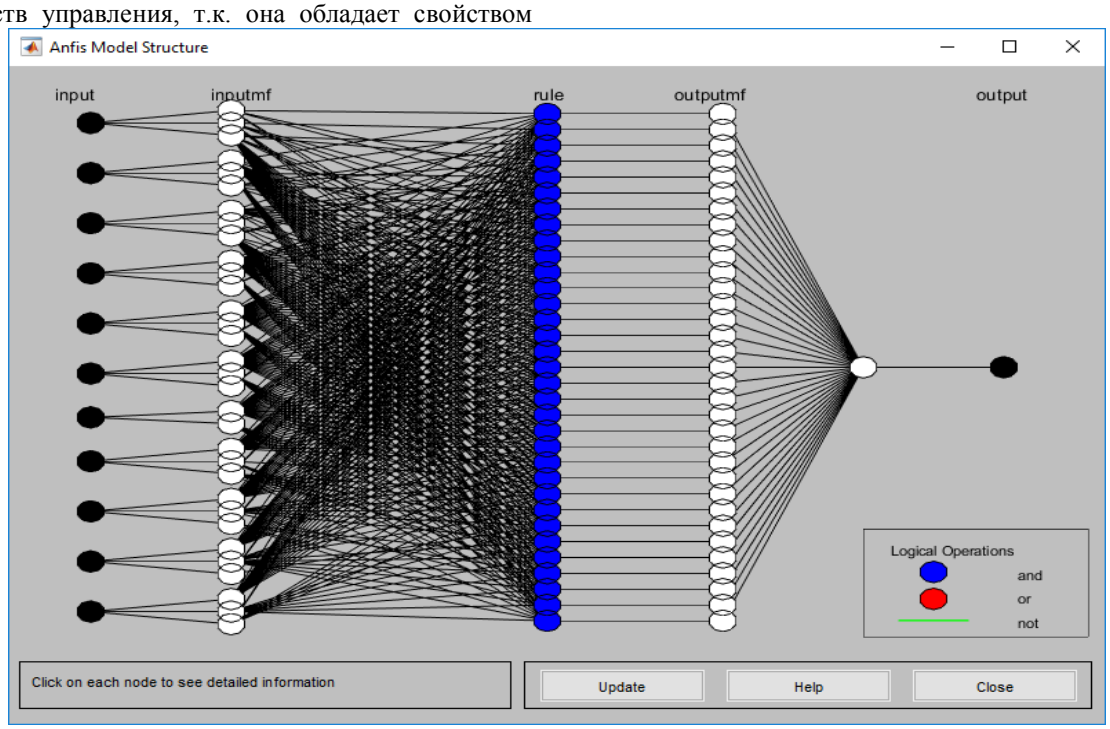

Рис. 4. Структура нечеткой нейронной сети

Показатель риска ИБ (R) определяется исходя из значений 11 входных факторов ($X_1 \div X_{11}$), определенных экспертом, с использованием системы правил, установленных экспертом.

В качестве *входных данных НС* будут использоваться значения 10 параметров (базовых метрик) для каждой угрозы информационной безопасности и значение уровня значимости информации (УЗ), обрабатываемой в выбранной зоне.

Угрозы информационной безопасности определены на основе «Методики определения угроз безопасности в информационных системах» [7], разработанной ФСТЭК России.

Для определения параметров (базовых метрик) угроз ИБ применим адаптированный для оценки угроз стандарт системы оценки уязвимостей CVSS [8]. Значения базовых метрик определяются экспертом на основе таблицы 1.

Таблица 1– Определение значений базовых метрик угроз ИБ АСУ ТП (фрагмент)

Параметр	Значение
f(Impact)	Характеризует актуальность угрозы ИБ и принимает следующие значения: 0 – если Impact = 0; 1,176 – если Impact ≠ 0
ConfImpact	Confidentiality Impact – влияние на конфиденциальность. Определяет степень воздействия угрозы ИБ на конфиденциальность информации и может принимать следующие значения: 0 – угроза ИБ не влияет на конфиденциальность; 0,275 – при определенных условиях угроза ИБ влияет на конфиденциальность; 0,66 – угроза ИБ влияет на конфиденциальность
Access-Complexity	Сложность доступа и реализации угрозы. Характеризует наличие контрмер угрозам ИБ АСУ ТП и может принимать следующие значения: 0,35 – существующие контрмеры значительно затрудняют реализацию угрозы ИБ АСУ ТП; 0,61 – существующие контрмеры недостаточны для противодействия угрозе ИБ АСУ ТП; 0,71 – контрмеры отсутствуют
Access-Vector	Вектор доступа. Определяет отношение источника угрозы к компонентам АСУ ТП и может принимать следующие значения: 0,395 – угроза ИБ может быть реализована при наличии локального (либо физического) доступа к компонентам АСУ ТП; 0,46 – угроза ИБ может быть реализована из сети передачи данных (СПД) предприятия (либо угроза может быть реализована внутри территории предприятия); 1 – угроза может быть реализована из внешних по отношению к СПД предприятия сетей (угроза может быть реализована вне территории предприятия)

Уровень значимости информации определяется на основе приказа ФСТЭК России N 31 [8]. В зоне критических устройств управления находятся: АРМ трубопровода, АРМ система обнаружения утечек и контроля активности (СОУиКА), АРМ АСУ ТП ППСН, АРМ СИКН и резервный АРМ СИКН. Уровень значимости информации определен в таблице 2.

Таблица 2– Уровень значимости информации

Ресурс	Информация	Степень ущерба	Уровень значимости
АРМ трубо-провода	Данные о состоянии задвижек	Средний	УЗ 2
АРМ СОУиКА	Данные об утечках нефтепродукта, о движениях грунта вблизи трубопровода, вибрации трубопровода, температуре	Средний	УЗ 2
АРМ АСУ ТП ППСН	Сигналы с датчиков технологи-ческого оборудования ППСН	Средний	УЗ 2
АРМ СИКН	Сигналы с датчиков СИКН	Средний	УЗ 2
Резервный АРМ СИКН			

Таким образом, информация, обрабатываемая на объекте защиты, имеет средний уровень значимости (УЗ 2), т.к. хотя бы для одного типа обрабатываемой информации определена средняя степень ущерба [9].

Входные данные вносятся в Microsoft Office Excel (рис. 5) и затем импортируются в рабочую область MATLAB.

Выходными данными НС являются показатели оценки риска ИБ (Ri) зоны критических устройств управления АСУ ТП ППСН, которые определяются по шкале от 1 до 4, где «1» – «низкий» уровень риска; «2» – «средний» уровень риска; «3» –«высокий» уровень риска; «4» - «критический» уровень риска.

Угрозы	Параметр (базовая метрика)						Impact	f(Impact)	Exploitability	BS	УЗ
	ConfImpact	IntegImpact	AvailImpact	Access-Complexity	Access-Vector	Authentication					
Просмотр информации на дисплее сотрудниками, не допущенными к администрированию АСУ, с целью дальнейшего разглашения	0,66	0	0	0,35	0,395	0,56	6,8706	1	1,5484	3,24172	2
Просмотр информации на дисплее посторонними лицами, находящимися в помещении, в котором ведется администрирование АСУ, с целью дальнейшего разглашения	0,66	0	0	0,35	0,395	0,56	6,8706	1	1,5484	3,24172	2
Угрозы уничтожения, изменения режимов функционирования, вывода из строя, хищения, разрушения оборудования АСУ и носителей информации путем физического доступа	0,275	0,66	0,66	0,35	0,395	0,56	9,537538	1	1,5484	4,841883	2
Угрозы внедрения вредоносных программ с АРМ	0,66	0,66	0,66	0,61	0,395	0,56	10,00085	1	2,69864	5,579963	2
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	0,275	0,275	0,275	0,61	0,395	0,56	6,442977	1	2,69864	3,445242	2
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение НСД с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	0,66	0,66	0,66	0,61	0,46	0,56	10,00085	1	3,14272	5,757595	2
Угрозы несанкционированного доступа к информации, хранящейся на сервере информационных систем	0,66	0,66	0,66	0,61	1	0,704	10,00085	1	8,5888	7,936027	2
Утрата ключей и атрибутов доступа	0,275	0,275	0,275	0,35	0,395	0,56	6,442977	1	1,5484	2,985146	2
Непреднамеренное разглашение информации о структуре АСУ сотрудниками	0,275	0	0	0,71	1	0,704	2,86275	1	9,9968	4,21637	2
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,275	0,66	0,66	0,35	0,395	0,45	9,537538	1	1,24425	4,720223	2
Непреднамеренное отключение средств защиты АСУ	0,275	0,275	0,275	0,35	0,395	0,45	6,442977	1	1,24425	2,863486	2
Непреднамеренное разглашение сведений о защите АСУ	0,275	0	0	0,71	1	0,704	2,86275	1	9,9968	4,21637	2

Рис. 5. Значения входных параметров (фрагмент)

Выходные данные НС определяются исходя из *правил*. Правила – способ представления знаний предметной области, на основе которых осуществляется принятие решений в той или иной ситуации, прогнозируется развитие ситуации с учетом состояния исследуемого объекта и внешней среды.

Правила оценки рисков ИБ зоны критических устройств управления приведены в таблице 3.

Таблица 3– Правила (фрагмент)

Риск	Правила
Низкий	- если уровень угрозы ИБ низкий и уровень значимости информации низкий; - если уровень угрозы ИБ низкий и уровень значимости информации средний;
Средний	- если уровень угрозы ИБ средний и уровень значимости информации низкий; - если уровень угрозы ИБ средний и уровень значимости информации средний; - если уровень угрозы ИБ низкий и уровень значимости информации высокий;

При оценке нейронной сети выборку, состоящую из 23 частей данных, разделили на обучающую и тестовую в соотношении 75% / 25%, т.е. на 17 частях данных провели обучение, а оставшиеся 6 частей использовали для тестирования НС.

В итоге получили следующие результаты эффективности обучения НС: train error (среднеквадратичная ошибка на обучающем множестве) = 0.0012; test error (среднеквадратичная ошибка на тестовом множестве) = 0.0817.

На рисунке 6 видно, что за 35 эпох обучения (1 эпоха = 1 цикл обучения) сеть обучена (Train) выдавать сигнал со среднеквадратичной ошибкой 0,00098363, а ошибка тестового набора (Test) менее 10^{-1}.

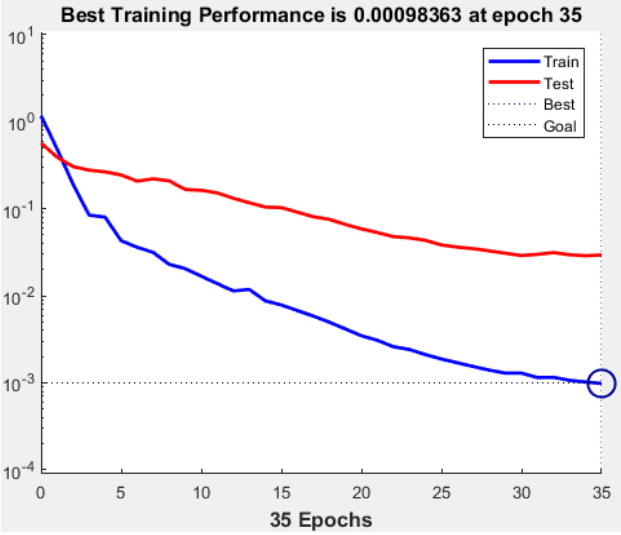

Рис. 6. График ошибки обучения НС

Таким образом, можно сделать вывод о высоком качестве обучения НС.

Результат выполнения программы и сравнение с Microsoft Excel представлены на рисунке 7.

MATLAB

```
trnMSE =

    0.0012


trainCompare =

    1.0292    1.0000
    1.0292    1.0000
    1.9877    2.0000
    2.0486    2.0000
    0.9999    1.0000
    2.0494    2.0000
    3.0000    3.0000
    1.0011    1.0000
    2.0292    2.0000
    1.9988    2.0000
    1.0115    1.0000
    2.0292    2.0000
    0.9965    1.0000
    0.9989    1.0000
    1.0000    1.0000
    2.0000    2.0000
    2.8884    3.0000


chkMSE =

    0.0817


trainCompare =

    3.0000    3.0000
    2.2872    2.0000
    2.2872    2.0000
    2.5698    2.0000
    2.0291    2.0000
    3.0000    3.0000


Обработка базы завершена за    2.675 с
```

Microsoft Excel

низкий	1
низкий	1
средний	2
средний	2
низкий	1
средний	2
высокий	3
низкий	1
средний	2
средний	2
низкий	1
средний	2
низкий	1
низкий	1
низкий	1
средний	2
высокий	3
высокий	3
средний	2
средний	2
средний	2
средний	2
высокий	3

Рис. 7. Сравнение результатов

Как видно из рисунка 7, выходные данные тестовой выборки и результаты, полученные с помощью Microsoft Excel, полностью совпадают.

Таким образом, результаты проведенных экспериментов показали, что разработанная ИСППР при оценке рисков информационной безопасности эффективна и может использоваться в повседневной практике.

Данная работа выполнена при поддержке гранта РФФИ-Поволжье № 17-48-020095.

Заключение

Предложена архитектура ИСППР, применение которой позволит повысить объективность принятия решений при оценке рисков информационной безопасности объектов критической информационной инфраструктуры.

Произведено моделирование объекта защиты, в результате которого построена зональная модель и выбрана зона, в которой будет производиться оценка рисков.

Определены угрозы и уровень значимости информации в выбранной зоне.

Определены входные, выходные данные и правила оценки рисков ИБ для нечеткой нейронной сети.

С помощью программного пакета MATLAB и редактора адаптивных нейронных сетей ANFIS разработана интеллектуальная система поддержки принятия решений при оценке рисков информационной безопасности на основе нечеткой нейронной сети.

Результаты проведенных экспериментов показали, что разработанная ИСППР эффективна и может использоваться в повседневной практике.

Список используемых источников

1. Кибератаки на критическую инфраструктуру / URL: http://www.jetinfo.ru/stati/kiberataki-na-kriticheskuyu-infrastrukturu-mif-ili-realnost (дата обращения: 14.01.2019).
2. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ / URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 14.01.2019).
3. Кибербезопасность АСУ ТП / URL: https://www.dialognauka.ru/press-center/article/13226/ (дата обращения: 14.01.2019).
4. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» / URL: http://docs.cntd.ru/document/1200114169 (дата обращения: 17.01.2019).
5. Слинин А.В. Моделирование АСУ ТП объекта нефтедобычи в контексте управления рисками ИБ. / Материалы Зимней школы-семинара аспирантов и молодых ученых – Уфа: УГАТУ, 2019 (в печати).
6. Нейросетевые технологии / URL: http://slidegur.com/doc/1681660/nejrosetevye-tehnologii-v-obrabotke-i-zashhite-dannyh (дата обращения: 25.01.2019).
7. Методика определения угроз безопасности в информационных системах. ФСТЭК России, 2015 г. / URL: http://fstec.ru/component/attachments/download/812 (дата обращения: 18.01.2019)..
8. A Complete Guide to the Common Vulnerability Scoring System Version 2.0 / URL: http://www.first.org/cvss/cvss-guide.html (дата обращения: 26.01.2019).
9. Приказ ФСТЭК России от 14.03.2014 N 31 "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" / URL: http://www.consultant.ru/document/cons_doc_LAW_165503/ (дата обращения: 18.01.2019).