УДК 004.89 Вестник УрФО № 1(39) / 2021, с. 54–61

Асяев Г.Д., Соколов А.Н.

DOI: 10.14529/secur210107

МОДЕЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ НА ОСНОВЕ МЕТОДА ПРЕДИКТИВНОЙ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ РЕКУРРЕНТНОЙ И ПОЛНОСВЯЗНОЙ НЕЙРОННЫХ СЕТЕЙ [1]

В статье проанализированы основные причины роста количества успешно реализованных кибератак, связанные с особенностями функционирования автоматизированных систем управления технологическими процессами (АСУ ТП). Показано, что традиционные подходы, связанные с разработкой моделей угроз и применением стандартных сертифицированных решений для обеспечения информационной безопасности АСУ ТП не всегда эффективны. На основе нового критерия защищенности автоматизированной системы и метода предиктивной защиты предложена модель на основе двух искусственных нейронных сетей, позволяющая по косвенным признакам (параметрам) системы определить возможность наступления кибератаки и спрогнозировать время, через которое она наступит, а также выбрать соответствующие меры защиты. В результате работы модели формируется перечень действий при обнаружении новых видов угроз, связанных с деструктивными воздействиями на объект, исходя из приемлемости прогнозируемых последствий работы АСУ ТП.

Ключевые слова: *автоматизированная система управления технологическим процессом (АСУ ТП), деструктивное воздействие, инцидент информационной безо-*

[1] Исследование выполнено при финансовой поддержке гранта РФФИ и Челябинской области в рамках научного проекта № 20-47-740006

пасности, искусственная нейронная сеть (ИНС), кибератака, конкатенация функций, критическая информационная инфраструктура, предиктивная защита.

Asyaev G.D., Sokolov A.N.

A MODEL FOR ENSURING INFORMATION SECURITY OF AN AUTOMATED PROCESS CONTROL SYSTEM BASED ON THE PREDICTIVE PROTECTION METHOD USING RECURRENT AND FULLY CONNECTED NEURAL NETWORKS

The article analyzes the main reasons for the growth in the number of successfully implemented cyberattacks related to the functions of functioning of automated process control systems (APCS). It is shown that the traditional approaches associated with the development of threat models and standard certified solutions for information security of ICS are not always effective. On the basis of a new criterion for the security of an automated system and a method of predictive protection, a model based on two artificial networks has been proposed, which makes it possible, by indirect signs (parameters), to determine the possibility of a cyber attack and predict the time after which it will come, as well as to select appropriate protection measures. As a result of the operation of the model, a list of actions is formed upon detection of new types of threats associated with destructive effects on the object, based on the acceptability of the predicted consequences of the operation of the APCS.

Keywords: *automated process control system (APCS), destructive impact, information security incident, artificial neural network (ANN), cyberattack, function concatenation, critical information infrastructure, predictive protection.*

1. Введение

Развитие информационных технологий сопровождается постоянным пополнением арсенала средств, используемых злоумышленниками для реализации кибератак, в том числе на объекты критической информационной инфраструктуры. При этом, несмотря на то, что на большинстве объектов используются средства защиты, количество успешно проведенных кибератак возрастает [1]. Вероятной причиной этого роста является несовершенство применяемых моделей информационной безопасности на основе традиционных подходов, связанных с разработкой моделей угроз и применением стандартных сертифицированных решений по защите информации.

Одним из подходов, связанных с обеспечением защиты информации в автоматизированной системе управления технологиче-

ским процессом (АСУ ТП), является подход, основанный на постоянном мониторинге трафика всех действий системы. Анализ трафика позволяет вовремя выявить аномальное поведение системы и сформировать меры по нейтрализации деструктивных воздействий. К аномальным относятся редкие данные, события или наблюдения, которые вызывают подозрения ввиду существенного отличия от большей части данных. Аномальным поведением называют нестандартное поведение системы, отличное от нормального, влекущее за собой отклонение от технологического процесса [2].

Важными особенностями функционирования АСУ ТП являются [3]:

• различная степень критичности выхода из строя отдельных элементов АСУ ТП в зависимости от технологического процесса;

• промышленные информационные системы могут работать годами, их остановка недопустима или невозможна. Это затрудняет установку обновлений для программного обеспечения для устранения уязвимостей, а также другое регулярное вмешательство в сам процесс работы [4];

• многие АСУ ТП используют закрытые проприетарные протоколы. Их производители, как правило, не реализуют адекватные политики поиска и исправления уязвимостей [4].

Перечисленные особенности приводят к выводу о необходимости постоянного аудита и оценки рисков для предотвращения инцидентов информационной безопасности АСУ ТП [5].

В [3] был сформулирован новый критерий защищенности автоматизированной системы (АС), используемой в замкнутом контуре управления объектом (функциональной подсистемой): система является защищённой, если под воздействием факторов, влияющих на информацию, передаточная функция АС меняется таким образом, что качество управления объектом управления остаётся в заданных пределах. При этом под передаточной функцией подразумевается зависимость сигнала, подаваемого вход объекта управления, от структуры управляющего информационного трафика, поступающего на вход АС. Деструктивное воздействие кибератаки приводит к изменению управляющего трафика и самой управляющей функции, в результате чего на объект поступает искажённый сигнал управления. Последствия деструктивного воздействия можно считать приемлемыми, если качество управления объектом управления при этом остаётся в заданных пределах.

На основании критерия защищенности АС в [1] сформулировано понятие предиктивной защиты как деятельности, позволяющей по косвенным признакам (параметрам) системы определить возможность наступления кибератаки и спрогнозировать время, через которое она наступит, а также выбрать соответствующие меры защиты.

С точки зрения предиктивной защиты весь процесс обеспечения безопасности можно представить в виде модели из трех блоков, связанных между собой, для каждого из которых характерны свои специфичные угрозы (рис. 1).

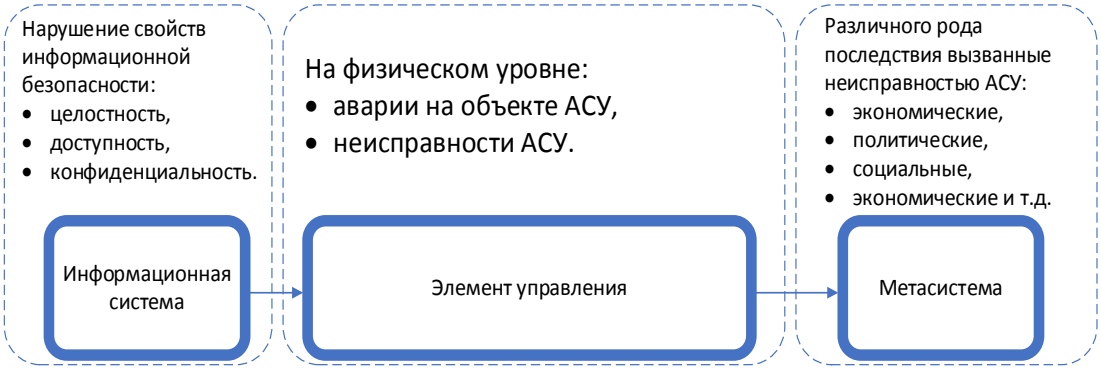


Рис. 1. Угрозы информационной безопасности на различных уровнях управления автоматизированной системы

Стоит также заметить, что модель, представленная на рис. 1, носит последовательный характер: нарушение свойств информации на уровне информационной системы АСУ приводит к определенным последствиям на уровне объекта управления и метасистемы. Для информационной системы АСУ ТП наиболее важными свойствами с точки зрения обеспечения безопасности информации

являются её целостность и доступность. Обеспечение конфиденциальности технологической информации при этом не является первоочередной задачей [1]. При выявлении нарушений каких-либо свойств безопасности на уровне управляющего устройства наступает нарушение работы на физическом уровне (сбои, аварии, отказ в обслуживании и т.д.). После этого рассчитываются последствия для системы при нарушении работы соответствующего управляющего блока.

Информационные потоки подразделяются на:

• поток данных, генерируемый функцией или элементом управления;

• поток данных, формируемый командами используемого программного обеспечения;

• набор данных, хранящихся непосредственно на элементе управления.

Потоки информации предназначены для обмена между различными элементами управления технологическим процессом или для реализации элементами контроля их внутренних функций. Элемент управления представляет собой промышленный контроллер или автономное устройство, принимающее сигналы от контролируемых функций. При этом верхний уровень управляется с помощью программного обеспечения, которое обеспечивает координацию всего технологического процесса, в то время как функции автоматизации нижнего уровня управляются посредством программного обеспечения исполнительных устройств и средств, которые управляют ими. Современные средства защиты информации представляют собой систему фильтрации трафика в соответствии с созданными черными и белыми списками, которые запрещают или разрешают выполнять соответствующие команды, пропускать трафик [6]. Стоит отметить, что списки разграничения доступа формируются из некой эвристической модели, составляемой администратором безопасности. Именно к новым типам кибератак (которые еще неизвестны или не были проведены) большинство современных средств защиты информации, как правило, неустойчивы.

Относительно недавно стали применяться интеллектуальные системы управления, основанные на использовании искусственных нейронных сетей (ИНС) [7]. Подобные системы могут обучаться на определенной выборке известных событий информационной безопасности и распознавать менее известные или абсолютно новые кибератаки [1]. Основной сложностью при создании таких систем является формирование обучающей выборки исходных данных требуемого объёма. В условиях постоянного изменения модели угроз информационной безопасности и вариативности характеристик объектов управления сформировать такую выборку за достаточно короткое время далеко не всегда возможно. Даже не смотря на то, что системы на основе ИНС позволяют классифицировать кибератаки на ранних стадиях, этого не всегда бывает достаточно.

2. Модель «раннего» обнаружения инцидентов информационной безопасности на основе метода предиктивной защиты. Постановка задачи и ее решение с использованием искусственных нейронных сетей

Целью представленного исследования является построение модели обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты, отличительной особенностью которой является способность «раннего» обнаружения инцидентов информационной безопасности, то есть прогнозировать инциденты, влекущие негативные последствия, до их появления. Поскольку в этой постановке задачи модель должна прогнозировать время, через которое возможно наступление кибератаки (в том числе ее временные и числовые характеристики) и формировать соответствующую стратегию защиты, для обучения использована нейронную сеть «с подкреплением» (с созданием «агента») [8]. В качестве такой сети выбрана рекуррентная нейронная сеть с сетью смеси распределений на выходе (Recurrent Neural Network with Mixture Density Network output, MDN-RNN). Такая сеть обладает особенностью – «мышлением наперед», важной с точки зрения поставленной задачи (рис. 2). Для рекуррентной нейронной сети долгосрочной памяти (LSTM) достаточно 256 слоев, чтобы выявить общие паттерны для прогнозирования и в то же время не переобучиться под конкретную выборку. Recurrent Neural Network фиксирует внутреннее текущее состояние безопасности управляющего объекта в своем окружении с целью предсказывать последующее состояние на основе предыдущего и совершённого действия.

Следующим шагом в рассматриваемой архитектуре представленной модели является выбор стратегии защиты. Этот механизм

реализован с помощью контроллера на основе полносвязной нейронной сети (рис. 3): на вход подается текущее состояние *z* и скрытое состояние *h* (для предсказания следующего значения), где *z* и *h* представляют собой числовые векторы [9]. На выходе контроллера формируется сигнал a, определяющий некую меру защиты как конкатенацию функций *z* и *h*.

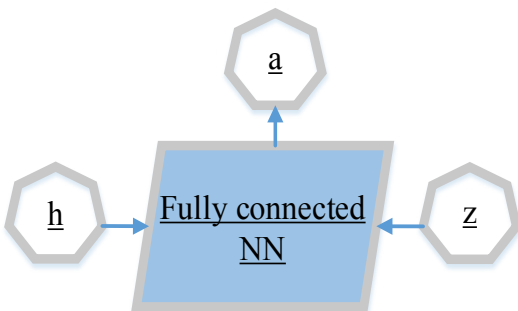


Рис. 3. Модель контроллера на основе полносвязной нейронной сети

На рис. 4 представлена общая модель обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты. Система по косвенным признакам определяет состояние АСУ ТП (аномальное поведение системы), прогнозирует время, при наступлении которого возможны негативные последствия. Далее выполняется расчет уровня прогнозируемых последствий, на основе которого контроллер выбирает оптимальный вариант защиты из некоторого множества [7].

Модель реализована в облачной среде разработке Google Collab. На рис. 5 показан фрагмент потока данных процесса вычисления последствий (damage) для каждой итерации (iteration), основной задачей при этом является минимизация значения уровня последствий. Общий уровень последствий для каждой эпохи определялся как арифметическое среднее значений последствий на 7 итерациях.

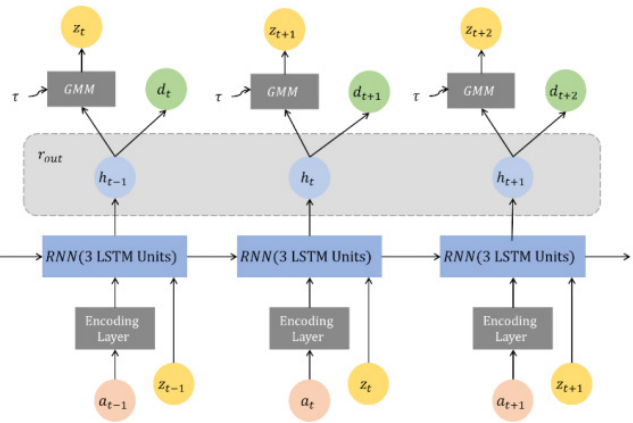


Рис. 2. Структура бокса LSTM RNN-MDN

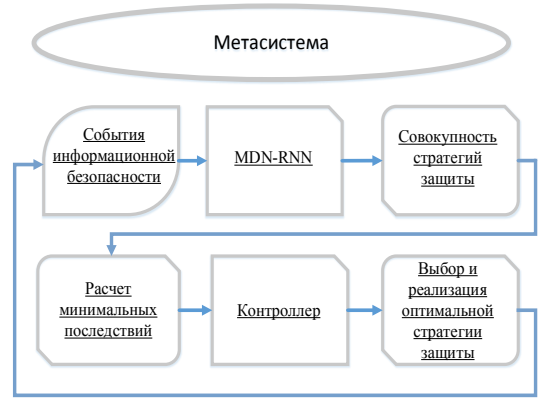


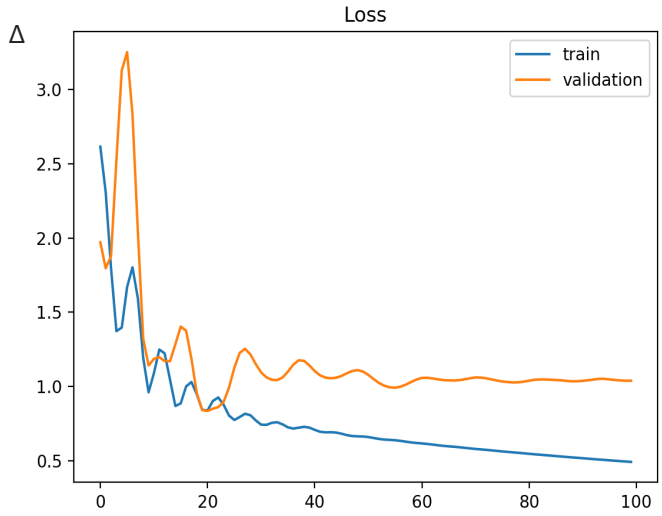
Рис. 4. Общая модель обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты

3. Результаты экспериментов

На рис. 6 представлен график зависимости значения уровня последствий от количества итераций. Чем выше это значение, тем более значительными являются негативные последствия для метасистемы. Из рисунка видно, что при увеличении количества итераций уровень последствий уменьшается. Синей (темной) линией (train) показано изменение уровня последствий на обучающей выборке, а оранжевой (светлой) линией (validation) – на валидационной выборке, т.е. на новых данных, которые модель еще не обрабатывала.

```
Iteration #50 damage: 0.8528947830200195
Iteration #100 damage: 0.8866778016090393
Iteration #150 damage: 0.8778553009033203
Iteration #200 damage: 0.6406872272491455
Iteration #250 damage: 0.673102080821991
Iteration #300 damage: 0.6530210971832275
Epoch #0 damage: 0.7833202557753672
Iteration #350 damage: 0.6791139841079712
Iteration #400 damage: 0.7526218891143799
Iteration #450 damage: 0.8202939629554749
Iteration #500 damage: 0.5508345365524292
Iteration #550 damage: 0.6866168975830078
Iteration #600 damage: 0.5532808899879456
Iteration #650 damage: 0.784627377986908
Epoch #1 damage: 0.7561166847349972
Iteration #700 damage: 0.7903854846954346
Iteration #750 damage: 0.7944695949554443
Iteration #800 damage: 0.8289942741394043
Iteration #850 damage: 0.5659400224685669
```

Рис. 5. Фрагмент потока данных процесса расчета уровня последствий



N – номер итерации;
Δ - значение уровня последствий

Рис. 6. Значение уровня последствий в зависимости от количества итераций на обучающей (train) и тестовой (validation) выборке

4. Заключение

Таким образом, в статье представлена общая модель обеспечения информационной безопасности АСУ ТП на основе метода предиктивной защиты, которая использует две ИНС:

• рекуррентную нейронную сеть с сетью смеси распределений на выходе (MDN-RNN), которая оценивает временные и числовые характеристики прогнозируемого инцидента информационной безопасности;

• полносвязную нейронную сеть, которая реализует контроллер, позволяющий осуществлять выбор стратегии обеспечения информационной безопасности из числа возможных.

В результате работы модели формируется перечень действий при обнаружении новых видов угроз, связанных с деструктивными воздействиями на объект, исходя из приемлемости прогнозируемых последствий работы АСУ ТП.

Литература

1. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности, 2019. №3(31). С. 30-36.

2. Боровков А.И. «Умные» цифровые двойники – основа новой парадигмы цифрового проектирования и моделирования глобально конкурентоспособной продукции нового поколения. Трамплин к успеху// Журнал АО «ОДК». 2018. № 13. С. 12-18.

3. Правиков Д.И. Об одном подходе к обеспечению информационной безопасности автоматизированных систем // Вопросы защиты информации. 2007. № 3. С. 17-19.

4. Гарбук С.В., Бурцев А.Г. Методические основы исследования уязвимостей компонентов АСУ ТП // Защита информации. Inside. 2012. № 3. С. 34-38.

5. Гарбук С.В. Перспективы применения интеллектуальных технологий для решения задач безопасности // Национальная безопасность / 2016. № 4. С. 451-457.

6. Башлыков А.А., Еремеев А.П. Методы и программные средства конструирования интеллектуальных систем поддержки принятия решений для объектов энергетики // Вестник МЭИ. 2018. № 1. С. 72—85.

7. Гарбук С.В. Интеллектуальные автоматизированные средства тематической обработки информации в системах безопасности // Искусственный интеллект и принятие решений. 2017. № 1. С. 95-104.

8. Гарбук С.В., Бакеев Р.Н. Конкурентная оценка качества технологий интеллектуальной обработки данных // Проблемы управления. 2017, № 6. С. 50-62.

9. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности 2019 №3 (31). С. 30-36.

References

1. Garbuk S.V., Pravikov D.I., Polyanskiy A.V., Samarin I.V. Obespechenie informatsionnoy bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoy zashchity // Voprosy kiberbezopasnosti, 2019. No. 3(31). pp. 30-36.

2. Borovkov A.I. «Umnye» tsifrovye dvoĭniki – osnova novoĭ paradigmy tsifrovogo proektirovaniya i modelirovaniya global'no konkurentosposobnoĭ produktsii novogo pokoleniya. Tramplin k uspekhu// Zhurnal AO «ODK». 2018. No. 13. pp. 12-18.

3. Pravikov D.I. Ob odnom podkhode k obespecheniyu informatsionnoĭ bezopasnosti avtomatizirovannykh sistem // Voprosy zashchity informatsii. 2007. No. 3. pp. 17-19.

4. Garbuk S.V., Burtsev A.G. Metodicheskie osnovy issledovaniya uyazvimosteĭ komponentov ASU TP // Zashchita informatsii. Inside. 2012. No. 3. pp. 34-38.

5. Garbuk S.V. Perspektivy primeneniya intellektual'nykh tekhnologiĭ dlya resheniya zadach bezopasnosti // Natsional'naya bezopasnost' / 2016. No. 4. pp. 451-457.

6. Bashlykov A.A., Eremeev A.P. Metody i programmnye sredstva konstruirovaniya intellektual'nykh sistem podderzhki prinyatiya reshenĭ dlya ob"ektov energetiki // Vestnik MEI. 2018. No. 1. pp. 72—85.

7. Garbuk S.V. Intellektual'nye avtomatizirovannye sredstva tematicheskoĭ obrabotki informatsii v sistemakh bezopasnosti // Iskusstvennyĭ intellekt i prinyatie reshenĭ. 2017. No. 1. pp. 95-104.

8. Garbuk S.V., Bakeev R.N. Konkurentnaya otsenka kachestva tekhnologiĭ intellektual'noĭ obrabotki dannykh // Problemy upravleniya. 2017, No. 6. pp. 50-62.

9. Garbuk S.V., Pravikov D.I., Polyanskiy A.V., Samarin I.V. Obespechenie informatsionnoy bezopasnosti ASU TP s ispol'zovaniem metoda prediktivnoy zashchity // Voprosy kiberbezopasnosti 2019 No. 3 (31). pp. 30-36.

АСЯЕВ Григорий Дмитриевич, аспирант кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: asiaevgd@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, д. 76. E-mail: sokolovan@susu.ru

ASYAEV Grigorii Dmitrievich, postgraduate student of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: asiaevgd@susu.ru

SOKOLOV Alexander Nikolaevich, Ph.D., Associate professor, Head of the department of information security of the school of electrical engineering and computer science in FSAEI HE «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru