Чернышев Л.О., Лебедев В.В., Семеенков Д.С. Проблемы защиты информации в автоматизированных системах управления. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XIX Междунар. научно-техн. конф. – Пенза: ПДЗ, 2019. – С. 117-120.

УДК 004.056.53

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Л.О. Чернышев, В.В. Лебедев, Д.С. Семеенков

PROBLEMS OF INFORMATION PROTECTION IN AUTOMATED MANAGEMENT SYSTEMS

L.O. Chernyshev, V.V. Lebedev, D.S. Semeenkov

Аннотация. В статье раскрыты актуальные проблемы защиты информации в системах управления технологическими процессами. Показано, что разнообразие элементов инфраструктуры предприятия обуславливает индивидуальный подход к каждому конечному узлу системы автоматизации. Перспективными в предметной области являются алгоритмы рекуррентных нейронных сетей, используемые для прогнозирования состояния системы. Раскрыты достоинства и основные недостатки использования методов машинного обучения в системах обнаружения вторжений.

Ключевые слова: безопасность, защита информации, системы автоматизации, машинное обучение.

Abstract. The article reveals the current problems of information security in process control systems. It is shown that the variety of infrastructure elements of the enterprise determines an individual approach to each end node of the automation system. Promising in the subject area are the algorithms of recurrent neural networks used to predict the state of the system. The advantages and the main disadvantages of using machine learning methods in intrusion detection systems are disclosed.

Keywords: security, information protection, automation systems, machine learning.

В публикации [1] были раскрыты особенности процессов интеллектуализации и детализованы подходы к обеспечению информационной безопасности с использованием технологии глубокого обучения в корпоративных сетях. Далее рассмотрим актуальные проблемы защиты информации в автоматизированных системах управления технологическими процессами (АСУ ТП).

Современная децентрализация обработки данных и взаимодействие распределенных систем с использованием сети Интернет приводит к необходимости качественного повышения уровня кибербезопасности автоматизированных систем управления технологическими процессами. Вместе с тем в большинстве корпоративных компаний по-прежнему наблюдаются проблемы с обеспечением элементарных мер защиты информации, а интеграция информационных технологий приводит к появлению уязвимостей, понятных только узкому кругу экспертов. Ситуацию ухудшает снижение порога входа в «киберпреступность», причем организация атак уже не требует приобретения специальных знаний и навыков, поскольку все необходимые для нее средства злоумышленник может найти в широком доступе с применением криптовалют [2].

Примером служит информация, представленная на сайте US ICS-CERT. Специалистами представлено 415 уязвимостей в подсистемах АСУ ТП, что на 93 угрозы превышает показатели прошлого года. Аналогичная ситуация наблюдается с компьютерами подсистемы АСУ, в которой на 3,2% возросло количество машин, зараженных вредоносными объектами.

Тенденции в сфере угроз и возможные риски потерь промышленных предприятий находятся в сфере внимания государственного аппарата. В 2017 году был принят закон 187-ФЗ о безопасности критической информационной инфраструктуры, который начал действовать с начала 2018 года. Согласно этому закону, все экономически значимые для страны объекты производства и обеспечения (объекты критической информационной инфраструктуры - КИИ) должны строго соответствовать требованиям регламента. Ключевым моментом в федеральном законе является процедура интеграции КИИ с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). ГосСОПКА представляет собой единый территориально распределенный комплекс, включающий силы и программно-технические средства обнаружения, предупреждения и ликвидации последствий компьютерных атак [3].

Комплексность и разнообразие элементов инфраструктуры промышленного предприятия обуславливает индивидуальный подход к каждому конечному узлу системы автоматизации. Комплексный характер средств защиты информации вместе с регламентацией доступа к корпоративным данным способствует снижению рисков нанесения вреда и потерь в процессах технологического управления и заключается в эшелонировании различных элементов инфраструктуры промышленных предприятий, основанном на разделении ответственности компонентов защиты программно-технического решения. Рынок существующих в настоящее время решений кибербезопасности АСУ ТП составляют комплексные проекты Positive Technologies, InfoWatch, Kaspersky и UserGate и ряда других компаний-производителей.

Комплексная защита информации на нижних уровнях АСУ ТП, формирующая взаимодействие с технологическим оборудованием, также предполагает внедрение программно-логических комплексов (ПЛК), которые обеспечивают: процедуру аутентификации; поддержку криптографических протоколов; использование возможностей СКУД и межсетевого экрана.

Использование комплексов защиты на этом уровне управления позволяет снизить риски потерь за счет делегирования полномочий системы внутренним специалистам, минимизации использования внешних программных средств (например, в случае клонирования и подделки ПО) и необходимости учёта рисков и угроз при сопровождении или модификации АСУ ТП.

Тем не менее адекватное реагирование на инциденты, связанные с ошибками управления, возможно только при наличии на рабочем месте квалифицированного специалиста, что послужило основанием для образо-

вания "Центров безопасности" (SOC), необходимых для централизованной поддержки предприятий в случае возникновения нестандартных ситуаций и для организации технического контроля. Механизмы обнаружения, предупреждения и ликвидации с использованием SOC относятся к сфере регулирования упомянутого выше закона 187-ФЗ "О безопасности критической информационной инфраструктуры".

Дальнейшей перспективой предметной области являются алгоритмы рекуррентных нейронных сетей, используемые для прогнозирования будущего состояния системы с целью определения отклонения фактических значений от ожидаемых. Рекуррентная нейронная сеть построена на последовательности элементов, образующих направленную структуру, вследствие чего модель способна запоминать серии событий. Недостатком этой архитектуры является низкая эффективность работы с долговременными закономерностями.

Решение проблемы с запоминанием долговременных зависимостей относится к архитектуре "долгая краткосрочная память" (Long short-term memory; LSTM), в которой используется несколько слоев, взаимодействующих определенным образом. Такой способ построения позволяет избежать ошибок при запоминании долгосрочных зависимостей и получил широкое распространение в разных областях интеллектуальной деятельности.

Важным преимуществом данных методов машинного обучения является стоимость и простота внедрения, поскольку участие эксперта при обучении нейронной сети практически не требуется, и она способна предсказывать неизвестные до настоящего времени типы вторжений. Однако невозможность объяснения итоговых показателей работы сети, отсутствие или малое количество примеров "атаки" на корпоративную сеть промышленной организации приводит к тому, что специалистам по кибербезопасности приходится моделировать эти ситуации посредством натурного или виртуального эксперимента. Поэтому к основной задаче машинного обучения в настоящий момент относится разработка технологий обучения, способствующих сокращению количества выборки, необходимой для обучения системы.

Библиографический список

1. Чернышев Л.О., Лебедев В.В., Семеенков Д.С. Информационная безопасность в технологиях интеллектуальных систем // Информационные ресурсы и системы в экономике, науке и образовании: сборник статей IX Международной научно-практической конференции / под ред. А.П. Ремонтова. Пенза, 2019. С. 194-197.

2. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018 // KASPERSKY LAB ICS CERT. URL: https://ics-cert.kaspersky.ru /reports /2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018 / (дата обращения: 30.05.19).

3. Закон Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 № 187-ФЗ // Российская газета. 31.07.2017. № 167.

Чернышев Леонид Олегович
Тверской государственный
технический университет,
г. Тверь, Россия

Лебедев Владимир Владимирович
Тверской государственный
технический университет,
г. Тверь, Россия

Семеенков Дмитрий Сергеевич
Тверской государственный
технический университет,
г. Тверь, Россия
E-mail: mr.semeenkov@mail.ru

Chernyshev L.O.
Tver State Technical University,
Tver, Russia

Lebedev V.V.
Tver State Technical University,
Tver, Russia

Semeenkov D.S.
Tver State Technical University,
Tver, Russia