Информатика, вычислительная техника и управление

УДК 004.056.53
DOI: 10.30987/1999-8775-2020-7-48-53

Н.М. Кузнецова, Т.В. Карлова, А.Ю. Бекмешов

РЕШЕНИЕ ЗАДАЧИ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ЗАЩИТЫ СТРАТЕГИЧЕСКИ ВАЖНЫХ РЕСУРСОВ ПРЕДПРИЯТИЯ ОТ КОМПЛЕКСНЫХ КИБЕР-АТАК НА ОСНОВЕ АНАЛИЗА ТАКТИК ЗЛОУМЫШЛЕННИКОВ

Решены задачи предотвращения реализации комплексных кибер-атак. Использованы методы информационного анализа основных тактик злоумышленников, повышен уровень безопасности стратегически важных ресурсов промышленного предприятия. Разработан соответствующий комплекс мер противодействия. Предложена модульная структура автоматизированной системы защиты.

Ключевые слова: автоматизация, защита информации, ресурсы, кибер-атаки, анализ тактик, злоумышленники.

N.M. Kuznetsova, T.V. Karlova, A.Yu. Bekmeshov

SOLUTION OF PROTECTION AUTOMATION PROBLEM OF COMPANY STRATEGIC RESOURCES AGAINST COMPLEX CYBER-ATTACKS BASED ON CRIMINAL TACTICS ANALYSIS

The purpose of the scientific work is maximum safety provision for industrial company resources. To achieve the purpose specified there is a necessity in the solution of the problem in the prevention of most dangerous modern cyber-attacks the attacks of *APT (advanced persistent threats)* class – complex cyber-attacks directed to the infrastructure changes of company basic automated systems.

Most modern industrial enterprises are related to the objects of critical information infrastructure: the development of state strategically significant branches and population safety depend on their operation quality.

Within the limits of the problem specified in the paper there are analyzed basic criminal tactics methods, revealed their peculiarities and offered corresponding measures for counteraction.

Besides, in the paper there are used methods for the information analysis of two basic tactics of criminals: "white" advantages – the "white" move first; "pawn attack" – inconspicuous penetration into majority of company systems with the purpose of their operation analysis and further reset.

In the paper there are revealed peculiarities of *APT* cyber-attacks, in particular, the stages of passive observation (analysis of company systems operation) and active intervention (changes introductions into in work algorithms).

The work novelty consists in the developed module structure of the automated protective system which includes a maximum possible amount of modern methods to ensure resources safety.

As a result of the analysis carried it was defined that the most efficient counteraction to *APT* cyber-attacks is the application of a complex approach including preventive protective measures.

Key words: automation, information protection, resources, cyber-attacks, tactics analysis, hackers.

Введение

Особенностью современных методов реализации угроз нарушения информационной безопасности стратегически важных ресурсов предприятия является их целенаправленность не столько на нарушение конфиденциальности, сколько на нарушение целостности ресурсов за счёт разрушения их инфраструктуры. Статья посвящена разработке комплекса мер противостояния данным целенаправленным кибер-атакам на основе анализа тактик злоумышленников.

Яркими примерами целевых кибер-атак (далее *APT – advancedpersistentthreats*

– целевая кибер-атака) являются *StuxNet*, поразившие автоматизированную систему управления технологическим процессом (далее АСУ ТП) *SCADA* предприятия ядерной промышленности Ирана в 2010 г, а также проекты *Aurora* и *Red October*, которые были направлены на крупные компании с целью осуществления кибершпионажа в отношении стран СНГ [1, 2].

Большинство современных промышленных предприятий относится к объектам критической информационной инфраструктуры (далее КИИ), требующих высокого уровня защиты информации [3]. Как правило, к стратегически важным ресурсам промышленного предприятия относятся: информационные, интеллектуальные, программно-аппаратные и технические ресурсы, входящие в состав основных АСУ ТП предприятия [4-7].

На языке шахмат к основным характеристикам *APT* можно отнести:

- «преимущество белых шахмат»: злоумышленники ходят первыми – так называемая атака нулевого дня («*zero-dayattack*»), на момент реализации которой не существует метода её предотвращения, так как она является абсолютно новой для систем защиты;
- «пешечный штурм»: злоумышленник выстраивает свою армию из, казалось бы, не значащих фигур (закладок, люков, найденных небольших брешей в системе защиты и т.д.) для дальнейшего совершения молниеносной единовременной атаки – «обрушения». Как правило, более 98 % времени у злоумышленника уходит на подготовку («выстраивание пешек»).

Анализ тактики злоумышленника «Преимущество белых шахмат»

Яркий пример *APTStux Net* отличается не столько новизной применяемых методов атаки, сколько новизной самого принципа: впервые в истории кибер-войн субъектом атаки стала физическая инфраструктура предприятия, а не информационные ресурсы [2, 8]. Информационные и программно-аппаратные ресурсы предприятия стали механизмом реализации, но не целью как таковой. В итоге система защиты не справилась со своей задачей, так как атака оказалась совершенно новой.

По сути *Stux Net* поразил предприятие КИИ – завод по обогащению урана. В настоящее время в нашей стране к предприятиям КИИ относятся:

- предприятия легкой промышленности;
- предприятия тяжелей промышленности;
- медицинские организации;
- организации транспортной отрасли;
- предприятия станкостроения, самолётостроения, автомобилестроения;
- предприятия энергетического сектора и т.д. [3]

Таким образом, объектом *APT* может оказаться большинство современных предприятий, в связи с чем задача обеспечения защиты является актуальной проблемой [9, 10].

Анализ тактики злоумышленника «Пешечный штурм»

Подготовка к штурму состоит из двух этапов.

Этап 1 – пассивное наблюдение.

1. Исследование особенностей защищаемых АСУ ТП:

- анализ особенностей функционирования основных процессов АСУ ТП;
- анализ взаимодействия ресурсов АСУ ТП;
- исследование основных информационных потоков АСУ ТП;

2. Исследование особенностей систем (механизмов) защиты:

- анализ методов защиты;
- анализ методов контроля со стороны систем (механизмов) защиты.

Этап 2 – активное, но малозаметное и долгосрочное вмешательство:

- малозаметное внесение изменений в настройки АСУ ТП;
- малозаметное внесение изменений в настройки систем (механизмов) защиты;

- применение методов социальной инженерии: сбор информации от бывших сотрудников; подкуп сотрудников; запугивание сотрудников; применение схем мошенничества; попытки влияния на процессы принятия решений.

Наиболее опасными являются методы социальной инженерии, направленные на сотрудников отдела информационной безопасности предприятия, так как именно они осведомлены о большинстве характеристик систем (механизмов) защиты.

Основные меры защиты стратегически важных ресурсов от *APT*

В связи с особенностями рассмотренных тактик злоумышленников система защиты (комплекс механизмов защиты) должна обеспечивать в первую очередь:

- мониторинг изменений АСУ ТП: настроек АСУ ТП; характеристик внутренних и внешних информационных потоков;

- применение мер противостояния социальной инженерии: составление правил обращения с ресурсами (в рамках политики информационной безопасности предприятия); проведение соответствующих мероприятий:

- по ознакомлению с принятыми на предприятии правилами обращения с ресурсами;
- с методами защиты;
- с типичными схемами мошенничества;

- анализ действий сотрудников:

- выявление нехарактерных действий в рамках информационных потоков (например, передача информации от сотрудника экономического отдела сотруднику отдела разработки является нехарактерным действием);
- выявление нехарактерного поведения (как правило, с помощью методов динамической биометрической аутентификации).

Таким образом, согласно проведенному анализу основных тактик злоумышленников и классификации методов противодействия их реализации, комплекс мер защиты формируется путем применения методов отслеживания изменений настроек защищаемых автоматизированных систем, а также методов противодействия социальной инженерии.

При выборе средств защиты необходимо использование аналоговой модели принятия решения – схемы информационного взаимодействия сотрудников предприятия с АСУ ТП. Также необходимо применение алгоритмов выявления причинно-следственных связей между событиями информационной безопасности путем анализа потоков данных (как внешних, так и внутренних).

Автоматизация процессов защиты стратегически важных ресурсов предприятия

К процессам защиты стратегически важных ресурсов предприятия, которые могут быть автоматизированы, относятся:

- мониторинг изменений АСУ ТП;
- формирование, хранение и распределение материалов базы знаний информационной безопасности (БЗИБ) (правила обращения со стратегически важными ресурсами, данные о методах защиты, актуальная информация о схемах мошенничества);
- анализ внутренних и внешних информационных потоков;
- анализ действий сотрудников.

Рационально создание автоматизированной системы защиты стратегически важных ресурсов предприятия (АСЗСВРП), включающей соответствующие модули автоматизации:

- модуль мониторинга изменений (ММИ);
- работы с базой знаний информационной безопасности (МРБЗИБ);
- анализа информационных потоков (МАИП);
- анализа действий сотрудников (МАДС), в который водят функции: анализа нехарактерных действий в рамках информационных потоков (АНДРИП); анализа характеристик поведения (АХП).

Структура модулей АСЗСВРП представлена на рис. 1.

Важно отметить, что БЗИБ формируется сотрудниками отдела информационной безопасности (обращение к БЗИБ по записи через МРБЗИБ), однако остальным сотрудникам предоставление информации из БЗИБ проводится только путем обращений к БЗИБ по чтению через специальный интерфейс, предоставленный МРБЗИБ (рис. 2).

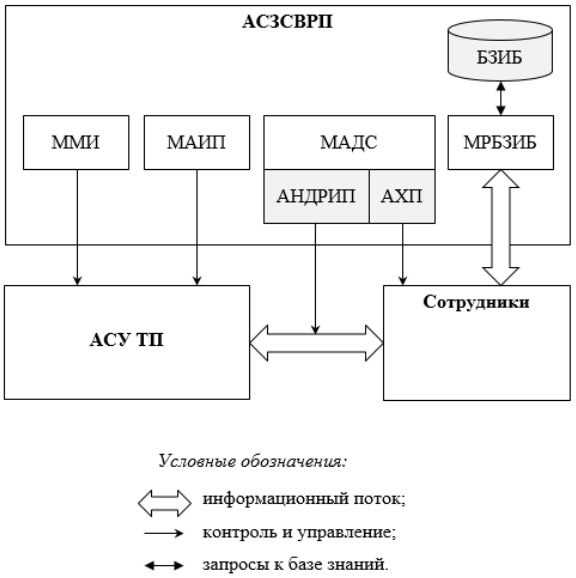

Рис. 1. Структура модулей АСЗСВРП

Рис. 2. Схема обращения к БЗИБ

Выводы

Современные предприятия, относящиеся к объектам КИИ, нуждаются в высоком уровне обеспечения безопасности стратегически важных ресурсов. В рамках поставленной задачи повышения уровня защиты проанализированы основные так-

тики злоумышленников, выявлены их особенности; классифицированы современные методы защиты от комплексных кибератак; сформирован комплекс мер защиты на основе результатов проведенного анализа и классификации.

Новизна работы состоит в разработанной модульной структуре автоматизированной системы защиты, основной задачей которой является повышение уровня рационального взаимодействия современных технологий информационной безопасности ресурсов предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Гостев А. Stuxnet в деталях //Secure List: «Лаборатория Касперского». URL: http://kaspersky.ru/about/news/virus/2014/stuxnet-v-detaliakh (дата обращения: 30.01.2020).
2. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1(1). С. 28–36.
3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. URL: http://www.consultant.ru/documents/cons_doc_LAW_220885 (дата обращения: 30.01.2020).
4. Karlova T.V., Bekmeshov A.Y., Kuznetsova N.M. Protection the Data Banks in State Critical Information Infrastructure Organizations // Proceedings of the 2019 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov, St. Petersburg, Russia: Saint Petersburg Electrotechnical University "LETI", 2019. P. 155–157.
5. Karlova T.V., Sheptunov S.A. , Kuznetsova N.M. Automation of Data Defence Processes in the Corporation Information Systems // Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov. St. Peterburg, Russia: Saint Petersburg Electrotechnical University "LETI". 2017. P. 199–202.
6. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие. М.: Академия, 2008. 256 с.
7. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие. М.: ФОРУМ: ИНФА-М, 2019. 352 с.
8. ATT&CK Matrix for Enterprise. URL: https://attacks.mitre.org (дата обращения: 30.01.2020).
9. Мельников В. П., Клейменов С.А., Петраков А.М. Информационная безопасность: учеб. пособие / под ред. С.А. Клейменова. М.: Академия, 2012. 336 с.
10. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных. М.: Горячая линия-Телеком, 2001. 148 с.

1. Gostev A. Stuxnet in detail // Secure List: Kaspersky Laboratory". URL: http://kaspersky.ru/about/news/virus/2014/stuxnet-v-detaliakh (address date: 30.01.2020).
2. Markov A.S., Fadin A.A. Organization-engineering problems in protection against target malware of Stuxnet type // *Matters of Cyber-safety*. 2013. No.1 (1). pp. 28-36.
3. The Federal Law "On safety of Critical Information Infrastructure of the Russian Federation" of 26.07.2017. No.187-F3. URL: http://www.consultant.ru/documents/cons_doc_LAW_220885 (address date: 30.01.2020).
4. Karlova T.V., Bekmeshov A.Y., Kuznetsova N.M. ProtectiontheDataBanksinStateCriticalInformation-InfrastructureOrganizations // Proceedings of the 2019 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov, St. Petersburg, Russia: Saint Petersburg Electrotechnical University "LETI", 2019. P. 155–157.
5. Karlova T.V., Sheptunov S.A. , Kuznetsova N.M. Automation of Data Defence Processes in the Corporation Information Systems // Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS) / Proceedings Edited by S. Shaposhnikov. St. Peterburg, Russia: Saint Petersburg Electrotechnical University "LETI". 2017. P. 199–202.
6. Khorev P.B. *Methods and Means for Information Protection in Computer Systems*: manual. M.: Academy, 2008. pp. 256.
7. Khorev P.B. *Software-Hardware Information Protection*: manual. M.: FORUM: INFA-M, 2019. pp. 352.
8. ATT&CK Matrix for Enterprise. URL: https://attacks.mitre.org (дата обращения: 30.01.2020).
9. Melnikov V.P., Kleimyonov S.A., Petrakov A.M. *Information Safety*: manual / under the editorship of S.A. Kleimyonov. M.: Academy, 2012. pp. 336.
10. Malyuk A.A., Pazizin S.V., Pogozhin N.S. *Introduction into Information Protection in Automated*. M.: Hotline-Telecom, 2001. pp. 148.

Ссылка для цитирования:
Кузнецова Н.М., Карлова Т.В., Бекмешов А.Ю. Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибер-атак на основе анализа тактик злоумышленников // Вестник Брянского государственного технического университета. 2020. № 7. С. 48 - 53. DOI: 10.30987/1999-8775-2020-7-48-53.

Статья поступила в редакцию 18.05.20.
Рецензент: к.т.н., доцент Брянского государственного технического университета
Рытов М.Ю.,
член редсовета журнала «Вестник БГТУ».
Статья принята к публикации 22.06.20.

Сведения об авторах:

Кузнецова Наталия Михайловна, к.т.н., доцент, Московский государственный технологический университет «СТАНКИН», тел.: 8-(903)-581-80-15, e-mail: knm87@mail.ru.
Карлова Татьяна Владимировна, д. соц. н., профессор, Институт конструкторско-технологической информатики РАН, тел.: 8-(903)-776-90-78, e-mail: karlova-t@yandex.ru.
Бекмешов Александр Юрьевич, к.т.н., доцент, Институт конструкторско-технологической информатики РАН, тел.: 8-(926)-582-34-35, e-mail: b-a-y-555@yandex.ru.

Kuznetsova Natalia Michailovna, Can. Sc. Tech., Assistant Prof., Moscow State Technological University "STANKIN", phone: 8 (903) 581 80 15, e-mail: knm87@mail.ru.
Karlova Tatiana Vladimirovna, Dr. Sc. Sociol., Prof., Institute of Design-Technological Informatics of the RAS, phone: 8 (903) 776 90 78, e-mail: karlova-t@yandex.ru.
Bekmeshov Alexander Yurievich, Can. Sc. Tech., Assistant Prof., Institute of Design-Technological Informatics of the RAS, phone: 8 (926) 582 34 35, e-mail: b-a-y-555@yandex.ru.