УДК 519:331.101.1
DOI: 10.30987/2658-4026-2021-2-97-102

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

Построение цифрового двойника основных автоматизированных систем промышленного предприятия с целью определения уровня информационной безопасности

Целью научной работы является оценка уровня информационной безопасности автоматизированных систем предприятия с помощью моделирования, основанного на концепции цифровых двойников производства. Статья посвящена решению задачи построения модели – цифрового двойника автоматизированных систем предприятия. В рамках системного подхода решение данной задачи подразумевает моделирование условий внешней среды, надежности программно-аппаратного обеспечения, а также человеческого фактора. Новизной работы является предложенная креативная концепция использования технологии цифровых двойников для детальной оценки уровня информационной безопасности автоматизированных систем. Результатом исследования являются рекомендации по оценке уровня информационной безопасности с помощью цифрового двойника.

Ключевые слова: автоматизация, информационная безопасность, моделирование, цифровой двойник, защита информации, человеческий фактор.

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

Building a digital twin of the main automated systems of an industrial enterprise to determine the level of information security

The aim of the scientific work is to assess the level of information security of the automated enterprise systems using modelling based on the concept of digital twins of production. The article is devoted to solving the problem of constructing a model that is a digital twin of the enterprise automated systems. Within the framework of a systematic approach, solving this problem implies modelling environmental conditions, software and hardware reliability, as well as the human factor. The novelty of the work is the proposed creative concept of using the digital twin technology for a detailed assessment of the information security level of the automated systems. The study findings are the recommendations for assessing the level of information security using a digital twin.

Keywords: automation, information security, modelling, digital twin, information security, human factor.

Введение

Для оценки уровня информационной безопасности автоматизированных систем (далее АС) в первую очередь необходимо создание модели тех систем, которые содержат стратегически важные ресурсы.

Стратегические ресурсы, в первую очередь, составляют трудовые, интеллектуальные, информационные, программно-аппаратные [1-3].

На современном промышленном предприятии, как правило, функционируют одновременно несколько взаимосвязанных АС. К основным АС относятся:

- автоматизированные системы электронного документооборота (далее АСЭД);
- автоматизированные системы управления технологическим процессом (далее АСУ ТП);
- автоматизированные системы управления предприятием (далее АСУП);
- автоматизированные системы технологической подготовки производства (далее АСТПП);
- автоматизированные системы защиты информации (далее АСЗИ).

Применение системного подхода при построении цифрового двойника автоматизированных систем предприятия

Цифровой двойник – виртуальная копия (модель) процессов физического объекта, созданная с целью их оптимизации [4].

Для моделирования АС необходимо использование системного подхода, позволяющего максимально точно описать процессы, ресурсы, информационные потоки, учесть взаимосвязи и условия их функционирования – другими словами, максимально точно «приблизить» модель к реальности.

Кроме того, наиболее точно необходимо описывать те процессы, влияние которых на уровень информационной безопасности АС максимальный.

Таким образом, в рамках комплексного подхода, при создании цифрового двойника основных АС предприятия необходимо учитывать следующие аспекты:

- особенности функционирования АС;
- особенности связей и коммуникации АС;
- особенности распределения и логику использования ресурсов АС;
- условия внешней среды;
- человеческий фактор.

На рисунке 1 представлена модель функционирования промышленного предприятия в рамках концепции *IDEF0 (Integrated DEFinition)*.

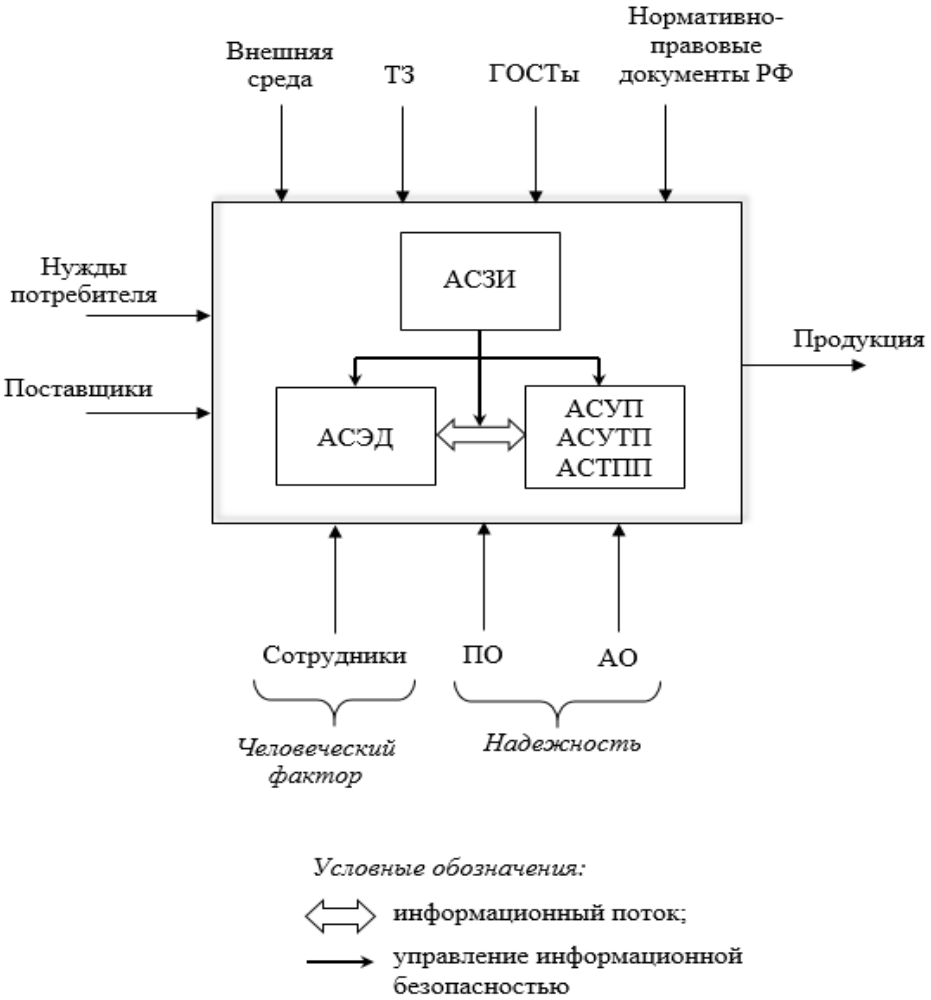

Рис. 1. Модель функционирования промышленного предприятия в рамках концепции *IDEF0*

Согласно рисунку 1, надежность программного обеспечения (далее ПО) и аппаратного обеспечения (далее АО), а также человеческий фактор являются важными аспектами оценки уровня информационной безопасности основных АС.

Также важную роль в оценке играют условия внешней среды.

Уровень информационной безопасности предприятия является относительной величиной, в связи с чем оценка уровня информационной безопасности проводится в процентах. Целью любой концепции защиты информации (в том числе применение АСЗИ) является

«приближение» данного уровня к 100 %.

Оценка уровня информационной безопасности в рамках концепции применения цифровых двойников производится во время моделирования условий внешней среды, человеческого фактора, надежности программно-аппаратного обеспечения.

Моделирование надежности программного и аппаратного обеспечения

Ввиду того, что ПО и АО, входящие в состав основных АС, являются сложными системами, состоящими из конечного числа элементов и связей между ними, наиболее подходящим методом моделирования является метод Монте-Карло. Данный метод позволяет определить надежность систем в зависимости от надежности входящих элементов и связей между ними.

Достоинством метода является сравнительно высокая точность оценки надежности как элементов ПО и АО, так и их упорядоченной совокупности (в АС).

Недостатком данного метода является потребность в больших объемах вычислительных ресурсов.

Моделирование условий внешней среды

Для моделирования условий внешней среды достаточно оценки нескольких параметров:

- влажность;
- температура;
- давление и т.д.

На первый взгляд, параметров для моделирования немного, однако значения данных параметров меняются в зависимости от их «места» (локализации) в АС предприятия. Например, для автоматизированных рабочих мест (далее АРМ) сотрудников температура должна быть комфортной прежде всего для человека. Для серверных ферм и вычислительных стоек, напротив, требуются специальные механизмы охлаждения, в связи с чем их размещают в отдельных помещениях.

От рациональности задания (и от обеспечения дальнейшего поддержания в заданных рамках) значений параметров внешней среды зависит надежность и долговечность работы ПО и АО основных АС предприятия, а также надежность работы АСЗИ, что в свою очередь напрямую влияет на уровень информационной безопасности.

Моделирование в рамках концепции применения цифровых двойников позволяет определить оптимальные значения параметров внешней среды, а также соответствующие допустимые интервалы, в которых значения параметров могут находиться.

Для моделирования условий внешней среды наиболее подходящими являются математические методы моделирования, основанные на принципах параллельных вычислений, в том числе с помощью инструментов *MPI (Message Passing Interface* – интерфейс передачи сообщений).

Оценка влияния человеческого фактора при построении цифрового двойника автоматизированных систем

В АС предприятия человек является лицом, принимающим решение (далее ЛПР). Таким образом, на процесс предприятия решения могут оказывать влияние такие факторы как:

- психоэмоциональное состояние;
- физическое состояние;
- уровень образования и воспитания;
- моральные качества и т.д.

Для построения «портрета личности» ЛПР необходимо составление алгоритма оценки рациональности принимаемого решения в зависимости от перечисленных факторов.

Помимо «портретов личности» при моделировании человеческого фактора (в рамках цифрового двойника) необходимо учитывать особенности человеко-машинных интерфейсов. Зачастую причиной ошибок ЛПР является неверно спроектированный «неудобный» человеко-машинный интерфейс. В частности, в большинстве таких интерфейсов не учтено, что ЛПР может быть левша.

Рекомендации по проведению оценки уровня информационной безопасности с использованием цифрового двойника автоматизированных систем

Применение системного подхода «не заканчивается» на моделировании надежности, условий внешней среды и человеческого фактора, описанных ранее. Системный подход подразумевает также моделирование взаимодействия данных факторов, причём с учётом времени.

Подобная стратегия реализована в известной игре «жизнь», в которой определяется состояние системы в каждый момент времени. Для определения состояния системы (уровня информационной безопасности АС) цифрово-

го двойника необходимо составить алгоритм, подобный алгоритму игры «жизнь», однако при этом увеличить количество входных факторов.

Важно также помнить, что уровень информационной безопасности системы определяется наименьшим уровнем защиты всех её частей.

На рисунке 2 представлена схема взаимодействия основных факторов моделирования цифрового двойника АС.

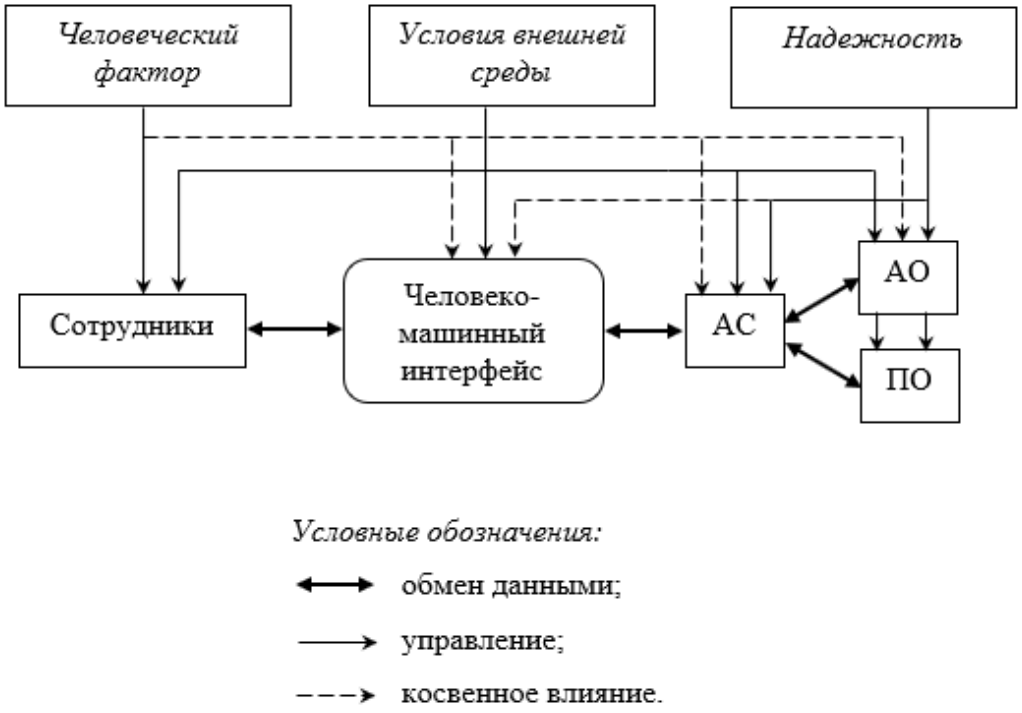

Рис. 2. Схема взаимодействия основных факторов моделирования цифрового двойника АС

Согласно рисунку 2, в рамках взаимодействия сотрудника предприятия (ЛПР) с основными АС через человеко-машинный интерфейс:

- человеческий фактор влияет на сотрудников (в процессе принятия решения). Строго говоря, человеческий фактор также косвенно влияет и на интерфейс, и на АС, т.к. они также разработаны людьми;
- условия внешней среды влияют на все объекты обмена данными (на сотрудников, интерфейс, АС);
- факторы надёжности влияют на АС (на входящие АО и ПО). Кроме того, факторы надёжности также косвенно влияют и на интерфейс.

На рисунке 2 косвенное влияние отражено пунктирной линией.

При построении цифрового двойника АС необходимо учитывать описанные на рисунке 2 особенности взаимодействия объектов управления.

Также необходимо производить моделирование изменения состояния цифрового двойника.

Дополнительные возможности использования цифрового двойника автоматизированных систем

В качестве дополнительных возможностей цифрового двойника можно отметить:

- функции управления ресурсами;
- превентивные функции защиты.

В связи с тем, что главная цель создания модели цифрового двойника является оценка уровня информационной безопасности исходя из значений факторов аппаратных, программных и трудовых ресурсов, одновременно решается задача оптимизации их распределения.

Также с помощью цифровой модели можно определить «тонкие места» АС предприятия и таким образом своевременно предотвратить реализации атак, в том числе атак класса *APT (Advanced Persistent Attack)* – целевых кибератак [5, 6].

Особенностью атак класса *APT* является их долгосрочность и сложность детектирования. Применение цифрового двойника АС позволит моделировать реализации тактик злоумышленников, выявить сопутствующие пат-

терны изменений основных информационных потоков и бизнес-процессов, произвести их анализ и применить комплекс защитных мер [7 – 10].

Выводы

Создание цифрового двойка АС предприятия для оценки уровня информационной безопасности позволит наиболее точно моделировать основные бизнес-процессы и информационные потоки АС, что в свою очередь предоставляет возможность своевременно определять «тонкие места» (локализовать уязвимости) и принимать меры по их устранению.

Наиболее важными факторами моделирования при создании цифрового двойника АС являются надежность АО и ПО, условия внешней среды, человеческий фактор. В рамках комплексного подхода необходимо также учитывать взаимосвязи факторов моделирования и параметр времени.

Важно отметить, что помимо решения основной задачи определения уровня информационной безопасности цифровой двойник АС также позволяет решить задачу оптимального распределения стратегически важных ресурсов предприятия.

СПИСОК ЛИТЕРАТУРЫ

1 **Chen, P.** A Study on Advanced Persistent Threats / P. Chen, L. Desmet, C. Huygens // Communications and Multimedia Security. – 2014. – P. 63-72. – DOI: 10.1007/978-3-662-44885-4_5.

2 **Virvilis, N**. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? / N. Virvilis, D. Gritzalis, T. Apostolopoulos // 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing., – 2013. – P. 396-403. – DOI: 10.1109/UIC-ATC.2013.80.

3 **ГОСТ Р ИСО/МЭК 15408-1-2012** Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель = Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model: нац. стандарт Российской Федерации : изд. офиц. : утв. и введ. в действие Приказом Федер. агенства по техн. регулированию и метрологии от 15 ноября 2012 г. № 814-ст. : введ. взамен ГОСТ Р ИСО/МЭК 15408-1-2008 : дата введ. 2013-12-01 / подг. Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), Федеральным государственным унитарным предприятием «Ситуационно-кризисный Центр Федерального агенства по атомной энергии» (ФГУП «СКЦ Росатома») : Стандартинформ, 2014.

4. **Digital twin.** – Текст : электронный // Wikipedia : свободная энциклопедия : сайт. – URL: https://en.wikipedia.org/wiki/Digital_twin (дата обращения: 07.11.2020).

5. **Methods Dedicated to Fight Against Complex Information Security Theats on Automated Factories Systems** /

REFERENCES

1 **Chen, P.** A Study on Advanced Persistent Threats / P. Chen, L. Desmet, C. Huygens // Communications and Multimedia Security. – 2014. – P. 63-72. – DOI: 10.1007/978-3-662-44885-4_5.

2 **Virvilis, N**. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? / N. Virvilis, D. Gritzalis, T. Apostolopoulos // 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing., – 2013. – P. 396-403. – DOI: 10.1109/UIC-ATC.2013.80.

3 **GOST R ISO / IEC 15408-1-2012** Information technology (IT). Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model: nat. Russian Federation standard : ed. official : approved and entered in effect by Order of Feder. agencies for tech. regulation and metrology of November 15, 2012 No. 814-art. : entered instead of GOST R ISO / IEC 15408-1-2008: date of entry 2013-12-01 / prep. By the Limited Liability Company “Information Security Centre” (LLC “CBI”), Federal Autonomous Institution “State Research and Testing Institute for Technical Information Protection Problems of the Federal Service for Technical and Export Control” (FAI “SRTITIPPFSTSC of Russia”), Federal State Unitary Enterprise “Situational Crisis Centre of the Federal Agency for Atomic Energy” (FSUE “ SCC of Rosatom”): Standartinform, 2014.

4. **Digital twin. -** Text: electronic / / Wikipedia: free encyclopedia: website. URL: https://en.wikipedia.org/wiki/Digital_twin (date accessed: 07.11.2020).

5. **Methods Dedicated to Fight Against Complex Information Security Theats on Automated Factories Systems** /

T.V. Karlova, N.M. Kuznetsova, S.A. Sheptunov, A.Y. Bekmeshov // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS) – 2016. – P. 23-27. – DOI: 10.1109/ITMQIS.2016.7751927

6. **Кузнецова Н. М.** Решение задачи автоматизации процессов защиты стратегически важных ресурсов предприятия от комплексных кибер-атак на основе анализа тактик злоумышленников / Н. М. Кузнецова, Т. В. Карлова, А. Ю. Бекмешов // Вестник Брянского государственного технического университета. – 2020. – № 7(92). – С. 48-53. – DOI: 10.30987/1999-8775-2020-7-48-53.

7. **Advanced social engineering attacks** / K. Krombholz, H. Hobel, et al. // Journal of Information Security and Applications. — 2015. — June. — P. 113—122. —DOI: 10.1016/j.jisa.2014.09.005

8. **ATT&CK Matrix for Enterprise.** – URL: https://attacks.mitre.org (дата обращения: 05.11.2020). – Режим доступа: для зарегистрир. пользователей. – Текст. : электронный.

9. **Kim, Y.** Involvers' Behavior-based Modeling in Cyber Targeted Attack / Y.Kim, I.Kim // Eighth International Conference on Emerging Security Information, Systems and Technologies. – 2014. — P. 132—137. — ISBN 978-1-61208-376-6.

10. **Марков, А. С.** Организационно-технические проблемы защиты от целевых вредоносных программ типа StuxNet / А.С. Марков, А.А. Фадин // Вопросы кибербезопасности. – 2013. – № 1(1). – С. 28–36.

.T.V. Karlova, N.M. Kuznetsova, S.A. Sheptunov, A.Y. Bekmeshov // 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS) – 2016. – P. 23-27. – DOI: 10.1109/ITMQIS.2016.7751927

6. **Kuznetsova N. M.** Solution of Protection Automation Problem of Company Strategic Resources against Complex Cyber Attacks Based on Criminal Tactics Analysis / N. M. Kuznetsova, T. V. Karlova, A. Yu. Bekmeshov // Bulletin of Bryansk State Technical university. – 2020. – no. 7 (92). – pp. 48-53. – DOI: 10.30987 / 1999-8775-2020-7-48-53.

7. **Advanced social engineering attacks** / K. Krombholz, H. Hobel, et al. // Journal of Information Security and Applications. — 2015. — June. — P. 113—122. —DOI: 10.1016/j.jisa.2014.09.005

8. **ATT&CK Matrix for Enterprise.** – URL: https://attacks.mitre.org (accessed: 05.11.2020). – Access mode: for registered users. users. - Text.: electronic.

9. **Kim, Y.** Involvers' Behavior-based Modeling in Cyber Targeted Attack / Y.Kim, I.Kim // Eighth International Conference on Emerging Security Information, Systems and Technologies. – 2014. — P. 132—137. — ISBN 978-1-61208-376-6.

10. **Markov A. S.** Organizational and Technical Problems of Protection Against Targeted Malware Such as StuxNet / A. S. Markov, A. A. Fadin // Cybersecurity Issues. – 2013. – no. 1 (1). – pp. 28-36.

Ссылка для цитирования:
Кузнецова Н.М. Построение цифрового двойника основных автоматизированных систем промышленного предприятия с целью определения уровня информационной безопасности / Н.М. Кузнецова, Т.В. Карлова, А.Ю. Бекмешов // Эргодизайн. – 2021 - №2 (12). – С. 97-102. DOI: 10.30987/2658-4026-2021-2-97-102.

Сведения об авторах:

Кузнецова Наталия Михайловна
кандидат технических наук, доцент
Московский государственный технологический университет «СТАНКИН»
Тел.: 8-(903)-581-80-15
E-mail: knm87@mail.ru

Карлова Татьяна Владимировна
Доктор социологических наук, кандидат технических наук, профессор
Институт конструкторско-технологической информатики Российской академии наук
Тел.: 8-(903)-776-90-78
E-mail: karlova-t@yandex.ru

Бекмешов Александр Юрьевич
Кандидат технических наук, доцент
Институт конструкторско-технологической информатики Российской академии наук
Тел.: 8-(926)-582-34-35
E-mail: b-a-y-555@yandex.ru

Abstracts:

N.M. Kuznetsova
Candidate of Technical Sciences, Associate Professor
Moscow State Technological University "STANKIN"

Тел.: 8-(903)-581-80-15
E-mail: knm87@mail.ru

T.V. Karlova
Doctor of Sociological Sciences, Candidate of Technical Sciences, Professor
Institute of Design and Technological Informatics of the Russian Academy of Sciences
Тел.: 8-(903)-776-90-78
E-mail: karlova-t@yandex.ru

A.Yu. Bekmeshov
Candidate of Technical Sciences, Associate Professor
Institute of Design and Technological Informatics of the Russian Academy of Sciences
Тел.: 8-(926)-582-34-35
E-mail: b-a-y-555@yandex.ru

Статья поступила в редколлегию 29.03.2021г.
Рецензент: к.т.н., доцент Брянского государственного технического университета
член редакционного совета журнала «Эргодизайн»
Рытов М.Ю.
Статья принята к публикации 09.04.2021 г.