ISSN 1814-1196
Научный вестник НГТУ
том 70, № 1, 2018, с. 167–176

http://journals.nstu.ru/vestnik
Science Bulletin of the NSTU
Vol. 70, No. 1, 2018, pp. 167–176

ИНФОРМАТИКА,
ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
И УПРАВЛЕНИЕ

INFORMATICS,
COMPPUTER ENGINEERIN
AND CONTROL

УДК 004.5

DOI: 10.17212/1814-1196-2018-1-167-176

Моделирование автоматизированных технологических процессов в условиях информационных угроз*

Р.Р. ФАТКИЕВА

199178, РФ, г. Санкт-Петербург, 14-я линия, 39, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, кандидат технических наук, доцент. E-mail: rikki2@yandex.ru

В настоящее время усиливается внедрение различных информационных технологий в производственные процессы. Это приводит к увеличению рисков и возможным срывам этих процессов из-за нарушения их информационной безопасности. Известные методы обнаружения деструктивных воздействий на программное и информационное обеспечение не всегда применимы в цикле изготовления продукции вследствие особенностей функционирования автоматизированного оборудования, персонала, самих технологических процессов и временных привязок потока выпуска изделий. Цель исследования – поиск подходов, позволяющих оперативно оценивать риски нарушения информационной безопасности производственного процесса. Предложена математическая модель процесса обработки деталей в условиях информационных угроз. Модель позволяет получать количественные оценки вероятностей нарушения информационной безопасности, на основе которых можно обосновать мероприятия по обеспечению этой безопасности. На конкретных примерах показана эффективность разработанного метода. Практическая значимость: за счет своевременного проведения комплекса мероприятий по уменьшению влияния деструктивных воздействий на программное и информационное обеспечение производственных процессов можно существенно снизить вероятность срыва выпуска продукции и возможные потери.

Ключевые слова: автоматизированная система управления технологическими процессами, информационная безопасность, системы обеспечения информационной безопасности, станки с числовым программным управлением

ВВЕДЕНИЕ

Одно из основных требований, выдвигаемых при внедрении информационных технологий в производственные процессы, является обеспечение их безопасности от случайных и злонамеренных воздействий. Если в предыдущем десятилетии распространенные угрозы были связаны с получением де-

* *Статья получена 02 октября 2017 г.*
Работа выполнена при поддержке грантов РФФИРФФИ №16-29-09482/17

нежной выгоды от реализации атаки, то в настоящее время увеличилось количество атак на промышленные объекты с целью шпионажа и с террористической направленностью.

Вектор атак с информационных систем перешел на производственные и промышленные сети. Например, статистика атак на промышленные сети в России за 2017 год выросла с 5 % до 15 % [1, 2].

Тем не менее сами технологические процессы из-за высокого уровня автоматизации стали более уязвимыми. Это обусловливает применение специальных развитых методов моделирования и прогнозирования угроз для оценки возможных рисков.

В настоящее время известны подходы к оценке рисков [3–11]. Однако не всегда возможности известных методов и моделей удовлетворяют потребностям практики по точности и оперативности, прогнозированию таких угроз и оценке рисков, они во многом не учитывают специфику реальных процессов. Для автоматизированных производств риски могут быть связаны с автоматизированным оборудованием, персоналом и самим технологическим процессом. Для таких производств понятие безопасности несколько отличается от традиционного. В статье рассмотрен подход, позволяющий оценить возможные риски, осуществить поиск уязвимостей и обосновать мероприятия по их устранению применительно к машиностроительному производству.

1. ПОСТАНОВКА ЗАДАЧИ

Рассмотрим постановку задачи на практическом примере технологического автоматизированного процесса обработки корончатой втулки. Процесс обработки состоит из последовательных операций (токарной, фрезерной и слесарной) на одношпиндельном оборудовании (рис. 1). В механосборочном цехе установлены станки, предполагающие автоматическую обработку детали по управляющей программе.

Рис. 1. Оборудование для обработки корончатой втулки

Требуется разработать подход, позволяющий оперативно оценивать риски от деструктивного воздействия.

Для оценки рисков и выработки мероприятий по противодействию необходимо в первую очередь определить операционные потоки, поскольку именно они являются наиболее доступным способом получения информации и несанкционированного воздействия. Для этого целесообразно представить схему функционирования предприятия, которая позволяет сформировать систему показателей деятельности. На основании этой схемы осуществляется мониторинг, прогнозирование и управление процессом производства.

Применение подобного подхода позволяет осуществлять следующие приемы анализа: сравнение полученных результатов текущего периода с ранее полученным; оценку реальных тенденций, происходящих в производственном цикле; выявление узких мест и проблем. В соответствии с существующей методологией оценки безопасности предприятия при формировании системы показателей эффективности в ее состав должны быть включены те из них, которые характеризуют назначение и доступность выполнения задачи за определенной период времени. В частности, информационная безопасность может характеризоваться через нарушения доступности, целостности и конфиденциальности информации. Однако применение данного подхода на практике может вызвать трудности, так как не всегда удается получить статистические данные по существующим нарушениям безопасности. В этом случае целесообразно использовать методы моделирования процесса производства для получения оценок нарушения работоспособности. В зависимости от иерархии представления производственного цикла в процессе нарушения безопасности могут возникнуть те или иные уязвимости. Соответственно, угрозы и показатели обеспечения безопасности на каждом из подуровней будут отличаться.

2. МОДЕЛЬ ПРОЦЕССА ОБРАБОТКИ ДЕТАЛЕЙ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ УГРОЗ

Для построения простейшей модели производственного процесса рассмотрим операционный поток обработки изделий (рис. 2).

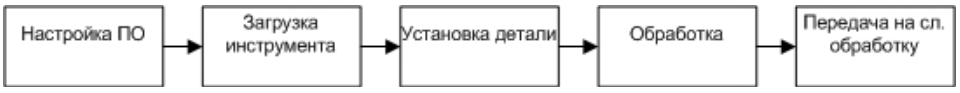


Рис. 2. Процесс механической обработки детали на станке с ЧПУ

Процесс обработки детали начинается с верификации установленного программного обеспечения (ПО) на станке с ЧПУ. Это необходимая операция, поскольку не все ошибки, содержащиеся в ПО, могут быть распознаны. Например, фреза может попасть не в ту координату, что приведет к нарушениям обработки детали. Затем осуществляется установка режущего инструмента в инструментальный магазин станка, при несоответствии которого может произойти поломка инструмента / станка или обрабатываемая деталь не будет соответствовать паспорту изделия. Неправильная установка обрабатываемой детали ведет к тому, что последовательность операций не может осуществиться в заданных координатах. Это может привести к одному или совокупности нарушений изготовления (испорченный инструмент / деталь / станок).

В этом случае процесс нарушения цикла обработки детали возможно представить в виде графа состояний (рис. 3), где S_1 – обработка детали в плановом режиме работы, S_2 – нарушение обработки из-за изменения структуры программного кода, S_3 – нарушение установки режущего инструмента, S_4 – нарушение установки обрабатываемой детали, S_5 – нарушение в механизмах обработки детали. Дуги графа соответствуют процессам перехода из одних состояний в другие.

Этот процесс (рис. 3) в ряде случаев можно рассматривать как марковский процесс, тогда дугам ставятся в соответствие значения интенсивности переходов $\lambda_{12},..., \lambda_{51}$ из одного состояния в другое, а $P_1(t),..., P_5(t)$ являются вероятностями нахождения процесса в состояниях $S_1,..., S_5$ на момент времени t.

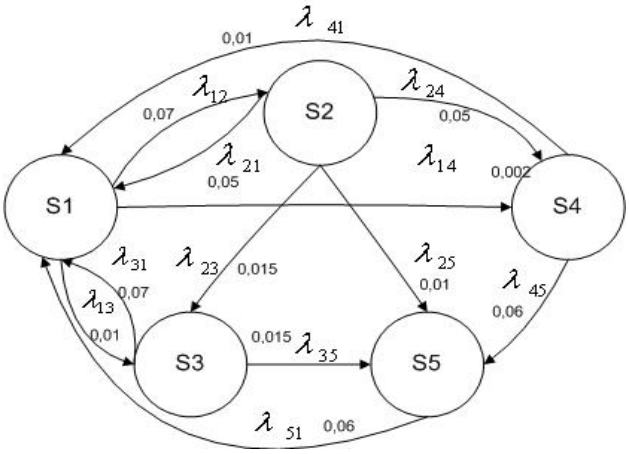


Рис. 3. Граф состояний операции при нарушении обработки детали

С учетом этого графу на рис. 3 можно поставить в соответствие систему из пяти дифференциальных уравнений [12]:

$$\begin{aligned}
&\frac{dP_1(t)}{dt} = \lambda_{21}P_2(t) + \lambda_{31}P_3(t) + \lambda_{41}P_4(t) + \lambda_{51}P_5(t) - \\
&-(\lambda_{12} + \lambda_{13} + \lambda_{14})P_1(t), \\
&\frac{dP_2(t)}{dt} = \lambda_{12}P_1(t) - (\lambda_{21} + \lambda_{23} + \lambda_{24} + \lambda_{25})P_2(t), \\
&\frac{dP_3(t)}{dt} = \lambda_{13}P_1(t) + \lambda_{23}P_2(t) - (\lambda_{31} + \lambda_{35})P_3(t), \\
&\frac{dP_4(t)}{dt} = \lambda_{24}P_2(t) + \lambda_{14}P_1(t) - (\lambda_{41} + \lambda_{45})P_4(t), \\
&\frac{dP_5(t)}{dt} = \lambda_{25}P_2(t) + \lambda_{35}P_3(t) + \lambda_{45}P_4(t) - \lambda_{51}P_5(t).
\end{aligned} \tag{1}$$

3. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

Для оценки возможности перехода из одного состояния в другое необходимо знать значения параметров $\lambda_{12},..., \lambda_{51}$. Их можно получить путем анализа производственного процесса или использования накопленной статистики [13, 14]. Зная $\lambda_{12},..., \lambda_{51}$ и исходные состояния процесса, возможно прогнозировать вероятности нарушения обработки детали.

Пусть вероятности нахождения процесса в выделенных состояниях на момент времени $t=0$ определены как $\overline{P}=[P_1(0), P_2(0), P_3(0), P_4(0), P_5(0)]=$ $=[1, 0, 0, 0, 0]$, а интенсивности перехода заданы вектором $\overline{\lambda}=[\lambda_{12}, \lambda_{13}, \lambda_{14}, \lambda_{21}, \lambda_{23}, \lambda_{24}, \lambda_{25}, \lambda_{31}, \lambda_{35}, \lambda_{41}, \lambda_{45}, \lambda_{51}]$ со значениями $\overline{\lambda}=[0.07, 0.01, 0.002, 0.05, 0.015, 0.05, 0.01, 0.07, 0.015, 0.01, 0.06]$.

Разрешая систему уравнений (1) при этих исходных данных с использованием пакета прикладных программ MathLab, получаем оценки вероятностей нахождения процесса в каждом из перечисленных состояний $\overline{P}=[0.35, 0.20, 0.08, 0.15, 0.22]$ на момент времени *T*. Анализ вектора $\overline{P}$ показал, что с наибольшими вероятностями из всех деструктивных состояний проявляются состояния S_2 нарушения обработки из-за изменения структуры программного кода и состояния S_5 нарушения в механизмах обработки детали. В рамках этого подхода представляет интерес обоснование мероприятий по уменьшению вероятности нарушения обработки из-за изменения структуры программного кода. Для уменьшения влияния ошибок в структуре программного кода на производственный процесс рассмотрим комплекс мероприятий, заключающийся в предотвращении их появления. Он может включать [15]:

– проверку процесса функционирования станка в холостом режиме на малых оборотах;

– верификацию программного обеспечения на эталонной детали с последующей проверкой качества;

– применение режима, при котором все ускоренные перемещения выполняются над поверхностью заготовки с выводом оснастки на безопасном расстоянии после каждой операции.

В этом случае интенсивности переходов из состояния в состояние могут быть определены на основе собранных статистических данных в ходе производственного процесса. Применение данного подхода на практике показало изменение интенсивностей переходов из состояния S_1 в состояние S_2 и из состояния S_2 в состояние S_1 с уменьшением $\lambda_{12}=0,03$ и увеличением $\lambda_{21}=0,09$. Вероятность нахождения в состоянии S_2 уменьшается (кривая *2* на рис. 4, *а*) за счет увеличения интенсивности возврата в работоспособное состояние.

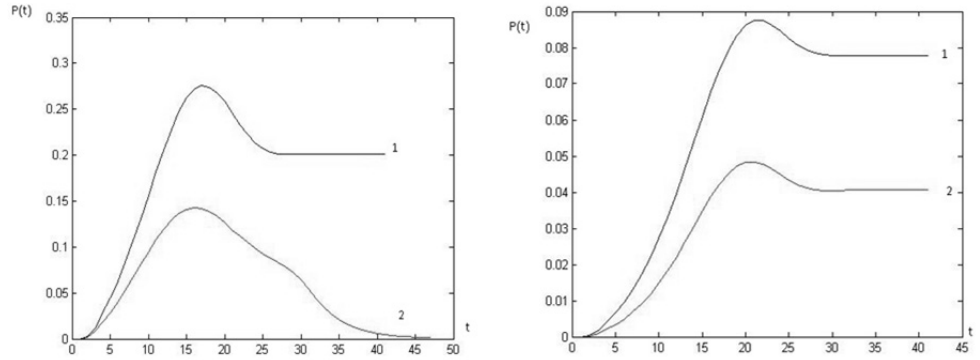
Для уменьшения вероятности перехода процесса из состояния S_1 в состояние S_3 было предусмотрено выполнение следующих мероприятий:

– инструктаж оператора станка по закреплению инструмента в стойке;

– использование динамометрического ключа для установки инструмента в оснастке;

– повторная верификация установленного в стойку инструмента измерительной техникой.

В этом случае интенсивности переходов из состояния S_1 в состояние S_3 и обратно изменились и стали равными $\lambda_{13} = 0{,}005$, $\lambda_{31} = 0{,}11$. Изменение поведения кривой на заданном временном интервале в этом случае также показывает уменьшение вероятности нахождения в состоянии S_3 (кривая *2* на рис. 4, *б*) за счет увеличения интенсивности возврата в работоспособное состояние, однако эффективность от данного вида мероприятий оказывается меньше по сравнению с первым комплексом мер.



а *б*

Рис. 4. Оценка вероятностей нахождения процесса в состоянии S_2 без осуществления комплекса мероприятий по ИБ (*а*) и при осуществлении комплекса мероприятий по ИБ (*б*)

Рассмотрим применение совокупности указанных ранее мероприятий и оценим вероятность нахождения процесса в состоянии S_1 с заданными ранее интенсивностями переходов (рис. 5).

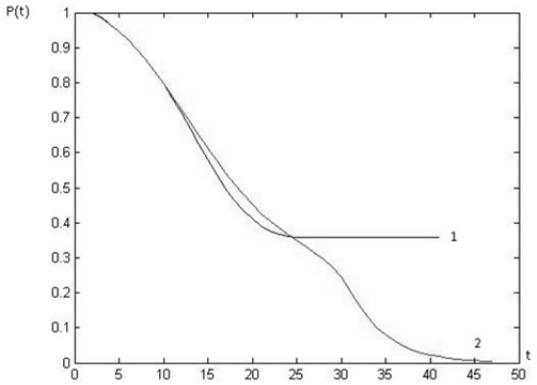


Рис. 5. Оценка вероятностей нахождения процесса в состоянии S_1 при осуществлении комплекса мероприятий

Важно отметить, что данный метод моделирует однородные и эргодические процессы, т. е. производственные процессы, установившиеся при заданных внешних условиях, что позволяет обнаружить аномальное поведение системы при сравнении реальных процессов с моделируемыми.

ЗАКЛЮЧЕНИЕ

Анализ результатов проведенных исследований по моделированию автоматизированных технологических процессов в условиях информационных угроз показал следующее. Текущее состояние защиты этих процессов от существующих и перспективных информационных угроз не в полной мере удовлетворяет потребностям практики. Одной из причин такого состояния выступает несовершенство научно-методического аппарата обоснования мероприятий такой защиты. В интересах совершенствования защиты автоматизированных технологических процессов от информационных террористических угроз на примере конкретной задачи раскрыт подход к обоснованию возможных мероприятий защиты. Предложена новая модель процесса обработки деталей в условиях информационных террористических угроз (нарушения и сбои в программном коде). По аналогии с этой моделью могут быть разработаны другие модели, свойственные различным автоматизированным технологическим процессам. Полученные результаты моделирования позволяют определять наиболее уязвимые элементы в анализируемых процессах и находить целесообразные мероприятия по защите. Полученные решения применимы на производстве при планировании мероприятий защиты критически важных технологических процессов от возможных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы. II квартал 2017 [Электронный ресурс]. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf (дата обращения: 22.03.2018).

2. Угрозы безопасности промышленных предприятий и IoT: прогноз на 2018 год [Электронный ресурс]. – URL: https://ics-cert.kaspersky.ru/media/KL_ICS_CERT_Predictions2018_ICS_IoT_RUS_30112017.pdf (дата обращения: 22.03.2018).

3. ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. – Введ. 2013-12-01. – М.: Изд-во стандартов, 2012. – 56 с.

4. *Осипов В.Ю., Носаль И.А.* Обоснование мероприятий информационной безопасности // Информационно-управляющие системы. – 2013. – № 2 (63). – С. 48–53.

5. *Осипов В.Ю., Носаль И.А.* Обоснование периода пересмотра мероприятий по защите информации // Информационно-управляющие системы. – 2014. – № 1 (68). – С. 63–68.

6. *Лившиц И.И.* Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. – 2015. – Вып. 6 (43). – С. 253–270. – doi: 10.15622/sp.43.14.

7. *Охтилев М.Ю., Соколов Б.В, Юсупов Р.М.* Теоретические и технологические основы концепции проактивного мониторинга и управления сложными объектами // Известия ЮФУ. Технические науки. – 2015. – № 1. – С. 162–174.

8. *Мухопад Ю.Ф., Мухопад А.Ю., Пунсык-Намжилов Д.Ц.* Контроль управляющих автоматов сложных технических систем реального времени // Научный вестник НГТУ. – 2017. – № 1 (66). – С. 53–62. – doi: 10.17212/1814-1196-2017-1-53-62.

9. *Давиденко О.Н., Баданин Д.Н., Кобзев Д.А.* Методика оценки угроз информационной безопасности автоматизированных систем управления технологическими процессами (АСУТП) // Наука и технологии трубопроводного транспорта нефти и нефтепродуктов. – 2016. – № 4 (24). – С. 84–91.

10. *Мусаев А.А., Нозик А.А., Русинов Л.А.* Прогностический анализ безопасности промышленного предприятия // Известия СПбГТИ. – 2016. – № 34 (60). – С. 87–93. – doi: 10.15217/issn1998984-9.2016.34.87.

11. *Юсупов Р.М., Мусаев А.А.* Особенности оценивания эффективности информационных систем и технологий // Труды СПИИРАН. – 2017. – Вып. 51. – С. 5–34. – doi: 10.15622/sp.51.1.

12. *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей и ее инженерные приложения. – М.: Academia, 2003. – 464 с.

13. *Пучков В.П., Якунин В.В.* Исследование надежности станков с ЧПУ ТПК-125 в реальных условиях эксплуатации // Приволжский научный вестник. – 2013.– № 12-2 (28). – С. 51–55.

14. *Новиков И.С.* Методы расчета количественных показателей надежности сложных программных комплексов на стадии проектирования и разработки // Труды СПИИРАН. – 2008. – Вып. 6. – С. 86–111. – doi: 10.15622/sp.6.8.

15. Введение в программирование обработки [Электронный ресурс]. – URL: http://planetacam.ru/college/learn/3-5/ (дата обращения: 22.03.2018).

Фаткиева Роза Равильевна, кандидат технических наук, старший научный сотрудник лаборатории информационно-вычислительных систем и технологий программирования Санкт-Петербургского института информатики и автоматизации Российской академии наук. Основное направление научных исследований – информационная безопасность. Имеет более 40 публикаций. E-mail: rikki2@yandex.ru

DOI: 10.17212/1814-1196-2018-1-167-176

Modeling of automated technological processes under conditions of information threats[*]

R.R. FATKIEVA

Federal State Institution of Science St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 39, K. 14-th Linia, St. Petersburg, 199178, Russian Federation, Ph.D. (Eng.), senior researcher. E-mail: rikki2@yandex.ru

Nowadays there is a common trend of incorporating information technologies into production processes. This leads to increasing risks and possible disruptions of these processes due to violations of their information security. The existing methods of detecting destructive impacts on software are not always applicable within the production cycle because of particular qualities of equipment functioning, staff, technological processes and timing conditions of the product release stream. The purpose of the research is to find approaches that make possible rapid assessment of information security violation risks in the production process. A mathematical model of processing parts under conditions of information threats is proposed. The model allows assessing the probabilities of information security violations. On the basis of these probabilities it is possible to determine measures to ensure security. The efficiency of the proposed method is shown on specific examples. Practical significance lies in the fact that due to timely taken measures to reduce the influence of destructive impacts on the production software the probability of disruption in the production process and possible losses can be significantly reduced.

[*] *Received 02 October 2017.*

Keywords: automated control system of technological processes, information security, information security systems, machine tools with numerical control

REFERENCES

1. *Aktual'nye kiberugrozy. II kvartal 2017* [Relevant cyberthreats the II quarter 2017]. Available at:https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf (accessed 22.03.2018).

2. *Ugrozy bezopasnosti promyshlennykh predpriyatii i IoT: prognoz na 2018 god* [Threats to security of the industrial enterprises and IoT: the forecast for 2018]. Available at: https://ics-cert.kaspersky.ru/media/KL_ICS_CERT_Predictions2018_ICS_IoT_RUS_30112017.pdf (accessed 22.03.2018).

3. GOST R ISO/MEK 15408-1–2012. *Informatsionnaya tekhnologiya (IT). Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii. Ch. 1. Vvedenie i obshchaya model'* [State Standard 15408-1–2012. Information technology. Security techniques. Evaluation criteria for IT security. Pt. 1. Introduction and general model]. Moscow, Standartinform Publ., 2012. 56 p.

4. Osipov V.Yu., Nosal' I.A. Obosnovanie meropriyatii informatsionnoi bezopasnosti [Substantiation of information security measures]. *Informatsionno-upravlyayushchie sistemy – Information and Control Systems*, 2013, no. 2 (63), pp. 48–53.

5. Osipov V.Yu., Nosal' I.A. Obosnovanie perioda peresmotra meropriyatii po zashchite informatsii [Substantiation of the period of revision of information security measures]. *Informatsionno-upravlyayushchie sistemy – Information and Control Systems*, 2014, no. 1 (68), pp. 63–68.

6. Livshits I.I. Formirovanie kontseptsii mgnovennykh auditov informatsionnoi bezopasnosti [Formation of the instantaneous information security audit concept]. *Trudy SPIIRAN – SPIIRAS Proceedings*, 2015, iss. 6 (43), pp. 253–270. doi: 10.15622/sp.43.14.

7. Okhtilev M.Yu., Sokolov B.V, Yusupov R.M. Teoreticheskie i tekhnologicheskie osnovy kontseptsii proaktivnogo monitoringa i upravleniya slozhnymi ob"ektami [Conception of complex objects proactive monitoring management and control: theoretical and technological foundations]. *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki – Izvestiya Southem Federal University. Engineering sciences*, 2015, no. 1, pp. 162–174.

8. Mukhopad Yu.F., Mukhopad A.Yu., Punsyk-Namzhilov D.Ts. Kontrol' upravlyayushchikh avtomatov slozhnykh tekhnicheskikh sistem real'nogo vremeni [Control automata of complex engineering real time systems]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Science bulletin of the Novosibirsk state technical university*, 2017 , no. 1 (66), pp. 53–62. doi: 10.17212/1814-1196-2017-1-53-62.

9. Davidenko O.N., Badanin D.N., Kobzev D.A. Metodika otsenki ugroz informatsionnoi bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami (ASUTP) [Assessment method for information security threats in industrial control systems (ICS)]. *Nauka i tekhnologii truboprovodnogo transporta nefti i nefteproduktov – Science & Technologies: Oil and Oil Products Pipeline Transportation*, 2016, no. 4 (24), pp. 84–91.

10. Musaev A.A., Nozik A.A., Rusinov L.A. Prognosticheskii analiz bezopasnosti promyshlennogo predpriyatiya [Predictive analysis ofsafety of an industrialbenterprise]. *Izvestiya Sankt-Peterburgskogo gosudarstvennogo tekhnologicheskogo instituta – Bulletin of the Saint Petersburg State Institute of Technology*, 2016, no. 34 (60), pp. 87–93. doi: 10.15217/issn1998984-9.2016.34.87.

11. Yusupov R.M., Musaev A.A. Osobennosti otsenivaniya effektivnosti informatsionnykh sistem i tekhnologii [Efficiency of information systems and technologies: features of estimation]. *Trudy SPIIRAN – SPIIRAS Proceedings*, 2017, iss. 2 (51), pp. 5–34. doi: 10.15622/sp.51.1.

12. Venttsel' E.S., Ovcharov L.A. *Teoriya veroyatnostei i ee inzhenernye prilozheniya* [Probability theory and its engineering applications]. Moscow, Academia Publ., 2003. 464 p.

13. Puchkov V.P., Yakunin V.V. Issledovanie nadezhnosti stankov s ChPU TPK-125 v real'nykh usloviyakh ekspluatatsii [Reliability examination of CNC turning chuck-type machine TПK-125 under actual operating conditions]. *Privolzhskii nauchnyi vestnik*, 2013, no. 12-2 (28), pp. 51–55.

14. Novikov I.S. Metody rascheta kolichestvennykh pokazatelei nadezhnosti slozhnykh programmnykh kompleksov na stadii proektirovaniya i razrabotki [Metody rascheta kolichestvennykh pokazatelei nadezhnosti slozhnykh programmnykh kompleksov na stadii proektirovaniia i razrabotki]. *Trudy SPIIRAN – SPIIRAS Proceedings*, 2008, iss. 6, pp. 86–111. doi: 10.15622/sp.6.8.

15. *Vvedenie v programmirovanie obrabotki* [Introduction to processing programming]. Available at: http://planetacam.ru/college/learn/3-5/ (accessed 22.03.2018).

Для цитирования:

Фаткиева Р.Р. Моделирование автоматизированных технологических процессов в условиях информационных угроз // Научный вестник НГТУ. – 2018. – № 1 (70). – С. 167–176. – doi: 10.17212/1814-1196-2018-1-167-176.

For citation:

Fatkieva R.R. Modelirovanie avtomatizirovannykh tekhnologicheskikh protsessov v usloviyakh informatsionnykh ugroz [Modeling automated technological processes under conditions of information threats]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Science bulletin of the Novosibirsk state technical university*, 2018, no. 1 (70), pp. 167–176. doi: 10.17212/1814-1196-2018-1-167-176.