УДК 004.056.53 DOI: 10.26102/2310-6018/2021.33.2.016

О выборе мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами

Д.В. Чернов, А.А. Сычугов
Тульский государственный университет,
Тула, Российская Федерация

Резюме. В данной работе проведен обзор основных отечественных и международных подходов к выбору мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами. Работа посвящена разработке метода выбора мер защиты на каждом уровне АСУ ТП с применением теории множеств в рамках анализа базовых наборов мер защиты. В рамках исследования рассмотрены актуальные атаки на промышленную инфраструктуру, построен алгоритм выбора мер защиты АСУ ТП, а также выдвинуты предположения о необходимости применения мер защиты для каждого уровня системы в соответствии с индивидуальной оценкой класса защищенности соответствующего уровня. В работе авторами предложены математические выражения для минимального, базового, адаптированного и уточненного базовых наборов мер защиты АСУ ТП. Сделан вывод о необходимости исключения из рассмотрения этапа «уточнение адаптированного базового набора» алгоритма выбора мер защиты АСУ ТП в случае, если адаптированный базовый набор мер защиты информации обеспечивает блокирование всех угроз безопасности на рассматриваемом уровне системы. Результаты исследований рекомендованы для использования при моделировании угроз информационной безопасности и разработке требований к средствам защиты информации в автоматизированных системах управления технологическими процессами.

Ключевые слова: автоматизированная система управления, мера защиты, базовый набор, информационная безопасность, система защиты информации, теория множеств.

Для цитирования: Чернов Д.В., Сычугов А.А. О выборе мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами. *Моделирование, оптимизация и информационные технологии.* 2021;9(2). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=954 DOI: 10.26102/2310-6018/2021.33.2.016

On the choice of information security measures for automated process control systems

D.V. Chernov, A.A. Sychugov

Tula State University, Tula, Russian Federation

Abstract: This paper reviews the main domestic and international approaches to the choice of information security measures for automated process control systems. The paper is devoted to the development of a method for selecting protection measures at each level of the automated process control system using set theory as part of the analysis of basic sets of protection measures. In the framework of the study, the current attacks on industrial infrastructure are considered, an algorithm for selecting the protection measures of the automated process control system is constructed, and assumptions are made about the need to apply protection measures for each level of the system in accordance with an individual assessment of the security class of the corresponding level. In this paper, the authors propose mathematical expressions for the minimum, basic, adapted and refined basic sets of automated process control system protection measures. It is concluded that it is necessary to exclude from the consideration of the stage "refinement of the adapted basic set" the algorithm for selecting the security measures of the automated process control system, if the adapted basic set of information

security measures provides blocking of all security threats at the considered system level. The research results are recommended for use in modeling information security threats and developing requirements for information security tools in automated process control systems.

Keywords: automated control system, security measure, basic set, information security, information security system, set theory.

For citation: Chernov D.V., Sychugov A.A. On the choice of information security measures for automated process control systems. *Modeling, Optimization and Information Technology*. 2021;9(2). Available from: https://moitvivt.ru/ru/journal/pdf?id=954 DOI: 10.26102/2310-6018/2021.33.2.016 (In Russ).

Введение

В современных условиях повышающейся информатизации различных сфер производства, когда большинство технологических процессов автоматизируются и выполняются под управлением средств вычислительной техники, важной проблемой является выбор мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами (далее – АСУ ТП).

В нашем исследовании поставлена цель разработки метода выбора мер защиты на каждом уровне АСУ ТП с применением теории множеств в рамках анализа базовых наборов мер защиты.

К основным задачам, которые необходимо выполнить, чтобы достичь цели исследования относятся: а) анализ международной и отечественной нормативно-методической базы выбора мер защиты АСУ ТП; б) постановка задачи выбора мер защиты АСУ ТП; в) разработка алгоритма выбора мер защиты АСУ ТП; г) формализация перехода от минимального набора мер защиты к уточнению адаптированного базового набора мер защиты АСУ ТП.

В 2020 году международные исследовательские группы в сфере информационной безопасности опубликовали исследования, подтверждающие, что хакеры использовали бэкдор Sunburst в программном обеспечении систем мониторинга сети SolarWinds, чтобы получить доступ к 15 электрическим, нефтяным, газовым и производственным предприятиям, которые были заражены вредоносным программным обеспечением [1-2]. Стоит отметить, что вирусная активность не привела к полной остановке технологических процессов зараженных предприятий, однако скомпрометированные сети предприятий не позволяли осуществлять процессы в полной мере ввиду наличия актуальных угроз, до принятия соответствующих мер информационной безопасности.

Меры информационной безопасности – меры защиты информации, обрабатываемой в промышленных системах, реализуемые в составе подсистем обеспечения информационной безопасности на основании следующих сведений:

- информация о классификации защищенности системы;
- актуальные угрозы информационной безопасности;
- структурное и функциональное описание АСУ ТП;
- используемые информационные технологии;
- особенности функционирования.

Меры защиты информации направлены на обеспечение конфиденциальности, целостности и доступности [3].

В рамках внедрения мер защиты информации необходимо учитывать их соотношение с мерами по обеспечению безопасности АСУ ТП: промышленными, физическими, пожарными и т. д. Внедряемые меры не должны оказывать негативного влияния на штатный режим функционирования АСУ ТП [4].

Меры защиты информации – это правовые, организационные и аппаратно-технические меры... Наборы вышеуказанных мер могут различаться для разных стран, компаний и отраслей [5]. Среди отраслевых стандартов, описывающих выбор мер защиты АСУ ТП, стоит выделить NERC CIP – стандарт защиты инфраструктуры передачи электроэнергии [6] и Guidance for Addressing Cyber Security in the Chemical Industry – группа стандартов защиты химических производств [7]. Примером общих подходов к выбору мер защиты АСУ ТП может служить международный стандарт [8], описывающий реализацию требований к мерам безопасности по шести основным направлениям, которые приведены на Рисунке 1. Каждое направление содержит ряд требований, комбинации которых определяют четыре уровня безопасности системы управления кибербезопасностью (Cyber security management system) и предлагаются к применению на основе оценки уровня риска АСУ ТП [9-11].

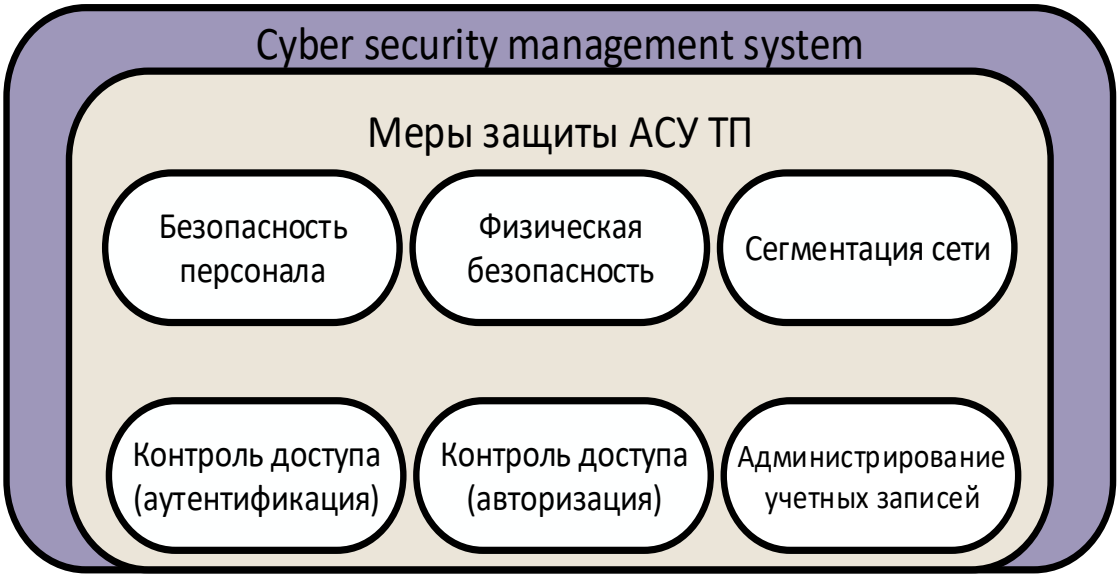

Рисунок 1 – Направления (меры) защиты АСУ ТП в соответствии с ISA/IEC 62443
Figure 1 – Directions (measures) for the protection of the automated process control system in accordance with ISA/IEC 62443

Среди отечественных подходов к выбору мер защиты АСУ ТП отметим методику, изложенную в документе [4]. Данная методика подразумевает объединение мер защиты в базовые наборы в зависимости от установленного класса защищенности АСУ ТП и соответствует алгоритму, представленному на Рисунке 2.

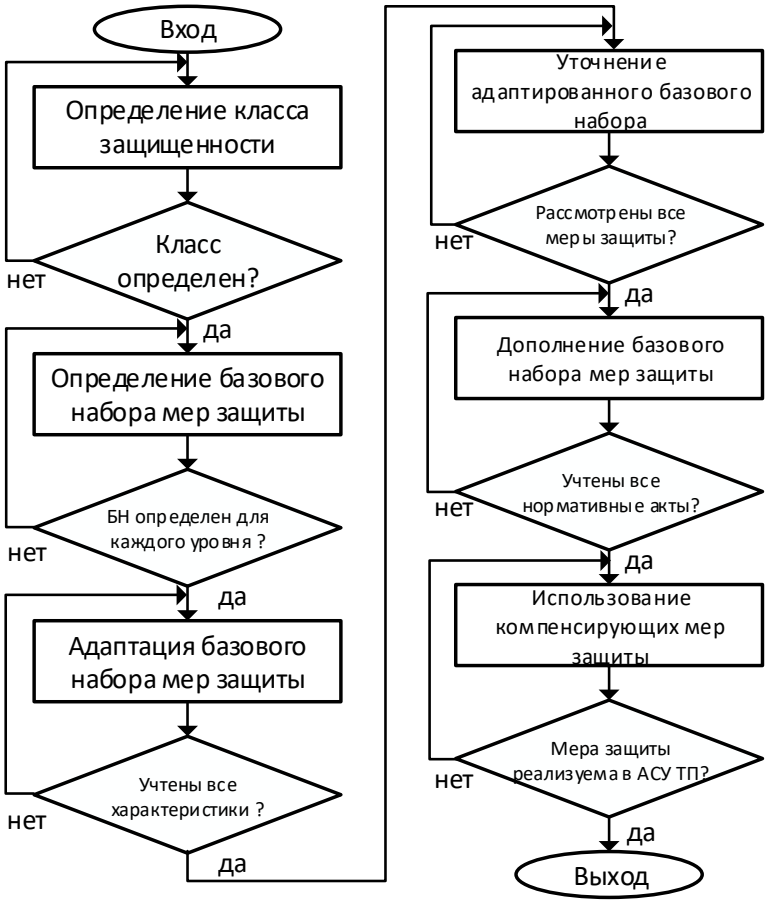

Рисунок 2 – Алгоритм выбора мер защиты АСУ ТП
Figure 2 – Algorithm for selecting security measures of the automated process control system

Постановка задачи выбора мер защиты АСУ ТП

Автоматизированные системы управления отличаются многоуровневой архитектурой исполнения. Каждый из уровней системы характеризуется отличающимся набором элементов, выполняющих определенные функции в рамках участия в технологическом процессе. Рассмотрение АСУ ТП как совокупности элементов на каждом из ее уровней дает возможность привлечь для ее математического описания аппарат теории множеств.

Вопросы применения теории множеств в решении задач информационной безопасности, и, в частности, для принятия решений о выборе мер защиты, рассматриваются многими авторами в своих работах [12-16].

Пусть A– конечное множество мер защиты информации, определенных методикой [4] $A = \{АВ3.0; АВ3Ф.1;.....; АВ3.4\}$.

Исходя из разделения мер защиты на базовые наборы на основании класса защищенности АСУ ТП, выдвинем предположение о необходимости применения мер защиты для каждого уровня системы в соответствии с индивидуальной оценкой класса защищенности соответствующего уровня. Для этого представим базовые наборы в виде подмножеств множества A следующим образом:

B – конечное подмножество, включающее в свой состав базовый набор мер, предписанный классу защищенности К3 ($B \subset A$);

C – конечное подмножество, включающее в свой состав базовый набор мер,

предписанный классу защищенности К2 ($C \subset A$);

E – конечное подмножество, включающее в свой состав базовый набор мер, предписанный классу защищенности К1 ($E \subset A$).

В настоящей работе рассмотрено условие, при котором каждый из трех уровней АСУ ТП характеризуется классом защищенности от двух других, а отдельная мера защиты $x \in A$ может быть как характерна для каждого из базовых наборов мер безопасности, так и быть применима для отдельных базовых наборов тех или иных классов защищенности АСУ ТП.

Метод выбора мер защиты АСУ ТП

Пусть *минимальный* набор мер защиты для всех уровней АСУ ТП соответствует пересечению рассматриваемых множеств

$$B \cap C \cap E = \{x \mid x \in B \,\&\, x \in C \,\&\, x \in E\}. \quad (1)$$

На основании выражения (1) получаем вывод: в минимальный набор включаются исключительно меры, необходимые для применения на каждом уровне АСУ ТП. Если мера защиты не применима в любом из уровней АСУ ТП, то она исключается из набора. Данный набор мер требует минимальных технических внедрений и финансовых вложений при построении системы защиты информации промышленного объекта автоматизации. Однако, с точки зрения информационной безопасности, минимальный набор является недостаточным при противодействии угрозам на информационную инфраструктуру, ввиду отсутствия мер защиты специфичных для отдельных уровней АСУ ТП. Устраним указанные недостатки, определив базовый набор мер защиты для каждого уровня АСУ ТП, в который включаются все меры, необходимые хотя бы для двух из уровней системы

$$(B \cap C) \cup (C \cap E) \cup (B \cap E) = (b \,\&\, e) \cup c) \cup (b \,\&\, e). \quad (2)$$

Использование базовых наборов мер защиты – оптимальный вариант организации системы противодействия угрозам информационной безопасности в АСУ ТП. Однако подход с применением мер исключительно из базового набора не учитывает структурно-функциональных характеристик, особенностей функционирования и внедряемых информационных технологий каждого из уровней АСУ ТП. Данная проблема решается на этапе адаптации базового набора мер защиты. На этом этапе предусматривается исключение мер, непосредственно связанных с информационными технологиями, не используемыми в АСУ ТП, или структурно-функциональными характеристиками, не свойственными системе. В целях недопущения дисфункции системы защиты информации введем выражение (3), описывающее *адаптированный* базовый набор мер защиты АСУ ТП

$$(B \cup C \cup E) \setminus (B \cap C) \cup (C \cap E) \cup (B \cap E). \quad (3)$$

Адаптированный базовый набор мер определяется совокупностью реакций СЗИ, направленных на ее приспособление под изменение условий внешней среды, структуры и функциональности АСУ ТП, а также достижения целей ее функционирования. В качестве примера адаптации рассмотрим добавление в базовый набор мер по контролю целостности информации, содержащейся в базах данных информационной системы, в случае если на верхнем уровне АСУ ТП применяются системы управления базами данных, или исключение из базового набора мер по защите средств терминального доступа, ввиду низкого потенциала нарушителей информационной безопасности, имеющих к ним доступ [17].

Главной проблемой использования адаптированного базового набора видится отсутствие сопоставления защитных мер с актуальными угрозами информационной безопасности промышленной автоматизации. Решением поставленной проблемы является уточнение адаптированного базового набора мер защиты.

Этап уточнения целесообразно проводить на основании полученных результатов оценки адаптированного базового набора на предмет возможности нейтрализации множества угроз, характерного для промышленных систем или вероятности минимизации негативных последствий от реализации угроз информационной безопасности в рамках функционирования АСУ ТП. Уточнение осуществляется с учетом не выбранных ранее мер из множества A и определяется выражением (4).

$$A \setminus B \cup C \cup E = \{x \mid x \in A \& x \notin B \& x \notin C \& x \notin E\} \quad (4)$$

Уточненный адаптированный базовый набор мер является наиболее приближенным к максимальному перечню возможных мер информационной безопасности, применимому на каждом из уровней АСУ ТП. Исходя из вышесказанного, можно сделать вывод о том, что если адаптированный базовый набор мер защиты информации обеспечивает блокирование всех угроз безопасности на рассматриваемом уровне системы, то этап «уточнение адаптированного базового набора» алгоритма выбора мер защиты АСУ ТП (Рисунок 1) необходимо пропускать.

Заключение

В результате проведенного исследования предметной области конкретизировано и сформулировано понятие уточнение адаптированного базового набора мер защиты АСУ ТП, под которым понимается изменение базового набора мер защиты на всех уровнях АСУ ТП, в части их максимальной оптимизации, применительно к структуре и условиям функционирования.

На основе теории множеств сформулирована и успешно решена задача выбора мер защиты АСУ ТП, включающая в себя максимальное приближение базового набора к структуре, реализации и особенностям эксплуатации АСУ ТП.

БЛАГОДАРНОСТИ

The reported study was funded by Russian Ministry of Science (information security), project number 15/2020.

Исследование выполнено при финансовой поддержке Минобрнауки России (Грант ИБ) в рамках научного проекта № 15/2020.

ЛИТЕРАТУРА

1. Фролов А.В., Фролова Е.С. Solarwinds для мониторинга сети. *Системный администратор*. 2019;(12):93-95.
2. SHIMOL S. B. SolarWinds SUNBURST Backdoor: Inside the Stealthy APT Campaign. Cybersecurity news, Threat research. *Varonis*. 2020. Доступно по: https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign (дата обращения 01.03.2021).
3. Цапко Г.П., Вериго А.А. Анализ рисков безопасности автоматизированных систем управления технологическими процессами. *Вестник евразийской науки*. 2016;36(5):1-9. Доступно по: https://cyberleninka.ru/article/n/analiz-riskov-bezopasnosti-

avtomatizirovannyh-sistem-upravleniya-tehnologicheskimi-protsessami (дата обращения 03.03.2021).
4. Приказ ФСТЭК от 14.03.2014 № 31 Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. 2014. Доступно по: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14- marta-2014-g-n-31 (дата обращения 04.03.2021).
5. Андреев Ю.С., Дергачев А.М. Информационная безопасность автоматизированных систем управления технологическими процессами. *Приборостроение*. 2019;(4):221-233.
6. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП. *Вопросы кибербезопасности*. 2015;10(2):56-59.
7. Response to National Institute of Standards and Technology (NIST) [Docket Number 130208119-3119-01] Request for Information. 2013. Доступно по: https://www.nist.gov/system/files/documents/2017/06/01/040513_cgi.pdf (дата обращения 03.03.2021).
8. International Society of Automation. The 62443 Series of Standards. 2015. Доступно по: http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf (дата обращения 03.03.2021).
9. Kulik T., Larsen P. Gorm Towards formal verification of cyber security standards. *Труды ИСП РАН*. 2018;(4):79-94.
10. Жуков С. А., Слугин А. Г. Проблема киберугроз в промышленных системах автоматизации. *Огарёв-Online*. 2015;61(20):1-5. Доступно по: https://cyberleninka.ru/article/n/problema-kiberugroz-v-promyshlennyh-sistemah-avtomatizatsii (дата обращения 08.03.2021).
11. Васильев В.И., Вульфин А.М. Анализ рисков обеспечения целостности телеметрической информации с использованием технологии когнитивного моделирования. *Вестник УГАТУ*. 2019;86(4):122-131.
12. Братченко А.И., Бутусов И.В. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления. *Вопросы кибербезопасности*. 2019; (29)1:18-24.
13. Медведев Н.В., Троицкий И.И. К вопросу об использовании аппарата теории нечетких множеств при анализе рисков информационной безопасности. *Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение»*. 2011;(Специальный выпуск):25-30.
14. Ненадович Д.М., Шахтарин Б.И. Методы теории нечетких множеств в задачах безопасности инфокоммуникационных сетей. *Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение»*. 2006;(3):88-95.
15. Sarvepalli Vi. Practical Math for Your Security Operations. 2013. Доступно по: https://insights.sei.cmu.edu/cert/2013/08/practical-math-for-your-security-operations---part-1-of--3.html (дата обращения 10.03.2021).
16. Вавичкин Н.А. Математические модели в информационной безопасности. *Безопасность информационного пространства – 2017 : XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых. Екатеринбург, издательство Уральского университета*. 2018;(1):148-150.

17. Chernov D.V., Sychugov A.A. Mathematical modeling of information security threats of automated process control systems. *2019 International Conference on Electrotechnical Complexes and Systems (ICOECS)*. 2019;(1):1-4. Доступно по: https://doi.org/10.1109/ICOECS46375.2019.8950023 (дата обращения 11.03.2021).

REFERENCES

1. Frolov A.V., Frolova E.S. Solarwinds for network monitoring. *System Administrator*. 2019; (12):93-95.
2. SHIMOL S.B. SolarWinds SUNBURST Backdoor: Inside the Stealthy APT Campaign. Cybersecurity news, Threat research. *Varonis*. 2020. Available at: https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign (accessed 01.03.2021).
3. Csapko G.P., Verigo A.A. Security risk analysis of automated process control systems. *Bulletin of the Eurasian science*. 2016;36(5):1-9. Available at: https://cyberleninka.ru/article/n/analiz-riskov-bezopasnosti-avtomatizirovannyh-sistem-upravleniya-tehnologicheskimi-protsessami (accessed 03.03.2021).
4. The Russia FSTEC order dated March 14 2014. № 31 “About the approval of requirements for ensuring the protection of information in automated control systems for production and technological processes at critical facilities, potentially dangerous Facilities, as well as facilities that pose an increased danger to human life and health and to the environment”. 2014. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14- marta-2014-g-n-31 (accessed 04.03.2021).
5. Andreev Yu.S., Dergachev A.M. Information security of automated process control systems. *Instrumentation*. 2019;(4):221-233.
6. Gordeychik S.V. Missiocentric approach to the cybersecurity of automated process control systems. *Cybersecurity issues*. 2015;10(2):56-59.
7. Response to National Institute of Standards and Technology (NIST) [Docket Number 130208119-3119-01] Request for Information. 2013. Available at: https://www.nist.gov/system/files/documents/2017/06/01/040513_cgi.pdf (accessed 03.03.2021).
8. International Society of Automation. The 62443 Series of Standards. 2015. Available at: http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf (accessed 03.03.2021).
9. Kulik T., Larsen P. Gorm Towards formal verification of cyber security standards. *Proc. ISP RAS*. 2018;(4):79-94.
10. Zhukov S.A., Slugin A.G. The problem of cyber threats in industrial automation systems. *Ogarev-Online*. 2015;61(20):1-5. Available at: https://cyberleninka.ru/article/n/problema-kiberugroz-v-promyshlennyh-sistemah-avtomatizatsii (accessed 08.03.2021).
11. Vasilyev V.I., Vulyvin A.M. Risk analysis of ensuring the integrity of telemetric information using cognitive modeling technology. *Vestnik USATU*. 2019;86(4):122-131.
12. Bratchenko A.I., Butusov I.V. Application of methods of the theory of fuzzy sets to the assessment of risks of violation of critical properties of protected resources of automated control systems. *Cybersecurity issues*. 2019; (29)1:18-24.
13. Medvedev N.V., Troickiy I.I. On the use of the fuzzy set theory apparatus in the analysis of information security risks. *Vestnik Moskovskogo Gosudarstvennogo Tekhnicheskogo Universiteta imeni N.E. Baumana, seriya “Priborostroenie”*. 2011;(special issue):25-30.
14. Nenadovich D.M., Shahtarin B.I. Methods of the theory of fuzzy sets in the security problems of infocommunication networks. *Vestnik Moskovskogo Gosudarstvennogo*

Tekhnicheskogo Universiteta imeni N.E. Baumana, seriya "Priborostroenie". 2006;(3):88-95.
15. Sarvepalli V. Practical Math for Your Security Operations. *Carnegie Mellon University*. 2013. Available at: https://insights.sei.cmu.edu/cert/2013/08/practical-math-for-your-security-operations---part-1-of--3.html (accessed 10.03.2021).
16. Vavichkin N.A. Mathematical models in information security. *Security of the information space-2017: the XVI All-Russian Scientific and Practical Conference of Students, Postgraduates, Young Scientists*. 2018;(1):148-150.
17. Chernov D.V., Sychugov A.A. Mathematical modeling of information security threats of automated process control systems. *2019 International Conference on Electrotechnical Complexes and Systems (ICOECS)*. 2019;(1):1-4. Available at: https://doi.org/10.1109/ICOECS46375.2019.8950023 (accessed 11.03.2021).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Чернов Денис Владимирович, старший преподаватель кафедры информационной безопасности, ФГБОУ ВО Тульский государственный университет, начальник сектора информационной безопасности АО ЦКБА, Тула, Российская Федерация.
e-mail:cherncib@gmail.com
ORCID:0000-0002-7223-8670

Denis V. Chernov Senior Lecturer Chair Of "Information Security", Tula State University, Head Of The Information Security Sector Of The JSC ADC, Tula, Russian Federation

Сычугов Алексей Алексеевич, кандидат технических наук, доцент, заведующий кафедрой информационной безопасности, директор института прикладной математики и компьютерных наук, Тульский государственный университет, Тула, Российская Федерация.
e-mail: xru2003@list.ru

Alexey A. Sychugov Candidate Of Technical Sciences, Docent, Head Chair Of "Information Security" Tula State University, Tula, Russian Federation