Автоматизация и моделирование в проектировании и управлении. 2023. № 4 (22). С. 12-17.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2023. № 4 (22). P. 12-17.

Научная статья
Статья в открытом доступе
УДК 004.056.5
doi: 10.30987/2658-6436-2023-4-12-17

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ РАЗРАБОТКИ МОДЕЛИ МИНИМИЗАЦИИ РИСКОВ КОНСТРУКТОРСКО-ТЕХНОЛОГИЧЕСКОГО ПРОЕКТА

Татьяна Владимировна Карлова[1], Александр Юрьевич Бекмешов[2], Алексей Эдуардович Тихомиров[3], Наталия Михайловна Кузнецова[4], Марианна Валериевна Михайлова[5], Анна Николаевна Запольская[6]
[1, 2, 3, 6] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[4, 5] Московский государственный технологический университет «СТАНКИН», г. Москва, Россия
[1] karlova-t@yandex.ru; [2] b-a-y-555@yandex.ru; [3] alexey.tikhomirov@list.ru; [4] knm87@mail.ru; [5] mari.mikhaylova@list.ru; [6] zap-ann@yandex.ru

Аннотация. *Минимизация рисков при разработке интеллектуалоемкой продукции, связанная с исключением несанкционированного вхождения в систему безопасности конструкторско-технологического проекта, является важнейшей задачей сохранения развития российского творческого потенциала. Методом исследования является выявление и анализ применения инженерно-психологических аспектов проектной деятельности интеллектуалоемкой продукции. Четко сформированные и оформленные требования к информационной и технологической безопасности, дополненные исследованиями в области инженерной психологии, дают возможность минимизировать риски угроз вхождения в систему по всей цепочке проектно-производственного процесса. Формирование модели минимизации рисков конструкторско-технологического проекта, позволяющей осуществлять контроль выполнения требований к технологической безопасности на основе разработки критериев оценки качества с учетом применения инженерно-психологических знаний является решением весьма актуальной задачи.*

Ключевые слова: автоматизация, управление, информационная безопасность, риски, интеллектуалоемкий продукт, веб-платформа, моделирование

Для цитирования: Карлова Т.В., Бекмешов А.Ю., Тихомиров А.Э., Кузнецова Н.М., Михайлова М.В., Запольская А.Н. Автоматизация процессов обеспечения информационной безопасности на основе разработки модели минимизации рисков конструкторско-технологического проекта // Автоматизация и моделирование в проектировании и управлении. 2023. №4 (22). С. 12-17. doi: 10.30987/2658-6436-2023-4-12-17.

Original article
Open Access Article

AUTOMATING INFORMATION SECURITY PROCESSES BY DEVELOPING A RISK MINIMIZATION MODEL FOR A DESIGN AND TECHNOLOGICAL PROJECT

Tatyana V. Karlova[1], Alexander Yu. Bekmeshov[2], Alexey E. Tikhomirov[3], Natalia M. Kuznetsova[4], Marianna V. Mikhailova[5], Anna N. Zapolskaya[6]
[1, 2, 3, 6] Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[4, 5] Moscow State University of Technology “STANKIN”, Moscow, Russia
[1] karlova-t@yandex.ru; [2] b-a-y-555@yandex.ru; [3] alexey.tikhomirov@list.ru; [4] knm87@mail.ru; [5] mari.mikhaylova@list.ru; [6] zap-ann@yandex.ru

Abstract. *Minimizing risks in developing intellectually intensive products, connected with the exclusion of unauthorized entry into the design and technological project security system, is the most important task of preserving the development of Russian creative potential. The research method is to identify and analyse the application of engineering and psychological aspects of the design activities of intellectual-intensive products. Clearly formed and documented requirements for information and technological security, supplemented by research in the field of engineering psychology, make it possible to minimise the risks of threats to enter the system along the entire chain of the design and production process. Building a model for minimising the risks of a design and technological project,*

which makes it possible to fulfil technological safety requirements based on developing quality assessment criteria, considering the use of engineering and psychological knowledge, is the solution to a very urgent problem.
Keywords: automation, management, information security, risks, intellectual-intensive product, web platform, modelling
For citation: Karlova T.V., Bekmeshov A.Yu., Tikhomirov A.E., Kuznetsova N.M., Mikhailova M.V., Zapolskaya A.N. Automating Information Security Processes by Developing a Risk Minimization Model for a Design and Technological Project. Automation and modeling in design and management, 2023, no. 4 (22). pp. 12-17. doi: 10.30987/2658-6436-2023-4-12-17.

Введение

Впервые кибернетический подход в развитии теории управления был использован американским математиком Норбертом Винером в 1948 году «Кибернетика или управление, связь в животном мире и в машине».

Достоинство кибернетического подхода заключается в использовании методов моделирования систем управления в процессах управления сложно-ориентированными объектами различной природы [4].

Основным условием функционирования сложно-ориентированного объекта является процесс. Вторым условием является вход в систему, включающий в себя набор подсистем, например, конструкторскую подсистему, технологическую подсистему, подсистему оборудования, подсистему кадрового ресурса. Следующим условием является входная информация, обеспеченная новейшими информационными технологиями [9] и предусматривающая подсистемы защиты информации на всех этапах конструкторско-технологического проекта.

Методология исследования

Обеспечение безопасности [2] на уровне разработки проекта требует повышенного внимания по предотвращению несанкционированных доступов, связанных с потерей творческих замыслов и идей, зафиксированных на различных носителях информации. Именно поэтому на данном этапе необходимо создавать наивысший уровень контроля по защите информации на основе автоматизации выявления уязвимых точек повышенного риска. Примером систем с высоким уровнем контроля могут служить веб-платформы космической безопасности.

Веб-платформа является одним из основных носителей, обеспечивающих передачу данных (рис. 1).

Рис. 1. Мониторинг этапов разработки проекта веб-платформы
Fig. 1. Monitoring the development stages of the web platform project

Для анализа данных о скорости реагирования системы защиты информации веб-платформы должны быть выполнены следующие требования:

– Соответствующие инструменты сбора данных. В качестве типовых инструментов для сбора данных об эффективности любых приложений могут использоваться:

а) анализ журнала веб-сервера;

б) метрика конверсии пользовательского решения.

– Необходимый объем данных. Чтобы получить четкое представление о производительности системы, необходимо иметь достаточно данных для анализа, требуемый объем которых не должен быть менее 50 000 пользовательских событий в день.

– Качество данных. Собранные данные должны быть точными и надежными, поэтому в качестве инструмента веб-аналитики был выбран сервис Yandex Metrika.

– Методы анализа. Собранные данные должны быть проанализированы с использованием соответствующих методов, таких как выявление рисков и обработка выбросов.

– Показатели производительности. Время загрузки страницы.

Результаты исследования и обсуждение

Чтобы обеспечить полноту данных состояния веб-платформы, также требуется соблюдение требований к ведению журнала (логирование). Это включает в себя сбор и запись информации об активности и поведении системы. Целью ведения журнала данных является предоставление информации о производительности системы и выявление потенциальных проблем, которые могут повлиять на стабильность функционирования. Ключевыми требованиями к ведению журнала являются:

– актуальность: регистрируемые данные должны иметь отношение к производительности и поведению системы. Журналы должны фиксировать такие данные, как использование ресурсов сервера, время отклика и сообщения об ошибках.

– своевременность: журналы должны записываться в режиме реального времени, чтобы гарантировать сбор данных по мере использования системы.

– согласованность: формат и структура журналов должны быть согласованными, чтобы упростить анализ и отчетность.

– хранение: журналы должны храниться в централизованном месте, чтобы их можно было легко извлечь и проанализировать.

– безопасность: журналы должны быть защищены, чтобы гарантировать, что конфиденциальная информация не будет раскрыта или утеряна.

– хранение: журналы должны храниться в течение достаточного периода времени, чтобы обеспечить возможность исторического анализа производительности системы.

– масштабируемость: система ведения журнала должна быть способна масштабироваться для обработки больших объемов данных, особенно по мере роста системы.

– доступность: журналы должны быть доступны уполномоченному персоналу с соответствующим уровнем доступа, чтобы обеспечить эффективный анализ и отчетность.

Удовлетворение данных требований позволяет системе веб-приложений хранить ценную информацию о своем поведении, позволяя разработчикам и администраторам выявлять потенциальные проблемы и принимать обоснованные решения для повышения не только общей производительности, но и защиты информации.

На основе имитационной модели в рамках соответствующих функций защиты производится количественная оценка рисков при выявлении информационных угроз [1].

Представленная на рис. 2 схема иллюстрирует возможности автоматизации процессов информационного реагирования (управления) на возникновение риска (утечки информации) при проектировании конструкторско-технологических решений.

Рис. 2. Модель автоматизации процесса реагирования на риск
Fig. 2. A model for automating the risk response process

Одной из важнейших подсистем является подсистема выбора моделей и методик расчета, входящая в комбинированный подход, и, которая учитывает как обеспечение физической безопасности IT-систем, так и разграничение уровней доступа к IT-системам с одновременным шифрованием особо важных/конфиденциальных данных.

На рис. 3 представлена модель методов защиты трех этапов разработки конструкторско-технологического проекта.

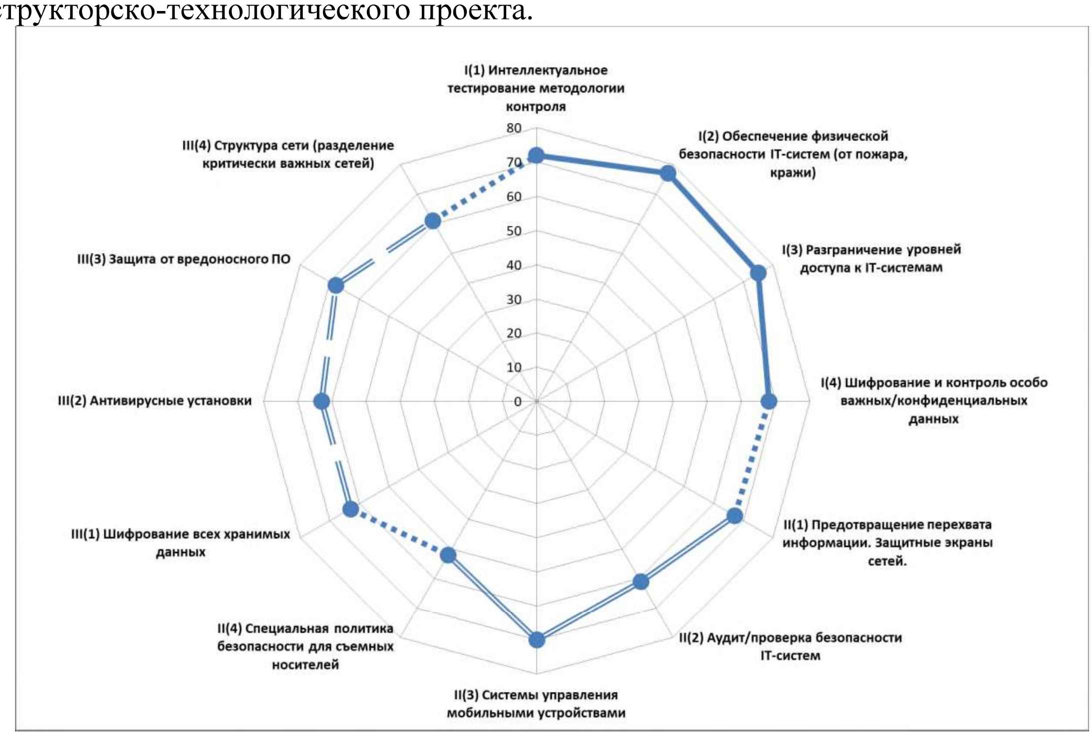

Рис. 3. Модель методов защиты этапов конструкторско-технологического проекта на основе анализа производственных процессов инженерного прогнозирования
Fig. 3. A model of methods for protecting the stages of a design and technological project based on the analysis of production processes of engineering forecasting

Этап I – концепция конструкции на основе анализа производственных процессов инженерного прогнозирования и планирования. Цель.

Этап II – разработка модели технологического проекта с учетом оптимизации конструкторских решений с выработкой технического задания (ТЗ).

Этап III – создание экспериментально-опытного образца.

Как видно из диаграммы, основными методами защиты [6] на первом этапе являются:

– интеллектуальное тестирование методологии контроля;

– обеспечение физической безопасности IT-систем (от пожара, кражи);

– разграничение уровней доступа к IT-системам;

– шифрование и контроль особо важных/конфиденциальных данных.

На втором этапе:

– предотвращение перехвата информации. Защитные экраны сетей;

– аудит/проверка безопасности IT-систем;

– системы управления мобильными устройствами;

– специальная политика безопасности для съемных носителей.

На третьем этапе:

– шифрование всех хранимых данных;

– антивирусные установки;

– защита от вредоносного ПО;

– структура сети (разделение критически важных сетей).

Из диаграммы видно, что второй и третий этапы нуждаются в усилении мер защиты по предотвращению рисков информационной безопасности.

Заключение

Моделирование методов защиты создания интеллектуалоемкой продукции предполагает разработку ряда вариантов конструкторско-технологических решений с инвариантными принципами функционирования, обладающих различными свойствами, но выполняющими все требования веб-платформы.

Для более эффективного и достоверного обеспечения уровня качества проектирования интеллектуальной продукции необходимо анализировать инженерно-психологический опыт процессов моделирования с использованием автоматизации процессов информационного реагирования (управления) на возникновение риска.

Разработка имитационной модели на основе сочетания методов и средств обеспечения информационной безопасности позволяет снизить риск потери авторского решения на этапе разработки, а также исключить несанкционированный доступ к значимым данным конструкторско-технологического проекта.

Список источников:

1. Вихорев С.В. Классификация угроз информационной безопасности. – [Электронный ресурс]. – http://www.cnews.ru/reviews/free/security (дата обращения 04.04.2020).
2. Галатенко В.А. Основы информационной безопасности. – Москва. – 2016. 264 с. – [Электронный ресурс]. – http://en.bookfi.net/book/584428 (дата обращения 16.03.2020).
3. Гацко М. О соотношении понятий «угроза» и «опасность» – [Электронный ресурс] – http://old.nasledie.ru/oboz/N07_97/7_06.HTM (дата обращения 25.03.2020).
4. Цветкова О.Л., Айдинян А.Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз // Вестник компьютерных и информационных технологий. – 2014. – №8 (122). – С. 48-53.
5. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология.
6. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.

References:

1. Vikhorev S.V. Classification of Threats in Information Security [Internet]. [cited 2020 Apr 04]. Available from: http://www.cnews.ru/reviews/free/security
2. Galatenko V.A. Fundamentals of Information Security [Internet]. Moscow; 2016 [cited 2020 Mar 16]. – http://en.bookfi.net/book/584428
3. Gatsko M. On the Relationship Between the Concepts of “Threat” and “Danger” [Internet]. 1997 [cited 2020 Mar 25]. Available from: http://old.nasledie.ru/oboz/N07_97/7_06.HTM
4. Tsvetkova O.L., Aidinyan A.R. Intelligent System Evaluation Information Security of the Enterprise From Internal Threats. Vestnik Komp'iuternykh I Informatsionnykh Tekhnologii. 2014;8(122):48-53.
5. GOST R ISO/IEC 27005-2010 Information Technology.
6. ISO/IEC 27005:2008. Methods and Means of Ensuring Safety.

7. Менеджмент риска информационной безопасности.

8. Information technology. Security techniques. Information security risk management.

9. ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

7. ISO/IEC 27005:2008. Information Security Risk Management.

8. ISO/IEC 27005. Information Technology. Security Techniques. Information Security Risk Management.

9. GOST R ISO/IEC 27001. Information Technology. Security Techniques. Information Security Management Systems. Requirements.

Информация об авторах:

Карлова Татьяна Владимировна
доктор социологических наук, кандидат технических наук, ведущий научный сотрудник, профессор Института конструкторско-технологической информатики Российской академии наук

Бекмешов Александр Юрьевич
кандидат технических наук, старший научный сотрудник, доцент Института конструкторско-технологической информатики Российской академии наук

Тихомиров Алексей Эдуардович
аспирант Института конструкторско-технологической информатики Российской академии наук

Кузнецова Наталия Михайловна
кандидат технических наук, доцент Московского государственного технологического университета «СТАНКИН»

Михайлова Марианна Валериевна
кандидат социологических наук доцент Московского государственного технологического университета «СТАНКИН»

Запольская Анна Николаевна
кандидат социологических наук, старший научный сотрудник Института конструкторско-технологической информатики Российской академии наук

Information about the authors:

Karlova Tatyana Vladimirovna
Doctor of Sociological Sciences, Candidate of Technical Sciences, Leading Research Fellow, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Bekmeshov Alexander Yurievich
Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Tikhomirov Alexey Eduardovich
Postgraduate Student of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Kuznetsova Natalia Mikhailovna
Candidate of Technical Sciences, Associate Professor of Moscow State University of Technology “STANKIN”

Mikhailova Marianna Valerievna
Candidate of Sociological Sciences, Associate Professor of Moscow State University of Technology “STANKIN”

Zapolskaya Anna Nikolaevna
Candidate of Sociological Sciences, Senior Researcher of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 22.09.2023; одобрена после рецензирования 20.10.2023; принята к публикации 27.10.2023.

The article was submitted 22.09.2023; approved after reviewing 20.10.2023; accepted for publication 27.10.2023.

Рецензент – Горбунов А.Н., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Gorbunov A.N., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.