DOI: 10.22184/1993-7296.FRos.2020.14.7.604.615

Производство и применение лазеров: актуальные вопросы информационной безопасности и непрерывности деятельности

К. Н. Темникова
Московский политехнический университет, ООО «Профконсалт ИСМ», Москва, Россия

В статье рассматриваются вопросы производства и применения лазеров и связанные с этим возможности проникновения в программное обеспечение промышленных лазерных систем. Рассмотрены цели, преимущества и порядок внедрения системы менеджмента информационной безопасности ISO / IEC 27001:2013 (серия стандартов ISO 270XX). Представлен пошаговый алгоритм, как сформировать систему менеджмента информационной безопасности на предприятиях, чтобы снизить риски, избежать системных ошибок. Показана взаимосвязь предложенных мер с обеспечением непрерывности бизнеса и повышением инвестиционной привлекательности предприятий. Перебои в бизнесе приводят к потере клиентов, доходов и репутации, при этом отсутствие системы менеджмента непрерывности бизнеса на предприятии свидетельствует о неготовности к быстрому восстановлению деятельности и несоответствии международному уровню.

Ключевые слова: промышленные лазерные системы, система менеджмента информационной безопасности, информационная безопасность, кибербезопасность, лазеры, корпоративные

Laser Production and Application: Topical Issues of Information Security and Business Continuity

K. N. Temnikova
Moscow Polytechnic University, LLC "Profconsult ISM", Moscow, Russia

The article deals with the production and application of lasers, and the related possibilities of penetration into the software of industrial laser systems. The goals, advantages and procedure for the implementation of the ISO / IEC 27001:2013 Information Security Management System (ISO 270XX series of standards) are considered. A step-by-step algorithm is presented on how to form an Information Security Management System at enterprises in order to reduce risks and avoid system errors. The relationship of the proposed measures with ensuring business continuity and increasing the investment attractiveness of enterprises is shown. Business disruptions lead to the loss of customers, income and reputation, while the lack of a Business Continuity Management System in the enterprise indicates an unpreparedness for a quick recovery of activities and inconsistency with the international level.

Key words: Industrial laser systems. Information security management system. Information security, cyber security, lasers, corporate information systems. Business continuity management system.

Received: 14.11.2020
Accepted: 19.11.2020

информационные системы, система менеджмента непрерывности бизнеса.

Статья поступила: 14.11.2020
Статья принята к публикации: 19.11.2020

ВОЗМОЖНОСТИ ПРОНИКНОВЕНИЯ В ПО ПРОМЫШЛЕННЫХ ЛАЗЕРНЫХ СИСТЕМ

Лазерные технологии развиваются быстрыми темпами. Лазерные технологические комплексы, предназначенные для реализации в промышленных условиях различных видов лазерных технологий обработки материалов, становятся все более востребованными. В этом смысле важно подчеркнуть, что «уникальные детали и изделия для заказчиков могут быть изготовлены со значительной экономией дорогостоящих материалов» [1, с. 65; 2].

Как отмечают эксперты, «продажи лазеров за десятилетие удвоилась, достигнув в 2018 году 13,76 млрд долл. объем продаж лазеров в 2019 году ожидается на уровне 14,6 млрд долл. 2018-й был еще одним рекордным годом в секторе продажи промышленных лазеров: на уровне 5 млрд долл., в основном благодаря волоконным лазерам. Мировой рынок лазерных систем для обработки материалов в 2018 году достиг рекордного объема в 19,8 млрд долл [3].

Промышленные лазерные системы становятся все более сложными. Расширяется круг актуальных вопросов, связанных с фотонными и оптическими технологиями, оптическими материалами и элементами, используемыми в оптических системах, оборудовании и станках [4–19]. При этом промышленные комплексы высокоскоростного лазерного раскроя металлопроката, машины, создающие высококачественные изделия из металла и др., имеют сложное программное обеспечение. Безопасность и эффективность промышленных лазерных систем в значительной мере зависит от качества программного обеспечения.

Технологии с участием высокомощных лазеров (термообработка, сварка и резка) тесно связаны с информационными технологиями, в том числе с технологиями передачи информации по сети интернет, подключением различных устройств и т.п. По мере того как усложняются промышленные лазерные системы, возрастают риски проникновения в программное обеспечение этих систем.

Возможности проникновения в программное обеспечение промышленных лазерных систем

POSSIBILITIES OF PENETRATION INTO SOFTWARE OF INDUSTRIAL LASER SYSTEMS

Laser technology is developing at a rapid pace. Laser technological complexes intended for industrial implementation of various types of laser technologies for processing materials are becoming more and more in demand. In this sense, it is important to emphasize that "unique parts and products for customers can be manufactured with significant savings in expensive materials" [1, p. 65; 2].

According to experts, "laser sales doubled over the decade, reaching 13.76 billion USD in 2018. Laser sales in 2019 are expected to reach 14.6 billion USD. 2018 was another record year in the industrial laser sales sector: at 5 billion USD, mainly due to fibre lasers. The world market for laser systems for material processing in 2018 reached a record volume of 19.8 billion USD [3].

Industrial laser systems are becoming more and more complex. The range of topical issues related to photonic and optical technologies, optical materials and elements used in optical systems, equipment and machine tools is expanding [4–19]. At the same time, industrial complexes for high-speed laser cutting of rolled metal, machines that create high-quality metal products, etc. have complex software. The safety and efficiency of industrial laser systems is highly dependent on the quality of the software.

Technologies involving high-power lasers (heat treatment, welding and cutting) are closely related to information technologies, including technologies for transmitting information over the Internet, connecting various devices, etc. As industrial laser systems become more complex, the risks of software penetration in these systems increase.

Opportunities for penetration into the software of industrial laser systems are associated, for example, with untimely software updates, neglect of security measures, excessive gullibility, non-compliance with password policies, dishonest suppliers, etc. It should also be noted that there is insufficient information security and a lack of highly qualified personnel in this area.

Penetration into the software of industrial laser systems is possible in several ways (consideration of these methods can serve as the subject of a separate article). Attackers use various

связаны, например, с несвоевременным обновлением программного обеспечения, пренебрежением средствами защиты, излишней доверчивостью, несоблюдением парольной политики, недобросовестностью поставщиков и др. Следует также отметить недостаточное обеспечение информационной безопасности, нехватку высококвалифицированных кадров в этой области.

Проникновение в программное обеспечение промышленных лазерных систем возможно несколькими способами (рассмотрение этих способов может послужить предметом отдельной статьи). Злоумышленники используют различные виды программного обеспечения, методы социальной инженерии, фишинга и мошенничества. Следует во многом согласиться с тем, что по мере того, как киберпреступные посягательства будут становиться все более частыми и изощренными, конкуренция вытеснит с рынка предприятия с большим количеством инцидентов.

Как предприятиям-производителям, так и предприятиям, использующим промышленные лазерные системы, необходимо повышать конкурентоспособность, инвестиционную привлекательность и в короткий период обеспечить рост инфраструктуры и ее импортонезависимость, надежность и защищенность.

Какие пути выхода из сложившейся ситуации возможны? Назовем лишь некоторые из них:

- решение кадрового вопроса в области информационной безопасности (при этом следует учитывать, что «нередко отстаивать хороших специалистов приходится у хакеров» [20]);
- использование средств защиты, своевременное обновление программного обеспечения;
- аудит поставщиков программного обеспечения (здесь следует обратить внимание на мнение экспертов в отношении смежных отраслей: «Проблему для энергетического сектора будут составлять «supply chain» – атаки со стороны поставщиков программного и аппаратного обеспечения» [21]);
- участие специалистов по информационной безопасности в работе кросс-функциональных продуктовых групп, то есть активно использовать принцип DevSecOps (этот принцип получает все большее распространение в мире);
- повышение компетенций самих разработчиков, уровня их культуры в области информационной безопасности;
- разумный баланс между удобством и безопасностью инновационных решений; проверка всех принимаемых решений с точки зрения

types of software, social engineering, phishing, and fraud. There is much to be agreed that as cybercriminal attacks become more frequent and sophisticated, competition will displace incident-intensive businesses from the market.

Both manufacturing enterprises and enterprises using industrial laser systems need to increase competitiveness, investment attractiveness and, in a short period, ensure the growth of infrastructure and its independence from imports, reliability and security.

What are the ways out of this situation? Let's name just a few of them:

- solving the personnel issue in the field of information security (it should be borne in mind that "often hackers have to defend good specialists" [20]);
- use of protection means, timely software update;
- audit of software suppliers (here you should pay attention to the opinion of experts in relation to related industries: "The problem for the energy sector will be "supply chain" – attacks from suppliers of software and hardware" [21]);
- participation of information security specialists in the work of cross-functional product groups, that is, actively use the DevSecOps principle (this principle is becoming more widespread in the world);
- increasing the competences of the developers themselves, the level of their culture in the field of information security;
- reasonable balance between convenience and safety of innovative solutions; verification of all decisions made in terms of information security (special attention is paid to laser technologies and innovation management technologies);
- implementation of information security management systems in accordance with ISO / IEC 27001 (ISO 270XX series of standards, best practices);
- implementation of business continuity management systems in accordance with ISO 22301;
- training of personnel, conducting trainings.

On specialized electronic resources [22], topical issues of the development of laser technologies are presented. At the same time, the issues of reducing the risks of penetration into the software of industrial laser systems are practically not considered.

информационной безопасности (лазерным технологиям и технологиям управления инновациями уделяется особое внимание);
- внедрение систем менеджмента информационной безопасности в соответствии с ISO/IEC 27001 (серией стандартов ISO 270XX, лучшими практиками);
- внедрение систем менеджмента непрерывности бизнеса в соответствии с ISO 22301;
- обучение персонала, проведение тренингов.

На специализированных электронных ресурсах [22] представлены актуальные вопросы развития лазерных технологий. Вместе с тем вопросы о снижении рисков проникновения в программное обеспечение промышленных лазерных систем практически не рассматриваются.

В целях сокращения возможностей проникновения в программное обеспечение промышленных лазерных систем необходимо уделять внимание выработке единого видения обеспечения информационной безопасности как при разработке таких систем, так и при их эксплуатации с учетом совершенно новых вызовов, возникающих в информационном пространстве. При этом необходимо принимать во внимание новые риски в информационной среде с учетом того, что «киберпреступный мир развивает свои технологии, ничуть не отставая от темпов «гражданской» цифровизации, а иногда и опережая их» [23].

В связи с этим необходимо обратить внимание на возрастающую роль импортозамещения в обе-

In order to reduce the possibilities of penetration into the software of industrial laser systems, it is necessary to pay attention to the development of a unified vision of ensuring information security both in the development of such systems and in their operation, taking into account completely new challenges arising in the information space. At the same time, it is necessary to take into account new risks in the information environment, taking into account the fact that "the cybercriminal world develops its technologies, keeping up with the pace of" civil "digitalization, and sometimes even ahead of them" [23].

In this regard, it is necessary to pay attention to the growing role of import substitution in ensuring information security, including in terms of the use of domestic software in industrial laser systems.

IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEM

In the specialized literature, there is an increase in the risks associated with the use of digital technologies, the spread and complexity of cyber threats [24–26]. In connection with the transition to remote work, the use of remote formats of interaction on the Internet, the risks increase significantly.

In order to reduce the risks of penetration into the software of industrial laser systems, to avoid system errors, it is advisable to implement and

	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	Ответственный	Срок
Gap – Анализ	★	★	★											
Окружение	★													
Политика и цели				★										
Риски			★	★										
Законодательство			★	★										
Осведомленность			★	★										
Операционная деятельность				★	★	★	★							
Мониторинг						★	★	★	★					
Оценка деятельности											★			
Аудиты						★	★	★	★	★	★			
Совершенствование								★	★	★	★	★		
Анализ со стороны руководства				★		★		★		★				
Решение о сертификации										★				

Рис. 1. *План проекта по внедрению системы менеджмента информационной безопасности (СМИБ)(вариант)*
Fig. 1. *Project plan for the implementation of an Information security management system (ISMS)(variant)*

спечении информационной безопасности, в том числе в части применения отечественного программного обеспечения в промышленных лазерных системах.

ВНЕДРЕНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В специальной литературе отмечается увеличение рисков, связанных с применением цифровых технологий, распространением и сложностью киберугроз [24–26]. В связи с переходом на удаленную работу, применением дистанционных форматов взаимодействия в сети интернет риски значительно возрастают.

Для того чтобы снизить риски проникновения в программное обеспечение промышленных лазерных систем, избежать системных ошибок, целесообразно внедрить и поддерживать систему менеджмента информационной безопасности.

Рабочая группа внедрения опирается на международные стандарты, в том числе:

- ISO/IEC 27001:2013(en) Information technology – Security techniques – Information security management systems – Requirements;
- ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary;
- ISO/IEC 27002:2013, Information technology – Security Techniques – Code of practice for information security controls;
- ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance;
- ISO/IEC 27004, Information technology – Security techniques – Information security management – Measurement;
- ISO/IEC 27005, Information technology – Security techniques – Information security risk management;
- ISO 31000:2018, Risk management – Principles and guidelines (https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

После приобретения международного стандарта, для разработки и внедрения системы управления информационной безопасностью в соответствии с ISO/IEC 27001 необходимо предпринять определенные последовательные действия, желательно с привлечением опытных экспертов.

Последовательность действий: диагностический аудит, подготовка рабочей группы и плана внедрения, тренинги по информационной безопасности, описание системных процедур и требо-

maintain an information security management system.

The Implementation Working Group is based on international standards, including:

- ISO/IEC 27001:2013(en) Information technology – Security techniques – Information security management systems – Requirements;
- ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary;
- ISO/IEC 27002:2013, Information technology – Security Techniques – Code of practice for information security controls;
- ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance;
- ISO/IEC 27004, Information technology – Security techniques – Information security management – Measurement;
- ISO/IEC 27005, Information technology – Security techniques – Information security risk management;
- ISO 31000:2018, Risk management – Principles and guidelines (https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en).

After the acquisition of an international standard, to develop and implement an information security management system in accordance with ISO/IEC 27001, it is necessary to take certain sequential actions, preferably with the involvement of experienced experts.

Sequence of actions: diagnostic audit, preparation of a working group and an implementation plan, training on information security, description of system procedures and requirements, description of basic procedures and requirements, adjustment of processes and procedures of existing management systems, methodological assistance in the development/revision of documents, audits, including internal based on the results of the created management system, analysis of the created management system. Accompanying a certification audit – if necessary.

The solution for the implementation of an information security management system in accordance with ISO/IEC 27001 includes the necessary documentation, consulting, training, audit, preparation for certification. The solution is applicable for individual enterprises, holdings, groups of companies.

ваний, описание базовых процедур и требований, корректировка процессов и процедур имеющихся систем менеджмента, методическая помощь по разработке/доработке документов, проведение аудитов, в том числе внутренних по итогам созданной системы менеджмента, проведение анализа созданной системы менеджмента. Сопровождение сертификационного аудита – в случае необходимости.

Решение по внедрению системы управления информационной безопасностью в соответствии с ISO/IEC 27001 включает необходимую документацию, консалтинг, обучение, аудит, подготовку к сертификации. Решение применимо для отдельных предприятий, холдингов, групп компаний.

При внедрении системы менеджмента информационной безопасности для предприятий будут полезны такие ресурсы, как:

- ISO/IEC 27001 – Руководство клиента – Информация о возможностях системы менеджмента информационной безопасности;
- ISO/IEC 27001 – Брифинг для руководителей – Информация о преимуществах ISO/IEC 27001 для бизнеса;
- ISO/IEC 27001 – Особенности и преимущества – Информация об особенностях и преимуществах стандарта ISO/IEC 27001;
- ISO/IEC 27001 – Руководство по внедрению – Подробное руководство по внедрению системы менеджмента информационной безопасности;
- ISO/IEC 27001 – Контрольный лист для самостоятельной проверки – контрольный лист

When implementing an information security management system for enterprises, resources such as:

- ISO/IEC 27001 – Customer Guide – Information on the capabilities of an information security management system;
- ISO/IEC 27001 – Executive Briefing – Information on the benefits of ISO/IEC 27001 for business;
- ISO/IEC 27001 – Features and Benefits – Learn about the features and benefits of ISO/IEC 27001;
- ISO/IEC 27001 – Implementation Guide – Detailed guidance for the implementation of an information security management system;
- ISO/IEC 27001 – Self-Review Checklist – Checklist for assessing the organization's readiness to implement an information security management system.

The implementation of an information security management system in accordance with ISO/IEC 27001 will allow increasing confidence in the information security of the enterprise, to fulfil the requirements of regulators and obligations to counterparties, and to optimize the costs of information security.

CREATION OF SECURITY OPERATIONS CENTRE (SOC)

It makes sense for enterprises to create their own cohesive, trained, and motivated Security Operations Centre (SOC) team. The alternative is to use commercial SOC services.

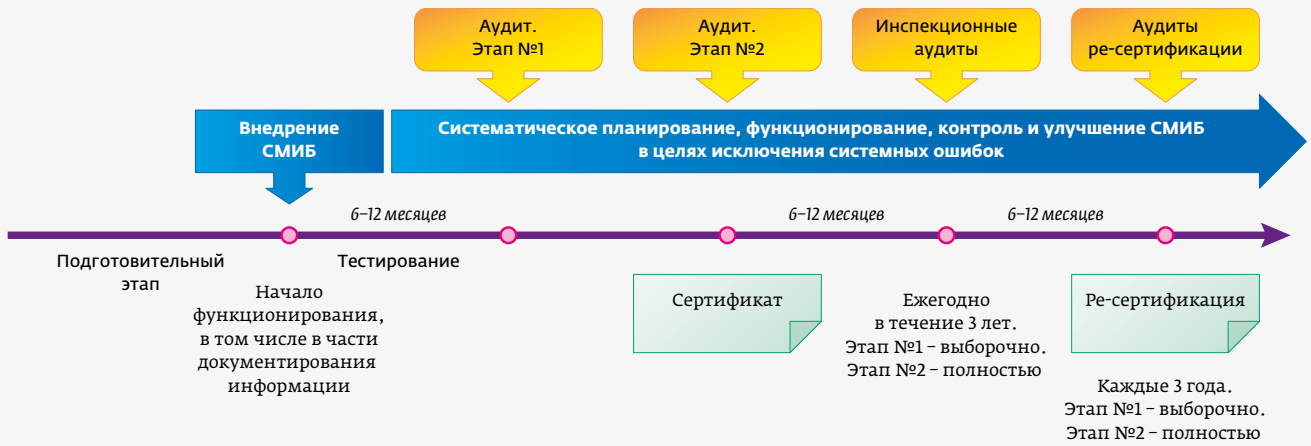

Рис. 2. *Примерный план-график*

Fig. 2. *Approximate plan of stages*

для оценки степени готовности организации к внедрению системы менеджмента информационной безопасности.

Внедрение системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001 позволит: повысить доверие к информационной безопасности предприятия, выполнить требования регуляторов и обязательства перед контрагентами, оптимизировать расходы на информационную безопасность.

СОЗДАНИЕ ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (SECURITY OPERATIONS CENTER, SOC)

Предприятиям целесообразно создать собственную сплоченную, подготовленную и мотивированную команду центра информационной безопасности (Security Operations Center, SOC). Альтернатива – использование услуг коммерческого SOC.

Согласно модели адаптивной архитектуры безопасности, разработанной Gartner, для того чтобы организация могла успешно бороться с киберпреступностью в современной среде угроз, ее команда SOC должна уметь прогнозировать, предотвращать и обнаруживать угрозы, а также эффективно реагировать на угрозы и прогнозировать будущие атаки [27].

На прошедшем SOC Forum 2019, в исследованиях SANS SOC 2018 и SANS SOC 2019 рассматривалась проблема кадрового обеспечения.

ВНЕДРЕНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА НЕПРЕРЫВНОСТИ БИЗНЕСА

Вопросы непрерывности бизнеса актуальны как в случае производства, так и в случае применения промышленных лазерных систем [28–30].

«Как сообщает портал BleepingComputer, IPG Photonics подверглась атаке вымогательского ПО, сорвавшей ее производственные процессы. Компании пришлось отключить компьютерные системы в своих представительствах по всему миру. В офисах были отключены телефоны и электронная почта, отсутствовала связь, на производстве остановились процессы изготовления деталей, не работала доставка» [31, 32].

Для устранения системных сбоев, которые могут быть связаны с проникновением в программное обеспечение промышленных лазерных систем, целесообразно внедрить международно признанный стандарт для системы менеджмента непрерывности бизнеса в соответствии с ISO 22301:2019, использовать лучшие практики.

In order for an organization to successfully combat cybercrime in today's threat environment, the SOC team must be able to predict, prevent, and detect threats, as well as effectively respond to threats and predict future attacks, according to Gartner's Adaptive Security Architecture Model [27].

At the last SOC Forum 2019, the SANS SOC 2018 and SANS SOC 2019 studies addressed the problem of staffing.

IMPLEMENTATION OF A BUSINESS CONTINUITY MANAGEMENT SYSTEM

Business continuity issues are relevant both in the case of production and in the case of using industrial laser systems [28, 29, 30].

"According to BleepingComputer, IPG Photonics was attacked by ransomware that disrupted its operations. The company had to shut down computer systems at its offices around the world. Phones and e-mail were disconnected in the offices, there was no communication, the production of parts stopped at the production, delivery did not work" [31, 32].

To eliminate system failures that may be associated with penetration into the software of industrial laser systems, it is advisable to implement an internationally recognized standard for a business continuity management system in accordance with ISO 22301:2019, and use best practices.

The ability of an organization to continue to operate during disruptions is becoming increasingly important. Business disruptions lead to the loss of customers, income and reputation, while the lack of a business continuity management system in the enterprise indicates an unpreparedness for a quick recovery of activities and inconsistency with the international level.

Business continuity management systems should take into account a range of issues, including the impact of product recalls, employee motivation and well-being, non-work related illness, the impact of organizational maturity on the approach and results of long-term trend analysis, and the organization's preparedness for unforeseen events such as extreme weather conditions, etc.

The business continuity management system is regarded as one of the most dynamically developing areas of strategic and operational management. It is important to correctly define

Способность организации продолжать работать во время сбоев становиться все более актуальной. Перебои в бизнесе приводят к потере клиентов, доходов и репутации, при этом отсутствие системы менеджмента непрерывности бизнеса на предприятии свидетельствует о неготовности к быстрому восстановлению деятельности и несоответствии международному уровню.

Системы менеджмента непрерывности бизнеса должна учитывать целый комплекс вопросов, включая последствия отзыва продукции, мотивации и благополучие сотрудников, фактор заболеваний, не связанных с работой, влияние организационной зрелости на подход и результаты анализа долгосрочных тенденций, готовность организации к непредвиденным событиям, например к экстремальным погодным условиям и др.

Система управления непрерывностью бизнеса рассматривается как одно из наиболее динамично развивающихся направлений стратегического и оперативного менеджмента. Важно корректно определить цели и задачи управления непрерывностью бизнеса, область применения (основная направленность связана с обеспечением непрерывности деловых операций на установленном приемлемом уровне).

В фокусе внимания:

- стратегия и планирование непрерывности бизнеса;
- анализ воздействия на бизнес (BIA). Определение RTO и PRO;
- оценка рисков. Модели и сценарии угроз;
- план обеспечения непрерывности бизнеса (BCP) и план восстановления бизнеса (DRP);
- разработка плана, ключевые факторы успеха и внедрение плана;
- программа повышения осведомленности сотрудников;
- обучение сотрудников, оценка осведомленности сотрудников;
- учения;
- тестирование плана обеспечения непрерывности бизнеса (BCP) и плана восстановления бизнеса (DRP). Типы тестирования;
- оценка текущего состояния и разработка дорожной карты для достижения целевого состояния.

В начале 2020 года проявились новые тренды, новые требования регулирующих органов, поставщиков, потребителей. Существенно изменились риски [33]. Для многих предприятий актуальными стали риски информационной безопасности, риски комплаенс, риски прерыва-

the goals and objectives of business continuity management, the scope (the focus is related to ensuring business continuity at a set acceptable level).

Focus of attention:

- Strategy and business continuity planning
- Business Impact Analysis (BIA). Definition of RTO and PRO.
- Risk assessment. Threat models and scenarios
- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- Plan development, key success factors and plan implementation.
- Employee awareness program
- Employee training, employee awareness assessment
- Exercise programme
- Testing the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). Test types
- Assessment of the current state and development of a roadmap to achieve the target state

At the beginning of 2020, new trends, new requirements of regulatory bodies, suppliers, consumers have appeared. Risks have changed significantly [33]. Information security risks, compliance risks, and supply chain interruption risks have become relevant for many enterprises. In the current environment, many orga-

Рис. 3. *Комплексная защита информации*

Fig. 3. *Comprehensive information protection*

ния цепочки поставок. В сложившихся условиях многие организации предпочитают использовать несколько стандартов, а не пройти сертификацию по одному стандарту. Для промышленных предприятий актуальны международные стандарты ISO 9001, ISO 14001, ISO 45001, ISO/IEC 27001, ISO 22301 и др.

Разработка и внедрение системы управления непрерывностью бизнеса в соответствии с ISO 22301 позволяет повысить эффективность управления, избежать системных ошибок. Основа этого стандарта гармонизирована с ISO 9001 и ISO/IEC 27001, что особенно важно в условиях цифровизации.

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Для безопасного развития бизнеса, особенно при использовании промышленных лазерных систем, необходима комплексная защита информации. В этом плане необходимо сочетание передовых научно-обоснованных решений и практический опыт. Где можно найти такое сочетание? Ответ: в научно-исследовательском центре информационной безопасности.

Такой центр создан и успешно развивается. «На базе АО «Научно-исследовательского института вычислительных комплексов им. М.А.Карцева» в целях изучения и проведения работ по комплексной защите информации действует Научно-исследовательский центр информационной безопасности (НИЦ ИБ). Лаборатории Центра для проведения специальных исследований и специальных проверок оснащены необходимым оборудованием, соответствующим всем требованиям ФСТЭК и ФСБ России.

Имеются лицензии Роспотребнадзора, ФСТЭК и ФСБ России, в том числе и лицензия ФСБ России на разработку и производство шифровальных средств. Налажено взаимодействие с органами государственной власти, интеграторами, государственными корпорациями, предприятиями радиоэлектронной промышленности» [34].

Основные виды деятельности НИЦ ИБ представлены в информационном буклете, и с ними можно ознакомиться [35]:

- специальные проверки технических средств и систем по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну;
- специальные исследования технических средств и систем с использованием

nizations prefer to use multiple standards rather than being certified against one standard. For industrial enterprises, international standards ISO 9001, ISO 14001, ISO 45001, ISO/IEC 27001, ISO 22301, etc. are relevant.

Development and implementation of a business continuity management system in accordance with ISO 22301 allows you to improve management efficiency and avoid system errors. The basis of this standard is harmonized with ISO 9001 and ISO/IEC 27001, which is especially important in the context of digitalization.

For the safe development of business, especially when using industrial laser systems, comprehensive information protection is required. This requires a combination of advanced science-based solutions and practical experience. Where can you find this combination? Answer: at the information security research center.

Such a center has been created and is developing successfully. “On the basis of JSC” Research Institute of computing systems named after M.A.Kartseva “for the purpose of studying and carrying out work on the comprehensive protection of information, the Research Center for Information Security operates. The center’s laboratories for conducting special studies and special checks are equipped with the necessary equipment that meets all the requirements of the FSTEC and the FSB of Russia.

There are licenses of Rospotrebnadzor, FSTEC and FSB of Russia, including the license of the FSB of Russia for the development and production of encryption tools. Interaction with government bodies, integrators, state corporations, enterprises of the radio-electronic industry has been established” [34].

The main activities of the SIC IB are presented in the information booklet and can be found [35]:

- special checks of technical means and systems for identifying electronic devices intended for secret receipt of information in technical means processing information containing information constituting a state secret;
- special studies of technical means and systems using instrumentation to identify possible technical channels of leakage of protected information;
- certification of objects of informatization according to information security requirements;

контрольно-измерительной аппаратуры для выявления возможных технических каналов утечки защищаемой информации;
- аттестация объектов информатизации по требованиям безопасности информации;
- испытания на электромагнитную совместимость;
- разработки программно-аппаратных средств и систем защиты информации.

В заключение хотелось бы отметить, что есть немало примеров успешного развития предприятий, деятельность которых непосредственно связана с промышленными лазерными системами.

Рекомендуется провести диагностический аудит, аудит поставщиков, провести обучение, внедрить системы менеджмента в соответствии с международными стандартами и лучшими практиками, повышать культуру информационной безопасности и выполнить комплекс других необходимых мер, включая выработку подхода к формированию и развитию собственной сплоченной, подготовленной и мотивированной команды SOC или использованию услуг коммерческих SOC. Важно принимать во внимание, что рано или поздно возникнет вопрос об окупаемости инвестиций в промышленные лазерные системы, а эти вопросы рассматриваются не только с точки зрения ESG-факторов, но и с точки зрения информационной безопасности, непрерывности бизнеса.

Нерешенность проблем в области информационной безопасности может привести не только к неверным данным о результатах работы, неверным выводам и неверным управленческим решениям, но и к более серьезным последствиям.

- tests for electromagnetic compatibility;
- development of software and hardware and information security systems.

In conclusion, I would like to note that there are many examples of successful development of enterprises whose activities are directly related to industrial laser systems.

It is recommended to conduct a diagnostic audit, audit of suppliers, conduct training, implement management systems in accordance with international standards and best practices, improve the information security culture and take a set of other necessary measures, including developing an approach to the formation and development of your own cohesive, trained and motivated SOC team or use of commercial SOC services. It is important to take into account that sooner or later the question of the return on investment in industrial laser systems will arise, and these issues are considered not only from the point of view of ESG factors, but also from the point of view of information security and business continuity.

Unresolved problems in the field of information security can lead not only to incorrect data on the results of work, incorrect conclusions and incorrect management decisions, but also to more serious consequences.

It is important that there are more examples of successful work of enterprises whose activities are directly related to industrial laser systems. This is a strategic task in the context of digitalization.

Важно, чтобы примеров успешной работы предприятий, деятельность которых непосредственно связана с промышленными лазерными системами, становилось больше. Это стратегическая задача в условиях цифровизации.

СПИСОК ЛИТЕРАТУРЫ

1. **Холтон К.** Рынок лазеров в 2020-м: обзор и прогноз. Лазерные рынки ищут свой курс в неспокойные времена. *Лазер-Информ.* 2020; 3 (666): 1-6.
2. Trumpf demonstrates additive manufacturing with copper and gold. I*ndustrial Laser Solutions*. 2019. JANUARY / FEBRUARY. P. 6. www.industrial-lasers.com.
3. **Белфорте Д.А.** Мировой рынок лазерного оборудования для обработки материалов в промышленности. *Лазер-Информ.* 2020; 17-18 (680-681), 4-7.
4. **Фоменко И.** Современные лазерные системы в промышленности. 20.35. Университет НТИ. URL: http://skvot.2035.university/sovremennye-lazernye-systemy (дата обращения 12.11.2020).
5. Отчетный доклад Президента Лазерной ассоциации И. Б. Ковша. *Лазер-Информ.* 2018; 5–6 (620–621): 1–7.
6. **Ковш И. Б.** Фотоника в России: состояние и задачи. *Лазер-Информ.* 2019; 4 (643): 1–16.
7. **Овертон Г., Ноджи А., Бельфорте Д., Геверт Б.** Мировой лазерный рынок в 2018-м и прогноз на 2019. *Лазер-Информ.* 2019; 5 (644): 1–8.
8. Lasers forge 21st century innovations. LASER MARKETPLACE 2014 / GAIL OVERTON, ALLEN NOGEE, and CONARD HOLTON. *Laser Focus World*, January 2014. P. 38–40, 42, 44, 46, 49, 51–54, 56–62.
9. Air Force to ask industry for 75-Watt sodium laser to create artificial stars for adaptive optics / John Keller // ; artificial-stars-adaptive-optics.html?cmpid=enl_mae_defense_executive_2019–0205&pwhid=faaefc33bfc7f79fa744508baa2ae2577c1d5af697871251a3c1ab-77b05cd2ce24b36fbd579d3e69c246472c18183959bfa 392b76b0c46b517d1af9e3ba51ab8&eid=324695413&bid=2360681 17 / 01 / 2019
10. Laser beam shaping for innovative applications / SAMI LAROUI. *Industrial Laser Solutions*, MARCH / APRIL 2019; 22–23. www.industrial-lasers.com.
11. Spectrum supplies laser marking system for use in manufacturing Mars lander. *Industrial Laser Solutions*, MARCH / APRIL 2019. P.10. www.industrial-lasers.com.
12. **Игнатов А. Г.** Военное применение лазерной техники набирает обороты и начинает определять технический уровень современного и перспективного вооружения. *Фотоника.* 2016; 56(2); 14–25.
13. **Pelaprat J. M. , Fritz R. , Finuf M., Zediker M.** High-power blue laser improves fabrication throughput . *Industrial Laser Solutions.* 2018; 1–2: 17–20.
14. Japan develops blue laser for advanced materials processing / KOJI TOJO, SHINICHIRO MASUNO, RITSUKO HIGASHINO, AND MASAHIRO TSUKAMOTO; Shimadzu Corporation.*Industrial Laser Solutions.* 2018, September / October, p. 27–31; www.industrial-lasers.com.
15. **Belforte D.** My view. Lasers make it better. *Industrial Laser Solutions.* 2018; № 1–2: 32.
16. Japan develops blue laser for advanced materials processing / KOJI TOJO, SHINICHIRO MASUNO, RITSUKO HIGASHINO, AND MASAHIRO TSUKAMOTO; Shimadzu Corporation. *Industrial Laser Solutions.* 2018, September / October, p. 27–31; www.industrial-lasers.com.
17. NUBURU has invented and is manufacturing the world's first revolutionary high-power blue laser // URL: http://www.nuburu. net / markets / 31 / 01 / 2019
18. Trumpf demonstrates additive manufacturing with copper and gold // Industrial Laser Solutions, 2019, JANUARY / FEBRUARY. P. 6. www.industrial-lasers.com.
19. 2018 was another record year, contending with turmoil / DAVID A. BELFORTE. *Industrial Laser Solutions.* 2019, JANUARY / FEBRUARY. P. 9–11. www.industrial-lasers.com.
20. Большой Национальный форум информационной безопасности. URL: https://infoforum.ru/main/17-i-nacionalnyi-forym-informacionnoi-bezopasnosti (дата обращения: 12 ноября 2020 года).
21. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast
22. Портал Photonica.Pro [Электронный ресурс]. URL: http://photonica.pro / (дата обращения: 12.11.2020).
23. Большой Национальный форум информационной безопасности. URL: https://infoforum.ru/main/17-i-nacionalnyi-forym-informacionnoi-bezopasnosti (дата обращения: 12 ноября 2020 года).
24. **Белоус А. И. , Солодуха В.А.** *Кибероружие и кибербезопасность. О сложных вещах простыми словами.* – Москва. Вологда: Инфра-Инженерия, 2020. – 692 с.

REFERENCES

1. **Holton K.** Rynok lazerov v 2020-m: obzor i prognoz. Lazernye rynki ishchut svoj kurs v nespokojnye vremena. *Lazer-Inform.* 2020; 3 (666): 1-6.
2. Trumpf demonstrates additive manufacturing with copper and gold. *Industrial Laser Solutions*. 2019, JANUARY / FEBRUARY. P. 6. www.industrial-lasers.com.
3. **Belforte D.A.** Mirovoj rynok lazernogo oborudovaniya dlya obrabotki materialov v promyshlennosti. Lazer-Inform. 2020; 17-18 (680-681), 4-7.
4. **Fomenko I.** *Sovremennye lazernye sistemy v promyshlennosti. 20.35. Universitet NTI.* URL: http://skvot.2035.university/sovremennye-lazernye-systemy (12.11.2020).
5. Otchetnyj doklad Prezidenta Lazernoj associacii I. B. Kovsha. *Lazer-Inform.* 2018; 5–6 (620–621): 1–7.
6. **Kovsh I. B.** Fotonika v Rossii: sostoyanie i zadachi. *Lazer-Inform.* 2019; 4 (643): 1–16.
7. **OVERTON G., NOGEE A., BELFORTE D., WALLACE J., GEFVERT B.** What goes up. ANNUAL LASER MARKET REVIEW & FORECAST 2019. *Laser Focus World*, January 2019. P. 40–45, 47, 49–54, 56–58, 60–61, 64–65.
8. Lasers forge 21st century innovations. LASER MARKETPLACE 2014 / GAIL OVERTON, ALLEN NOGEE, and CONARD HOLTON. *Laser Focus World*, January 2014. P. 38–40, 42, 44, 46, 49, 51–54, 56–62.
9. Air Force to ask industry for 75-Watt sodium laser to create artificial stars for adaptive optics / John Keller // ; artificial-stars-adaptive-optics.html?cmpid=enl_mae_defense_executive_2019–0205&pwhid=faaefc33bfc7f79fa744508baa2ae2577c1d5af697871251a3c1ab-77b05cd-2ce24b36fbd579d3e69c246472c18183959bfa 392b76b0c46b517d1af9e3ba51ab8&eid=324695413&bid=2360681 17 / 01 / 2019
10. Laser beam shaping for innovative applications / SAMI LAROUI // Industrial Laser Solutions, MARCH / APRIL 2019. P. 22–23. www.industrial-lasers.com.
11. Spectrum supplies laser marking system for use in manufacturing Mars lander // Industrial Laser Solutions, MARCH / APRIL 2019. P.10. www.industrial-lasers.com.
12. **Ignatov A. G.** Voennoe primenenie lazernoj tekhniki nabiraet oboroty i nachinaet opredelyat' tekhnicheskij uroven' sovremennogo i perspektivnogo vooruzheniya. *Fotonika.* 2016; 56(2); 14–25.
13. High-power blue laser improves fabrication throughput / J. M. Pelaprat, R. Fritz, M. Finuf, M. Zediker. *Industrial Laser Solutions.* 2018; 1–2: 17–20.
14. Japan develops blue laser for advanced materials processing / KOJI TOJO, SHINICHIRO MASUNO, RITSUKO HIGASHINO, AND MASAHIRO TSUKAMOTO; Shimadzu Corporation. *Industrial Laser Solutions.* 2018, September / October, p. 27–31; www.industrial-lasers.com.
15. **Belforte D.** My view. Lasers make it better. *Industrial Laser Solutions.* 2018; 1–2: 32.
16. Japan develops blue laser for advanced materials processing / KOJI TOJO, SHINICHIRO MASUNO, RITSUKO HIGASHINO, AND MASAHIRO TSUKAMOTO; Shimadzu Corporation. *Industrial Laser Solutions.* 2018, September / October, p. 27–31; www.industrial-lasers.com.
17. NUBURU has invented and is manufacturing the world's first revolutionary high-power blue laser // URL: http://www.nuburu. net / markets / 31 / 01 / 2019
18. Trumpf demonstrates additive manufacturing with copper and gold // Industrial Laser Solutions, 2019, JANUARY / FEBRUARY. P. 6. www.industrial-lasers.com.
19. 2018 was another record year, contending with turmoil / DAVID A. BELFORTE // Industrial Laser Solutions, 2019, JANUARY / FEBRUARY. P. 9–11. www.industrial-lasers.com
20. *Bol'shoj Nacional'nyj forum informacionnoj bezopasnosti.*URL: https://infoforum.ru/main/17-i-nacionalnyi-forym-informacionnoi-bezopasnosti (12/11/2020).
21. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast
22. *Photonica.Pro.* URL: http://photonica.pro / (12/11/2020).
23. *Bol'shoj Nacional'nyj forum informacionnoj bezopasnosti.* URL: https://infoforum.ru/main/17-i-nacionalnyi-forym-informacionnoi-bezopasnosti (12/11/2020).
24. **Belous A. I., Soloduha V. A.** *Kiberoruzhie i kiberbezopasnost'. O slozhnyh veshchah prostymi slovami.* – Moskva. Vologda: Infra-Inzheneriya, 2020. – 692 p.
25. **Vajl P., Vorner S.** *Cifrovaya transformaciya biznesa: Izmenenie biznes-modeli*

25. **Вайл П., Ворнер С.** *Цифровая трансформация бизнеса: Изменение бизнес-модели для организации нового поколения* . – М.: Альпина Паблишер, 2019. – 257 с.
26. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам* / Под редакцией профессора РАН, д.т.н. Д. П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.
27. https://media.kaspersky.com/ru/business-security/enterprise/brochure-soc-powered-by-kl.pdf
28. **Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.** *Управление инцидентами информационной безопасности и непрерывностью бизнеса*. Учебное пособие для вузов. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2019. – 170 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 3».
29. **Андрианов В. В. , Зефиров С.Л., Голованов В.Б., Голдуев Н.А.** *Обеспечение информационной безопасности бизнеса* / 2-е изд., перераб. и доп. – М.: ЦИПСиР: Альпина Паблишерз, 2011. – 373 с. + 8 с. вкл.
30. **Конеев И. Р.** *Система управления непрерывностью бизнеса: Почему она должна быть внедрена на каждом предприятии?* – М.: ЛЕНАНД, 2016. – 352 с.
31. URL: http://www.itsec.ru/news/krupneyshiy-v-ssha-proizvoditel-volokonnih-lazerov-stal-zhertvoy-vimogatelksogo-po
32. URL: https://www.securitylab.ru/news/512278.php
33. https://reports.weforum.org/global-risks-report-2020/executive-summary/
34. http://www.niivk.ru/index.php?id=107
35. http://www.niivk.ru/images/ISRC.pdf

АВТОР

Темникова Ксения Николаевна, Московский политехнический университет, доц. кафедры «Информационная безопасность», ООО «Профконсалт ИСМ», эксперт, к. э. н.
ORCID 0000-0002-9645-7886,
идентификатор в РИНЦ SPIN-код: 6988-2051.
Профиль: консультирование, внедрение и аудит систем менеджмента информационной безопасности и систем менеджмента непрерывности бизнеса, инвестиции в промышленных роботов, лазерные технологические комплексы.

dlya organizacii novogo pokoleniya. – M.: Al'pina Pablisher, 2019. – 257 p.
26. *Kiberbezopasnost' cifrovoj industrii. Teoriya i praktika funkcional'noj ustojchivosti k kiberatakam* / Pod redakciej professora RAN, doktora tekhnicheskih nauk D. P. Zegzhdy. – M.: Goryachaya liniya – Telekom, 2020. – 560 s.: il.
27. https://media.kaspersky.com/ru/business-security/enterprise/brochure-soc-powered-by-kl.pdf.
28. **Miloslavskaya N. G., Senatorov M. YU., Tolstoj A. I.** *Upravlenie incidentami informacionnoj bezopasnosti i nepreryvnost'yu biznesa*. Uchebnoe posobie dlya vuzov. – 2-e – M.: Goryachaya liniya – Telekom, 2019. – 170 p.– Seriya "Voprosy upravleniya informacionnoj bezopasnost'yu". Vypusk 3.
29. **Andrianov V. V., ZefirovS. L., Golovanov V. B. , GolduevN. A.** – 2-e izd., pererab. i dop. *Obespechenie informacionnoj bezopasnosti biznesa*– M.: CIPSiR: Al'pina Pablisherz, 2011. – 373 p.
30. **Koneev I. R.** *Sistema upravleniya nepreryvnost'yu biznesa: Pochemu ona dolzhna byt' vnedrena na kazhdom predpriyatii?* – M.: LENAND, 2016. – 352 p.
31. URL: http://www.itsec.ru/news/krupneyshiy-v-ssha-proizvoditel-volokonnih-lazerov-stal-zhertvoy-vimogatelksogo-po
32. URL: https://www.securitylab.ru/news/512278.php
33. https://reports.weforum.org/global-risks-report-2020/executive-summary/
34. http://www.niivk.ru/index.php?id=107
35. http://www.niivk.ru/images/ISRC.pdf

AUTHOR

Ksenia N. Temnikova, Moscow Polytechnic University, Associate Professor of the Department of Information Security, Profconsult ISM expert, Candidate of Economic Sciences,
ORCID 0000-0002-9645-7886,
RSCI identifier SPIN code: 6988-2051.
Profile: consulting, implementation and audit of Information Security Management Systems and Business Continuity Management Systems, investments in industrial robots, investments in laser technological complexes.