УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2021 Том 21 № 1 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2021 Vol. 21 No 1 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

ОБЗОРНАЯ СТАТЬЯ

REVIEW PAPER

doi: 10.17586/2226-1494-2021-21-1-1-14
УДК 004.056

К вопросу обеспечения безопасности промышленных систем

Илья Иосифович Лившиц

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Livshitz.il@yandex.ru ✉, http://orcid.org/0000-0003-0651-8591

Аннотация

Для обеспечения безопасности промышленных систем на современном уровне известно несколько методических подходов. Наибольшее внимание за последние годы получили два кардинально различающихся методических подхода: предложение реализации дополнительных мер защиты информации, без изменения базовой ИТ-инфраструктуры, и создание новой концепции тотальной изоляции (например, архитектуры Zero Trust). Как отмечается мировыми центрами компетенции в России (Group-IB, Positive Technology и др.) и в мире (IBM, MS, Cisco, CheckPoint и пр.), эти методические подходы не приводят к улучшению стабильности и безопасности промышленных систем. Постоянно появляются сообщения о новых критических уязвимостях, в том числе в отношении промышленных систем. Проблема обеспечения безопасности появилась еще в XX веке, прошла несколько стадий развития, и в настоящий момент наиболее очевидным является подход «от функциональности». Подход заключается в том, что формирование и решение проблемы начинается в тот момент, когда производитель создает решение по спецификации, состоящей из требований функциональной безопасности, и далее проводит оценку по требованиям доверия. Для общего процесса обеспечения безопасности промышленных систем характерно то, что до настоящего времени в отрасли еще не сложилась целостная культура потребления безопасных ИТ-компонент, имеющих доказательства безопасности, проверяемые до необходимого уровня. Только несколько поставщиков в мире и в России готовы предложить компоненты, имеющие доказанный уровень обеспечения безопасности Safety Integrity Level в соответствии с требованиями IEC серии 61508 и/или 61511. В настоящей работе рассмотрена проблема обеспечения безопасности промышленных систем в технических аспектах: требуемых ресурсов, заданного быстродействия, качества управления, методов подтверждения соответствия, формирования оценок остаточных рисков и иных исчислимых оценок. Дан краткий обзор существующих подходов, и предложены некоторые возможные решения поставленной проблемы.

Ключевые слова

безопасность, функциональная безопасность, информационная безопасность, стандарт, аудит, менеджмент рисков, меры защиты, оценка соответствия

Ссылка для цитирования: Лившиц И.И. К вопросу обеспечения безопасности промышленных систем // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, №1. С. 1–14. doi: 10.17586/2226-1494-2021-21-1-1-14

On safety issue of industrial control systems

Ilya I. Livshitz

ITMO University, Saint Petersburg, 197101, Russian Federation
Livshitz.il@yandex.ru ✉, http://orcid.org/0000-0003-0651-8591

Abstract

There are several various methodological approaches well known for the current level safety ensuring of industrial control systems. Two worlds apart methodological approaches have been considered fundamentally over the past few years: the proposal to implement additional information security countermeasures without changing the basic IT-infrastructure, and creation of a new total isolation concept (for example, the Zero Trust Architecture). These methodological approaches do not lead to stability and security of industrial control systems as noted by the world centers of competence in Russia (Group-IB, Positive Technology) and in the world (IBM, MS, Cisco, CheckPoint). Reports of

new and new critical vulnerabilities never stop, including a significant number in relation to industrial control systems. The problem of safety ensuring dates from the XX century, has passed several stages of maturity, and, presently, the approach “from functionality” is the most obvious. In general, this approach consists in the fact that the formation and solution of a problem begins when the manufacturer creates a solution based on a specification consisting of functional safety requirements. Then the safety assessment based on trust requirements is carried out. For the overall process of the safety ensuring of industrial control systems, unfortunately, it is typical, that, so far, the industry has not yet developed a holistic culture of consumption of secure IT-components with security evidence that can be traced to the required level. Only a few suppliers in the world and in Russia are ready to offer components that have a proven level of Safety Integrity Level in accordance with the requirements of IEC 61508 and/or 61511 series. The present publication considers the issue of the safety ensuring of industrial control systems in such technical aspects as: the required resources, the specified speed, the management quality, the validation methods, estimation of residual risks and other computable estimates. A brief overview of existing approaches is presented and some possible solutions for the defined problem are given.

Keywords
safety, functional security, IT-security, standard, audit, risk management, protective actions, conformance evaluation

For citation: Livshitz I.I. On safety issue of industrial control systems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 1, pp. 1–14 (in Russian). doi: 10.17586/2226-1494-2021-21-1-1-14

Введение

Проблема обеспечения безопасности для промышленных систем различного назначения (Industrial Control System, ICS) имеет давнее происхождение. Первые работы в данной области появились еще в XX веке при возникновении промышленных систем управления сложными техническими объектами. Все они имели схожие по замыслу архитектуры построения, единые централизованные системы управления, простые каналы первичных преобразователей и каналы обмена данными.

К особенностям предшествующих периодов можно отнести важное архитектурное обстоятельство — для зарубежных и отечественных центров экспертиз в данной области не существовало раздельного определения сущностей информационных технологий (ИТ) и информационной безопасности (ИБ). В связи с этим системы проектировались, создавались, проходили испытания и эксплуатировались как единое целое [1, 2]. Начиная с XX века основными требованиями были: обеспечение реализации заложенного функционала и устойчивая работоспособность программных (программно-аппаратных) комплексов [3–5]. В XXI веке появились и законодательные инициативы, призванные упорядочить значительное количество отраслевых и регуляторных документов. Новации в этой области, в определенной мере, вызваны принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ, в котором дано определение систем ИБ, а в подзаконных актах (постановление Правительства № 127, приказы Федеральной службы по техническому и экспортному контролю (ФСТЭК) № 235, № 239 и пр.) определены угрозы и меры защиты для обеспечения защищенности объектов критической информационной инфраструктуры (КИИ).

Можно отметить, что в ряде отраслей продолжают действовать системы нормативно-методических документов (НМД), созданных для целей собственного регулирования. Например, СТО Газпром серии 4.2 определяет требования к функционированию ИТ-компонент, но не затрагивает требования функциональной безопасности, равно как и процедуры управления рисками. СТО Газпром 4.2-5-002–2009[1] описывает только подтверждение соответствия в Системе добровольной сертификации ГАЗПРОМСЕРТ, риск-менеджмент не отмечен. Единственный СТО Газпром 4.2-5-003–2009[2] содержит только перечисление функциональных требований (п. 7.2), риск-менеджмент не упомянут.

Отметим современные риск-ориентированные стандарты, признанные не только в международной, но и в национальной практике Российской Федерации (РФ). Например, в стандарте ICAO Doc 9284 EN[3] в главе 5 описаны требования к оценке:

— nature of security risks (природа рисков безопасности);
— national security plan (национальный план безопасности);
— reduce security risks (снижение рисков безопасности).

Необходимо признать, что и в стандартах ICAO встречаются весьма спорные тезисы, вызывающие справедливые нарекания. Например, в стандарте ICAO Doc 9756[4] в главе 8 указано требование обеспечения абсолютной безопасности данных (*absolute data security*), в технических системах подобные категории не применимы. В стандарте ICAO Doc 9859[5] в главе 1 представлены рекомендации по созданию интегрированной системы менеджмента рисков (*Integrated Risk Management*), и даются определения важных терминов: «Информационная безопасность» (*Security*) и

[1] СТО Газпром 4.2-5-002–2009 «Система обеспечения информационной безопасности ОАО «Газпром». Методика сертификационных испытаний автоматизированных систем управления технологическими процессами».

[2] СТО Газпром 4.2-5-003–2009 «Система обеспечения информационной безопасности ОАО «Газпром». Методика испытаний средств и систем обеспечения безопасности информационных технологий».

[3] ICAO. URL: https://www.icao.int/publications/Documents/guidance_doc_infectious_substances.pdf (дата обращения: 14.10.2020).

[4] ICAO. URL: https://store.icao.int/en/manual-of-aircraft-accident-and-incident-investigation-part-iv-reporting-doc-9756-part-5 (дата обращения: 14.10.2020).

[5] ICAO. URL: https://store.icao.int/en/safety-management-manual-doc-9859 (дата обращения: 14.10.2020).

«Безопасность» (*Safety*). Отмечается, что термин *Safety* относится к любому проявлению негативного ущерба для производительности систем в силу неожиданных последствий комбинаций факторов, а термин *Security* относится к намеренным срывам производительности систем персоналом. Необходимо отметить, что в стандартах IEC серии 61508[1] и/или 61511[2] не приводится такого разделения, а природа рисков, равно как и методы обработки рисков (например, ISO 31000, IEC 31010, ISO/IEC 27005 и пр.), отличается очень широко. Важным преимуществом методики в системе ISO следует признать установленные ограничения, в частности, по времени, глубине экспертизы, точности результатов и пр. Описание требований функциональной безопасности, изложенных в стандартах ISO, даны в [6, 7], а IEC серии 61508 и/или 61511 в [8, 9] соответственно.

Цель работы — исследование существующего в мире уровня решения проблемы обеспечения безопасности промышленных систем, в том числе относящихся к объектам критической инфраструктуры.

Оценка безопасности встроенных мер защиты

Известно о российском проекте по испытаниям PT Industrial Security Incident Manager и ProfiDIODE компании Oreol Security[3]. Испытания включали проверку корректной работы и целостности данных в получаемой копии трафика, среда тестирования ограничена 100 Мбит/с, что соответствует стандартному значению в реальных ICS. Показано, что база экспертизы PT Industrial Security Threats Indicators превышает 4 тыс. правил, в том числе для выявления рисков в технологических сетях и поиска уязвимостей, которые эксплуатируются вредоносным программным обеспечением (ПО), например, Trisis, Triton. Несмотря на данные предложения, для оценки безопасности встроенных мер защиты необходимо определить состав функций, помимо базовых требований подсистемы аварийной защиты, например, в соответствии с IEC серии 61508 и/или 61511. Следует также заметить, что необходим серьезный анализ и достаточность быстродействия для анализа трафика, циркулирующего в реальных ICS. В отчете Positive Technology[4] показаны неутешительные результаты тестирования промышленных сетей, что позволило выявить узлы, на которых раскрывается важная информация (например, содержимое конфигурационных файлов). Показано, что причина многих инцидентов кроется в небезопасной конфигурации служб, и выявлены известные уязвимости, начиная с 2013–2014 гг. (рис. 1). Нотация уязвимостей приводится в соответствии с принятой системой CVE (Common Vulnerabilities and Exposures) для общеизвестных уязвимостей ИБ.

Национальные стандарты России

Важно отметить, что в национальной юрисдикции РФ существуют «целевые» стандарты в системе ГОСТ Р (ГОСТ РВ), позволяющие установить требования и выполнять экспертизу по объективным и согласованным критериям в отношении непрерывности функционирования критичных систем (еще задолго до появления терминологии КИИ). Одним из стандартов является ГОСТ Р 53131-2008[5] [10–12], который вводит ряд терминов:

— критичный компонент: компонент информационно-телекоммуникационной системы, нарушение непрерывности функционирования которого может нанести значительный ущерб организации (п. 3.1.19);
— технические средства защиты ИБ: оборудование, используемое для защиты ИБ организации (п. 3.1.21).

В тексте ГОСТ Р 53131 упоминается термин «оценка риска», а в Приложении В.2 — «остаточный риск».

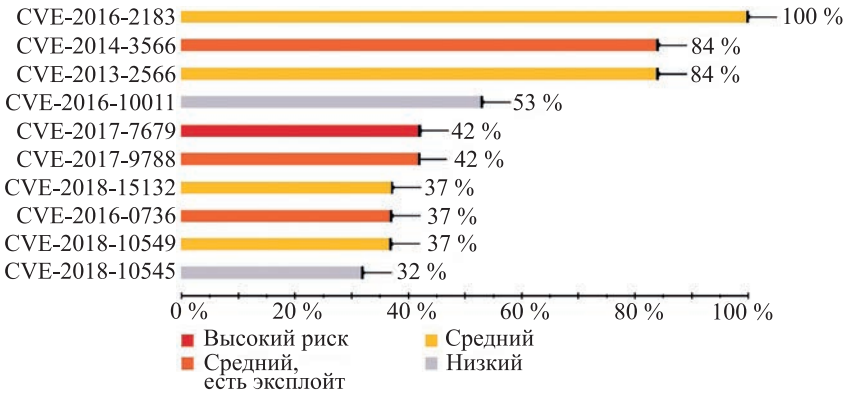

Рис. 1. Распространенные уязвимости в программном обеспечении

Fig. 1. Ubiquitous vulnerabilities in ICS Software

[1] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems

[2] IEC 61511-1:2016 Functional safety — Safety instrumented systems for the process industry sector

[3] Security Lab. URL: https://www.securitylab.ru/news/510891.php (дата обращения: 14.10.2020).

[4] Positive Technologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/vulnerabilities-corporate-networks-2020-rus.pdf (дата обращения: 14.10.2020).

[5] ГОСТ Р 53131–2008 Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен 01.10.2009. М.: Стандартинформ, 2011. 54 с.

Отметим, что риск-ориентированный подход был реализован в РФ примерно в одно время с первыми стандартами ISO серии 31000 версии 2008 г. В п. А.6.5 ГОСТ Р 53131 говорится об аудитах в отношении услуг провайдеров: *«...Провайдеры услуг должны также обеспечить проведение ими регулярных аудитов всех физических, логических и других необходимых средств контроля»* и п. В.14.6.1: *«Провайдеры услуг должны обеспечить, чтобы: были установлены процедуры периодических аудиторских проверок каждого элемента физических мощностей и оборудования...»*. В НМД в части, касающейся обеспечения безопасности КИИ (ФЗ-187, приказы ФСТЭК и пр.), к сожалению, аудиты не указаны.

Рассмотрим далее ГОСТ РВ 51987–2002[1] [13, 14]. Известна модель оценки надежности:

$$P_{\text{над}} = \frac{T_{\text{нар}}^2}{(T_{\text{вос}} + T_{\text{нар}})(T_{\text{зад}} + T_{\text{нар}})}, \qquad (1)$$

где $T_{\text{нар}}$ — среднее время наработки системы на отказ; $T_{\text{вос}}$ — среднее время восстановления системы после отказа; $T_{\text{зад}}$ — задаваемый период надежного функционирования системы.

Если $T_{\text{зад}} = T_{\text{нар}}$, а $T_{\text{вос}} \to 0$, то $P_{\text{над}} \to 0{,}5$. Это только приблизительная оценка, но в большинстве рекламных предложений «наложенных» средств защиты информации (СЗИ) нет никаких данных. Формула (1) может быть стартовой точкой на этапе научно-исследовательских и/или опытно-конструкторских работ при оценке роли «наложенных» СЗИ, в частности, для повышения безопасности ICS. Для раскрытия цели настоящей работы отметим термины:

— (п. 3.12.13) *Надежность представления информации* — свойство информационной системы (ИС) обеспечивать прием, автоматическую обработку запроса или команды и представление или принудительную выдачу выходной информации (реализацию технологической операции) согласно функциональному алгоритму при соблюдении эксплуатационных условий применения и технического обслуживания ИС;
— (п. 3.12.21) *Своевременность представления требуемой информации* — свойство ИС обеспечивать представление запрашиваемой или выдаваемой принудительно выходной информации (выполнения технологической операции по команде или автоматически) в задаваемые сроки, гарантирующие выполнение соответствующей функции согласно целевому назначению системы.

Исходя из опубликованных каталогов известных компаний-производителей ICS, в частности, Siemens[2] и Yokogawa[3], можно видеть, что функции подсистемы аварийной защиты реализованы на достаточной и точной математической базе. Соответственно, нет необходимости применения «наложенных» СЗИ для дополнительного дублирования функциональной безопасности. В актуальном Государственном реестре сертифицированных СЗИ ФСТЭК (обновлено 18 сентября 2020 г.) доступна информация о системах SMART-SPRECON (сертификат №4221) и ЭКОМ-3000 (сертификат №4229), которые соответствуют требованиям задания по безопасности. Отдельной проблемой следует признать практическое отсутствие оценок поставщиков систем мониторинга в РФ о расчетной способности обеспечивать своевременность и надежность (в терминах п. 3.12.13 и п. 3.12.21 ГОСТ РВ 51987–2002) представления требуемой информации, в том числе конкретно для персонала, реализующего эти проверки.

В п. 6.2.2 ГОСТ РВ 5198–2002 определено, что в техническом задании на разработку ИС и/или в постановках функциональных задач должны быть установлены системные требования к качеству процессов представления запрашиваемой выходной информации, а также выполнения задаваемых критичных технологических операций.

Можно рекомендовать следующие важнейшие требования:

— «вероятность надежного представления $P_{\text{над}}$ и/или доведения запрашиваемой (выдаваемой принудительно) выходной информации в течение заданного периода $P_{\text{зад}}$ функционирования ИС должна быть не ниже $P_{\text{над зад}}$»;
— «вероятность надежного выполнения технологических операций $P_{\text{над}}$ в течение заданного периода $T_{\text{зад}}$ функционирования ИС должна быть не ниже $P_{\text{над зад}}$. При этом непредставление требуемой информации или невыполнение критичной технологической операции может привести к **недопустимому** ущербу;
— «среднее время выполнения конкретных технологических операций $T_{\text{полн}}$ должно быть не более $T_{\text{зад}}$» или при функционировании ИС в режиме жесткого реального времени.

Отметим, что терминологический аппарат ГОСТ РВ хорошо стыкуется с требованиями к подсистеме аварийной защиты в IEC серии 61508 и/или 61511 и с общей реализацией требований риск-менеджмента при анализе требований компонентов ICS. Кратко рассмотрим минимальные требования функциональной безопасности по IEC 61508-1. В п. 5.1.1 сформирована ясная цель — указание информации, которая должна быть документально оформлена для того, чтобы эффективно выполнять все стадии жизненного цикла всей системы безопасности, а также для ПО. Соответственно, установлено, что документация должна содержать достаточную информацию для управления функциональной безопасностью (п. 5.2), и должна содержать достаточную информацию, необходимую для процесса реализации оценки функциональной безопасности, а также результаты, полученные при этой оценке (п. 5.2.3).

[1] ГОСТ РВ 51987–2002 Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем.

[2] Siemens. URL: https://www.siemens-pro.ru/docs/simatic/s7-1200/03_S7-1200_2015_ru.pdf (дата обращения: 14.10.2020).

[3] Yokogawa. URL: http://www.yokogawa.ru/products/upravlenie-proizvodstvom-i-bezopasnostyu/sistema-avtomaticheskoy-protivoavariynoy-zashchity-prosafe-rs (дата обращения: 14.10.2020).

Стандарт IEC 61508-1 определяет значения уровня полноты безопасности системы безопасности (Safety Integrity Level, SIL) и, в зависимости от того, как часто требуется система безопасности, различают два значения (рис. 2):

1) PFH — вероятность опасного отказа в течение часа, рабочий режим с непрерывной частотой запроса («высокий» запрос);
2) PFDavg — средняя вероятность опасного отказа при запросе функциональной безопасности («низкий» запрос).

В настоящей работе крайне важно, что стандарт IEC 61508-1 явно различает два типа компонентов:

1) тип A — характеристика отказа определена полностью и отказы установлены;
2) тип B — компоненты с неопределенной характеристикой отказа по крайней мере одного элемента, например, для микропроцессоров.

В стандарте IEC 61508-1 определены виды отказов:
— λ_{SU}, безопасные, необнаруживаемые;
— λ_{SD}, безопасные, обнаруживаемые;
— λ_{DD}, опасные, обнаруживаемые;
— λ_{DU}, опасные, необнаруживаемые.

Тогда параметр SFF (доля безопасных отказов) определяется как:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda_{DU} + \lambda_{DD} + \lambda_S}, \quad (2)$$

где $\lambda_S = \lambda_{SU} + \lambda_{SD}$.

Соответственно, с учетом типов компонент и определенных выше видов отказов получим следующие соотношения для максимального уровня полноты безопасности компонентов ICS (рис. 3).

Отметим, что в РФ уже сейчас известно множество примеров расчета функциональной безопасности широкого перечня: поставляемых компонент[1], блоков управления[2] и сложных систем[3] по указанным выше требованиям IEC серии 61508 и/или 61511.

Проблемы оценки доверия ИТ-компонент

В международных публикациях показана высокая доля рисков безопасности ICS в исходном коде ИТ-компонент [4]. Аналогичные тезисы представлены в докладе РЦУП[4], в частности, предлагается обеспечить безопасность объектов КИИ с помощью гаммы дополнительных «наложенных» СЗИ: систем сбора и корреляции событий ИБ (Security Information Event Management, SIEM), анализаторов уязвимостей, межсетевых экранов, реагирования на инциденты и пр. Необходимо отметить, что применение «наложенных» СЗИ вносит свои риски, поскольку они также содержат множество уязвимостей, и, в том числе потенциально недоверенный исходный код. Применительно к нормативному регулированию отметим, что в РФ принят ГОСТ Р 57580.1-2017[5], в котором определена мера ЖЦ.8 по оценке прикладного ПО в соответствии с оценочным уровнем доверия ОУД 4. Кроме указанного ГОСТ Р, можно рекомендовать и иные НМД, специально посвященные оценке доверия, в частности: X.1254/ ISO 29115 «Information Technology. Security techniques. Entity authentication assurance framework», в которых упомянуты спецификации уровней доверия к аутентификации: LoA1 — LoA4. Отметим также известные требования по аутентификации: ISO 29115:2013[6] и ISO/ IEC 10181-2:1996[7]. В РФ принят ГОСТ Р 54581–2011[8], которые определяет требования к оценке уверенности (confidence), как «убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком» (пп. 2.4, 10, 11).

Опубликован новый реестр инцидентов КИИ Critical Infrastructures Ransomware Attacks[9], в котором представлены публичные данные, в том числе раскрытые в официальных уведомлениях по безопасности. По частоте упоминания лидирует вредоносное ПО Maze, далее WannaCry, NetWalker, CryptoLocker и пр. Для выполнения целей данной работы важно, что по области охвата лидируют правительственные учреждения, среди которых службы реагирования на чрезвычайные ситуации, далее – производственные объекты, транспортные системы, финансовые сервисы. Общая динамика роста инцидентов КИИ весьма тревожная: в 2018 г. раскрыто 68 инцидентов, в 2019 г. — 209 инцидентов (+ 207 %), за первое полугодие 2020 г. уже — 209 инцидентов. Не всегда и не все технические решения можно протестировать, и заранее определить векторы атак, и выявить критические уязвимости. Например, компания Industrial Defenica[10] в рамках эксперимента для изучения угроз ICS развернула сеть Honeypot, принявшую на себя десятки тысяч атак. Важно, что Honeypot весьма эффективна в поиске 0-day уязвимостей и анализе «целевых» атак, но именно для «реалистичного» представления объектов КИИ могут быть сложности, например, IP-адреса в облачной платформе не будут выглядеть правдоподобно.

При формировании оценки доверия ИТ-компонент важно использовать базовый уровень обеспечения

[1] Wika. URL: https://www.wika.ru/upload/DS_IN0019_ru_ru_73327.pdf (дата обращения: 14.10.2020).

[2] Auma. URL: https://www.auma.com/en/products/controls/ac-sil-and-acexc-sil/?amp%3BL=0&cHash=1de66e33bc10ce9db902f8b1d2974327 (дата обращения: 14.10.2020).

[3] Ista. URL: https://ista-01.ru/userful/sertifikat-funktsionalnoy-bezopasnosti-sil-2.htm (дата обращения: 14.10.2020).

[4] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/06%20Akimov.pdf (дата обращения: 14.10.2020).

[5] ГОСТ Р 57580.1–2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер. Введен 01.01.2018. М.: Стандартинформ, 2017. 67 с.

[6] ISO/IEC 29115:2013 Information technology – Security techniques — Entity authentication assurance framework.

[7] ISO/IEC 10181-2:1996 Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.

[8] ГОСТ Р 54581–2011 Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы. Введен. 01.07.2012. М.: Стандартинформ, 2012. 28 с.

[9] Temple University. URL: https://sites.temple.edu/care/ci-rw-attacks (дата обращения: 14.10.2020).

[10] Security Lab. URL: https://www.securitylab.ru/blog/company/axxtel/348955.php (дата обращения: 14.10.2020).

Уровень полноты безопасности (SIL)	Средняя вероятность опасного отказа при запросе функции безопасности (PFDavg).	Средняя частота опасного отказа в течение часа (PFH)
4	≥ 10^{-5} до < 10^{-4}	≥ 10^{-9} до < 10^{-8} ч$^{-1}$
3	≥ 10^{-4} до < 10^{-3}	≥ 10^{-8} до < 10^{-7} ч$^{-1}$
2	≥ 10^{-3} до < 10^{-2}	≥ 10^{-7} до < 10^{-6} ч$^{-1}$
1	≥ 10^{-2} до < 10^{-1}	≥ 10^{-6} до < 10^{-5} ч$^{-1}$

Рис. 2. Ограничение SIL всей системы значениями PFDavg и PFH

Fig. 2. SIL limitation for PFDavg and PFH values

SFF	Допуск на отказы аппаратного обеспечения					
	0		1		2	
	Тип A	Тип B	Тип A	Тип B	Тип A	Тип B
< 60 %	SIL 1	недопустимо	SIL 2	SIL 1	SIL 3	SIL 2
60... < 90 %	SIL 2	SIL 1	SIL 3	SIL 2	SIL 4	SIL 3
90... < 99 %	SIL 3	SIL 2	SIL 4	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4

Рис. 3. Максимальные уровни полноты безопасности компонентов

Fig. 3. Maximum levels of components security integrity levels

функциональной безопасности в ICS по факту создания, иначе говоря «as is». В некоторых публикациях, рассмотренных автором, показано, что поставщики СЗИ полагают все ИТ-компоненты (контроллеры, инженерные станции и пр.) изначально абсолютно незащищенными перед любыми угрозами, и рекламируемые «наложенные» СЗИ просто необходимы. Более того, все рекламные публикации (даже на научно-практических на форумах «SOC», «ИБ КВО АСУТП», «КЗИ» и пр.), не содержат технических выкладок, сопровождающих технический анализ: достаточное быстродействие, потребляемая память, пропускная способность и пр.

Рассмотрим пример иерархии управления в ICS [4], которая показывает время, характеризующее выполнение операций и, соответственно, время ответной реакции (рис. 4). Этот пример отлично подходит для сопоставления технических требований для реализации функциональной безопасности для ИТ-компонент ICS (например, на уровне программируемого логического контроллера (ПЛК) или, в английском варианте, Programmable Logic Controller (PLC)) и предлагаемых «наложенных» СЗИ по формулам (1) и (2).

Необходимо пояснить, что на рис. 4 применены следующие сокращения: ERP — Enterprise Resource Planning (Корпоративная система управления), MES — Manufacture Execution System, (Система управления производственными процессами), SCADA — Supervisory Control And Data Acquisition (Диспетчерское управление и сбор данных) и HNI — Human Machine Interface (Человеко-машинный интерфейс).

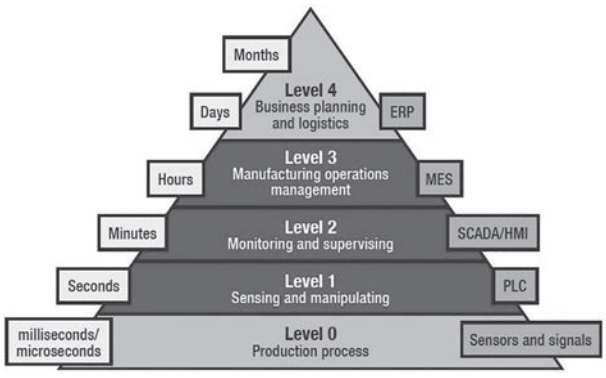

Рис. 4. Иерархия управления в ICS

Fig. 4. ICS control hierarchy

Очевидно, что если компоненты ПЛК проходят жесткое тестирование на соответствие известным требованиям IEC серии 61508 и/или 61511 и обладают доказанной реализацией заданного множества функциональной безопасности, то к «наложенным» СЗИ таких требований не предъявляется и, соответственно, они не проверяются. Подобное упущение может привести к серьезным нарушениям «сплошного» равнопрочного поля функциональной безопасности в целом для ICS. Примером может служить публикация Solar JSOC[1] (рис. 5), в которой показаны интервалы от публикации уязвимости до времени ее первого использования.

Необходимо пояснить, что на рис. 5 указаны некоторые наиболее известные уязвимости, в частности «Shellshock» и «Blue Keep».

С учетом иерархии управления в ICS очевидно, что для каждого уровня должны быть явно определены свои требования, и чем ниже уровень, тем более жесткие должны быть требования к обеспечению функциональной безопасности. Хорошим примером здесь мог бы служить указанный выше ГОСТ РВ. Соответственно, вопрос применения «наложенных» СЗИ[2], способных обеспечить информационный обмен (прием информации с датчиков, анализ и выдача управляющего воздействия) с гарантированным откликом в установленное нормативное время (секунды и менее для уровня PLC и ниже) вызывает серьезные сомнения, поскольку является областью неопределенности и значимого риска, о чем явно указано в ГОСТ РВ. Дополнительно учтем требования IEC серии 61508 и/или 61511, согласно которым все пространства со-

[1] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/09%20Drukov.pdf (дата обращения: 14.10.2020).

[2] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/33%20Suhih.pdf (дата обращения: 14.10.2020).

	Публикация уязвимости	Время до разработки эксплоита	Публикация эксплоита	Время до первого использования	Первая массовая атака
Shellshock	12.09.2014	2 недели	24.09.2014	1 день	25.09.2014
Eternal Blue	n/a	n/a	14.04.2017	1 неделя	21.04.2017 12.05.2017
CVE-2018-15982	28.08.2018	3,5 месяца	05.12.2018	1 сутки	07.12.2018
Blue Keep	14.05.2019	2 месяца	25.07.2019	4 месяца	04.11.2019

Рис. 5. Интервалы от публикации уязвимости до времени ее первого использования

Fig. 5. Intervals from the vulnerability publication to the time of its first usage

стояний (возможные сочетания открытых клапанов, вентилей, положений манипуляторов и пр.), а также переходы между ними, должны быть заранее определены и многократно протестированы на уровне всех ИТ-компонент ICS. В обязательном случае реализуется контур безопасности подсистемы аварийной защиты, который, уместно напомнить, является обязательной и неотъемлемой частью любой ICS. Вызывает серьезное сомнение способность «наложенных» СЗИ[1] «выдать» в канал управления верное управляющее воздействие, согласующееся с реакцией встроенной подсистемы аварийной защиты. В наилучшем случае «наложенное» СЗИ успевает не позже подсистемы аварийной защиты, но возникает не менее важная следующая проблема арбитража между логикой управления подсистемы аварийной защиты (зачастую является коммерческой тайной каждого производителя) и логикой СЗИ, также не являющейся публично доступной.

Предлагаемые меры защиты

В качестве СЗИ предлагается комбинация известных реализаций, в том числе:
- авторизация, аутентификация и аккаунтинг («принцип AAA»);
- многофакторная аутентификация;
- сегментирование сети;
- безопасный удаленный доступ;
- физическая безопасность;
- «белые списки»;
- доверенная загрузка/управление процессами.

Следует отметить, что предложенные СЗИ хорошо известны, например, «принцип AAA» или сегментирование сети известны с XX века. Кроме того, формулировка одной из проблем — оценка достижимости компромисса, позволяет изначально задать правильный вектор технического анализа, который в единичных работах учитывает не простую «переносимость» СЗИ из офисного полигона в условия иной «промышленной реальности» ICS [15, 16]. Обратим внимание, что схожие рекомендации представлены в отчете [4]. В отчете European Union Agency for Cybersecurity[2] (май 2020 г.) появился критерий «*Timeliness*», и некоторые рекомендации в области обеспечения ИБ оцениваются по данному критерию. Этот критерий поддерживает режим жесткого реального времени, и его следует применять для получения сопоставимых оценок коммерческих предложений СЗИ, предназначенных для ICS:
- Network flow monitoring (мониторинг сетевых потоков);
- Full packet capture (захват всех потоков);
- Monitoring of Internet routing (мониторинг интернет-соединений);
- Passive monitoring of unused IP space (пассивный мониторинг неиспользуемых IP-адресов).

В указанном отчете приведены примеры СЗИ, предназначенных для защиты критичных приложений (Critical Security Controls):
- CSC 1 Inventory and Control of Hardware Assets (инвентаризация и контроль аппаратуры);
- CSC 2 Inventory and Control of Software Assets (инвентаризация и контроль ПО);
- CSC 15 Wireless Access Control (контроль беспроводного доступа);
- CSC 18 Application Software Security (контроль прикладного ПО).

Уместны самые широкие аналогии с мерами обеспечения безопасности из Annex 1 стандарта ISO/IEC 27001, NIST SP-800-53 и SANS. В докладе Ростелеком[3] описаны предпосылки для применения Zero Trust Architecture (ZTA), в частности возрастающее количество угроз, вызванных ростом количества уязвимостей в прикладном и общесистемном ПО, и следует заметить, что это шаблонная фраза, которую используют длительное время все продавцы СЗИ. В докладе рассматриваются следующие проблемы безопасности:
- подрядчиков, осуществляющих наладку и эксплуатацию;
- эксплуатации, самая большая проблема – это люди;

[1] CheckPoint. URL: https://research.checkpoint.com/sending-fax-back-to-the-dark-ages (дата обращения: 14.10.2020).

[2] ENISA.URL: https://www.enisa.europa.eu (дата обращения: 14.10.2020).

[3] SOC-Forum URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/37%20Karantaev.pdf (дата обращения: 14.10.2020).

— системы удаленного мониторинга (турбины, процессы).

Можно относиться к любой инициативе оптимистично, но, следует принять во внимание, что помимо «презентационных» функций, SOC[1] предлагает всего лишь новую визуализацию, при этом многие значимые риски остаются нерассмотренные:
— роли и назначения доступа;
— безопасность конечных устройств;
— доступ с мобильных устройств;
— риски компрометации электронных сертификатов.

Относительно возможных последствий рекомендованного перехода к ZTA в ICS отмечается, что «проще сказать, чем сделать», по причине выбора тех же самых СЗИ из хорошо известных нотаций: ISO, IEC, NIST, SANS, например:
— идентификация и аутентификация объектов и субъектов доступа;
— точечное назначение и мониторинг привилегий;
— применение криптографических методов защиты сетевого трафика;
— удаленная «аттестация» платформ в процессе взаимодействия;
— реализация встроенных механизмов защиты.

В презентации ГК «Содружество»[2] показано, что в качестве области тестирования выбран один из действующих заводов, и были подключены автоматизированные рабочие места инженеров, расположенных в корпоративном сегменте. Далее показано, что на этапе тестирования осуществлялся мониторинг событий:
— логи безопасности;
— системные логи;
— SQL Server;
— планировщики задач.

Отметим, что эти события «поставляются» из базовых системных источников, которые используют штатные системы безопасности автоматизированной системы управления технологическим процессом (АСУ ТП), и, объективно, нет никакой необходимости разрабатывать дополнительные дорогостоящие коннекторы SIEM. Были запущены сценарии по пяти определенным категориям угроз:
1) компрометация сегмента АСУ;
2) критическая атака в сегменте АСУ;
3) нарушение технологических процессов;
4) нарушение целостности сегмента АСУ;
5) нарушение изоляции сегмента АСУ.

Всего было зафиксировано 165 событий ИБ и получено 25 уведомлений от специалистов JSOC (все квалифицированы как легитимные). В статистике данных событий определено, что наибольшее количество зарегистрировано по сценариям «Критическая атака в сегменте АСУ» — 120 событий. Эта информация дает основание для более детального исследования, например, на каком уровне иерархии управления ICS осуществлялся сбор событий — наличие логов указывает, как минимум, на уровень SCADA (HMI), т. е. в определенном смысле «сырые» события отсекались на уровне обработчиков ПЛК. В то же время из анализа упускается, намеренно или случайно, участие интегрированной компоненты – подсистемы аварийной защиты, которая на уровне конструкторского замысла и протестированной аппаратной реализации предназначена именно для обеспечения функциональной безопасности. В этой связи не рассмотрена и роль «наложенных» СЗИ, которые, как указано в докладе, входили в контур мониторинга. Следующий вопрос касается оценки результативности подсистемы аварийной защиты, поскольку внешний Security Operation Center (SOC) выявил ничтожно малое по объемам даже для офисных приложений количество событий, к тому же оцененных как легитимные. Весьма интересно детально изучить, работали ли подсистема аварийной защиты и «наложенные» СЗИ совместно, или подсистема аварийной защиты была отключен для обеспечения «чистоты эксперимента», и роль системы функциональной безопасности взяли на себя автоматизированные, т. е. с учетом связки «человек-оператор», системы SOC.

В докладе Positive Technologies[3] утверждается, что наличия SCADA достаточно для управления производством, поскольку это включает как минимум:
— подсистему аварийной защиты;
— системы диагностического контроля;
— системы пожарной сигнализации;
— системы контроля доступа;
— технологическое видеонаблюдение.

Уместно напомнить, к чему приводят отключения вручную одной или нескольких систем безопасности — как при аварии в Бхопале (Индия), так и в Чернобыле. Примеры бесконтрольного вмешательства персонала в автоматические системы защиты, к сожалению, появляются и сегодня. Например, компания Angara[4] опубликовала аналитику результатов анализа защищенности на объектах топливно-энергетического комплекса. При тестировании применялись только технические атаки (атаки с использованием социальной инженерии не применялись):
— в 93 % компаний удалось преодолеть внешний периметр;
— в среднем на атаку требовалось 4 дня, минимально — 30 минут;
— большой брешью остается парольная политика;
— использование устаревших версий ПО, и, соответственно, старых уязвимостей (например, CVE-2017-10271).

Проблема слабой парольной политики весьма актуальна в мире, в частности, в обзоре ImmuniWeb[5] упоминаются «лидеры»: «*password*», «*123456*», «*qwerty*».

[1] MediumCom. URL: https://medium.com/anton-on-security/back-in-2015-while-working-on-a-gartner-soc-paper-i-coined-the-concept-of-soc-nuclear-triad-8961004c734 (дата обращения: 14.10.2020).

[2] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/34%20Balandin.pdf (дата обращения: 14.10.2020).

[3] Positive Technologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/vulnerabilities-corporate-networks-2020-rus.pdf (дата обращения: 14.10.2020).

[4] Security Lab. URL: https://www.securitylab.ru/blog/company/AngaraTech/348487.php (дата обращения: 14.10.2020).

[5] Immuniweb. URL: https://www.immuniweb.com/blog/state-cybersecurity-dark-web-exposure.html#4 (дата обращения: 14.10.2020).

В докладе компании «Касперский»[1] поставлены вопросы:

— заказчикам нужны критерии для выбора эффективных систем кибербезопасности АСУ ТП;
— заказчикам нужны критерии для оценки эффективности возможности систем кибербезопасности АСУ ТП и SOC целиком;
— SOC и поставщикам систем кибербезопасности АСУ ТП нужны критерии для оценки эффективности своих возможностей.

Следует согласиться с рекомендациями: планировать свои действия в области обеспечения безопасности на базе ATT&CK[2] (базы знаний и классификации техник, атакующих на различных этапах жизненного цикла), проводить учения (например, S4x19 ICS Detection Challenge), создавать промышленные полигоны (например, SUTD, Сингапур)[3]. Уместно отметить требования к аудиту, изложенные в IEC 61508-1 (например, п. 6.2.7, п. 7.16.2.2, п. 8.2.7). Помимо указанных рекомендаций следует принимать во внимание уже хорошо известные и многократно отработанные на практике техники (методики) оценки рисков, в частности, в новой версии IEC 31010:2019[4] представлено более 40 методик рисков.

Для решения задачи настоящей работы наиболее подходят HAZOP, HAZID, но есть и новые: VaR, CVaR и пр. На этом этапе снова возникает вопрос, для чего в НМД РФ сохраняется раздельное понимание «наложенных» СЗИ при существующей подсистеме аварийной защиты, поскольку это противопоставление является искусственным. Приходиться оценивать объективно, как определено время на дополнительный мониторинг и/или анализ? Как определены вычислительные ресурсы, необходимые для соблюдения режима жесткого реального времени? Каким образом учтены ошибки от средств дополнительной обработки информации (операторов и/или алгоритмов)?

Корреляционный анализ

В докладе Jet CSIRT[5] предложен сценарий детектирования технических векторов атак на основании MITRE ATT&CK и противодействие с помощью мощных DLP. В данном подходе не учитывается время, которое потребуется для выполнения детектирования атак в режиме жесткого реального времени, что требуется в соответствии с рассмотренным ранее ГОСТ РВ. В условиях ICS эти подходы должны быть рассчитаны и достоверно проверены для оценки гарантированного достижения целей в условиях жестких ограничений. Известно, что значительные сложности вызывает корректная настройка корреляции событий, при этом различают первичную и вторичную корреляции [17–19]. Правила первичной корреляции применяются для обнаружения аномального поведения на основе анализа логов и выставления необходимых меток для дальнейшей обработки правилами вторичной корреляции. Правила вторичной корреляции используются для обработки сообщений от СЗИ, «поставляющих» в SIEM-систему информацию об обнаруженных подозрениях на инциденты. Важно, что эти правила используются для непосредственного обнаружения событий, представляющих собой индикаторы наступления определенных этапов «киллчейна».

Этот аспект хорошо изложен в публикации Lockheed Martin[6]. Важным практическим вопросом является «троянизация» (*trojanization*), когда в цепочках доставки компонент ПО появляются неконтролируемые и необнаруживаемые замены исходных файлов (библиотек) специальным образом инфицированных подделок. Такой класс атак называли «*complex supply chain*» [4]. Как известно, SIEM — это автоматизированная система, следовательно, всегда есть оператор, и, даже с учетом множества фильтров данных, все равно еще требуется время (не нулевое) для разрешения инцидента [20]. Отдельно следует принять во внимание и другое дополнительное время в случае эскалации инцидента, особенно если L2 (L3) линии поддержки расположены в других временных поясах. Для начала формализации корреляционного анализа учтем типы моделей поведения атакующих:

— собственный работник (системные администраторы);
— финансово мотивированные злоумышленники;
— желающие повлиять на репутацию атакуемого предприятия;
— желающие похитить интеллектуальную собственность ICS.

Соответственно, рассмотрим в качестве примера «дерево» ресурсов правил вторичной корреляции в системе ArcSight для системы из десятков хостов и нескольких серверов (по данным Матвиенко Д., гр. N42491, Университет ИТМО, рис. 6).

Очевидно, что для крупной промышленной установки, включающей сотни ПЛК (каталог Yokogawa[7]) потребуются значительные вычислительные ресурсы, а если принять во внимание средний промышленный объект, который включает десятки сложных установок различного назначения, проблема ограничений (вычислительных и/или временных) может стать критической. В докладе BI.Zone[8] рекомендуется просто взять аналитику из доступных форумов, например, наполнять Backlog по разработке правил из Twitter, блогов, конференций

[1] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/36%20Shipulin.pdf (дата обращения: 14.10.2020).

[2] MITRE. URL: https://attack.mitre.org (дата обращения: 14.10.2020).

[3] Itrust. URL: https://itrust.sutd.edu.sg/ciss-2019 (дата обращения: 14.10.2020).

[4] IEC 31010:2019 Risk management — Risk assessment techniques

[5] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/28%20Malnev.pdf (дата обращения: 14.10.2020).

[6] Lockheed Martin. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения: 14.10.2020).

[7] Yokogawa. URL: https://yokogawa.nt-rt.ru/images/showcase/Catalog.pdf (дата обращения: 14.10.2020).

[8] SOC-Forum. URL: https://soc-forum.ib-bank.ru/files/files/SOC2019/29%20Heirhabarov.pdf (дата обращения: 14.10.2020).

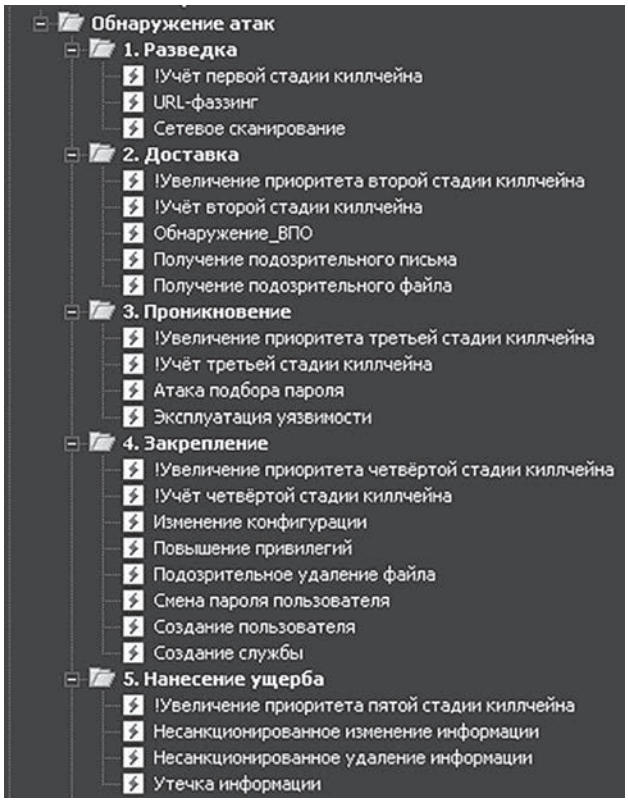

Рис. 6. Ресурсы типа «Правила вторичной корреляции»

Fig. 6. Resources of the "Secondary correlation rules" type

и пр. Однако в отчетах [4, 5] обоснованно говорится об обратном — корреляция терминов ИБ составляет только единицы процентов по отношению к общему числу «Сообщество» (в источнике даны подробные ссылки на эти сообщества), «Аффилиация», «Год начала индексации», «Общее количество пользователей», «Общее количество тематик», «Общее количество комментариев и откликов», «Общее количество тематик, связанных с областью информационной безопасности». Необходимо отметить, что в указанном отчете говорится о «анекдотичном» сопоставлении слов («*security*», «*vulnerability*», «*attack*») в минимальной коннотации по тексту. Это, действительно, подтверждает известное положение, что специалисты ИБ и операционные инженеры говорят на разных языках. Этот тезис можно развернуть и в более широком смысле: учет множества скрытых угроз и уязвимостей, возможность считывания и анализа «фирменной» логики, которая, как отмечено в том же отчете, как правило, является объектом патентной защиты. Соответственно, простое обещание «взять с форума» и наполнить базу корреляции множества «наложенных» СЗИ всеми необходимыми правилами для множества производителей и огромной номенклатурой ПЛК, объективно, выглядит слабо реализуемым.

В обзоре «Operational Risk Horizon 2020»[1] показаны приоритетные риски 2020 г., среди которых явно выделяются Information Security (в том числе Cyber Security) и в общем рейтинге 5 рисков, и в рейтинге 5 опасных рисков.

На рис. 8 показаны две группы рисков: 5 самых важных рисков 2020 г. и 5 самых опасных рисков соответственно. Важно, что ИБ риски (*Information Security*) входят в «тройку призеров» в обоих группах: среди финансовых преступлений (*finance crime*), соблюдения законодательства (*regulatory compliance*), технологиям (*technology*), руководства (*conduct*) и, со-

Community	Affiliation	Indexed since	Total number of users	Total number of topics	Total number of replies or comments	Overall number of mentions of security-related terms
Control.com[18]	N/A	1997	N/A	N/A	69,700	**5,068**
PLC.MyForum.ro[19]	N/A	2012	93,948	41,841	N/A	**1,968**
Mr.PLC[20]	N/A	2006	46,144	33,540	164,787	**1,810**
Robotforum[21]	Robtec	2006	17,611	19,166	90,134	**892**
Reddit - robotics[22]	N/A	2008	83,614	N/A	N/A	**638**
Adam Forum[23]	N/A	2010	33,286	3,783	6,702	**170**
Automation Forum[24]	N/A	2012	220	1,900	7,800	**147**
DoF[25]	Robotiq	2016	N/A	1,500	N/A	**83**
ABB Robotics[26]	ABB	2013	19,723	8,959	19,723	**68**
Universal Robots[27]	Universal Robots	2017	N/A	N/A	N/A	**24**
SolisPLC[28]	SolisPLC	2018	134	36	87	**0**

Рис. 7. Итоги анализа специализированных форумов по безопасности

Fig. 7. Results of the analysis of specialized security forums

тематических вопросов автоматизации ICS (рис. 7).

Необходимо дать пояснения по рис. 7: заголовки столбцов, последовательно, на русском языке:

[1] Managing Risk. URL: https://managingrisktogether.orx.org/research/operational-risk-horizon-2020 (дата обращения: 14.10.2020).

Рис. 8. Оценки приоритетных рисков информационной безопасности 2020

Fig. 8. Assessment of the 2020 priority IT-security risks

ответственно, для наиболее опасных рисков: геополитических (*Geopolitical*), цифрового разрушения (*digital disruption*), обмена (*change*) и третьей стороны (*third party*). В обзоре «Reimagining Operational Risk»[1] отмечена стабильная значимость операционных рисков в эпоху цифровой трансформации, а также факт, что изменения многих факторов риска приводит к невозможности использовать традиционные методы риск-менеджмента. Это особенно интересно с учетом практики статичных моделей угроз ФСТЭК и формальной аттестации сложнейших объектов КИИ, не принимая во внимание изменившиеся мировые парадигмы создания объектов оценки и риск-ориентированных требований к обеспечению безопасности, в том числе функциональной безопасности. В отчете Verison Data Breach Investigations Report 2020[2] отмечается, что категории «системные администраторы» и «пользователи» совместно дают более 20 % рисков ИБ, а еще около 60 % составляют риски криминальных организаций.

На рис. 9 показаны шесть рисков ИБ в порядке убывания их значимости: риски криминальных организаций (*Organized crime*), государственных хакеров (*National-state or State-affiliate*), системных администраторов (*System admin*), пользователей (*End user*), прочих категорий (*Other*) и неаффилированных злоумышленников (*Unaffiliated*).

Как пример «сращивания» международных криминальных интересов, рассмотрим пример атаки Lazarus group в сентябре 2019 г. на предприятия Kudankulam Nuclear Power Plant. Опубликованы данные, что атака не повлияла на системы управления производством ядерного топлива и систем электроснабжения всех производственных систем. В отчете [4] показано распределение векторов атак по итогам анализа 3,950 проникновений в системы ICS. Наибольшее внимание следует уделять не общим и хорошо известным в офисной обстановке техникам защиты (прежде всего, конфиденциальности и, отчасти, целостности), а пока еще недостаточно изученным аспектам обеспечения доступности ИТ-компонент ICS.

На рис. 10 показана «нацеленность» рисков ИБ по трем основным направлениям: конфиденциальность (*Confidentiality*) — до 80 %, целостность (*Integrity*) — до 30 % и доступность (*Availability*) — до 7 % соот-

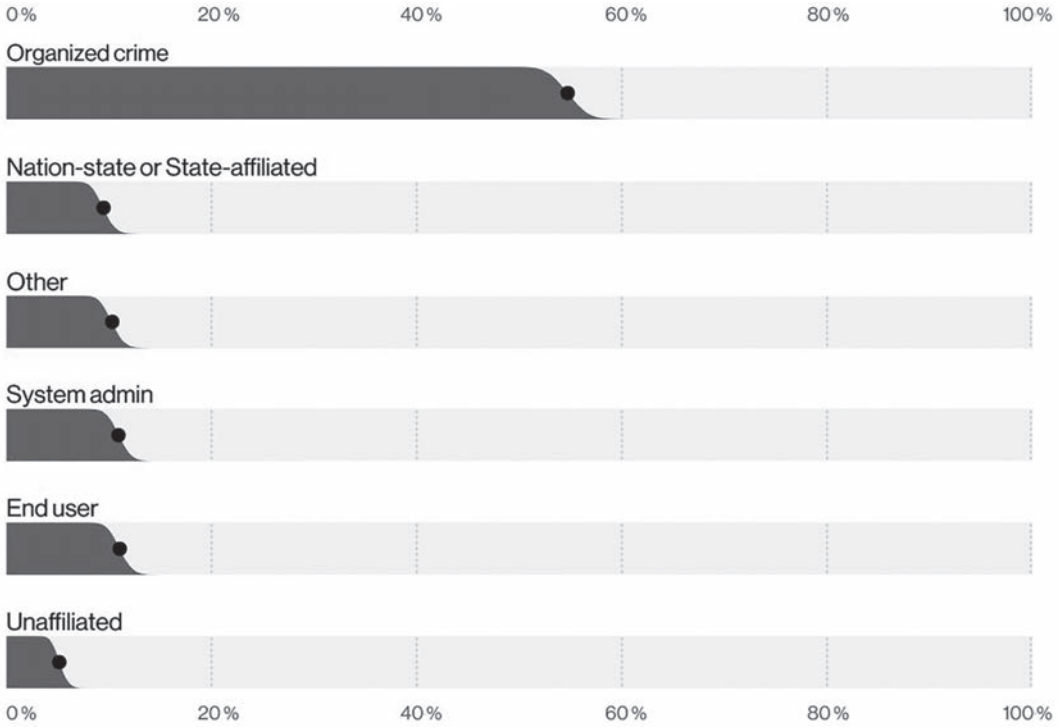

Рис. 9. Значимость рисков 2020

Fig. 9. Significance of risks 2020

[1] Managing Risk. URL: https://managingrisktogether.orx.org/op-risk-strategic-development/reimagining-operational-risk (дата обращения: 14.10.2020).

[2] Verizon. URL: https://enterprise.verizon.com/resources/reports/dbir (дата обращения: 14.10.2020).

Рис. 10. Нацеленность рисков 2020
Fig. 10. Risk targeting 2020

ветственно. Для целей данной работы крайне важно, чтобы проблеме обеспечения доступности, именно для ИТ-компонент ICS, уделялось такое же внимание, как целостности и конфиденциальности. Для офисных приложений традиционно обеспечение конфиденциальности имеет важное значение и, следует признать, что этот фактор реализуется в настоящее время на достаточном уровне. Но для ИТ-компонент ICS значение доступности несоизмеримо выше, и в данном направлении следует предпринять значительные усилия в приоритетном порядке.

Одновременно многие исследователи стали задаваться вопросом о нарушении функциональности «smart» производств в обход установленных ограничений. Направлений таких исследований было множество, среди основных — встраивание специально подготовленного ПО в библиотеки сторонних разработчиков, поскольку почти все поставщики компонент для АСУ ТП в той или иной мере вовлекают в свой процесс выпуска ПО команды по схеме аутсорсинга. В отчете [4] отмечается, что многие внешние консультанты в процессе работы имели прямой доступ к оборудованию на производстве. Тема широкого доступа консультантов к ИТ-компонентам КИИ является отдельной очень важной проблемой [9] и, соответственно, основной вопрос формулируется так: каковы существующие угрозы и какие модели атакующих могут привести к негативным последствиям. Для ответа на поставленный вопрос могут быть предложены различные схемы, в том числе полигон — «пилотный» завод (проект Fenix) [4], исследования показали, что в современных smart-производствах не уделяется достаточное внимание экспертизе обеспечения ИБ в КИИ.

Известна тенденция (вероятно, после громких инцидентов Stuxnet, Black Energy, Triton и пр.) по контролю индустриальных сетей ICS [21, 22]. Попытки простого «переноса» SIEM для архитектуры SOC не дают быстрого успеха: количество объектов измеряется тысячами, наличие иных значений критичности и жесткие регламенты использования системных утилит [20]. По сути, имеется тот же самый объект — ИТ-компонент, к которому устанавливаются требования доверия IEC серии 61508 и/или 61511, и который проходит оценку соответствия в установленном порядке [23–26]. На физическом уровне перемещаются те же электроны, их обрабатывают те же микропроцессоры (Тип B IEC 61508), поэтому имитация «переноса» SOC в область АСУТП не является решением серьезной проблемы. В обзорах [4, 5] эти рассуждения о реализации протоколов, инвентаризации компонент и о построении архитектуры дополнительно отражают необходимость практики создания, оценки и внедрения изначально безопасных ИТ-компонент в соответствии с требованиями стандартов IEC серии 61508 и/или 61511.

Заключение

В работе предложен обзор существующих подходов для решения проблемы обеспечения безопасности промышленных систем. Приняты во внимание все доступные источники, как мировых, так и российских центров экспертизы, в том числе и ведущих поставщиков средств защиты информации. Отмечается, что формирование и решение указанной проблемы актуально и требует комплексного учета многих факторов: устаревшего подхода моделей угроз, игнорирования национальных ГОСТ Р/ГОСТ РВ и риск-ориентированных стандартов, попыток раздельного анализа ИТ-компонент и решений ИБ.

Необходимо проблему обеспечения безопасности промышленных систем рассматривать в технических аспектах: требуемых ресурсов, заданного быстродействия, качества управления, методов подтверждения соответствия, формирования оценок остаточных рисков и иных исчислимых оценок. Требуется уделять первостепенное внимание развитию подхода «от функциональности», при котором обобщенно формирование и решение проблемы начинается в тот момент, когда производитель создает решение по спецификации, состоящей из требований функциональной безопасности, и далее проводит оценку по установленным и известным требованиям доверия.

Для решения проблемы обеспечения безопасности промышленных систем больше внимания следует уделять поставке ИТ-компонент, безопасных изначально и прошедших объективную и полную оценку соответствия функций безопасности в аккредитованных лабораториях в соответствии с требованиями применимых международных и национальных стандартов. Также необходимо и более широкое привлечение специализированных научных организаций и поставщиков ИТ-компонент.

Результаты работы могут быть применены для обеспечения безопасности значимых объектов критической инфраструктуры. В качестве направлений дальнейших исследований предполагается рассмотрение оценок значимости создания безопасных ИТ-компонент и обеспечения цифрового суверенитета Российской Федерации.

Литература

1. Баранов С.Н., Соколов Б.В., Тележкин А.М., Мустафин Н.Г. Модели рисков в программных проектах // Перспективные направления развития отечественных информационных технологий: материалы II Межрегиональной научно-практической конференции. Севастополь: Севастопольский государственный университет, 2016. С. 45–46.
2. Соколов Б.В., Иванов Д.А., Павлов А.Н., Слинько А.А. Имитационное моделирование живучести критических инфраструктур // Седьмая всероссийская научно-практическая конференция «Имитационное моделирование. Теория и практика» (ИММОД-2015): труды конференции в 2 т. Т. 1. М.: Институт проблем управления им. В.А. Трапезникова РАН, 2015. С. 162–167.
3. Верзилин Д.Н., Соколов Б.В., Юсупов Р.М. Неокибернетика: состояние исследований и перспективы развития // Системный анализ в проектировании и управлении: сборник научных трудов XXIII Международной научно-практической конференции. СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2019. С. 81–98.
4. Maggi F., Pogliani M. Attacks on Smart Manufacturing Systems: A Forward-looking Security Analysis [Электронный ресурс]. URL: https://documents.trendmicro.com/assets/white_papers/wp-attacks-on-smart-manufacturing-systems.pdf (дата обращения: 14.10.2020).
5. Claroty Biannual ICS Risk & Vulnerability Report: 1H 2020 [Электронный ресурс]. URL: https://f.hubspotusercontent20.net/hubfs/2553528/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H2020.pdf (дата обращения: 14.10.2020).
6. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation — “hybryd” approach and risk of its implementation // Journal of Physics: Conference Series. 2018. V. 1015. N 4. P. 042030. doi: 10.1088/1742-6596/1015/4/042030
7. Лившиц И.И., Неклюдов А.В. Методика оптимизации программы аудитов информационной безопасности // Комплексная защита информации: материалы XXII научно-практической конференции. Новополоцк: Полоцкий государственный университет, 2017. С. 135–139.
8. Лившиц И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов // Труды СПИИРАН. 2020. Т. 19. № 2. С. 383–411. doi: 10.15622/sp.2020.19.2.6
9. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности. 2020. № 1(35). С. 42–51. doi: 10.21681/2311-3456-2020-01-42-51
10. Костогрызов А.И., Зубарев И.Ю., Родионов В.Н. Методическое руководство по оценке качества функционирования информационных систем (в контексте стандарта ГОСТ РВ 51987). М., 2004. 352 с.
11. Костогрызов А.И. Эффективное управление рисками для критически и стратегически важных объектов РФ // ИТ-Стандарт. 2015. № 2(3). С. 1–8.
12. Костогрызов А.И. Пути решения некоторых проблем комплексной безопасности методами системной инженерии // ИТ-Стандарт. 2017. № 4(13). С. 5–12.
13. Жидков И.В., Кадушкин И.В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1(2). С. 40–48.
14. Бойко А.А., Гриценко С.А., Храмов В.Ю. Система показателей качества баз данных автоматизированных систем // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2010. № 1. С. 39–45.
15. Tiri K.J.V. Design for Side-channel attack resistant security ICS. Los Angeles: University of California, 2005. 141 p.
16. A Trusted and Cyber Secure Europe [Электронный ресурс]. URL: https://www.enisa.europa.eu/ (дата обращения: 14.10.2020).
17. Fedorchenko A., Kotenko I. IOT Security event correlation based on the analysis of event types // Dependable IoT for Human and Industry: Modeling, Architecting, Implementation. 2018. С. 147–168.
18. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. № 4(47). С. 5–27. doi: 10.15622/sp.47.1
19. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. № 6(49). С. 208–225. doi: 10.15622/sp.49.11

References

1. Baranov S.N., Sokolov B.V., Telezhkin A.M., Mustafin N.G. Models of risks in program projects. *Proc. 2nd Interregional Scientific and Practical Conference “Promising Areas of Development of Domestic Information Technologie”*, Sevastopol, Sevastopol State University, 2016, pp. 45–46. (in Russian)
2. Sokolov B.V., Ivanov D.A., Pavlov A.N., Slinko A.A. Simulation of critical infrastructure survivability. *Proc. 7th All-Russian scientific and practical conference Simulation modeling. “Theory and practice”*, in 2 vol, vol. 1. Moscow, V.A.Trapeznikov Institute of Control Sciences Russian Academy of Sciences, 2015, pp. 162–167. (in Russian)
3. Verzilin D.N., Sokolov B.V., Yusupov R.M. Neocibernetics: state of research and development prospects. *Proc. 23rd International Scientific and Practical Conference “Systems Analysis in Design and Management”*, St. Petersburg, Peter the Great St. Petersburg Polytechnic University, 2019, pp. 81–98. (in Russian)
4. Maggi F., Pogliani M. *Attacks on Smart Manufacturing Systems: A Forward-looking Security Analysis*. Available at: https://documents.trendmicro.com/assets/white_papers/wp-attacks-on-smart-manufacturing-systems.pdf (accessed: 14.10.2020).
5. *Claroty Biannual ICS Risk & Vulnerability Report: 1H 2020.* Available at: https://f.hubspotusercontent20.net/hubfs/2553528/Claroty_Biannual_ICS_Risk_Vulnerability_Report_1H2020.pdf (accessed: 14.10.2020).
6. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation — “hybryd” approach and risk of its implementation. *Journal of Physics: Conference Series*, 2018, vol. 1015, no. 4, pp. 042030. doi: 10.1088/1742-6596/1015/4/042030
7. Livshitc I.I., Nekliudov A.V. Information security audit program optimization technique. *Proc. 22nd Scientific and Practical Conference “Comprehensive information protection”*. Novopolotsk, Polotsk State University, 2017, pp. 135–139. (in Russian)
8. Livshitz I. Method for evaluating security of cloud IT-components based on existing standards criteria. *SPIIRAS Proceedings*, 2020, vol. 19, no. 2, pp. 383–411. (in Russian). doi: 10.15622/sp.2020.19.2.6
9. Livshitz I. Practice of cyber-risks management in oil and gas projects of holding companies. *Voprosy kiberbezopasnosti*, 2020, no. 1(35), pp. 42–51. (in Russian). doi: 10.21681/2311-3456-2020-01-42-51
10. Kostogryzov A.I., Zubarev I.Iu., Rodionov V.N. *Methodological guidelines for assessing the quality of information systems functioning (in the context of GOST RV 51987)*, Moscow, 2004, 352 p. (in Russian)
11. Kostogryzov A.I. Effective risk management for critical and strategically important objects of the Russian Federation. *IT-Standard*, 2015, no. 2(3), pp. 1–8. (in Russian)
12. Kostogryzov A.I. The ways of solving some problems of complex safety by methods of system engineering. *IT-Standard*, 2017, no. 4(13), pp. 5–12. (in Russian)
13. Zhidkov I., Kadushkin I. About the signs of potentially dangerous events in information systems. *Voprosy kiberbezopasnosti*, 2014, no. 1(2), pp. 40–48. (in Russian)
14. Boyko A.A., Gricenko S.A., Khramov V.U. System of the factors quality database of the automatic systems. *Proceedings of Voronezh State University. Series: Systems analysis and information technologies*, 2010, no. 1, pp. 39–45. (in Russian)
15. Tiri K.J.V. *Design for Side-channel attack resistant security ICS*. Los Angeles, University of California, 2005, 141 p.
16. *A Trusted and Cyber Secure Europe*. Available at: https://www.enisa.europa.eu/ (accessed: 14.10.2020).
17. Fedorchenko A., Kotenko I. IOT Security event correlation based on the analysis of event types. *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*, 2018, pp. 147–168.
18. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An analysis of security event correlation techniques in SIEM-systems. Part 1. *SPIIRAS Proceedings*, 2016, no. 4(47), pp. 5–27. (in Russian). doi: 10.15622/sp.47.1
19. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An analysis of security event correlation techniques in SIEM-systems. Part 2. *SPIIRAS Proceedings*, 2016, no. 6(49), pp. 208–225. (in Russian). doi: 10.15622/sp.49.11
20. Bryant B.D., Saiedian H. Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. *Computers and Security*, 2020, vol. 94, pp. 101817. doi: 10.1016/j.cose.2020.101817
21. Tsochev G., Yoshinov R., Zhukova N. Some Security issues with the industrial internet of things and comparison to SCADA systems. *SPIIRAS Proceedings*, 2020, vol. 19, no. 2, pp. 358–382. doi: 10.15622/sp.2020.19.2.5

20. Bryant B.D., Saiedian H. Improving SIEM alert metadata aggregation with a novel kill-chain based classification model // Computers and Security. 2020. V. 94. P. 101817. doi: 10.1016/j.cose.2020.101817
21. Tsochev G., Yoshinov R., Zhukova N. Some Security issues with the industrial internet of things and comparison to SCADA systems // Труды СПИИРАН. 2020. Т. 19. № 2. С. 358–382. doi: 10.15622/sp.2020.19.2.5
22. Тарабрин М.О. Индустриальный интернет (IIOT) и применение телеметрической очереди сообщений (MQTT) при разработке АСУТП для нефтегазового предприятия // Информационно-измерительные и управляющие системы: межвузовский сборник научных статей. Самара, 2019. С. 260–270.
23. Марков А.С., Шеремет И.А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник Академии военных наук. 2019. № 2(67). С. 82–90.
24. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1(22). С. 53–61. doi: 10.21681/2412-8163-2017-1-53-61
25. Барабанов А.В., Марков А.С., Цирлов В.Л. Международная сертификация в области информационной безопасности // Стандарты и качество. 2016. № 7. С. 30–33.
26. Барабанов А.В., Марков А.С., Рауткин Ю.В. Тенденции международной оценки соответствия средств защиты информации по линии «Общих критериев» // Информационные технологии и системы: труды Шестой Международной научной конференции. Научное электронное издание. Челябинск: Челябинский государственный университет, 2017. С. 18–20.

22. Tarabrin M.O. Industrial Internet (IIOT) and the use of telemetric message queue (MQTT) in the development of process control systems for an oil and gas enterprise. *Information-Measuring and Control Systems*, Samara, 2019, pp. 260–270. (in Russian)
23. Markov A.S., Sheremet I.A. Software safety in the context of strategic stability. *Bulletin of the Academy of Military Sciences*, 2019, no. 2(67), pp. 82–90. (in Russian)
24. Markov A., Tsirlov V. Structured content of information security requirements. *Monitoring of Law Enforcement*, 2017, no. 1(22), pp. 53–61. (in Russian). doi: 10.21681/2412-8163-2017-1-53-61
25. Barabanov A.V., Markov A.S., Tsirlov V.L. International certification in the information security. *Standards and Quality*, 2016, no. 7, pp. 30–33. (in Russian)
26. Barabanov A.V., Markov A.S., Rautkin Iu.V. Trends in the international assessment of compliance of information security tools under the "Common Criteria". *Proc. 6th International Scientific Conference "Information Technology and Systems"*, Chelyabinsk, Chelyabinsk State University, 2017, pp. 18–20. (in Russian)

Автор

Лившиц Илья Иосифович — доктор технических наук, профессор практики, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57191569306, Livshitz.il@yandex.ru, http://orcid.org/0000-0003-0651-8591

Author

Ilya I. Livshitz — D.Sc., Full Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57191569306, Livshitz.il@yandex.ru, http://orcid.org/0000-0003-0651-8591

Статья поступила в редакцию 19.11.2020
Одобрена после рецензирования 15.12.2020
Принята к печати 18.01.2021

Received 19.11.2020
Approved after reviewing 15.12.2020
Accepted 18.01.2021

Лившиц Илья Иосифович — родился в 1971 г. в Ленинграде. В 1995 г. закончил с отличием факультет технической кибернетики Санкт-Петербургского государственного технического университета. В 2012 году защитил в Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) кандидатскую диссертацию на тему «Методы оценки защищенности систем менеджмента информационной безопасности, разработанных в соответствии с требованиями международного стандарта ИСО/МЭК 27001:2005». В 2018 году подготовлена и успешно защищена диссертация на соискание ученой степени доктора технических наук по теме «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами» по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

В настоящее время работает профессором практики факультета безопасности информационных технологий (Мегафакультет компьютерных технологий и управления) Университета ИТМО. Область научных интересов — системный анализ, защита информации, риск-менеджмент. Имеет свыше 100 научных публикаций.

Ilya I. Livshitz was born in Leningrad in 1971. In 1995 he graduated with high honors from the Technical Cybernetics Faculty of St. Petersburg State Technical University. He received the PhD degree with the thesis on the topic "Methods for security assessment of IT-security management systems developed in accordance with the requirements of the International Standard ISO/IEC 27001:2005" in 2012 and the Doctor of Science degree with the thesis on the topic "Models and methods of IT-security audit of integrated management systems for complex industrial facilities" in 2018 in St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. At present, he is the Full Professor of the IT-security Faculty (Computer Science and Technology Mega-Faculty) at ITMO University. The research interests include: system analyses, IT-security, risk-management. The number of publications is over 100.