в сотрудничестве с предприятиями и институтами различных отраслей промышленности РФ.

Список литературы

1. *Одинец А.И.* Цифровые устройства: учебное пособие. Минобрнауки РФ, ОмГТУ. – Омск: Изд-во ОмГТУ, 2016. – 90 с.
2. *Дружинин В.И., Кузьмин О.В.* Коды Рида – Соломона в системах обнаружения и исправления ошибок при передаче данных // Современные технологии. Системный анализ. Моделирование. – 2015. – № 1. – С. 116 - 124.
3. *Сидоркина Ю.А., Шахтарин Б.И., Балахонов К.А.* Анализ эффективности современных помехоустойчивых кодов // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». – 2014. – № 6. – С. 108 - 116.
4. *Калашников А.А.* Справочник по настройке промышленных гидростатических уровнемеров. – М.: Инфра-Инженерия, 2017. – 194 с.
5. *Бронников К.А., Иващук В.Д. и др.* Эволюция системы единиц измерений. К будущей ревизии международной системы единиц (СИ) // Законодательная и прикладная метрология. – 2018. – № 1. – С. 11 - 16.

Калашников Александр Александрович *– канд. техн. наук, доцент Национального исследовательского университета «Московский энергетический институт», главный эксперт АО «Русатом автоматизированные системы». E-mail: aakalashnikov@list.ru*

DOI: 10.25728/avtprom.2020.12.02

Исследование оценок защищенности промышленных систем

И.И. Лившиц (Университет ИТМО)

В настоящее время при организации защиты промышленных систем различного назначения наблюдаются две крайности – внедрение несовместимых средств защиты информации, не затрагивая базовую ИТ-инфраструктуру, или реализация различных режимов тотальной изоляции (например, архитектуры Zero Trust). Как следует из ежегодных аналитических отчетов мировых экспертов (IBM, MS, Group-IB, Positive Technology и др.), наблюдается постоянный рост сообщений о закрытии очередных критических уязвимостей, но проблема обеспечения безопасности промышленных систем все еще не решена. Известно, что данная проблема признана многими экспертами актуальной и важной.

Существенным негативным фактом является сохранение практики текущего раздельного оценивания двух сущностей – ИТ и ИБ, что не в полной мере обеспечивает оптимальное решение поставленной выше проблемы. В представленной работе дается краткий обзор существующих подходов оценки защищенности промышленных систем. Сформулированные рекомендации могут быть применены для совершенствования существующих и создания перспективных решений для обеспечения безопасности промышленных систем, в том числе и при обеспечении национального цифрового суверенитета.

Ключевые слова: информационная безопасность, промышленная система, менеджмент рисков, меры защиты, оценка соответствия.

Введение

Обеспечение безопасности в широком толковании (*Safety*) для промышленных систем различного назначения (*Industrial Control System, ICS*) имеет давние традиции, сопоставимые по времени зарождения с первыми проектами в области систем управления вооружением и атомных реакторов. Отметим, что ранее в работах зарубежных и отечественных центров экспертиз в данной области не существовало раздельного определения сущностей информационных технологий (ИТ) и информационной безопасности (ИБ), соответственно системы проектировались, создавались, проходили испытания, эксплуатировались как единое целое [1, 2]. Начиная с XX века основным требованием было обеспечение реализации заложенной функциональности, устойчивая работоспособность программных (программно-аппаратных) комплексов [3]. Новации в этой области в определенной мере вызваны принятием ФЗ «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017 N 187-ФЗ, в котором явно указано отдельное определение систем ИБ. А в ряде подзаконных актов (постановление Правительства № 127, приказы ФСТЭК № 235, № 239 и пр.) определены фиксированные списки угроз и мер защиты для обеспечения защищенности объектов критической информационной инфраструктуры (КИИ).

В СТО Газпром серии 4.2 (Система обеспечения ИБ) представлены требования к функционированию ИТ-компонентов, но требования функциональной безопасности (ФБ), равно как и порядок проектирования, испытаний и управления рисками не опреде-

лены. В частности, в Р Газпром 4.2–5-002–2009 «Система обеспечения информационной безопасности ОАО «Газпром» Методика сертификационных испытаний АСУТП» упоминается только подтверждение соответствия в Системе добровольной сертификации ГАЗПРОМСЕРТ. В Р Газпром 4.2–5-003–2009 «Система обеспечения информационной безопасности ОАО «Газпром» Методика испытаний средств и систем обеспечения безопасности информационных технологий» единственное упоминание функциональных требований есть в п. 7.2, но ни в одном документе не упоминается менеджмент рисков.

Целью статьи является исследование проблемы обеспечения безопасности промышленных систем и формирование предложений по обеспечению национального цифрового суверенитета РФ.

Нарушения безопасности промышленных систем

Для возможных вторжений в ИТ-инфраструктуру промышленных систем созданы негативные «условия», основные из которых показаны в отчете TrendMicro [4]:

– на сайтах поставщиков индустриального программного обеспечения (ПО) часто отсутствует регистрация (зараженные поддельные компоненты ПО можно загрузить анонимно);

– не используется HTTPS, только «чистый» HTTP без SSL;

– многие индустриальные компьютеры под управлением ОС Microsoft Windows не используют технологии «изолированного песчаного ящика» (*sandbox*) для безопасного тестирования потенциально опасных приложений;

– многие HMI (*Human machine Interface*, человеко-машинный интерфейс) подключаются по беспроводным протоколам (Wi-Fi или Bluetooth) без всякой защиты;

– многие компоненты ПО содержат в своем коде алгоритмы генерации паролей, что может быть вскрыто методом структурного анализа исходного кода «обратной инженерии» (*reverse-engineering*);

– многие компоненты ПО не имеют корректно настроенных функций, что может привести к опасным вторжениям через подстановку специальных некорректных входных данных;

– отсутствуют защиты от сканирования сетей, перехвата и эксфильтрации данных из файлов, направляемых от промышленных машин и механизмов.

Сравнение данных компании Claroty [5] об уязвимостях промышленных систем за 1 полугодие 2019 г. и 1 полугодие 2020 г. показано на рис. 1.

Лидирующие позиции занимает удаленное выполнение кода (*Execute unauthorized code*), чтение прикладных данных (*Read application*) и атаки DoS (*Denial of services*). Хотя число уязвимостей, которые могут привести к удаленному выполнению кода, снизилось на 7,7%, две другие уязвимости из «тройки лидеров» показали существенный рост: чтение прикладных данных +25,4% и DoS +9,2% соответственно. В отчете отмечается, что любое из этих потенциальных воздействий может серьезно повлиять на целостность и доступность устройств промышленных систем.

Отдельно рассмотрим возможности компрометации технологии «цифровых двойников», как важную частную проблему. В отчете [4] исследованы уязвимости для данной технологии, от которых практически нет защиты в реальных приложениях промышленных систем, например:

– уязвимости при цифровой подписи кода;

– незащищенный (нешифрованный) трафик в сетях;

– отсутствие протоколов аутентификации;

– возможности подделки «цифровых двойников» — нет гарантии, что ПО, загруженное на конечные узлы, не было изменено;

– невозможность гарантировать выполнение аварийных остановов в соответствии с требованиями применимых стандартов.

Известно, что исходные коды ПО (Microsoft, Adobe, Qualcomm, Motorola и др.) были опубликованы в репозитории на GitLab (https://safe.cnews.ru). Причинами утечки стали слабые настройки интеграции и развертывания ПО, кроме того, обнаружены реквизиты доступа, «вшитые» в исходники. В компонентах системы управления известного зарубежного вендора были выявлены критические уязвимости (https://www.securitylab.ru/news/510809.php). Эту систему используют более 10 тыс. предприятий нефтегазовой, химической, энергетической отрасли, то есть субъекты КИИ по законодательству РФ. Одна из уязвимостей (с критической оценкой 8.1 из 10 возможных по шкале CVSS v3.0) связана с отсутствием аутентификации, что позволяет злоумышленнику взаимодействовать с сервером. Отметим, что значимость применяемой системы оценки уязвимостей (*Common Vulnerability Scoring System, CVSS*) для промышленных технологий является предметом дискуссии, так как изначально она была разработана для оценки уязвимости ИТ [5]. Хотя CVSS основана на классической «триаде» — конфиденциальности, целостности и доступности, тем не менее не в полной мере пригодна для «целевых» задач оценки компонентов промышленных систем — надежности и безопасности, что может создавать проблемы при оценке физического вреда.

Проблемы безопасности встроенных мер защиты

Проблема безопасности промышленных систем стоит очень остро в современном цифровом мире. Об этом свидетельствуют отчеты известных мировых лидеров в области ИБ. Так, в отчете Positive Technology [6] показаны результаты тестирования промышленных сетей, при этом утверждается, что выявлены узлы, на которых раскрывается важная информация (например, содержимое конфигурационных файлов). Показано, что причина многих инци-

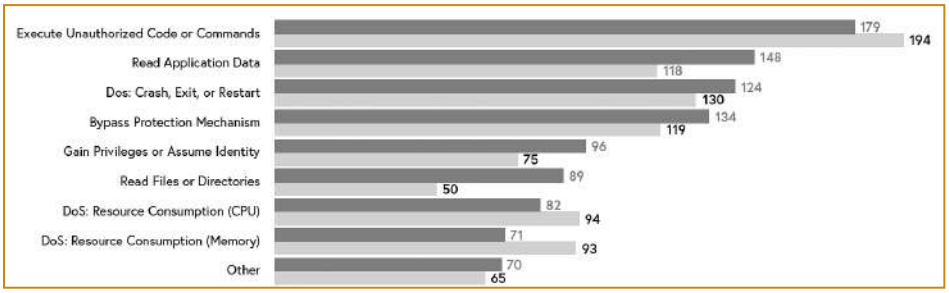

Рис. 1. Сравнение данных об уязвимостях ICS за 1 полугодие 2019 г. и 2020 г. [5]

дентов кроется в небезопасной конфигурация служб, и выявлены известные уязвимости даже 2013–2014 гг.

В отчете компании Claroty показано распределение выявленных уязвимостей (всего 365 ед.) в промышленных системах по 53 производителям средств и систем автоматизации. Отмечается, что более 75% всех выявленных уязвимостей имеют статус «высокий» и «критичный» по классификации CVSS [5]. Важно, что в отчете упомянуты все лидеры рынка автоматизации промышленных систем. Cybersecurity in Application, Research, and Education (CARE) Lab в 2020 г. выпустила новую версию реестра инцидентов КИИ, связанных с атаками вымогательского ПО (https://sites.temple.edu/care/ci-rw-attacks), которая содержит 651 запись о кибератаках на КИИ за период с ноября 2013 г. по июль 2020 г. Всего на КИИ с использованием вымогательского ПО было раскрыто в 2018 г. — 68 инцидентов, в 2019 г. — 209 инцидентов, в 2020 г. — уже 209 (на 05.08.2020 г.).

Для борьбы с киберугрозами предлагаются все новые и новые методы, средства и системы. В настоящее время наблюдается «смещения фокуса» от дополнительных средств защиты информации (СЗИ) к встроенным технологиям промышленных систем или к «гибридным» системам. Так, компании Positive Technologies и Oreol Security провели успешные испытания на совместимость системы анализа трафика сетей АСУТП PT Industrial Security Incident Manager (PT ISIM) и устройства однонаправленной передачи данных ProfiDIODE. Тестирование включало проверку корректной работы решения, его устойчивости при резкой смене нагрузки, целостности данных в получаемой копии трафика. Совместное решение позволяет обеспечить защиту технологических систем, гарантируя изолированность сегмента АСУТП. PT ISIM помогает обнаружить кибератаки или неправомерные действия персонала, уязвимости компонентов АСУТП и проводить расследования инцидентов, а интеграция с ProfiDIODE исключает возможность негативного влияния на сегмент АСУТП за счет однонаправленной передачи данных (https://www.securitylab.ru/news/510891.php). Отметим, что предлагаемое решение не использует базовую функциональность подсистемы аварийной защиты (ПАЗ), которая присутствует в составе АСУТП.

Кембриджским университетом совместно с компанией Industrial Defenica проведен эксперимент для изучения потенциальных угроз промышленных систем. В рамках исследования была развернута географически распределенная сеть из 120 Honeypot[1], за 13 мес. принявшая на себя 80 тыс. атак и 9 попыток эксплуатации промышленных протоколов, в том числе четыре попытки использования неизвестных ранее уязвимостей (https://www.securitylab.ru/blog/company/axxtel/348955.php). Системы Honeypot существуют уже несколько десятилетий и в очередной раз подтвердили свою эффективность в поиске уязвимостей «нулевого дня» и анализе целевых атак на информационные системы. Важным результатом данного исследования являются рекомендации по построению сетей Honeypot. В частности, выделим рекомендации по созданию реалистичного окружения (это касается и IP-адресов — например, ПЛК, развернутый на облачной платформе, не будет выглядеть правдоподобно) и использованию Honeypot с высокой степенью взаимодействия. Указанные меры помогают избежать быстрого раскрытия Honeypot и заставляют злоумышленника дольше задерживаться на нем, как будто он является ценной целью.

Наличие уязвимостей в кодах ПО компонентов промышленных систем может иметь самые негативные последствия, поскольку нет гарантий блокировки трафика от «зараженного» приложения или по причине невозможности успешного анализа различных форматов файлов и/или протоколов [4]. В связи с этим бесполезны сканеры безопасности, так как не существует предварительно подготовленных шаблонов для анализа всех форматов, и межсетевые экраны — если определенный хост внесен в «белый список», то не существует алгоритмов для блокирования неожиданных команд управления (поворот, перемещение и пр.) исполнительными устройствами. Для устранения этих недостатков и организации защищенного обмена данными между компонентами промышленных систем предлагается внедрять решения для тотальной аутентификации всех пакетов в промышленной сети. Но в этом случае возникает новый ряд проблем по достоверности криптографических функций, техническим возможностям хостов, критичности задержек и пр. Эти и другие вопросы, в частности, специальной криптографии[2], предназначенной для быстрой и надежной защиты всех передаваемых данных между компонентами промыш-

[1] Honeypots – оборудование или ПО, которые специально развертываются отделами безопасности для изучения угроз. Honeypots служит ловушкой для сбора информации о злоумышленнике и защиты реальной целевой системы.

[1] https://csrc.nist.gov/projects/lightweight-cryptography

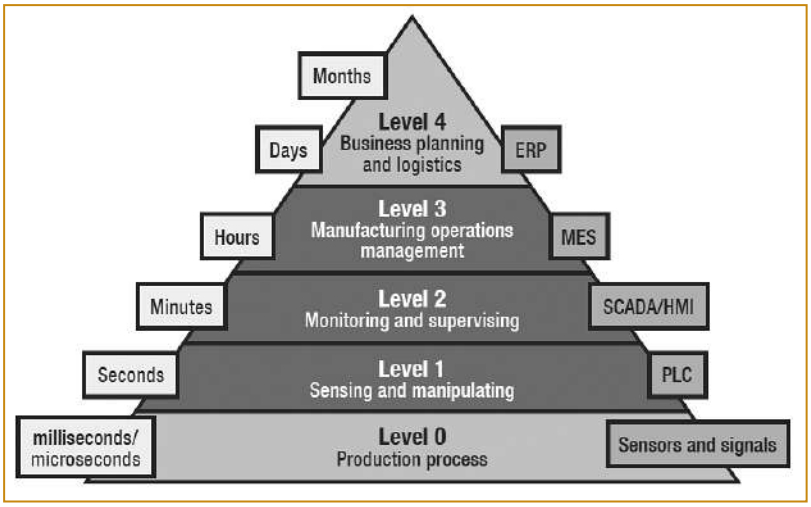

Рис. 2. «Пирамида» промышленной системы [4]

ленных систем, очевидно, должны быть согласованы с национальными регуляторами.

На уровне национального регулятора в РФ, к сожалению, заложена устаревшая архитектура раздельного применения СЗИ, и этот поход не позволяет принять во внимание весь накопленный опыт создания ИТ-компонентов, безопасных изначально. Отметим, что в стандартах ГОСТ Р ИСО 31000, ГОСТ Р МЭК 31010, ГОСТ Р ИСО/МЭК 27005 не приводится раздельного определения сущностей ИТ и ИБ. Описание требований к функциональной безопасности (ФБ) промышленных систем, изложенных в стандартах ГОСТ Р, даны в публикациях [7–10], а оценки рисков — в публикациях [11–15] соответственно.

Важным преимуществом методики, описанной в системе ISO, являются установленные ограничения, в частности, по времени, по глубине экспертизы, по точности результатов и пр.

Исследование оценки доверия

В современных исследованиях отмечается высокая доля рисков безопасности промышленных систем со стороны уязвимостей в исходном коде ИТ-компонентов [4]. В этой связи предлагается обеспечить безопасность значимых объектов КИИ с помощью систем сбора и корреляции событий ИБ (Security information event management, SIEM), платформ реагирования на инциденты (Incident Response Platform) и пр. При этом упускается из виду тот факт, что применение указанных и многих других дополнительных СЗИ вносит свои риски, поскольку они также содержат потенциально недоверенный исходный код. Для оценки этих рисков необходимо анализировать соответствующие уровни доверия и формировать системы требований к оценке уровней доверия к применяемым СЗИ.

Дополнительно в документе X.1254/ISO 29115 «Information technology. Security techniques. Entity authentication assurance framework» указаны четыре уровня доверия к аутентификации: LoA1 — LoA4. Также описаны требования по аутентификации в ГОСТ Р 58833-2020, ISO 29115 или ISO/IEC 10181. Кроме оценки доверия к аутентификации применяется оценка уверенности как «убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком» в соответствии с ГОСТ Р 54581-2011 (п. 2.4, 10, 11).

Рассмотрим «пирамиду» промышленной системы [4], которая показывает иерархию управления и время выполнения операций и ответной реакции. На «нулевом» уровне установлены многочисленные датчики и сенсоры производственных линий, а время обработки сигналов составляет микро- и миллисекунды. На первом уровне сигналы от датчиков поступают в ПЛК, которые имеют собственную логику (тип «В» по ГОСТ Р МЭК 61508), а время обработки уже составляет секунды. На следующем втором уровне данные от ПЛК поступают на уровень систем SCADA и HMI, соответственно, время обработки уже становится приемлемым для человека-оператора и измеряется минутами. На третьем уровне действуют компоненты системы управления производственными процессами (Manufacturing execution system, MES), а время реакции может измеряться часами. На верхнем уровне иерархии находятся общие корпоративные системы управления (Enterprise Recourse Planning, ERP), для которых компоненты MES поставляют свою часть специальной управляющей информации. На высшем четвертом уровне иерархии время принятия решений стратегического уровня может измеряться днями.

Все оценки доверия для компонентов промышленной системы должны быть взаимоувязаны с соответствующими уровнями управления, что обеспечит четкое понимание тех целей и задач, которые могут быть достигнуты, и формирование достоверных и объективных доказательств приемлемого уровня безопасности (например, по ГОСТ Р МЭК 61508 и/или 61511). В общем упрощенном варианте можно полагать, что на каждом уровне управления применяются свои методы обеспечения функциональной безопасности и установлена своя совокупность требований к оценкам доверия. Всего установлено семь уровней доверия, минимальные требования определены для первого уровня, соответственно, максимальный уровень функциональной безопасности определен на седьмом уровне. Подробные спецификации всех требования доверия для каждого уровня подробно описан в стандартах ГОСТ Р ИСО/МЭК серии 15408.

На этом примере удобно сопоставить технические требования как для реализации ФБ для ИТ-компонентов промышленной системы (например, на уровне ПЛК) и дополнительных СЗИ. Очевидно, что если компоненты ПЛК проходят должное тестирование на соответствие известным требованиям ГОСТ Р МЭК серии 61508 и/или 61511 и обла-

дают доказанной реализацией заданного множества ФБ, то к дополнительным СЗИ таких требований не предъявляется и, соответственно, они не проверяются. Подобное упущение может привести к серьезным нарушениям «сплошного» равнопрочного поля ФБ в целом для промышленной системы.

Экономическая эффективность СЗИ

На сегодняшний день все понимают, что реакция на воздействия в промышленных системах не может быть сравнима с реакцией на возможные события ИБ в офисе. Для обеспечения реакции в промышленных системах требуется учесть несколько важных проблем. Первая проблема — технический ресурс вычислительной системы. В докладе Бенгина представлены результаты анализа промышленных систем по типам обнаруженных инцидентов ИБ, в том числе: сканирование внутренней сети, получение данных с контроллера домена и пр. В указанном отчете не представлено никаких данных о ресурсах технических средств промышленных систем; успеют ли они выполнить не только мониторинг, но и необходимый анализ? Хватит ли вычислительной мощности для специфических процессов? В самом худшем случае в офисе можно подождать 5...10 мин, потом перегрузить MS Word, но в реальном производственном цикле это может быть неприемлемо, как показано в ГОСТ РВ и/или IEC серии 61508 [11].

В докладе Hoffmann (Radar Cyber Security)[4] предложен подход валидации гипотез при выявлении и оценке угроз безопасности на основании сбалансированного анализа достоверных и оперативных данных (в частности, SIEM). Однако встает вопрос о вычислительных возможностях, способных обработать значительный объем событий и число инцидентов ИБ, требующих реакции в режиме жесткого реального времени (ЖРВ). В офисных сетях, по оценкам Infotecs[5], за 1-е полугодие 2019 г. оперативный центр по обеспечению безопасности (*Security Operation Center, SOC*) обработал 433 083 046 событий ИБ, из них 573 инцидентов ИБ, а за 1-е полугодие 2018 г. — 149 009 215 событий ИБ и 177 инцидентов ИБ. Таким образом, доля инцидентов ИБ составляет примерно одну миллионную, для выявления которой потребовалось обработать огромные объемы информации. В 2020 г. эти цифры могут увеличиться, так как в условиях пандемии в большинстве компаний разрешено подключение к рабочему столу по протоколу удаленного доступа, при этом у некоторых серверов разрешена авторизация без пароля, что представляет значительную опасность[6].

Следующий важный вопрос — изучение объема «переработанных» событий ИБ, которые генерируют дополнительные СЗИ, и допустимое время на их обработку, применительно к жестким условиям функционирования промышленных систем. Известно, что SOC предоставляют свои услуги на основании специальных соглашений об уровне сервисов (Service Level Agreement, SLA). В презентация JSolar[7] показано, что SOC способен обработать 72 млрд. событий в сутки, а SLA предусматривает 10 мин. на обнаружение и 30 мин. на реагирование по инциденту ИБ. В докладе SOC Angara[8] подтверждается лимит 15 мин. SLA на обнаружение и до 90 мин. на расследование инцидента ИБ. В «ландшафте» комфортных офисных приложений, например, MS Office, эти показатели выглядят достойно, но 10 мин. объективно недопустимо, когда речь идет о сложных реакциях в нефтехимии или процессах на объектах атомной промышленности.

Возникает вопрос, стоит ли внедрять дорогостоящие дополнительные СЗИ в промышленных системах, результативность которых явно не окупается с учетом более чем значимых затрат на проект. В рекламных докладах умышленно, по всей видимости, упускается из вида факт, что все промышленные системы оснащены в обязательном порядке ПАЗ. Это не опция, это обязательное требование международных стандартов по обеспечению ФБ, например, IEC серии 61508/61511. Безусловно, ПАЗ проектируется как неотъемлемая часть АСУТП, входит в ее стоимость и не требует «заката солнца вручную», поскольку функционирует в режиме ЖРВ. В общем упрощенном сценарии уровень безопасности АСУТП как раз определяется уровнем функциональной безопасности в реализованной подсистеме ПАЗ, например, по определенному заданному проектировщиками уровню доверия.

В рекомендациях National Institute of Standards and Technology — NIST SP 800-61 R2 «Computer Security Incident Handling Guide» рассмотрены несколько сценариев атак на объекты АСУТП: от DoS (Denial of Service, отказ в обслуживании) атаки на DNS сервер (Сценарий № 1) до кражи документов (Stolen Documents) (Сценарий № 3). В докладе Check Point[9] рассматривается вектор атаки от сетевого принтера, что должно привести к реализации внутренней сегментации и защите конечных станций. Из данной публикации можно сделать вывод о важности моделирования сценариев возможных атак на промышленные системы и формирования соответствующих требований функциональной безопасности, наиболее оптимально применимых для обеспечения общей устойчивости защищаемых систем. Дополнительно можно

[3] https://soc-forum.ib-bank.ru/files/files/SOC2019/12%20Bengin.pdf
[4] https://soc-forum.ib-bank.ru/files/files/SOC2019/13%20Rublev.pdf
[5] https://soc-forum.ib-bank.ru/files/files/SOC2019/14%20Danilov.pdf
[6] https://www.kommersant.ru/doc/4366208?from=main_2
[7] https://soc-forum.ib-bank.ru/files/files/SOC2019/21%20Judakov.pdf
[8] https://soc-forum.ib-bank.ru/files/files/SOC2019/23%20Kohanko.pdf
[9] https://research.checkpoint.com/sending-fax-back-to-the-dark-ages

Афоризмы - это интерфейсы, по которым передается оценка и понимание.
Алан Перлис

рекомендовать определять наиболее подходящие нормативные документы (ГОСТ Р, ГОСТ Р ИСО, ГОСТ Р МЭК) для цели обеспечения национального цифрового суверенитета применительно к объектам КИИ.

Заключение

Решение проблемы обеспечения безопасности промышленных систем актуально и требует комплексного учета многих факторов функциональной безопасности, в том числе обеспечения оценки доверия и экономической эффективности. На основании краткого обзора можно сформировать несколько рекомендаций.

1. Предлагается применять известные и многократно отработанные на практике методики менеджмента рисков (например, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000).

2. Предлагается пересмотреть порядок раздельного применения дополнительных СЗИ при существующей системе ПАЗ в промышленных системах, поскольку это противопоставление является во многом искусственным.

Предложенное позволит в перспективе избежать затрат на дополнительный мониторинг (анализ) событий безопасности, оптимизировать вычислительные ресурсы, необходимые для соблюдения режима ЖРВ в промышленных системах, а также исключить ошибки при дополнительной обработке информации (операторов и/или алгоритмов). Данные предложения могут быть востребованы при решении проблемы создания безопасных промышленных систем, что в определенной мере будет способствовать общей цели обеспечения цифрового суверенитета РФ.

Список литературы

1. *Баранов С.Н., Соколов Б.В., Тележкин А.М., Мустафин Н.Г.* Модели рисков в программных проектах // Тр. II межрегиональной научно-практич. конф. «Перспективные направления развития отечественных информационных технологий». Севастопольский государственный университет. 2016. С. 45-46.
2. *Соколов Б.В., Иванов Д.А., Павлов А.Н., Слинько А.А.* Имитационной моделирование живучести критических инфраструктур // Тр. VII конференции "Имитационное моделирование. Теория и практика" (ИММОД-2015). ИПУ РАН. Под ред. С.Н. Васильева, Р.М. Юсупова. 2015. С. 162-167.
3. *Верзилин Д.Н., Соколов Б.В., Юсупов Р.М.* Неокибернетика: состояние исследований и перспективы развития//Сб. трудов XXIII междунар. научно-практич. конф. «Системный анализ в проектировании и управлении». 2019. С. 81-98.
4. Attacks on Smart Manufacturing Systems. [Электронный ресурс]. https://documents.trendmicro.com
5. Claroty Biannual ICS Risk & Vulnerability Report [Электронный ресурс]. https://f.hubspotusercontent20.net
6. Уязвимости периметра корпоративных сетей [Электронный ресурс]. https://www.ptsecurity.com
7. *Livshitz I.I., Neklyudov A.V., Lontsikh P.A.* IT-Security evaluation – “Hybryd” approach and risk of its implementation. В сборнике: Journal of Physics: Conference Series. International Conference Information Technologies in Business and Industry 2018 - Enterprise Information Systems. 2018. С. 042030.
8. *Лившиц И.И., Неклюдов А.В.* Методика оптимизации программы аудитов информационной безопасности//Тр. XXII научно-практич. конф. «Комплексная защита информации». 2017. С. 135-139.
9. *Лившиц И.И.* Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов. SPIIRAS Proceedings. 2020. Vol. 19 No. 2. С. 383-411.
10. *Лившиц И.И.* Практика управления киберрисками в нефтегазовых проектах // Вопросы кибербезопасности. 2020. № 1(35). С. 42–51.
11. *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., 2004.
12. *Костогрызов А.И.* Эффективное управление рисками для критических и стратегически важных объектов РФ//ИТ-Стандарт. 2015. № 2 (3). С. 1-8.
13. *Костогрызов А.И.* Пути решения некоторых проблем комплексной безопасности методами системной инженерии // ИТ-Стандарт. 2017. № 4 (13). С. 5 - 12.
14. *Жидков И.В., Кадушкин И.В.* О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. №1(2). стр. 40 - 48.
15. *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. стр. 39-45.

Лившиц Илья Иосифович *– д-р техн. наук, университет ИТМО.*
Контактный телефон +7 (921) 934-48-46.
E-mail: Livshitz.il@yandex.ru