ПРАКТИКА ОБУЧЕНИЯ ПО НАПРАВЛЕНИЮ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УНИВЕРСИТЕТЕ ИТМО

***Лившиц И.И.*[1], *Перлак П.В.*[2]**

Цель исследования: *разработка и практическая апробация новой программы обучения по направлению функциональной безопасности для технических ВУЗов. Важной особенностью поставленной цели является независимость ее решения от конкретной области функционирования сложных промышленных объектов. Ставится задача применения единого инженерного подхода для обучения по направлению функциональной безопасности – как в теоретической, так и в практической (расчетной) части.*

Методы исследования: *системный анализ, методы аналитического моделирования, статистические методы, методы сопоставления и методы практической апробации.*

Полученный результат: *исследованы требования, предъявляемые при создании и оценке компонент с точки зрения функциональной безопасности. Произведен обзор отечественной и мировой научной литературы за последние 10 лет и краткий анализ существующих решений по оценке компонент с точки зрения функциональной безопасности. Предложена структура нового учебного курса, кратко описаны основные части – теоретическая (лекционная) и расчетная (практическая). Дается описание обобщенных процедур оценивания функциональной безопасности различных компонент, а также результаты их апробации в учебном курсе Университета ИТМО в 2022/2023 учебном году. Рассмотрены оценки обеспечения степени доверия наложенных средств защиты. Представлены примеры блока из 4-х практических работ и даны рекомендации их последовательного выполнения. Показано на практике, как важно определять порядок верификации и валидации требований функциональной безопасности, которые оформляются в виде формальных процедур.*

Научная новизна *заключается в систематизации и достаточно обширном обзоре применимых нормативно-методических документов (ГОСТ Р, ISO, IEC) за последние десять лет, посвященных оценке функциональной безопасности компонентов. Предложен новый курс для студентов технических ВУЗов, который в равной мере сочетает практические и теоретические знания, прошел полный цикл апробации.*

Ключевые слова: *АСУТП, импортозамещение, риски, остаточные риски, аудит, оценка соответствия, цифровой суверенитет; сложные промышленные объекты; критическая информационная инфраструктура; надежность; степень доверия.*

DOI:10.21681/2311-3456-2023-3-50-61

Введение

В настоящее время проблема обучения по направлению обеспечения функциональной безопасности (далее – ФБ) получает высокий приоритет как в силу важности практической реализации данного направления в Российской Федерации, так и известного дефицита доступного квалифицированного персонала. Известно, что с момента создания систем автоматизации сложных промышленных объектов (обобщенно назовем этот класс объектов АСУТП), объективно наблюдается как постоянное увеличение функциональных возможностей компонент, так и рост обеспокоенности относительно уверенности в безопасной работе в штатном режиме в современных условиях. Как показывает доступная аналитика, за прошедшие десятилетия существенных изменений в области обеспечения ФБ компонентов АСУТП не произошло, соответственно, общие принципы обучения в технических ВУЗах также остались прежними. Для обеспечения цифрового суверенитета в РФ необходимо не только обеспечить полный жизненный цикл национальных компонент АСУТП, но и обеспечить должную квалификацию персонала, способного осуществлять корректное и устой-

1 Лившиц Илья Иосифович, д.т.н., профессор практики факультет ФБИТ, Университет ИТМО, Санкт-Петербург, Россия. E-mail: Livshitz.il@yandex.ru

2 Перлак Павел Викторович, аспирант факультета ФБИТ, Университет ИТМО, Санкт-Петербург, Россия. E-mail: ntn_isun@mail.ru

чивое функционирование с учетом известных и новых рисков. Можно подобрать множество «комфортных» причин объяснения текущего положения, при котором в ВУЗах практически нет практики обучения по направлению обеспечения ФБ. Простая логика подсказывает верное решение – для обеспечения полного процесса ФБ в национальном масштабе необходимо обеспечить подготовку в ВУЗах Российской Федерации достаточного количества квалифицированных специалистов, готовых соблюдать известные инженерные принципы, в том числе – обеспечить заданный расчетный уровень безопасности компонентов. Недостаток профессионалов в условиях «эффективного менеджмента» может привести к серьезным финансовым издержкам, например, известно, что затраты на сертификацию системы противоаварийной защиты (далее – ПАЗ) для АЭС[3] могут составлять до 10% стоимости проекта, но и последствия некоторых аварий могут оказаться катастрофически неприемлемыми.

В представленной публикации предложены реальные примеры курса «Обеспечение функциональной безопасности», разработанного и апробированного в 2022 г. в Университете ИТМО. Ключевыми факторами разработки курса были выбраны – неукоснительное соблюдение применимого законодательства и ориентация на объективную численную оценку безопасности (доверенных) компонент. Рассмотрены известные попытки применения недоверенных компонент, которые при настойчивом игнорировании «инженерной базы» приводят к серьезным инцидентам. Важное внимание уделяется объективному оцениванию «наложенных» средств защиты и известных методов оценки соответствия на основании действующего законодательства. Представляется целесообразным настоятельно рекомендовать усиление внимания к проблеме подготовки необходимого количества специалистов в технических ВУЗах и построения вертикальной «доверенной» системы компонент АСУТП в Российской Федерации. Полученные результаты могут быть применены при выполнении разработки и применения учебных программ по направлению обеспечения ФБ в современных условиях для обеспечения «цифрового суверенитета».

Ключевые факторы

Дефицит специалистов в области обеспечения ФБ в настоящее время стал признанной проблемой, для решения которой предпринимаются различные действия. В частности, в Университете ИТМО в 2022 г. был разработан и прошел практическую апробацию курс по ФБ (включает лекционные занятия, лабораторные и практические работы). Ключевыми факторами разработки курса по ФБ были выбраны в равной мере: неукоснительное соблюдение применимого законодательства (первый фактор) и ориентация на оценку безопасности (доверенных) компонент (второй фактор).

В отношении первого ключевого фактора можно отметить несколько фундаментальных законодательных норм Российской Федерации: Доктрина информационной безопасности[4] 2016 г., в которой обновлена концепция защиты информации, а также уточнено понятие «критическая информационная инфраструктура» (далее – КИИ), а также Федеральный закон от 26.07.2017 N 187-ФЗ[5] «О безопасности критической информационной инфраструктуры Российской Федерации» и Постановление Правительства РФ от 08.02.2018 N 127[6] «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Применительно к теме КИИ важно отметить Указ Президента Российской Федерации от 01.05.2022 №250[7] «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [1,2]. Непринятие мер по защите на объектах КИИ приводит к серьёзным инцидентам, известны примеры из различных отраслей (железнодорожный транспорт, управление воздушным движением, нефтепереработка, морские логистические комплексы и пр.) [3,4].

В отношении второго ключевого фактора важно принять во внимание, что, несмотря на указанные выше национальные нормативные документы, ФСТЭК[8] не рассматривает ПАЗ как фактор, снижа-

3 Функциональная безопасность, Часть 4. – [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/486614.php, свободный. Яз. рус. (дата обращения 07.04.2023)

4 Указ Президента Российской Федерации от 05.12.2016 г. № 646. – [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41460, свободный. Яз. рус. (дата обращения 07.04.2023)

5 Федеральный закон от 26.07.2017 №187. – [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/?ysclid=l8d73e934i5010228, свободный. Яз. рус. (дата обращения 07.04.2023)

6 Постановление Правительства РФ от 08.02.2018 N 127. – [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71876120/?ysclid=l8d75l1svw618900114, свободный. Яз. рус. (дата обращения 07.04.2023)

7 Указ Президента Российской Федерации от 01.05.2022 г. № 250. – [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/47796, свободный. Яз. рус. (дата обращения 07.04.2023)

8 https://step.ru/upload/pdf/87877a75035badbaed3ab8f792ea0ca5.pdf?ysclid=lbku7xqzi0829124745

ющий риск и не доверяет мерам предотвращения компьютерных инцидентов[9] (противоаварийная автоматика, предохранительные клапана и т.д.). В ряде публикаций приводятся примеры, когда ошибки в архитектуре ПО[10] (в частности, в сетевом протоколе), приводили к серьёзным проблемам, хотя в технической документации необходимые меры кибербезопасности были описаны. Более того, эксперты[11] обоснованно задают вопрос: «...что будет делать ФСТЭК, когда будет рассчитано, что внедрение систем безопасности против компьютерных атак понизило надежность системы в целом?». Из материалов ФСТЭК в 2022 г. «Справка-доклад о ходе работ по плану ТК 362 на 2022 год (по состоянию на 16.01.2023 г.) следует, цитата: «проводились работы по доработке окончательных редакций проектов национальных стандартов ГОСТ Р ИСО/МЭК 15408-1-20XX «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Это нужная инициатива, но, к сожалению, уже несколько лет в планах регуляторов в РФ не фигурируют специальные стандарты МЭК (IEC) серии 61508 и 61511, разработанные как раз для области обеспечения ФБ. Систематизация рассмотренной нормативной базы ставит своей целью не только анализ и критериальное сравнение применимых систем требований, но и создание единой инженерной базы, необходимой для эффективного обучения специалистов в области ФБ [5 – 9].

Аналитические данные по уязвимостям АСУТП

При разработке курса ФБ исходно были проанализированы несколько широко известных в отрасли стандартов в исторической ретроспективе, в том числе – один из первых нормативных документов FIPS 199 [10] (опубликованный в 2004 г.). Полезные материалы были взяты также из аналитического обзора «SCADA под прицелом: анализ защищенности АСУ ТП», опубликованного компанией НТЦ «Станкоинформзащита»[12] еще в 2011 г. Численные параметры для спецификации компонентов, входящих в состав АСУТП, могут быть определены через показатели надёжности MTTR, MTTF, MTBF, например:

- MTTR (*Mean Time To Repair*) – среднее время восстановления;
- MTTF (*Mean Time To Failure*) – среднее время работы устройства или системы до наступления отказа любого вида;
- MTBF (*Mean Time Between Failures*) – среднее время между двумя последовательными отказами.

При оценивании показателей надёжности систем диспетчеризации АСУТП предложено применять усреднённые показатели надёжности компонент различных производителей, например: при MTTR = 20 часов и MTBF = 60 000 часов (средний по отрасли для АСУТП), получаем: MTTF = MTBF – MTTR = 60 000 – 10 = 59 980 часов. Переходя на язык «девяток» можно оценить такой пример как 99,96%, что на современном уровне объективно считается крайне низким показателем. Например, введенный в декабре 2022 г. группой компаний Softline[13] новый ЦОД в г. Минск (Республика Беларусь) соответствует уровню Tier II+, обеспечивая SLA до 99,982%. Соответственно, важно показать на хорошем численном примере, насколько современные требования применительно к ФБ должны отличаться от требований к обычным офисным приложениям, и какая динамика наблюдается при оценке требований к ФБ компонент АСУТП за последние 10 лет. Важно объективно показать, что если некоторый компонент АСУТП действительно подвергнется длительному негативному воздействию, то управляемое оборудование (в терминах ГОСТ Р МЭК (IEC) серии 61508) может быть неработоспособно даже несколько дней. Даже в 2010 г. были известны серьёзные инциденты на инженерной инфраструктуре крупных компаний (Marathon Oil, ExxonMobil, ConocoPhillips, Deutsche Bahn и пр.), подробно описанные в технической литературе.

Для проведения обучения представляется важным показать «смещение рисков» в современных реалиях обеспечения ФБ. Например, в обзоре «Уязвимости в АСУ ТП: итоги 2018 года»[14] показано, сколько и каких конкретно уязвимостей обнаружено в компонентах

9 https://www.securitylab.ru/blog/personal/valerykomarov/350200.php

10 Сегодня АСУ ТП не защищают ни воздушный зазор, ни проприетарные протоколы. – [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/company/solarsecurity/347320.php, свободный. Яз. рус. (дата обращения 07.04.2023)

11 Публичная активность ФСТЭК в регионах. – [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/valerykomarov/351171.php, свободный. Яз. рус. (дата обращения 07.04.2023)

12 SCADA под прицелом: анализ защищенности АСУТП. – [Электронный ресурс]. – Режим доступа: https://xakep.ru/2011/08/09/56432/ свободный. Яз. рус. (дата обращения 07.04.2023)

13 Softline объявила о запуске нового ЦОДа в Белоруссии – [Электронный ресурс]. – Режим доступа: https://www.cnews.ru/news/line/2022-12-28_softline_obyavila_o_zapuske_novogo?yscli d=lc8x6gpppy316385500 свободный. Яз. рус. (дата обращения 07.04.2023)

14 Уязвимости в АСУ ТП: итоги 2018 года. – [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ics-vulnerabilities-2019/ свободный. Яз. рус. (дата обращения 07.04.2023)

АСУТП известных производителей (ABB, Hirschmann, Moxa, Schneider Electric, Siemens и пр.) При этом 14 из них присвоена критическая, а 11 — высокая степень риска на основе значения CVSS v3. Важно показать, что часто для получения актуальной версии «прошивки» с исправлением выявленных уязвимостей пользователи должны самостоятельно запросить ее у производителя. Следует принять во внимание, что указанные существенные ограничения в возможности получении новых «прошивок», фирменных «патчей» и иных «заплаток» со стороны какого-либо производителя, определенным образом критически влияют на степень безопасности отдельных компонент АСУТП. Следовательно, существенно деградируют показатели MTTR, MTTF и MTBF всего объекта КИИ в целом, что, в свою очередь, опосредованно влияет на степень устойчивости бизнес-процессов, как было показано ранее.

В процессе построения курса ФБ, важно обратить внимание на доступные и объективные данные статистики, согласно которым количество уязвимостей, выявляемых в оборудовании различных производителей, из года в год растет, а количество компонентов АСУТП, подключенных и доступных через потенциально недоверенную сеть интернет, не снижается. Является фактами, что среднее время устранения уязвимостей разработчиком остается достаточно долгим – более 6 месяцев, а иногда исправление отдельных уязвимостей занимает более 2 лет. Соответственно, для многих потребителей риск прерывания нормального функционирования «подотчетной» системы АСУТП повышается многократно, без выбора приемлемых по стоимости и по времени реализации вариантов [5 – 9].

В отчете 2020 г. «Встроенные функции АСУ ТП подвергают системы риску атак»[15] показано, что в 10 тыс. промышленных систем было обнаружено около 380 тыс. известных уязвимостей, в том числе связанных с выходными данными, ЧМИ (человеко-машинный интерфейс), использованием «вшитых» в программный код учетных данных и пр. В отчете 2022 г. «Уязвимость АСУ ТП. Как оценить критичность»[16] представлены данные по анализу выявленных командой Claroty (Team82) уязвимостях в продуктах Rockwell Automation. В частности, при оценке уязвимости CVE-2021-22681 (позволяет удалённому неаутентифицированному пользователю производить любые операции с контроллерами и ПАЗ), отмечено, что компания Rockwell Automation даже спустя 4,5 года не «закрыла» обнаруженную уязвимость, поскольку «корень» проблемы находится в архитектуре, на уровне протокола сетевого взаимодействия.

Анализ целесообразности применения «наложенных» мер защиты

Важным вопросом является оценка реальной безопасности предлагаемых «наложенных» мер защиты. В курсе ФБ настоятельно рекомендуется обратить внимание на возможность закрытия простых уязвимостей, например, по примерам, доступным на сайте ФСТЭК (https://bdu.fstec.ru/vul). Важно акцентировать внимание на существенные сложности с обработкой уязвимостей на уровне архитектуры защищаемой системы. Необходимо заложить четкую логическую структуру – каким именно признанным доверенным способом обеспечить гарантии отсутствия уязвимостей в самом «наложенном» средстве защиты? Не будет ли недоверенная система, защищаемая еще и недоверенной мерой защиты, еще более опасной в силу декларируемой, но реально мнимой оценки безопасности? До настоящего времени объективных ответов на данные вопросы не представлено, к сожалению [11].

Хорошим примером в учебном процессе может быть анализ атаки Stuxnet на урановые центрифуги. По данным публикации «Современные угрозы информационной безопасности АСУ ТП»[17] важно принять во внимание:

- вирус использовал 4 ранее неизвестных уязвимости ОС Microsoft Windows;
- вирус может заразить версию Windows, начиная с XP, как 32-разрядную, так и 64-разрядную;
- вирус позволяет заражать систему через USB, причём даже отключенном автозапуске;
- вирус умеет перепрограммировать PLC Simatic фирмы Siemens.

Для учебного курса важно сформировать восприятие и другой существенной неустранимой уязвимости – Siemens официально не рекомендует менять стандартные пароли на своих системах, так как «это может повлиять на работоспособность системы», а,

15 Встроенные функции АСУ ТП подвергают системы риску атак. – [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/504058.php?ysclid=lbd9j93qz2231439954 – свободный. Яз. рус. (дата обращения 07.04.2023)

16 Уязвимость АСУ ТП. Как оценить критичность. – [Электронный ресурс]. – Режим доступа: https://ics-cert.kaspersky.ru/publications/news/2022/04/20/vulnerability-in-ics-assessing-the-severity — свободный. Яз. рус. (дата обращения 07.04.2023)

17 Современные угрозы информационной безопасности АСУ ТП. – [Электронный ресурс]. – Режим доступа: https://club.cnews.ru/blogs/entry/kak_ne_obestochit_gorod_sovremennye_ugrozy_informatsionnoj_bezopasnosti_asu_tp?ysclid=lbdblatqil153931065 – свободный. Яз. рус. (дата обращения 07.04.2023)

соответственно, использование Stuxnet стандартных паролей гарантирует почти 100% успешных авторизаций. В этом примере уместно обратить внимание на принципиальную способность множества весьма дорогих «наложенных» мер защиты противодействовать таким угрозам – как можно блокировать такие пароли, если защищаемые системы выбрали вариант соответствия полученным официальных рекомендациям от иностранных поставщиков?

Рекомендуется рассмотреть кратко, какие решения предлагают различные компании в РФ в качестве «наложенных» мер защиты для обеспечения ФБ компонент АСУТП. Например, в докладе «Современные вызовы кибербезопасности для промышленных систем и построение эффективной защиты АСУ ТП»[18] представлено несколько доступных, по мнению авторов, решений в области обеспечения ФБ:

- Kaspersky Industrial CyberSecurity;
- MaxPatrol SIEM;
- Код безопасности – Secret Net Studio;
- PT Industrial Security Incident Manager;
- Программный комплекс «Аркан-М»;
- InfoWatch ARMA;
- ИнфоТеКС ViPNet Industrial Security;
- Dallas Lock 8.0.

Представляется необходимым обратить внимание на крайне широкий диапазон представленных решений – от «тяжелых» систем класса SIEM до простейших классических СЗИ НСД, заявленная способность которых реализовать «особый функционал» конкретно для обеспечения ФБ компонент АСУТП не выглядит абсолютно безупречной и достоверно обоснованной. Если сместить фокус аналитики на собственные публикации производителей, то общее впечатление о способности успешно обеспечить ФБ компонент АСУТП объективно становится еще более негативным. В подтверждение данного тезиса рассмотрим пример компании «Уральский Центр Систем Безопасности» — в докладе «Гибкий подход к обеспечению информационной безопасности АСУ ТП»[19] на слайде 8 указано явно, цитата: «При разработке АСУ ТП про ИБ не думали», а на слайде 18 указано, цитата: «Качественный аудит ИБ АСУ ТП позволит», что явно указывает на незнание инженерной базы – системных базовых требований стандарта IEC серии 61508 или аналогичного ГОСТ Р МЭК серии 61508 (подробно будет рассмотрено далее).

Проблема импортозамещения компонентов АСУТП

Далее рассмотрим весьма актуальную проблему импортозамещения. Рекомендуется рассмотреть в учебном курсе методы, как возможно оценить степень доверия некоторого определенного компонента АСУТП по сравнению с его аналогом? Предположим, доступ к оборудованию (поддержке, «патчам» безопасности и пр.) определенной страны более не может быть возможен, и, по определенным прогнозам, этот риск не будет успешно демпфирован в ближайшее время. Этот риск описан достаточно давно, и рекомендуемые компенсирующие меры достаточно подробно описаны в специальной литературе (например, доступен подробный анализ инцидентов с технической поддержкой HPE, Oracle, AutoCAD и пр.).

Что же следует предпринять: закупать опять иное иностранное оборудование (мнимое иностранное «импортозамещение») или действительно развивать собственный научно-практический потенциал и реализовать в обозримой перспективе действительно реальное импортозамещение и обеспечить гарантированный национальный «цифровой суверенитет» [12,13]? Рассмотрим в этой связи характерный пример: на сайте DFMC[20] предлагается китайское оборудование для управления производством угля, в том числе – системы MES. На сайте указано, цитата: «Система представляет собой комплексную платформу управления, интегрирующую мониторинг, статистику, планирование, измерения, тестирование, оборудование, безопасность и другие услуги». Для целей обучения важно, что не представлено никаких объективных данных, подтверждающих какую-либо (национальную и/или международную) оценку соответствия, в частности нет оценок SIL по IEC (ГОСТ Р МЭК) серии 61508. Аналогичный пример можно привести для другой компании из РФ, позиционирующей себя как инжиниринговый центр в области разработки и внедрения АСУТП. На сайте «Этаир Инжиниринг»[21] указан перечень программируемых контроллеров (Simatic,

18 Современные вызовы кибербезопасности для промышленных систем и построение эффективной защиты АСУ ТП. – [Электронный ресурс]. – Режим доступа: https://www.all-over-ip.ru/hubfs/AoIP%20ADAPT/AoIP_4-12-2020_%D0%95%D1%80%D1%8B%D1%88%D0%BE%D0%B2.pdf?hsLang=ru – свободный. Яз. рус. (дата обращения 07.04.2023)

19 Гибкий подход к обеспечению информационной безопасности АСУ ТП. – [Электронный ресурс]. – Режим доступа: https://www.pta-expo.ru/ural/documents/%D0%9A%D0%BE%D0%BC%D0%B0%D1%80%D0%BE%D0%B2%20%D0%90.%D0%92..pdf?ysclid=lbdbpvvsg290401843 . – свободный. Яз. рус. (дата обращения 07.04.2023)

20 DFMC. – [Электронный ресурс]. – Режим доступа: — https://ru.dfmc.cc/ – свободный. Яз. рус. (дата обращения 07.04.2023)

21 Этаир Инжиниринг – [Электронный ресурс]. – Режим доступа https://etair.ru/uslugy/, – свободный. Яз. рус. (дата обращения 07.04.2023)

ControlLogix, Modicon TSX Quantum, и т.д.), которые используют конкретные промышленные сети (Profibus, CANbus). Несмотря на то, что компания работает в РФ, на сайте также недоступны объективные данные, подтверждающие какую-либо (национальную и/или международную) оценку соответствия, в частности, также нет оценок SIL.

Можно привести и другие примеры, которые показывают, что полной оценкой безопасности компонентов АСУТП занимаются, к сожалению, не производители и не инжиниринговые компании (внедренцы), а только специальные компании, например, ITGlobal[22]. Именно специализированные компании принимают во внимание базовые системные инженерные требования к кибербезопасности АСУТП: Приказ ФСТЭК № 31 от 14 марта 2014 г. и международный стандарт IEC 62443. Соответственно, выводы аудита специализированных компаний позволяют объективно повысить безопасность и получить оценку соответствия требованиям Российских и международных стандартов. Даже при условии, что специализированные компании стараются исследовать доступные решения АСУТП с точки зрения ФБ, нет полной гарантии, что будет проведено полное «покрытие» при тестировании всех доступных компонент всех возможных производителей. Этот остаточный риск крайне важно учесть в процессе обучения студентов технических ВУЗов.

Необходимая нормативная база для оценки компонентов АСУТП

С учетом ранее приведенных фактов, известных инцидентов, примеров «наложенных» решений, требований учебно-методического комплекса и пр., представляется логичным обратиться к нормативной базе, которая содержит требования для оценки безопасности [14 – 17]. Принято полагать, что семейство стандартов IEC 61508 «Functional safety of electrical/electronic/programmable electronic safety-related systems» является необходимой базой как в качестве словаря, системы требований, критериев для оценки уровня полноты безопасности (УПБ или SIL). Весьма примечательно, что эти стандарты выпущены в 2010 г., в 2012 г. приняты в национальной системе ГОСТ Р МЭК серии 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью». Далее представлены наиболее важные требования (фрагмент) из стандартов ГОСТ Р МЭК серии 51608 применительно для курса обеспечения ФБ компонентов АСУТП (см. Табл. 1). Наиболее важные требования выделены особо.

Практическая часть курса ФБ

Важной частью курса ФБ, разработанного в Университете ИТМО, является блок практических занятий. Всего в курсе запланировано 4 практических занятия, успешная апробация которых выполнена в 2021/2022 учебном году. Далее будут кратко рассмотрены некоторые примеры каждого практического занятия (что рассматривалось, что определялось и что рассчитывалось) в рекомендованной последовательности их выполнения.

Первое практическое занятие

На первом практическом занятии определяется объект исследования – управляемое оборудование (в терминах ГОСТ Р МЭК серии 61508) и система АСУТП. В качестве примера выбран навигационный модуль железнодорожного локомотива (далее – Модуль). Пример структурной схемы аппаратной части модуля приведен на рис. 1.

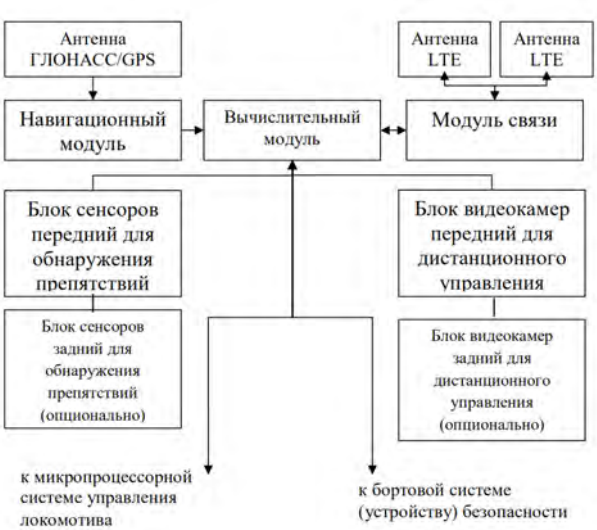

Рис.1. – Структурная схема аппаратной части (пример)

Далее определяется основной функционал модуля, например:

- Ф1: определение расстояния от локомотива до препятствия или светофора;
- Ф2: определение зоны местонахождения препятствия относительно пути следования по ходу движения в красной и желтой зонах;
- Ф3: обнаружение на расстоянии человека;

22 Зачем и как проводить пентест АСУ ТП. – Режим доступа: — https://itglobal.com/ru-ru/company/blog/zachem-i-kak-provodit-pentest-asu-tp/ – свободный. Яз. рус. (дата обращения 07.04.2023)

Таблица 1

Требования ГОСТ МЭК серии 61508 (фрагмент)

Стандарт	Требования
51608-1	Устанавливает нижнюю границу для целевых мер отказов для функции безопасности в режиме: — низкой интенсивности запросов на обслуживание: нижняя граница для выполнения функции, для которой система предназначена, устанавливается в соответствии со средней вероятностью опасного отказа по запросу, равной $\mathbf{10^{-5}}$; — высокой интенсивности запросов на обслуживание или в непрерывном режиме: нижняя граница устанавливается в соответствии со средней частотой опасных отказов $\mathbf{10^{-9}}$ в час.
	Должны быть определены требования к периодическому аудиту ФБ
	— Соответствие компетентности должно рассматриваться для конкретной области применения с учетом всех факторов, включая инженерные знания: — соответствующие области применения и технологии; — в области безопасности, соответствующие применяемой технологии; — законодательной базы и нормативно-правовой базы в области безопасности
61508-2	— Требования по управлению систематическими сбоями — к любым остаточным ошибкам проектирования аппаратных средств, если вероятность ошибок проектирования аппаратных средств не может быть исключена; — внешним влияниям, включая электромагнитные воздействия; — ошибкам оператора управляемого оборудования
	Поставщик должен документально обосновать всю информацию, которая представлена в каждом руководстве по безопасности для применяемых изделий. — Могут существовать коммерческие или юридические ограничения на доступность доказательств. Если такие ограничения не обеспечивают необходимого доступа к доказательствам оценки ФБ, то такой элемент в системах, связанных с безопасностью, не используется.
	Рекомендации по предотвращению ошибок при подтверждении соответствия безопасности (по УБП) – **испытания в наихудших случаях**
61508-3	Причины появления запроса на модификацию могут быть, например, связаны: — накопленным опытом о систематических отказах; — появлением нового или изменением действующего законодательства, относящегося к безопасности; — анализом характеристик эксплуатации и технического обслуживания, который показывает, что эти характеристики имеют значения ниже запланированных; — текущим аудитом систем ФБ
61508-4	**безопасность** (safety): Отсутствие неприемлемого риска
	случайный отказ аппаратных средств (random hardware failure): Отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик в аппаратных средствах.
	систематический отказ (systematic failure): Отказ, связанный детерминированным образом с какой-либо причиной, которая может быть исключена только путем модификации проекта либо производственного процесса, операций, документации, либо других факторов.
	аудит функциональной безопасности (functional safety audit): Систематическое и независимое исследование, проводящееся с тем, чтобы определить, насколько эффективно реализованы процедуры, предназначенные для согласования требований к ФБ с запланированными мероприятиями и определения, насколько они пригодны для достижения поставленных целей.

Стандарт	Требования
61508-5	Разработка целостной модели (как описано в ИСО/МЭК 31010) Концепция ALARP (как описано в ИСО/МЭК 31010)
61508-7	— Расширенное функциональное тестирование — **Испытания в наихудших случаях** — Испытания с введением неисправностей
	Программный элемент считается **проверенным в эксплуатации**, если он соответствует следующим критериям: — продолжительность эксплуатации соответствует уровню полноты безопасности или соответствующему числу запросов; для демонстрации частоты отказов, не связанных с безопасностью, менее: — **10^{-2}** на один запрос (в год) с 95%-ным уровнем доверия необходимо 300 эксплуатационных прохождений (в год); — **10^{-5}** на один запрос (в год) с 99,9%-ным уровнем доверия необходимо 690.000 эксплуатационных прохождений (в год).

— Ф4: обнаружение на расстоянии крупного статического объекта;
— Ф5: обнаружение на расстоянии малого статического объекта;
— Ф6: определения факта сцепки/расцепки с подвижным составом;
— Ф7: контроль наличия сцепки с подвижным составом.

Второе практическое занятие

На втором практическом занятии описываются риски (в нашем примере – для модуля). Вводится понятие «опасного отказа» — отсутствие корректной реакции локомотива при возникновении препятствия или дефекта инфраструктуры (в терминах ГОСТ Р МЭК серии 61508). Вводятся классы объектов (в примере – вагоны, светофоры, не классифицируемые объекты определенного размера (маленький, средний и большой).

Определяется концепция обеспечения безопасности:
— баланс между пропуском препятствия и ложным обнаружением настроен так, что вероятность пропуска препятствия существенно ниже вероятности ложного обнаружения;
— одиночный отказ или последовательность отказов, которые в совокупности с другими отказами могут приводить к опасному отказу, должны обнаруживаться с заданной вероятностью до наступления опасного отказа.

Определяются основные принципы для реализации концепции обеспечения безопасности модуля, например:
— использование не менее двух сенсоров для обнаружения препятствий во всех зонах (дальняя зона и мертвая зона);
— принятие решения о препятствии при накоплении данных за время от 300 мс до 500 мс в зависимости от дальности до препятствия;
— использование дублирования каналов обработки данных (CAN и RS232)
— использование резервирования камер дальней зоны;
— организация кольцевой топологии сети в блоке вычислителей;
— использование аппаратного контроля работоспособности блока вычислителей через воздействие на электро-пневмо клапан.

Определяются искажения, отнесённые к опасным последствиям, например:
— передача информации об отсутствии препятствия при фактическом наличии с достоверностью не менее 90%;
— передача информации о дальности до препятствия с погрешностью более 20%;
— ошибка определения зоны местонахождения препятствия: передача о «желтой» зоне, когда фактически «красная» зона.

Третье практическое занятие

На третьем практическом занятии описываются меры ФБ, например: уровень безопасности модуля в условиях и режимах эксплуатации должен характеризоваться следующими показателями:

— интенсивность опасных отказов программно-аппаратных средств модуля должна быть не более 10^{-6} 1/ч в течение заданного срока службы во всех условиях и режимах работы при обязательном выполнении технического обслуживания и ремонта, установленных в технической документации.

Далее определяются требования к полноте безопасности, которая состоит из двух составляющих:

— полнота безопасности аппаратных средств;

— систематическая полнота безопасности.

На практическом занятии рассматривается, что первая составляющая полноты безопасности связана со случайными опасными отказами аппаратных средств. Для данного случая факт достижения УПБ оценивается при помощи расчета вероятности наступления такого события, пользуясь показателями отказоустойчивости исследуемой системы.

Для второй составляющей исследуются систематические отказы в работе модуля (например, ошибки при проектировании). Такие ошибки сложно предсказать, поэтому важно минимизировать риск их возникновения. При взаимодействии модуля с управляемым оборудованием необходимо выполнять ряд мероприятий (применить несколько методов), которые контролируют правильность этого взаимодействия (см. табл. 2).

Далее определяются опасности, контрольные функции и действия при отказе (см. табл. 3).

Важно показать, что УПБ определяется, как обобщающий показатель безопасности, определяющий необходимую степень уверенности в том, что объект будет выполнять заданные функции безопасности. УПБ включает в себя значение количественного целевого показателя безопасности и комплекс мероприятий, осуществляемых для достижения полноты безопасности в отношении систематических отказов.

Необходимо показать на практике, как важно определить порядок верификации и валидации требований ФБ, которые оформляются в виде формальных процедур. Эти процедуры должны проводиться в обязательном порядке в соответствии с планом и повторяются при последующей модификации модуля.

Таблица 2

Мероприятия и методы контроля выполнения функций модуля (фрагмент)

Функция системы	Контроль правильности исполнения	Действия при возникновении отказа
Ф1, Ф2, Ф3,Ф4, Ф5	По картинке и лидарным данным	Немедленная остановка
Ф6	Если от БОПМЛ нет данных, то произошла расцепка	Немедленная остановка
Ф7	По картинке и лидарным данным	Немедленная остановка

Таблица 3

Основные опасности и действия при отказе (фрагмент)

Опасность	Контрольные функции	Действия при отказе
Ошибка детектирования на расстоянии обнаружения объекта	Функция контроля наличия статических препятствий, определенных по цифровой модели пути (система позиционирования)	Отправление команды на торможение до полной остановки и отправление запроса на переход в дистанционное управление (допускается однократное срабатывание контрольной функции)
Ошибка определения зоны нахождения объекта относительно путей следования	1. Функция контроля наличия статических препятствий, определенных по цифровой модели пути (качественная оценка определения координат объекта) 2. Функция контроля погрешности определения пути по данным цифровой модели пути (система позиционирования)	Отправление команды на торможение до полной остановки и отправление запроса на переход в дистанционное управление (допускается однократное срабатывание контрольной функции)

Состав документов для доказательства безопасности должен быть представлен в орган по сертификации для независимого подтверждения заявленного УПБ.

Четвертое практическое занятие

На четвертом практическом занятии выполняется расчет УПБ. В соответствии с требованиями стандартов МЭК серии 61508 определяется средняя вероятность отказа по запросу (PVD_{AVD} – Average Probability of failure on demand). Для ПАЗ необходимо выбирать схему с резервированием (например, архитектуру 1oo2). Для данного примера формула расчета PFD_{AVG}:

$$PFD_{AVG} \approx \frac{\lambda_{DU,1}\,\lambda_{DU,2}\,([1-\beta]T)^2}{3} + \frac{\beta\,\lambda_{DU}^{min}T}{2}$$

где:

PVD_{AVD} – средняя вероятность отказа по запросу (*Average Probability of failure on demand*);

$\lambda_{DU,1}$ – частота опасных необнаруживаемых отказов в элементе *n (Dangerous undetected failure rate of item n);*

λ_{DU}^{min} – наименьшая частота из всех опасных необнаруживаемых отказов *(Smallest of all dangerous undetected failure rate);*

T – Время, необходимое для проведения тестов (*Test period*);

β – Общая причина, β-фактор (*Common cause factor*).

Для определения β-факторов применяют приложение D стандарта IEC (ГОСТ Р МЭК) 61508, в конкретном примере β = 0,5%. Примеры расчета PFD_{AVG} некоторых компонент модуля показаны соответственно на рис. 2 и рис. 3.

Тогда PFDavg = 4.84E-4, что соответствует УПБ 3 (см. рис.4).

Особо ценно, что студенты учатся получать на практике навык расчета показателей надежности ПАЗ с учетом отказов типа «несрабатывание». Стандарты ГОСТ Р МЭК серии 61508 описывают методы оценки и устанавливают количественные требования к показателям ФБ – PFDavg для соответствия необходимому, полученному на основе анализа риска, уровню полноты безопасности (УПБ, SIL). Необходимо объективно признать, что разработанные методики

Подсистема датчиков			
Архитектура		1oo2	
Частота необнаруженных отказов	$\lambda_{DU,1}$	4,00E-05	/h
Фактор общей причины	β	0,5	%
Испытательный период	T	0,5	years
Покрытие для пробных испытаний	PTC	100	%
Продолжительность жизни	LT	10	years
Average PFD	PFD_{avg}	4,38E-04	

Рис.2. Пример расчета PFD_{AVG} для подсистемы датчиков

Подсистема исполнительных элементов			
Архитектура		1oo2	
Частота необнаруженных отказов	$\lambda_{DU,1}$	4,00E-07	/h
Фактор общей причины	β	0,5	%
Испытательный период	T	0,5	years
Покрытие для пробных испытаний	PTC	95	%
Продолжительность жизни	LT	10	years
Average PFD	PFD_{avg}	8,54E-06	

Рис.3. Пример расчета PFD_{AVG} для подсистемы исполнительных механизмов

Total PFD		
Подсистема датчиков	4,38E-04	
Логическая подсистема	1,18E-06	
Подсистема исполнительных элементов	8,54E-06	+
Total PFD_{avg}	4,48E-04	→ SIL 3

Рис.4. Общая оценка УПБ

оценки и нормирование показателей надежности ПАЗ с учетом отказов типа «ложное срабатывание» в настоящее время отсутствуют, поскольку производители не публикуют полные достоверные инженерный расчеты. Это должно быть учтено в практических работах в рамках учебного курса как важное граничное условие. Общей проблемой для расчетов надежности ПАЗ как с учетом отказов типа «несрабатывание», так и отказов типа «ложное срабатывание», является отсутствие достоверных справочных данных по надежности компонентов, которые могут быть использованы в учебных целях при реализации программ обучения, связанных в ФБ.

Практика показала, что риск-ориентированный подход требует наличия системы управления рисками, например, на базе национальных стандартов ГОСТ Р ИСО/МЭК серии 31010 или 27005. Основной задачей управления рисками (остаточными рисками) является повышение надежности и безопасности объектов КИИ на базе достоверных и исходных данных, при этом в связи с ростом количества АСУТП, задача обеспечения ФБ на заданном уровне приобретает важную роль.

Выводы

1. Как показывает аналитика, за прошедшие десятилетия существенных изменений в области обеспечения функциональной безопасности компонентов АСУТП не произошло – проблема сохраняет свою актуальность и высокую значимость. Практически не представлены достоверные и объективные расчеты экономической целесообразности применения рекомендуемых «наложенных» мер защиты, объективно наблюдаются существенные ограничения при оценке данных от производителей;

2. В учебном процессе предлагается обеспечить неукоснительное соблюдение известных инженерных принципов, дополненное контролируемой государственной экспертизой для обеспечения заданного уровня безопасности компонентов АСУТП, что позволит реализовать необходимый «цифровой суверенитет» в РФ. Известные попытки внедрять недоверенное «импортозамещение» без надлежащей объективной государственной экспертизы не смогут решить поставленную задачу именно в силу игнорирования «инженерной базы».

3. Представляется целесообразным рекомендовать настоятельно усиление внимание к неукоснительному соблюдению фундаментальных инженерных требований обеспечения функциональной безопасности, включая подготовку необходимого количества специалистов в технических ВУЗах и построения вертикальной национальной системы «доверенных» компонент АСУТП на объектах КИИ в РФ.

Литература

1. Смирнов Е.В. Методика оценки политической значимости угроз объекту критической информационной инфраструктуры на примере объекта инфокоммуникаций // Право. 2020. – №2. – С. 49-56.
2. Новикова Е.Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. – № 4. – С. 127-135.
3. Щелкин К.Е., Звягинцева П.А., Селифанов В.В. Возможные подходы к категорированию объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2019. – Т. 6. – С.128-133 №. 1. DOI: 10.33764/2618-981X-2019-6-1-128-133.
4. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Принципы и задачи асимптотического управления безопасностью критических информационных инфраструктур // Информатика, 2019. № 12. С. 29-35. DOI 10.24411/2072-8735-2018-10330
5. Герасимова К.С., Михайлова У.В., Баранкова И.И. Разработка ПО для оптимизации категорирования объектов критической информационной инфраструктуры // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2 (44). – С. 30-36.

6. Наталичев Р.В., Горбатов В.С., Гавдан Г.П., Дураковский А.П. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры // Безопасность информационных технологий. – 2021. – Т. 28. – № 3. – С. 6-27.
7. Соловьев С.В., Тарелкин М.А., Текунов В.В., Язов Ю.К. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах // Вопросы кибербезопасности. – 2023. – № 1 (53). – С. 41-57.
8. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. – 2018. – № 4 (28). – С. 9-20.
9. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности. – 2019. – № 3 (31). – С. 63-71.
10. Alan C. NIST Cybersecurity Framework: A Pocket Guide // Ely, Cambridgeshire, United Kingdom:ITGP. 2018.
11. Гордейчик С.В. «Миссиоцентрический подход к кибербезопасности АСУ ТП» // Вопросы кибербезопасности №2(10) – 2015. – Стр. 56 – 59
12. Лившиц И.И., Неклюдов А.В. Суверенные информационный технологии России // Стандарты и качество. – 2018. – № 4. – С. 68-72
13. Лившиц И.И., Неклюдов А.В. Суверенные информационный технологии России. Окончание // Стандарты и качество. – 2018. – № 5. – С. 66-70
14. Лившиц И.И. К вопросу управления уязвимостями в компонентах АСУТП // Автоматизация в промышленности. – 2022. – № 8. – С. 12-16.
15. Лившиц И.И. К вопросу оценивания безопасности промышленных систем управления // Автоматизация в промышленности. – 2021. – № 7. – С. 3-7.
16. Лившиц И.И. Исследование оценок защищенности промышленных систем // Автоматизация в промышленности. – 2020. – № 12. – С. 13-18.
17. Лившиц И.И., Зайцева А.А. Проблемы обеспечения безопасности облачной компоненты информационных технологий // Автоматизация в промышленности. – 2019. – № 7. – С. 10-16.

PRACTICAL TRAINING IN THE FIELD OF FUNCTIONAL SAFETY AT ITMO UNIVERSITY

Livshitz I.I.[23], Perlak P.V.[24]

Abstract

The purpose of the study: *development and practical testing of a new training program in the field of functional safety for technical universities. An important feature of this goal is the independence of its solution from the specific area of operation of complex industrial facilities. The task is to apply a unified engineering approach for training in the field of functional safety – both in the theoretical and in the practical (computational) part.*

Research methods: *system analysis, analytical modeling methods, statistical methods, comparison methods and practical testing methods.*

The result obtained: *the requirements for the creation and evaluation of components from the point of view of functional safety are investigated. A review of the domestic and world scientific literature over the past 10 years and a brief analysis of existing solutions for evaluating components from the point of view of functional safety are made. The structure of the new training course is proposed, the main parts are briefly described – theoretical (lecture) and computational (practical). The generalized procedures for assessing the functional safety of various components are described, as well as the results of their testing in the ITMO University training course in the 2022/2023 academic year.*

The scientific novelty *lies in the systematization and a fairly extensive review of applicable regulatory and methodological documents (GOST R, ISO and IEC) over the past ten years devoted to the assessment of the functional safety of components. A new course for students of technical universities has been proposed, which equally combines practical and theoretical knowledge, has passed a full cycle of approbation.*

Keywords: *automated control system, import substitution, risks, residual risks, audit, conformity assessment, digital sovereignty.*

23 Ilya I. Livshitz, Dr.Sc., Professor of FBIT Faculty, ITMO University, St.Peterburg, Russia. E-mail: Livshitz.il@yandex.ru

24 Pavel V. Perlak, Postgraduate student of FBIT, ITMO University, St.Peterburg, Russia. E-mail: ntn_isun@mail.ru