ФОРМИРОВАНИЕ СИСТЕМАТИЗАЦИРОВАННОГО ПЕРЕЧНЯ ТРЕБОВАНИЙ К ПРОВЕДЕНИЮ ИСПЫТАНИЙ АСУ ТП В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кемкин В.В., Сахаров К.В., Кузнецова Ю.А., Дорошенко Б.А., Салов И.В., Черняев А.Н.

Национальный Исследовательский Университет «Московский Энергетический Институт», Россия, г. Москва ул. Красноказарменная д.14,
Акционерное Общество «Русатом Автоматизированные Системы Управления» Россия, г. Москва, Каширское ш., корп. 2, стр. 16

KemkinVV@mpei.ru, SaharovKV@mpei.ru, KuznetsovYulAl@mpei.ru, b19902110@yandex.ru, SalovIV@mpei.ru, ChernyaevAN@mpei.ru

Аннотация: в докладе рассматривается существующая нормативно-техническая документация, содержащая в себе данные о требованиях к испытаниям информационной безопасности АСУ ТП АЭС, анализируются критерии систематизации этих требований. Результатом работы является создание систематизированного перечня требований к испытаниям АСУ ТП АЭС в области информационной безопасности.

Ключевые слова: информационная безопасность, информационная безопасность, кибербезопасность комппьютерная безопасность, АСУ ТП, испытания, программное обеспечение.

Введение

В новой энергетической стратегии Российской Федерации на период до 2035 г. [1] основной целью установлена цифровизация энергетики, являющаяся фактором, максимально содействующим динамичному социально-экономическому развитию и обеспечению национальной безопасности Российской Федерации. В связи с развитием новых цифровых и компьютерных технологий особенно остро встаёт вопрос информационной безопасности (ИБ) объектов энергетики, в частности автоматизированных систем управления технологическими процессами атомных электростанций (АСУ ТП АЭС) - критически важной инфраструктуры (КИИ) для экологической, техногенной и национальной безопасности РФ.

Одним из способов определения уровня информационной безопасности является проведение испытаний подсистем АСУ ТП в части информационной безопасности для разрабатываемых и уже существующих систем.

Согласно ГОСТ 34.603-92 [2] проведение испытаний автоматизированных систем (АС) включает в себя:

- предварительные испытания;
- опытную эксплуатацию;
- приёмочные испытания.

Как правило подсистемы АСУ ТП включают в себя большое количество аппаратных, программных и программно-аппаратных средств, имеющих свои технологические особенности и известные и не выявленные уязвимости. Этот факт устанавливает необходимость в системном подходе к проведению испытаний АСУ ТП в части ИБ для определения и контроля выполнения всех установленных требований к защите информации.

Систематизация информации о требованиях к проведению испытаний ИБ АСУ ТП необходима для разработки программного обеспечения, предназначенного для формирования программ и методик испытаний АСУ ТП в части ИБ.

1 Источники данных о требованиях об испытаниях ИБ АСУ ТП

Следует выделить следующие группы документов, содержащих в себе требования к проведению испытаний в части обеспечения информационной безопасности АСУ ТП:

- государственные стандарты и иные нормативно-правовые документы РФ,
- отраслевые стандарты в сфере атомной энергетики,
- международные стандарты и рекомендации,
- зарубежные государственные стандарты.

1.1 Российские источники данных, регулирующие информационную безопасность АСУ ТП

Правительством Российской Федерации приняты следующие федеральные законы:

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3] ;
2. Федеральный закон от 22 декабря 2020 г. N 184-ФЗ «О техническом регулировании» [4].
3. На территории России и СНГ в рамках стандартизации и технического регулирования в соответствии с [4] применяются следующие межгосударственные стандарты:
4. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы;
5. ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем;
6. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
7. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности;
8. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности;
9. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении;
10. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство;
11. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
12. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний;
13. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
14. ГОСТ Р МЭК 60880-2010 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А;
15. ГОСТ Р МЭК 62138-2011. Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С;
16. ГОСТ Р МЭК 62566-2012 Атомные станции. Контроль и управление, важные для безопасности. Использование программируемых интегральных схем для применения в системах, выполняющих функции категории А.
17. Федеральным органом исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области информационной безопасности АСУ ТП является Федеральная служба по техническому и экспортному контролю (ФСТЭК России), выпускающая приказы и методические документы в сфере информационной безопасности:
18. Приказ Федеральной службы по техническому и экспортному контролю России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
19. Приказ Федеральной службы по техническому и экспортному контролю России от 14 марта 2014 г. № 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды";
20. Приказ Федеральной службы по техническому и экспортному контролю России от 21 декабря 2017 г. №235 «Об утверждении Требований к созданию систем безопасности

значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

21. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» утвержденные приказом Федеральной службы по техническому и экспортному контролю России от 2 июня 2020 г. №76.

1.2 Отраслевые стандарты атомной энергетики

В Российской Федерации организацией, задающей отраслевые требования к ИБ АСУ ТП АЭС, оператором АЭС является компания-оператор АЭС АО «Концерн Росэнергоатом». В сфере информационной безопасности АСУ ТП данная организация применяет следующий стандарт:

1. Стандарт АО «Концерн Росэнергоатом» СТО 1.1.1.04.001.1447-2020 «Обеспечение безопасности систем контроля и управления атомных станций в отношении компьютерных атак».

Международное агентство по атомной энергии (сокр. МАгАтЭ; англ. International Atomic Energy Agency, сокр. IAEA) – международная организация развития сотрудничества в сфере атомной энергетики. Деятельность данной организации направлена на повышение эксплуатационной безопасности АЭС за счёт обмена опытом эксплуатации, накопленным в мире, и выпуска руководств и иных документов в сфере инжиниринга и эксплуатации АЭС в целом, и ИБ АСУ ТП в частности. В контексте АСУ ТП в МАГАТЭ в качестве аналога термина «информационная безопасность» используется термин «компьютерная безопасность». В настоящей работе рассматриваются следующие документы МАГАТЭ:

2. IAEA Nuclear Security Series №17 “Technical Guidance – Computer Security at Nuclear Facilities – Reference Manual“;
3. IAEA Nuclear Security Series №33-T “Technical Guidance – Computer Security of Instrumentation and Control Systems at Nuclear Facilities“;
4. NST 047 “Computer Security Methods for Nuclear Facilities”;
5. NST 045 “Computer Security For Nuclear Security”;
6. TDL-006 “Conducting Computer Security Assessments at Nuclear Facilities“;
7. SSG-39 “Design of Instrumentation and Control Systems for Nuclear Power Plants”.

1.3 Документы МЭК

Международная электротехническая комиссия (сокр. МЭК; англ. International Electrotechnical Commission, сокр. IEC) - международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий. Необходимо отметить, что МЭК в некоторых стандартах применяет термин «кибербезопасность» в качестве аналога термина «информационная безопасность» в контексте АСУ ТП. В настоящей работе рассматриваются следующие документы МЭК:

1. IEC 62645:2019 “Nuclear power plants Instrumentation, control and electrical power systems - Cybersecurity requirements”;
2. IEC 62859:2016 “Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity“;
3. IEC 63096:2020 “Nuclear power plants - Instrumentation and control systems – Security Controls “;
4. ISO/IEC 27001:2013 “Information technology - Security techniques - Information security management systems – Requirements";
5. IEC/TS 62443-1-1:2009 “Industrial communication networks - Network and system security - Part 1- 1 : terminology, concepts and models”;
6. IEC/TS 62443-2-1:2010 “Industrial communication networks - Network and system security - Part 2- 1 : establishing an industrial automation and control system security program”;
7. IEC/TS 62443-3-3:2013 “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels“.

1.3 Документы зарубежных организаций

1. NIST SP 800-82 Rev.2 "Guide to Industrial Control Systems (ICS) Security";
2. RG 5.71 “Cyber security programs for nuclear facilities”.

2 Систематизация требований

Первым критерием систематизации установлена обязательность соответствия подсистем АСУ ТП выделенному требованию:

- требование к испытанию обязательно к исполнению;
- требование к испытанию носит рекомендательный характер.

Вторым критерием для систематизации может являться применимость требований к этапам испытаний автоматизированных систем в защищённом исполнении (АСЗИ) из ГОСТ Р 51583-2014:

- предварительные испытания системы ЗИ АСЗИ;
- опытная эксплуатация и доработка системы ЗИ АСЗИ;
- приемочные испытания системы ЗИ АСЗИ;
- аттестацию АСЗИ на соответствие требованиям безопасности информации.

Третьим критерием систематизации является применимость требований к испытаниям в части ИБ к типам испытуемого компонентов подсистем АСУ ТП. В АСУ ТП существуют следующие типы оборудования:

- аппаратные средства;
- программные средства;
- программно-аппаратные средства.

Четвертым критерием систематизации является применимость технических средств проведения испытаний для проверки реализации требований к ИБ АСУ ТП. В частности, соответствие требованиям может проверяться с помощью:

- антивирусного программного обеспечения;
- симуляторов атак отказа в обслуживании;
- анализаторов уязвимостей;
- средств тестирования программного обеспечения.

Заключение

В процессе исследования были собраны требования нормативно-технической документации в части обеспечения информационной безопасности АСУ ТП АЭС, результатами проведенной работы можно считать:

1. Перечень источников данных о требованиях к испытаниям информационной безопасности АСУ ТП АЭС;
2. Систематизированный перечень требований к испытаниям АСУ ТП АЭС в области информационной безопасности.

Результаты данной работы в дальнейшем будут использованы при разработке методик проверок и испытаний АСУ ТП в части информационной безопасности.

Работа выполнена в рамках проекта «Оценка защищенности АСУ ТП от компьютерных атак» на реализацию программ научных исследований «Энергетика», «Электроника, радиотехника и IT» и «Технологии индустрии 4.0 для промышленности и робототехника» в 2020-2022 гг.

Литература

1. *Распоряжение Правительства Российской Федерации от 09.06.2020 № 1523-р* «Об Энергетической стратегии РФ на период до 2035 г.».
2. *ГОСТ 34.603-92* Информационная технология. Виды испытаний автоматизированных систем.
3. *Федеральный закон от 26 июля 2017 г. N 187-ФЗ* «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Федеральный закон от 22 декабря 2020 г. N 184-ФЗ «О техническом регулировании».