DOI: 10.25728/mlsd.2022.0139

ОЦЕНКА РИСКА И ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

Промыслов В.Г., Абдулова Е.А., Жарко Е.Ф., Исхаков А.Ю., Мещеряков Р.В., Полетыкин А.Г., Семенков К.В.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва ул. Профсоюзная д.65
vp@ipu.ru, consoft@ipu.ru, zharko@ipu.ru, iay@ipu.ru, mvr@ipu.ru, poletik@ipu.ru, semenkovk@ipu.ru

Акимов Н.Н., Голубев П.А., Лепехин И.Ю.

Филиал РФЯЦ-ВНИИЭФ "НИИИС им. Ю.Е. Седакова" Нижний Новгород, Бокс № 486
nakimov@niiis.nnov.ru, ilepehin@niiis.nnov.ru, pgolubev@niiis.nnov.ru

Аннотация: В работе рассматривается проблема оценки риска кибербезопасности для систем управления технологическими процессами (АСУ ТП) критически важных объектов. На примере АСУ ТП атомных электростанций рассматривается внутренний и внешний контекст оценки риска. Приводиться две методики: для этапа жизненного цикла разработки и этапа эксплуатации АСУ ТП.

Ключевые слова: АСУ ТП, АЭС, кибербезопасность.

Введение

Проблема обеспечения безопасности промышленных систем является комплексной. В полной мере это проявляется при рассмотрении безопасности атомной электростанции (АЭС). Безопасность АЭС тесно связана с обеспечением промышленной (в том числе, ядерной и радиационной) безопасности [1,2,3], а из-за высокой компьютеризации автоматизированной системы управления технологическим процессом (АСУ ТП) АЭС и с обеспечением информационной безопасности (ИБ) [4,5,6].

ИБ может рассматриваться в широком контексте. Информационная безопасность, помимо технических и организационных аспектов, человеческих факторов и социальных вопросов, затрагивает сферы национальной и международной безопасности. В настоящей работе основное внимание будет уделено методическим и техническим аспектам защиты информации и системы ее обработки, поэтому в большинстве случаев вместо информационной безопасности будет использоваться более подходящий термин кибербезопасность (КБ), который делает акцент на технические и методические вопросы информационной безопасности.

В международной практике атомной промышленности для выделения кибербезопасности из информационной безопасности принята модель МАГАТЭ [7] показанная на Рис. 1.

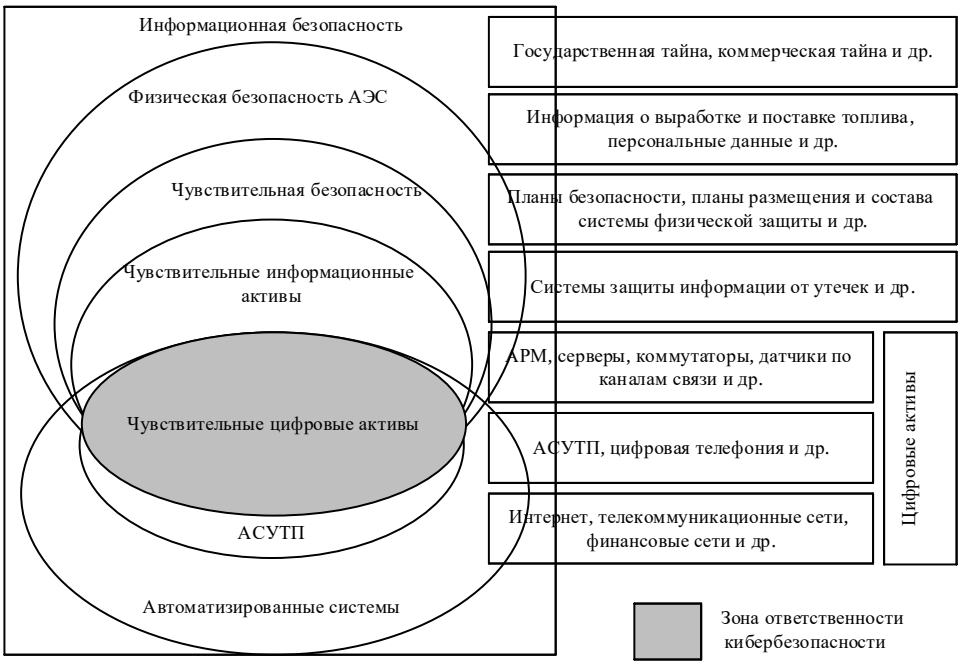

Рис. 1. Кибербезопасность в контексте безопасности АЭС

В представленной на Рис. 1 модели, кибербезопасность заключается в поддержании в заданных пределах значений рисков (экономических, экологических, социальных), связанных с возможными (умышленными и неумышленными) нарушениями доступности, целостности или конфиденциальности информации (алгоритмов, данных и сигналов) в АСУ ТП АЭС.

Кибербезопасность АСУ ТП АЭС достигается посредством комплекса организационно-технических мероприятий. Весь комплекс мероприятий направлен на выявление (обнаружение) различного вида угроз, на защиту (реагирование) от этих угроз и устранение последствий от реализации этих угроз. Реализация угроз способна привести к нарушению доступности, целостности или конфиденциальности обрабатываемой информации и утрате управляемости, наблюдаемости и устойчивости технологического процесса АЭС. Кибербезопасность АСУ ТП АЭС обеспечивается в рамках соответствующей программы, которая определяет и координирует деятельность организаций, вовлеченных в жизненный цикл АСУ ТП АЭС (разработчики, проектировщики, поставщики и др.), по выявлению и ликвидации (нейтрализации) угроз объектам АСУ ТП АЭС, снижению рисков и размера возможного ущерба на стадиях жизненного цикла АСУ ТП АЭС.

Проблема кибербезопасности АСУ ТП АЭС во многом развивается в русле общих проблем обеспечения ИБ промышленных объектов [8,9]. В настоящее время вопросы информационной безопасности приобрели огромное значение как для граждан и общества, так и для государства. Это связано с появлением новых обстоятельств, характерных для современного периода развития информатизации общества. Сформулируем основные вопросы в этой сфере:

- во-первых, все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, таким образом, формируется задача обеспечения информационной безопасности, как органической совокупности задач защиты информации и защиты от информации.
- во-вторых, с самого начала регулярного использования автоматизированных технологий обработки информации актуальность задачи обеспечения требуемого качества информации возрастает, а сама задача усложняется. Следовательно, обеспечение информационной безопасности невозможно без учета задач обеспечения качества информации.
- в-третьих, решение задач защиты информации, задач защиты от информации и обеспечения качества информации обуславливает эффективность функционирования промышленных объектов. В свою очередь, учет задач управления информацией необходим при формировании, поддержке и использовании концепции информационного обеспечения деятельности промышленных объектов.
- в-четвертых, серьезное внимание на новом этапе развития теории защиты информации должно быть уделено регулярности решения проблем информационной безопасности, так как от этого зависят многие процессы, имеющие в своей основе регулярный обмен информацией.

В контексте современного развития общества соответственно выявляются следующие перспективные направления обеспечения кибербезопасности промышленных объектов:

- формализация положений теории информационной безопасности для обеспечения кибербезопасности промышленных объектов. Разработка эталонных моделей кибербезопасности, более точно отражающих существующий уровень развития техники и информационных технологий и более удобных для практического использования и анализа защищённости реальных систем управления промышленными объектами;
- вопросы обеспечения безопасности промышленных объектов в глобальных информационных сетях, например, Internet;
- безопасность в системах искусственного интеллекта (ИИ) в контексте автономного управления промышленными объектами;
- вопросы безопасности обработки информации мобильными (удаленными) пользователями в контуре управления промышленными объектами. В атомной промышленности удаленное управление рассматривается в качестве возможного решения в контексте управления модульными реакторами.

Целью работы является идентификация и анализ основных проблем в обеспечении кибербезопасности АСУ ТП АЭС и их связь с оценкой риска.

1 Методы и средства обеспечения кибербезопасности промышленных объектов

Обеспечение кибербезопасности на любой стадии жизненного цикла учитывает конкретные особенности защищаемого объекта. Данные об объекте являются исходными данными для модели угроз в части уязвимостей объекта, модели нарушителя, сценарии атак при оценке риска составляются с учетом функций, реализуемых объектом.

Существует устойчивое мнение, что каждая АСУ ТП для крупного промышленного объекта уникальна, так как уникален объект управления. Даже при типовом строительстве нельзя добиться полной идентичности объектов в серии. Поэтому невозможно привести единое описание энергоблока и его АСУ ТП АЭС пригодное для всех случаев. В основном, исходя из конкретного опыта авторов, когда необходимо учитывать специфику объекта автоматизации, говориться об АСУ ТП АЭС для энергоблоков с реакторами ВВЭР-1000, ВВЭР-1200, хотя это не единственный вид реакторов. В России и за рубежом существует ряд реализаций АСУ ТП АЭС для каждого из типов реакторов [10].

Видимо, одним из первых в основном проектов современных цифровых АСУ ТП АЭС для реакторов типа ВВЭР стал проект АЭС Бушер 1 [11,12]. Данный проект задал вектор развития АСУ ТП АЭС на десятилетия. Сейчас на его основе разработано несколько независимых проектов АС ТП АЭС, реализуемых в России и за рубежом. Основные методы оценки риска, изложенные в работе, были апробированы на проектах относящимся к данному типу реакторов, хотя авторы не видят принципиальных трудностей в адаптации методов для других АСУ ТП АЭС и критически важных объектов (КВО).

1.1 Основные принципы построения систем защиты

Защита АСУ ТП АЭС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от несанкционированного доступа к информации и включает в себя комплекс программно-технических средств защиты и поддерживающих их организационных мер. Защита АСУ ТП АЭС обеспечивается на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ на объекте.

Применяемые меры защиты не должны приводить к нарушению требований к функциональным характеристикам защищаемой системы (надежность, быстродействие, возможность изменения конфигурации). Приведем основные принципы построения систем защиты [13,14], справедливые так же применительно к АСУ ТП АЭС:

1) Законность и обоснованность защиты. Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.
2) Системность. Системный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:
    a) при всех видах информационной деятельности и информационного проявления;
    b) во всех структурных элементах;
    c) при всех режимах функционирования;
    d) на всех этапах жизненного цикла;
    e) с учетом взаимодействия объекта защиты с внешней средой.

При обеспечении безопасности информационной системы необходимо учитывать уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и пути несанкционированного доступа к информации. Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3) Комплексность. Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.
4) Непрерывность защиты. Защита информации – это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

5) Разумная достаточность. Создать абсолютно непреодолимую систему защиты принципиально невозможно, так как при наличии достаточного времени и средств можно преодолеть любую защиту. Следовательно, возможно достижение лишь некоторого приемлемого уровня безопасности. Высокоэффективная система защиты требует больших ресурсов (финансовых, материальных, вычислительных, временных) и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).
6) Гибкость. Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности, средства защиты должны обладать определенной гибкостью.
7) Открытость алгоритмов и механизмов защиты. Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты. Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна, необходимо обеспечивать защиту от угрозы раскрытия параметров системы.
8) Простота применения средств защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

2 Концепция обеспечения глубоко эшелонированной защиты кибербезопасности АСУ ТП АЭС

2.1 Общие подходы к обеспечению глубоко эшелонированной защиты

Глубоко эшелонированная защита (ГЭЗ) с точки зрения ядерной безопасности определяется в серии стандартов ядерной безопасности МАГАТЭ № SSR 2/1 [1]. В документе МАГАТЭ [5,6] отмечается, что одного анализа ядерной безопасности недостаточно для управления риском кибербезопасности, поскольку сбои, вызванные кибератаками, могут поставить АЭС и систему управления в условия, не рассматриваемые в анализе ядерной безопасности. Например, кибератака может вызвать одновременные сбои в нескольких уровнях ГЭЗ ядерной безопасности. Поэтому необходим отдельный подход, обеспечивающий реализацию эшелонированной защиты, применительно к кибербезопасности.

Эшелонированная защита, применительно к кибербезопасности (ГЭЗК), чтобы отличить ее от ГЭЗ [4] (пункт 4. 142), определена следующим образом: «Глубокоэшелонированная защита от компрометации активов по кибербезопасности включает в себя обеспечение нескольких последовательных мер защиты, которые необходимо обойти для того, чтобы кибератака прогрессировала и повлияла на подсистему АСУ ТП АЭС и ее функции».

Следует учесть, что ГЭЗК достигается не только путем реализации барьеров на границах уровней и зон безопасности в рамках защитной архитектуры кибербезопасности АСУ ТП АЭС, но и путем создания и поддержания надежной программы кибербезопасности, которая обеспечивает оценивание, предотвращение, обнаружение, защиту, реагирование, смягчение последствия атаки и восстановление функционирования АСУ ТП АЭС после ее завершения.

Концепция эшелонированной защиты кибербезопасности обеспечивает защиту от нежелательных последствий, потенциально возникающих в результате кибератаки так же, как ГЭЗ для ядерной безопасность способна предотвратить сбой и/или уменьшить последствия сбоя функционирования защищаемой системы.

2.2 Реализация эшелонированной защиты кибербезопасности

2.2.1 Разнообразие мер защиты

Разнообразие является важным фактором, который следует учитывать, как для обеспечения ядерной безопасности, так и для обеспечения глубокоэшелонированной защиты кибербезопасности. Это принципиально обеспечивает дополнительную защиту от общих причин отказа и является эффективной и крайне важной мерой, как в области кибербезопасности, так и в области ядерной безопасности.

Общий подход в обеспечении ГЭЗК включают в себя пункты, необходимые для обеспечения кибербезопасности с использованием комбинации независимых и разнообразных мер. Данные меры должны быть преодолены нарушителем для достижения целей атаки путем компрометации актива. Выбранный из каталога подмножество мер защиты определяет совокупность мер защиты, которые гарантируют, что компрометация или отказ одной меры защиты не приведет к серьезным или неприемлемым последствиям.

Разработчики подсистем при выборе компенсирующих мер защиты должны учитывать воздействие конкретной меры защиты на определенную угрозу.

2.2.2 Объединение активов в зоны безопасности

Зоны безопасности предназначены для предотвращения или задержки кибератак, поскольку нарушителю может потребоваться пересечь несколько зон, чтобы скомпрометировать функции объекта. В идеале, меры защиты, используемые в зонах на одном уровне, разнообразны и независимы от мер защиты, используемых в зонах на соседних уровнях, чтобы смягчить общие причины сбоев механизмов защиты. Данный принцип при проектировании подсистем АСУ ТП АЭС реализуется посредством независимых групп разработчиков основных подсистем.

Эшелонированную защиту между зонами, имеющими различный уровни кибербезопасности, можно поддерживать, с требованием того, чтобы каждая зона, назначенная определенному уровню, была защищена от кибератак, исходящих из зон на том же или нижних уровнях кибербезопасности. Отдельный документ «План кибербезопасности» определяет меры защиты, назначенные каждому уровню кибербезопасности, которые реализуются на границах каждой зоны. В документе [5] приведены дополнительные указания по выбору и назначению мер защиты. Иллюстративный пример зонной модели АСУ ТП АЭС показан на Рис.2.

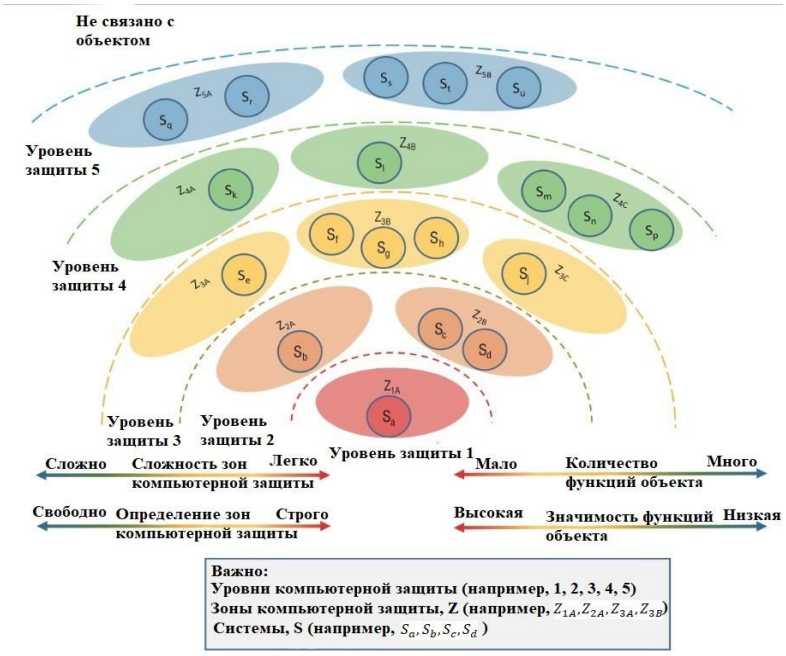

Рис. 2. Концептуальная модель уровней и зон кибербезопасности [5] в рамках ГЭЗК

3 Комплексная модель кибербезопасности АСУ ТП АЭС

3.1 Общие характеристики жизненного цикла программируемых цифровых систем АСУ ТП АЭС

Жизненный цикл работ по обеспечению кибербезопасности программируемой цифровой АСУ ТП АЭС на уровне систем приведен на Рис.3.

Документация по информационной безопасности и, как ее части, кибербезопасности разрабатывается на АСУ ТП АЭС в течении всего ее жизненного цикла. Она включают в себя как проектную, так и эксплуатационную документацию.

Основополагающим документом по кибербезопасности АСУ ТП АЭС служит политика безопасности [6,9], разрабатываемая как для каждого из этапов жизненного цикла, так и для каждого из уровней представления системы в виде политик отдельных подсистем из состава АСУ ТП АЭС.

Для проведения детального анализа кибербезопасности АСУ ТП АЭС может быть применено большое разнообразие методов моделирования. Наличие модели позволяет проводить систематический анализ риска и оценку роли мер кибербезопасности в смягчении последствий действий злоумышленника.

Одним из методов анализа кибербезопасности АСУ ТП АЭС является комплексное функциональное моделирование информационных потоков АСУ ТП АЭС [15], которое позволит получить количественную оценку поверхности атаки, провести анализ архитектуры безопасности АСУ ТП АЭС в части уровней кибербезопасности и зон.

Рис. 3. Жизненный цикл работ по обеспечению кибербезопасности АСУ ТП АЭС на уровне подсистем

Комплексное моделирование кибербезопасности зависит от идентификации активов и расположения систем АСУ ТП АЭС. Уровень детализации зависит от цели моделирования, и модель допускает несколько уровней абстракции. Для АСУ ТП АЭС основным уровнем абстракции является подсистема АСУ ТП АЭС.

Комплексная модель может применяться для оценки дальнейших мероприятий, связанных с кибербезопасностью:

- определение приоритетов в тестировании (создание профиля атак);
- создание документации, необходимой подготовки персонала по вопросам кибербезопасности АСУ ТП АЭС;
- разработка процедур реагирования на события и инцидентов кибербезопасности.

Для некоторых подсистем разработчиком подсистемы может быть принято решение провести отдельное моделирование на уровне подсистемы. В этом случае разработчик может использовать эту модель на более низком уровне абстракции.

3.2 Модель архитектуры кибербезопасности АСУ ТП АЭС

Различные уровни системы управления АЭС имеют различные приоритеты свойств кибербезопасности. В основном АСУ ТП АЭС имеет приоритетом цели доступности и целостности [6,9], кроме данных которые содержат конфиденциальную информацию, используемую для авторизации. В этом случае система предъявляет высокие требования к конфиденциальности и целостности, а к свойству доступности таких высоких требований не предъявляется.

В работе основное внимание уделяется свойству целостности. Связь целостности и конфиденциальности обсуждается ниже. Для обзора методов и моделей оценки доступности можно рекомендовать работы [16,17].

В руководстве МАГАТЭ [5] приведена спецификация архитектуры кибербезопасности, как часть процесса управления рисками кибербезопасности объекта. Спецификация использует поэтапный подход к кибербезопасности, основанный на уровнях кибербезопасности, и определяет требования,

которые обеспечивают более высокую степень защиты функций, назначенных более высоким уровням кибербезопасности. Это включает в себя требования кибербезопасности для ограничения и контроля связи между функциями объекта и требования физической безопасности для оборудования, выполняющего эти функции. Спецификация гарантирует, что функции объекта с самой высокой значимостью отнесены к самому высокому уровню кибербезопасности.

Требования спецификации для связи между системами объекта включают требования кибербезопасности для управления потоком данных как между системами, назначенными различным уровням кибербезопасности, так и между системами с одним и тем же уровням кибербезопасности.

4 Оценка риска на этапе проектирования в части обоснования архитектуры безопасности и мер технической защиты

Для управления риском рассмотрен двухэтапный подход к оценке риска кибербезопасности [18]. Целью первоначальной оценки рисков кибербезопасности является получение базовой оценки риска для системы, когда ее свойства известны только в самом общем виде.

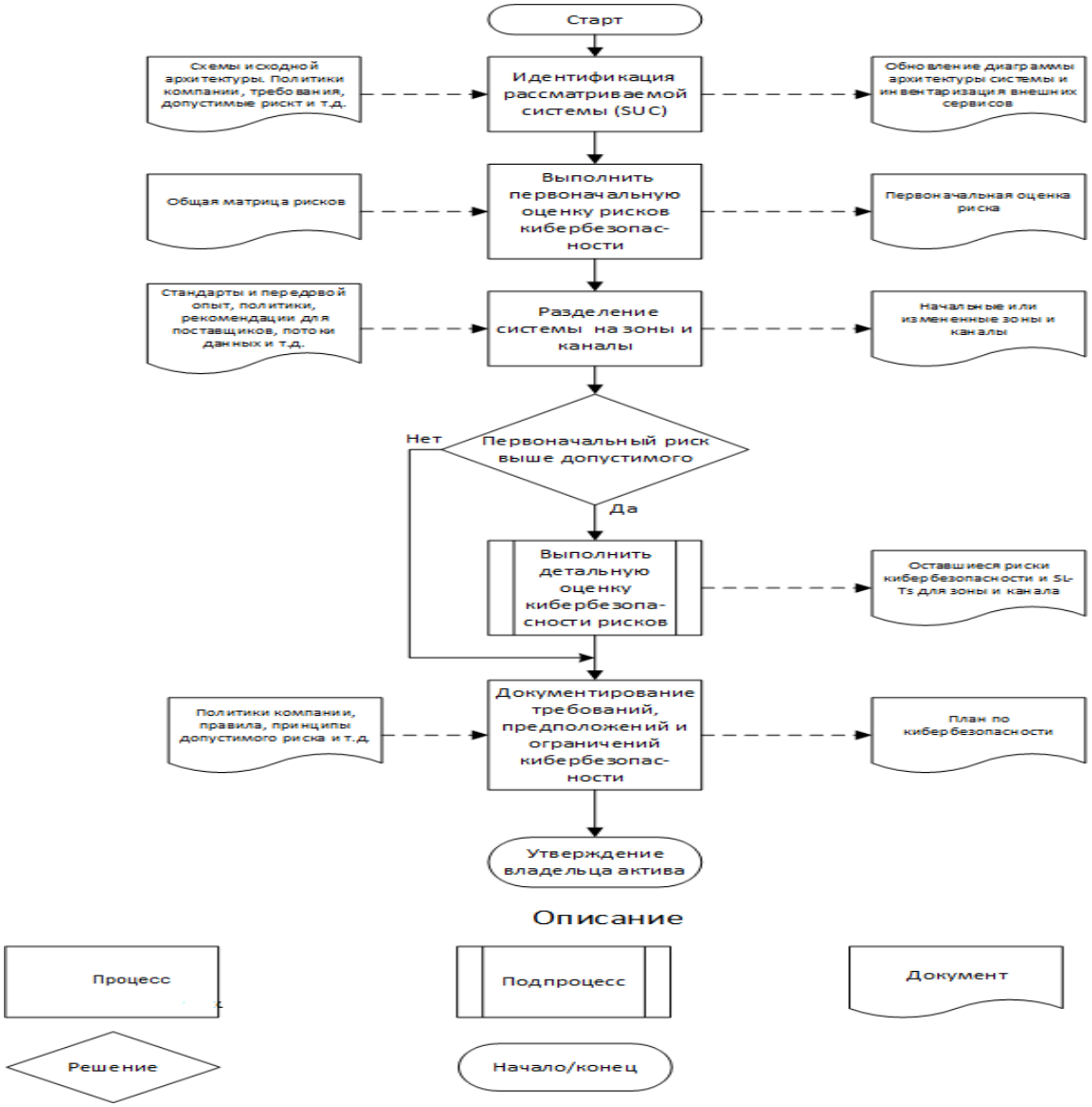

Рис. 4. Процесс управления риском на первом этапе [18]. SL-T – целевой уровень кибербезопасности

Эта оценка помогает с установлением приоритетов детальной оценки рисков и облегчает разработку архитектуры безопасности АСУ ТП АЭС, например, в части деления на зоны безопасности или классификации активов. Базовая оценка риска связывает риск с целевым уровнем кибербезопасности.

Оценка риска в контексте безопасного проектирования позволяет оценить степень соответствия архитектуры системы предъявляемым требованиям по кибербезопасности. Результат оценки риска служит исходным событием для проведения синтеза архитектуры безопасности, т.е. процесса

приведения информационных связей между активами в соответствие с ограничениями, задаваемыми политикой ИБ на АСУ ТП АЭС.

Процесс управления риском на первом этапе графически представлен на Рис. 4

Оценка риска для АСУ ТП должна проводиться с приоритетом по целям “Целостность”, и “Доступность” (см. раздел 5.2 МЭК 62443-1-1 [9]) в модели КЦД.

Весь процесс является итеративным по своей природе, когда результат предыдущих шагов может быть просмотрен и изменен в соответствии с результатом выполнения любого шага.

5 Управления рисками информационной безопасности на этапе эксплуатации

Поддержание уровня ИБ АСУ ТП АЭС на этапе эксплуатации включает два процесса, указанные на Рис. 5, куда как составная часть входит оценка рисков.

При оценке риска основное внимание должно быть уделено оценке эффективности реализованных мер защиты, для поддержания достигнутого уровня ИБ не ниже целевого уровня ИБ, присвоенного активу на этапе проектирования.

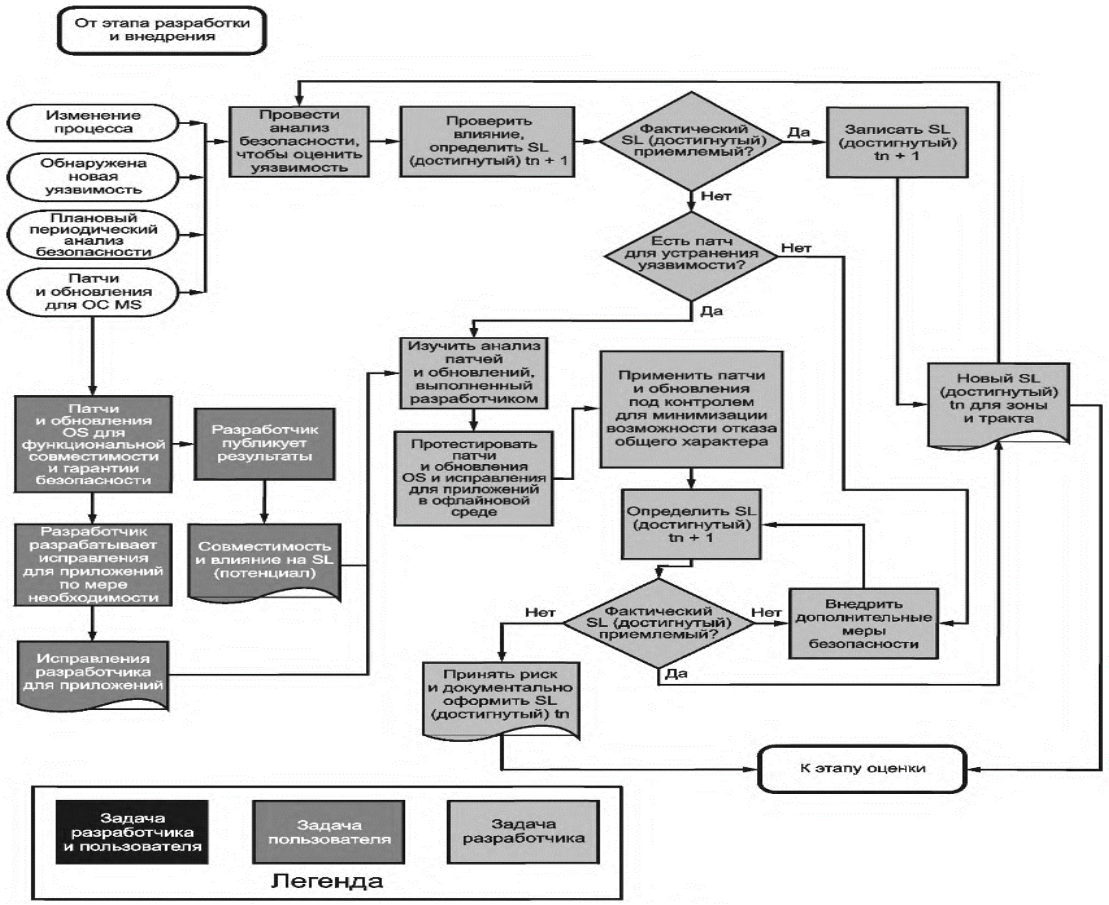

Рис.5. Процессы кибербезопасности АСУ ТП АЭС на этапе эксплуатации [9]

Достигнутый уровень кибербезопасности, определенный для актива или зоны, является функцией от времени и снижается с течением времени из-за снижения эффективности контрмер, новых уязвимостей, эволюционировавших угроз или скорректированных методов атак, уязвимостей в уровнях безопасности и внутренне присущих свойств безопасности устройств и систем до их проверки, замены или модернизации.

Заключение

АЭС относятся к объектам с повышенным риском эксплуатации, поэтому проблемы обеспечения кибербезопасности имеют для них многоплановый характер. Многоплановость проявляется как в многообразии угроз, которые должны рассматриваться для объекта – фактически от уровня государственного противостояния до внутренних личностных и производственных мотивов, так и на уровне возможных уязвимостей и последствий кибератаки.

Проблема обеспечения кибербезопасности АСУ ТП АЭС до сих пор является непроработанным вопросом в общей структуре обеспечения безопасности АЭС. Несмотря на то, что существуют нормы и формальные правила (в виде набора мер) по обеспечению кибербезопасности АСУ ТП АЭС, отсутствуют методики согласования функциональных требований АСУ ТП АЭС и решений по кибербезопасности.

Сформулированы основные задачи обеспечения кибербезопасности АСУ ТП АЭС. Обозначены принципы построения архитектуры безопасности. Рассмотрена связь между классическим принципом глубоко эшелонированной защиты (ГЭЗ) применимой для обеспечения ядерной безопасности АЭС и ее проекцией на область информационной безопасности АСУ ТП АЭС. Обосновано утверждение, что основная цель киберзащиты АСУ ТП АЭС состоит в недопущении нарушения норм ядерной безопасности, и это определяет сильную связь классификации систем АСУ ТП АЭС по ядерной и кибербезопасности.

В работе рассмотрены вопросы, связанные с процессом управления кибербезопасностью АСУ ТП АЭС на различных этапах жизненного цикла. Анализируются практические вопросы оценки риска на этапе проектирования и эксплуатации АСУ ТП АЭС.

Литература

1. IAEA Safety Standards Series No. SSR-2/1. Safety of Nuclear Power Plants: Design Specific Safety Requirements 2012.
2. *Бабаев Д. И., Полетыкин А. Г., Промыслов В. Г., Тимофеев М. Ю.* Управление архитектурой кибербезопасности АСУ ТП атомных электростанций // Проблемы управления. – 2018 – № 3. - с. 47–55.
3. IEC 62859:2016. Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity.
4. IAEA Nuclear Security Series No. 33-T Computer Security of Instrumentation and Control Systems at Nuclear Facilities Technical Guidance. 2018
5. IAEA 17-T, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).
6. IEC 62645 ed.2. 2020. Nuclear power plants – Instrumentation and control systems – Requirements, International Electrotechnical Commission.
7. IAEA, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).
8. ФСТЭК России от 14.03.2014 № 31 (ред. от 23.03.2017) «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, представляющую повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Зарегистрировано в Минюсте России 30.06.2014, № 32919.
9. ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.
10. *Бывайков М.Е., Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г.* Технологии ИПУ РАН для АСУ ТП: Верхний уровень, Диагностика, Информационная безопасность, Надежность, Импортозамещение. Автоматизация и IT в энергетике. 2016. №8 (85). С. 45-52.
11. *Бывайков М.Е., Жарко Е.Ф., Менгазетдинов Н.Э. и др*. Опыт проектирования и внедрения системы верхнего блочного уровня АСУ ТП АЭС // Автоматика и телемеханика. – 2006. – Т. 5. – с. 65–79.
12. *Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г., Зуенкова И.Н., Бывайков М.Е., Прокофьев В.Н., Коган И.Р., Коршунов А.С., Фельдман М.Е., Кольцов В.А.* Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУ ТП ДЛЯ АЭС «БУШЕР» на основе отечественных технологий. М.: ИПУ РАН, 2013. – 95 с.
13. *Промыслов В.Г., Полетыкин А.Г., Менгазетдинов Н.Э.* Новые кибернетические угрозы и методы обеспечения кибербезопасности в цифровых системах управления // Энергетик. 2012. №7. с. 18-23.
14. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
15. ГОСТ Р МЭК 61226-2011. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления.
16. *Промыслов В.Г., Семенков К.В., Шумов А.С.* Синтез архитектуры кибербезопасности для систем управления атомных электростанций. // Проблемы управления. – 2019. – № 3. – с. 61–71.
17. *Baybulatov A., Promyslov V.* Industrial Control System Availability Assessment with a Metric Based on Delay and Dependency / IFAC-PapersOnLine. Amsterdam: Elsevier, 2021. Volume 54, Issue 13. p. 472-476.
18. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.