УДК 621.039.68 DOI: https://doi.org/10.25728/pu.2018.3.7

УПРАВЛЕНИЕ АРХИТЕКТУРОЙ КИБЕРБЕЗОПАСНОСТИ АСУТП АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

Д.И. Бабаев, А.Г. Полетыкин, В.Г. Промыслов, М.Ю. Тимофеев

Рассмотрены методы оценки риска, назначения уровней кибербезопасности, требования к мерам защиты и построения архитектуры кибербезопасности. Сформулированы основные задачи обеспечения кибербезопасности. Обозначены принципы построения архитектуры кибербезопасности. Обсужден пример практической реализации архитектуры.

Ключевые слова: информация, кибербезопасность, безопасность, автоматизированная система управления, атомная электростанция.

ВВЕДЕНИЕ

Безопасность общества и государства в существенной мере зависит от безопасности системообразующих инфраструктурных объектов, к которым относятся, например, объекты транспортной, химической, энергетической и других сфер.

На различных уровнях управления обращаются огромные массивы информации, требующие соответственной защиты от несанкционированных воздействий, таких как, например, компьютерные атаки. Наличие цифровых систем управления, непосредственно связанных с технологическим процессом и выполняющих также противоаварийные функции, расширяет возможное пространство атаки, поскольку часть данных в системе может быть критически важным активом для поддержания функционирования объекта. Изложенное справедливо и для системы управления технологическими процессами на атомной электростанции (АЭС). На АЭС цифровая АСУТП выполняет как функции безопасности, так и функции нормальной эксплуатации [1]. Проблема обеспечения безопасности АСУТП АЭС комплексна и связана с обеспечением промышленной (энергетической, ядерной и радиационной, функциональной) безопасности [2, 3], а из-за высокой степени централизации управления на основе компьютеризированных систем на объекте, и с обеспечением информационной и кибербезопасности [4]. Проблематика обеспечения кибербезопасности критических систем описана в ряде работ и документов российских и международных организаций. Например, описаны общие подходы к обеспечению кибербезопасности [5], представлен подход к оценке кибербезопасности АСУТП на базе методов структурно-логического анализа надежности и безопасности с применением вероятностных моделей [6], рассмотрен метод анализа кибербезопасности на основе теории графов и дискреционной модели доступа [7]. Среди комплексных работ отметим профильные документы, разработанные Международной электротехнической комиссией (МЭК) и МАГАТЭ [8—10], серию стандартов ISO/IEC 27000, документ [11] в части общих принципов обеспечения безопасности цифровых систем управления и др. Однако ни в специальных, ни публикациях общего характера на данный момент не удалось полностью учесть всю специфику и сложность АСУТП АЭС.

В настоящей статье рассмотрена общая модель взаимодействия различных компонентов безопасности АЭС, стратегия управления кибербезопасностью в рамках жизненного цикла АСУТП АЭС. Систематизирован процесс анализа рисков, которые позволяют оценивать кибербезопасность проектных решений в части архитектуры безопасности и определяют функционирование компонентов АСУТП АЭС. Рассмотрена типовая реализация архитектуры кибербезопасности АСУТП.

1. ОБЩАЯ СТРАТЕГИЯ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

В международной практике для выделения кибербезопасности из информационной безопасности принята модель МАГАТЭ [12], которая в основном используется в настоящее время и на национальном уровне РФ для атомной промышленности[1].

[1] С 1 января 2018 г. общая модель взаимодействия на национальном уровне определяется федеральным законом [5].

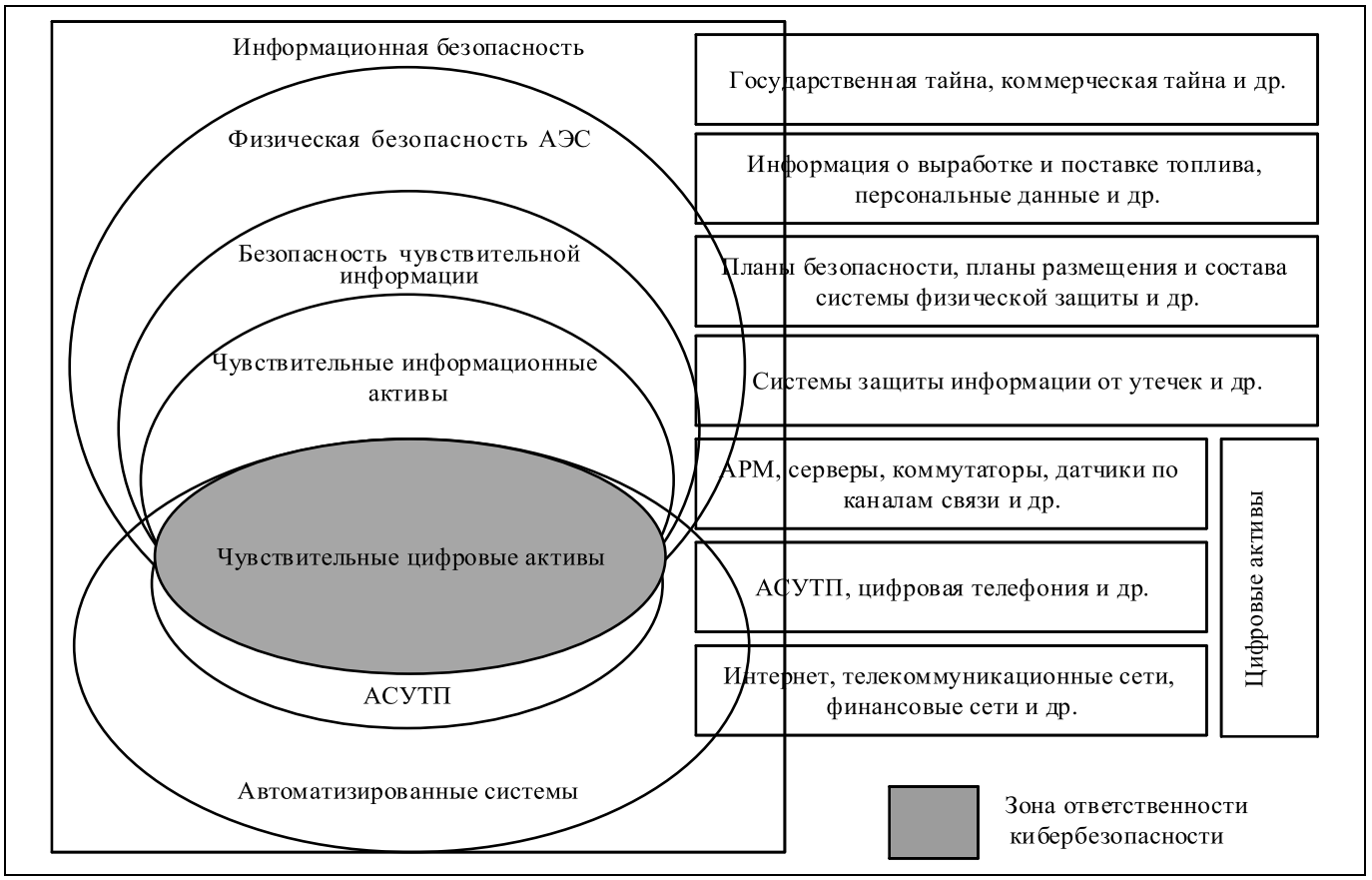

Рис. 1. Общая модель взаимодействия информационной и кибербезопасности для атомной промышленности

В соответствии с этой моделью взаимодействия (рис. 1) в рамках обеспечения информационной безопасности выделяются следующая ее внутренняя структура и соответствующие процессы:

— данные классифицируются по уровням важности и к ним предъявляются общие требования по защите информации [13]; требования по защите информации распространяются как на собственно данные в электронной форме, так и на компьютерные системы, используемые для их хранения, передачи и обработки;

— дополнительные требования на информацию налагаются в рамках законов и регулирующих документов, связанных с атомной энергетикой [2];

— собственник АЭС, в соответствии с требованиями в рамках программы информационной безопасности, определяет политики и процедуры безопасности для критически важной информации, нарушение доступности, целостности или конфиденциальности которой может привести к нарушению штатного режима функционирования АСУ [11];

— собственником идентифицируются и выделяются критически важные информационные активы;

— собственник идентифицирует цифровой актив и тип актива, который осуществляет обработку, хранение, передачу информации в цифровой форме.

Кибербезопасность заключается в поддержании в заданных пределах значений рисков (экономических, экологических, социальных), связанных с возможными нарушениями (умышленными и неумышленными) доступности, целостности или конфиденциальности информации (алгоритмов, данных и сигналов) в АСУТП АЭС.

Процесс управления кибербезопасностью АСУТП АЭС в общем случае можно представить в виде последовательности выполнения следующих шагов [8, 9]:

— по оценкам риска на системном уровне назначаются уровни кибербезопасности для подсистем АСУТП;

— в соответствии с уровнем кибербезопасности назначаются требования к мерам защиты;

— определяется архитектура кибербезопасности АСУТП, в том числе правила разграничения доступа;

— оценивается остаточный риск на уровне подсистем и их элементов и при необходимости на-

значаются дополнительные меры кибербезопасности.

Кибербезопасность АСУТП 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 таких угроз способна привести к нарушению целостности, доступности или конфиденциальности обрабатываемой и утрате управляемости, наблюдаемости и устойчивости технологического процесса АЭС. Кибербезопасность АСУТП АЭС обеспечивается в рамках соответствующей программы, которая определяет и координирует деятельность организаций, вовлеченных в жизненный цикл АСУТП (разработчики, проектировщики, поставщики и др.) по выявлению и ликвидации (нейтрализации) угроз объектам АСУТП, снижению рисков и размера возможного ущерба на стадиях жизненного цикла АСУТП.

Основополагающим документом по кибербезопасности АСУТП АЭС служит политика безопасности, разрабатываемая как для каждого из этапов жизненного цикла, так и для каждого из уровней представления системы. Политики безопасности определяются на различных уровнях, начиная от политики управления или администрирования, устанавливаемой на уровне предприятия, и заканчивая политикой эксплуатации, описывающей конкретные меры по управлению безопасностью. Дополнением к политике безопасности служат процедуры и регламенты. Разделение политики (описания) и действий (процедур) по воплощению политики безопасности позволяет более гибко реагировать на изменение рисков, связанных с кибербезопасностью. Поскольку угрозы реализуются посредством уязвимостей в политике безопасности, для уменьшения связанного с кибербезопасностью риска возможно воздействовать как на угрозы, так и на уязвимости. Уязвимости, в отличие от угроз, подвержены прямому воздействию со стороны владельца защищаемого объекта, поэтому управление риском посредством минимизации уязвимостей является более гибким и чаще применяемым методом.

Основные задачи обеспечения кибербезопасности должны заключаться в:

— плановом выявлении и устранении угроз кибербезопасности и их источников;

— развитии и совершенствовании системы обеспечения кибербезопасности, включая разработку новых и совершенствование существующих способов, методов и средств выявления, оценки, прогнозирования, нейтрализации и ликвидации угроз, а также средств и методов противодействия этим угрозам;

— эффективном противодействии угрозам кибербезопасности;

— выявлении, предотвращении и ликвидации последствий воздействий, вызывающих нарушения целостности, доступности и конфиденциальности информации и данных, приводящих к нарушению технологического процесса;

— сертификации средств защиты информации, программного обеспечения, технологий, их разработки и применения в соответствии с требованиями безопасности;

— совершенствовании приемов, способов, методов и средств защиты от кибератак;

— своевременной и непрерывной подготовке кадров.

2. ОЦЕНКА РИСКА НА СИСТЕМНОМ УРОВНЕ

Контекст кибербезопасности, как на общесистемном уровне, так и на уровне элементов подсистем АСУТП АЭС основан на концепциях угроз, рисков и контрмер, а также взаимосвязях между ними. Анализ рисков должен проводиться для взаимосвязанной системы «человек—машина». Для АСУТП АЭС и информационных систем используется простая контекстная модель анализа рисков ISO [14] (рис. 2). Специфичным для АСУТП АЭС является контекст, связанный с необходимостью обязательного рассмотрения сценариев инцидентов ядерной и радиационной безопасности (ЯРБ) из-за очень высокого уровня риска, связанного с этими сценариями и намного превосходящего любой другой возможный риск. Реализуемые меры кибербезопасности позволяют обеспечить надежное и качественное функционирование АЭС и уменьшение рисков нарушения ЯРБ при эксплуатации уязвимостей цифровых компонентов АСУТП АЭС.

Стандартный подход к оценке рисков основан на сценарии ISO 27005 [15]. Сценарии риска строятся с учетом трех элементов.

- Активы. Первый шаг в классификации и обеспечении информации заключается в идентификации активов, важных для кибербезопасности, с учетом выбранного уровня представления системы. Для идентификации активов выполняется анализ функциональной безопасности с целью выделения активов, критически важных для обеспечения выполнения проектных функций всей системы.
- Уязвимость, которая связана с воздействием на актив в обход политики безопасности системы.
- Угроза, которая связана с вероятностью (частотой) использования уязвимости.

В таком понимании контекста кибербезопасности предлагается выделять следующие риски:

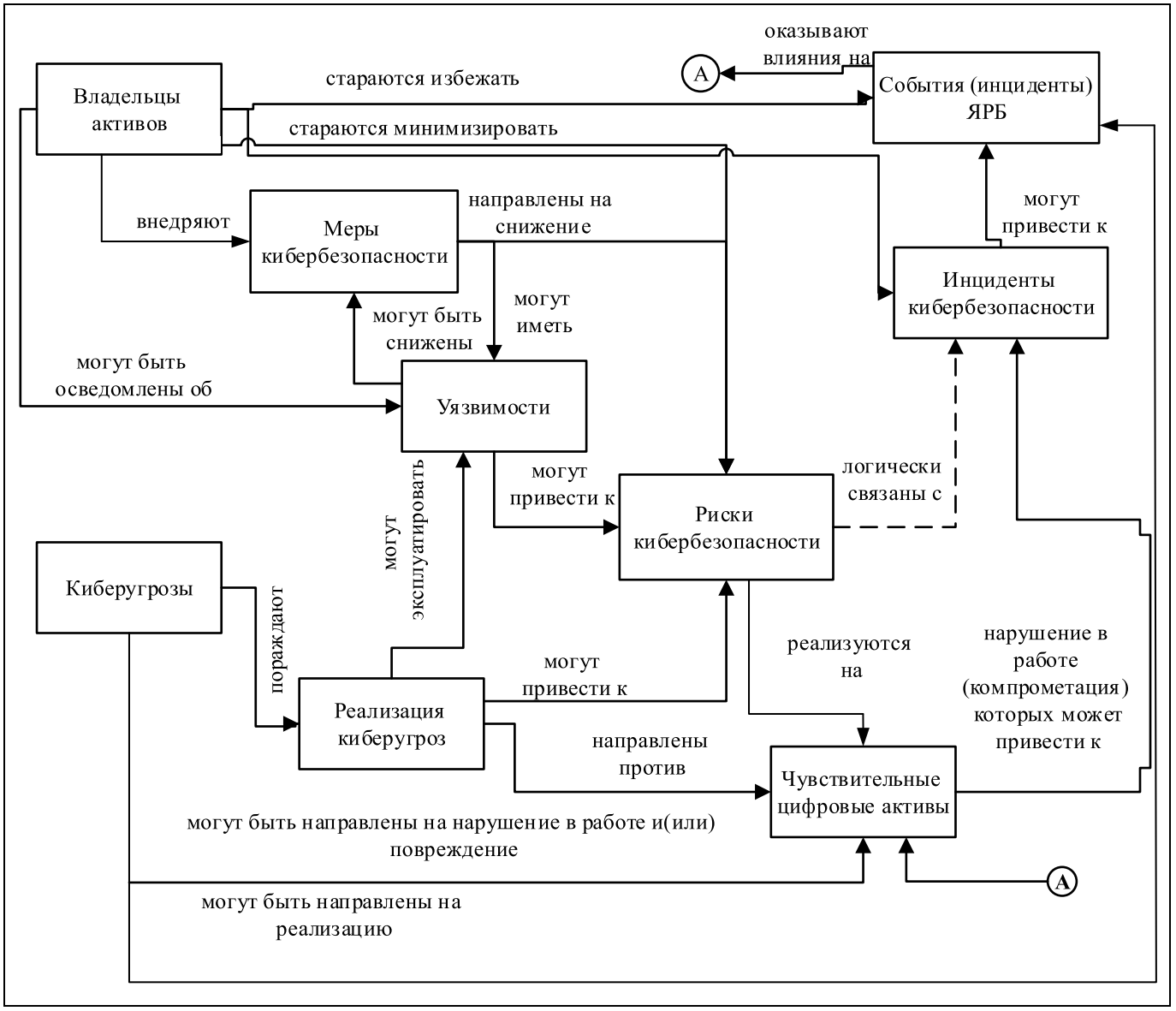

Рис. 2. Взаимосвязи между элементами контекста анализа риска

— системный, определяемый системообразующими факторами;

— правовой, определяемый оценками действующих юридических норм;

— экономический, определяемый эффективностью функционирования объекта;

— функциональный, определяемый факторами, влияющими на достижение цели, заложенной при проектировании компонента.

Многие руководства и нормативные документы, например, ISO 27005, определяют стандартный набор уязвимостей для информационных систем, а также вводят градации для активов, уязвимостей и угроз вместе с правилами расчета риска для их комбинаций. Однако, как показывает практика, для индустриальных систем из-за их узкой специализации стандартные подходы малоприменимы. Разработчики чаще всего вынуждены создавать собственные методики оценки риска, адаптированные к их системам.

Основная тенденция, которая прослеживается в общих подходах МЭК и МАГАТЭ, заключается в адаптации результатов оценки ядерной безопасности на системном и функциональном уровнях для классификации систем по кибербезопасности вместо проведения отдельной оценки риска вследствие нарушения целостности, доступности и конфиденциальности информации. Особенно такой подход часто используется на начальном этапе для общей оценки риска в системе. Схема назначения

уровней кибербезопасности в соответствии с категориями ядерной безопасности для выполняемых системой функций, применяемая МЭК [8], рассматривается далее.

3. НАЗНАЧЕНИЕ УРОВНЕЙ КИБЕРБЕЗОПАСНОСТИ

3.1. Непрямая оценка риска кибербезопасности

Для атомной отрасли характерно наличие глубокой проработки технологии и результатов по оценке ядерных рисков. Результаты представлены в виде классификаторов по ядерной опасности как для систем, так и для выполняемых системой функций. В атомной промышленности как на национальном, так и на международном уровне разработана система классификации, связывающая системы или функции с их влиянием на ядерную безопасность [16, 17]. Класс ядерной безопасности, присвоенный системе, в значительной мере определяет ценность системы, так как с ним однозначно связан ущерб в случае выхода системы из строя (шкала ущербов INES).

Рассмотрим подробнее схему классификации активов по уровням кибербезопасности, исходя из назначенных им классов по ядерной безопасности. В классификационной схеме МЭК определяется три уровня безопасности: S1, S2 и S3. При назначении уровней безопасности функции и системы должны анализироваться для определения максимальных последствий для безопасности АЭС в случае выполнения вредоносных действий или возникновения связанных с ними событий (рис. 3). Системы должны быть отнесены к уровням от S1 (наиболее строгие требования по кибербезопасности) до S3 в соответствии с максимальными последствиями кибератаки для ядерной безопасности (ЯРБ) и экономических характеристик объекта. Алгоритм присвоения уровней кибербезопасности для АСУТП АЭС основан на категории функций безопасности, которые выполняет система:

- системы, выполняющие функции категории A, относятся к уровню кибербезопасности S1;
- системы, выполняющие функции категории B, а также системы с прямым (непосредственным) воздействием на безопасность АЭС или отказы которых могут привести к нарушению технологического процесса и введению в действие функций категории A, относятся к уровню кибербезопасности не ниже S2;
- системы, поддерживающие функции категории C в соответствии с максимально возможными последствиями от реализации кибератак на них, а также системы, обеспечивающие эксплуатацию и техническое обслуживание АЭС до уровня кибербезопасности S3.

При этом уровень кибербезопасности может быть повышен по итогам проведения углубленной оценки рисков.

Отметим, что МАГАТЭ приводит только классификацию по ЯРБ систем и оборудования в составе АСУТП АЭС [10], а также определяет число и свойства уровней кибербезопасности. Всего определяются пять уровней кибербезопасности, три высших из которых соответствуют уровням МЭК.

3.2. Прямая оценка риска кибербезопасности

Кроме классификации активов по кибербезопасности, с учетом их классификации по ЯРБ, может быть использована схема классификации,

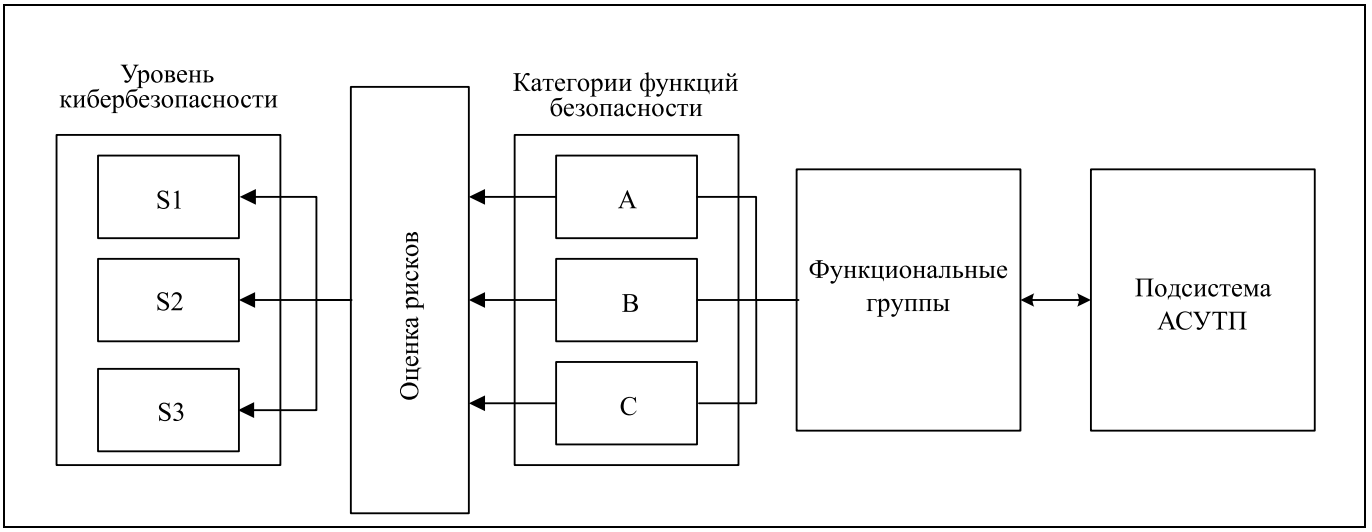

Рис. 3. Схема назначения уровней кибербезопасности

напрямую не связанная с ядерной безопасностью, например, схема приведенная в документе [11]. В ней также выделяются три уровня защищенности: К1 (самый высокий), К2 и К3. Для назначения класса защищенности определяется уровень значимости обрабатываемой информации в зависимости от степени возможного ущерба от нарушения целостности, доступности или конфиденциальности (при необходимости) обрабатываемой информации. Уровень значимости (критичности) информации определяется степенью возможного ущерба от нарушения ее целостности (неправомерное уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которых возможно нарушение штатного режима функционирования АСУ или незаконное вмешательство в процессы функционирования АСУ. Уровень значимости отдельных подсистем в составе АСУ определяется экспертным путем.

3.3. Сравнительный анализ методик

По мнению авторов правильное и квалифицированное применение перечисленных выше методик классификации активов (систем) АСУТП АЭС по кибербезопасности приводит к похожим результатам и реализации фактически аналогичного набора мер защиты.

На практике применение и выбор методик, в основном, определялось тем, на какой рынок — национальный или международный ориентирована защищаемая система, а также опытом работы разработчика. Для АСУТП АЭС, поставляемых на международный рынок, применялась обычно методика МЭК или МАГАТЭ, для отечественного рынка — методика, изложенная в [11]. Некоторое преимущество имеет методика классификации МЭК, специально ориентированная на применение в атомной промышленности — с простым и понятным алгоритмом, связанным с ЯРБ, что уменьшает объем работ по оценке риска кибербезопасности на начальном этапе.

4. ВЫБОР МЕР ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Обеспечение кибербезопасности является составной частью работ по созданию и эксплуатации АСУТП АЭС. Обеспечение кибербезопасности осуществляется на стадиях (этапах) жизненного цикла АСУТП АЭС путем выполнения организационно-технических мероприятий, направленных на блокирование (нейтрализацию) угроз. Мероприятия по обеспечению кибербезопасности должны быть соизмеримы по своей эффективности.

Если определенная мера кибербезопасности не может быть реализована по техническим, экономическим или иным причинам или если ее применение противоречит требованиям ЯРБ, то применяются некоторые компенсирующие меры (организационные, меры физической защиты и др.). Формальное обоснование эффективности применения мер должно быть продемонстрировано анализом угрозы и риска. Если компенсирующая мера, также не может быть применена, риск кибербезопасности, связанный с неприменением данной меры, должен быть принят.

Цель компенсирующих мер безопасности заключается в том, чтобы снизить уровень риска кибербезопасности до уровня, который будет поддерживать рекомендованный контроль безопасности.

Различные меры кибербезопасности по-разному воздействуют на целостность, доступность и конфиденциальность критических активов АСУТП АЭС. Применение мер кибербезопасности специфично для различных этапов жизненного цикла АСУТП АЭС.

Для обеспечения кибербезопасности АСУТП АЭС необходимы следующие организационно-технические мероприятия [5]:

— по определению объектов защиты;

— по формированию требований к защите от киберугроз;

— по классификации систем по кибербезопасности;

— по выделению актуальных угроз;

— по выбору мер обеспечения кибербезопасности;

— по проектированию и разработке системы обеспечения кибербезопасности;

— организационные мероприятия по обеспечению кибербезопасности;

— оценка соответствия требованиям кибербезопасности подсистем и АСУТП АЭС в целом;

— обеспечение кибербезопасности при вводе в эксплуатацию;

— обеспечение кибербезопасности в ходе эксплуатации;

— обеспечение кибербезопасности при выводе из эксплуатации.

В атомной промышленности такой список мер приводится в документах МЭК и МАГАТЭ [9, 10]. Для АСУТП других систем подобный список мер, отнесенный к уровням кибербезопасности, приведен в документе [11]. Набор мер МАГАТЭ и [11], в отличие от документов МЭК, не разделен по этапам жизненного цикла, что является недостатком.

5. АРХИТЕКТУРА КИБЕРБЕЗОПАСНОСТИ

5.1. Аспекты архитектуры кибербезопасности

Достигнутая реальная кибербезопасность АСУТП АЭС, как объекта защиты, на этапе эксплуатации в большой мере зависит от той архитектуры кибербезопасности [18], которая была реализована в ходе выполнения программы кибербезопасности. Для разработки, внедрения и обслуживания программы кибербезопасности предполагается реализация следующих действий:

— анализ цифровых систем и локально-вычислительных сетей ядерных установок;

— выявление и оценка критических ресурсов в смысле безопасности;

— внедрение безопасной архитектуры в соответствии с определенными нормативами;

— анализ потенциальных рисков нарушений кибербезопасности;

— разработка детальной архитектуры кибербезопасности.

Архитектура кибербезопасности определяет связанную с кибербезопасностью структуру АСУТП АЭС как системы систем, включая основные функции, класс и границы каждой системы, взаимосвязь или независимость систем, приоритетность целей, одновременно действующих в системе, и порядок взаимодействия между человеком и системой. Архитектура кибербезопасности также включает в себя план и набор правил, описывающих сервисы безопасности, которые должны обеспечивать защиту системы и ее пользователей, необходимые меры для реализации этих сервисов, требуемые показатели эффективности функционирования элементов.

Архитектура кибербезопасности охватывает такие аспекты как:

— рекомендуемые компоновки сетей передачи данных между элементами системы;

— рекомендуемые конфигурации межсетевого экрана;

— процедуры авторизации и аутентификации пользователей;

— барьеры между различными сетями управления процессами;

— применение беспроводных коммуникаций;

— управление обновлениями и патчами (включая аутентификацию при их проведении);

— управление средствами обеспечения кибербезопасности;

— усиление защиты систем путем закрытия программных портов, блокировки или отказа от неиспользуемых или опасных сервисов и отказа от применения съемных накопителей данных;

— доступ к внешним сетям передачи данных за пределами АСУТП АЭС (включая Интернет);

— надлежащее применение средств электронной связи между персоналом (например, электронной почты).

Архитектуры кибербезопасности АЭС строится на основе системного подхода, при котором верхнеуровневые стратегические цели и принципы наследуются всеми функциями и активами объекта (включая персонал). Концептуально это находит отражение в реализации дифференцированного подхода к кибербезопасности и назначению уровней кибербезопасности для активов АСУТП АЭС и интеграции уровней кибербезопасности в модель разграничения доступа, определяемой политикой безопасности системы.

5.2. Дифференцированный подход и разграничение доступа

Реализация архитектуры кибербезопасности основывается на дифференцированном подходе, при котором критическим активам объекта назначаются уровни в соответствии с их критичностью для безопасности АЭС. Между классифицированными активами, согласно принципу глубоко эшелонированной защиты, реализуются соответствующие барьеры, препятствующие распространению угрозы. Каждому активу назначается набор мер для предупреждения, выявления и реагирования на кибератаки. Степень защиты каждого из активов должна соответствовать присвоенному для него уровню кибербезопасности.

Одна из проблем, которая решается при проектировании архитектуры заключается в установлении соответствия уровней кибербезопасности с иерархией (системой уровней) доступа. Уровень доступа, присваиваемый активу, однозначно определяется структурой информационных связей, существующих в системе. Правильно спроектированная система должна иметь однозначное и прямое соответствие между уровнями кибербезопасности и доступа, что обеспечит отсутствие слабых мест в защите системы и, как следствие, снижение риска кибербезопасности.

Существует два основных подхода к заданию уровней доступа — это рассмотрение доминирования и информационных потоков. Для основных целей проектирования архитектуры кибербезопасности оба подхода фактически одинаковы и различаются лишь семантикой проблемы. Далее рассмотрим более понятный для специалистов АСУТП подход информационных потоков.

В соответствии с этим подходом:

— каждому активу присваивается уровень доступа (или метка безопасности), и передача информации между активами подразумевает передачу информации между соответствующими уровнями доступа;

— определен оператор объединения уровней $A \oplus B = C$, т. е. активы, содержащие информацию из уровней A и B, должны быть помечены уровнем C;

— определено отношение $A \to B$, чтобы указать, что информация разрешена для потока от актива уровня доступа A до актива уровня доступа B.

Отношение $A \to B$ определяет отношение частичного упорядочения, посредством которого можно указать иерархию уровней доступа, и которое разбивает множество активов на непересекающиеся подмножества, упорядоченные так, что если актив входит в подмножество с номером i, то *следующий* за ним входит в подмножество с номером, большим чем i, такое отношение транзитивно и антисимметрично.

Определение 1. Полученные непересекающиеся подмножества называются уровнями доступа.

Определение 2. Актив x «выше», чем актив y, если $A \to B$ верно, а и $B \to A$ ложно. В этом случае говорят, что B «ниже», чем A.

Определение 3. Два актива x и y находятся на одной высоте (или уровне), если x и y принадлежат одному уровню. Аналогично говорят, уровень доступа $L2$ выше, чем уровень $L1$, если для каждой вершины $l2 \in L2$ и для каждой вершины $l1 \in L1$, $l2 > l1$. Аналогично для случая, когда один уровень ниже другого. ♦

В основе известных архитектур кибербезопасности [11, 19] АСУТП АЭС, в том числе и рассмотренной далее, лежит реализация иерархии уровней доступа в виде решетки для свойств целостности (модель Биба [20]).

5.3. Архитектура кибербезопасности RG 5.71

Архитектура RG 5.71 [19] получила широкое распространение, и основные ее положения повторяются во многих документах, посвященных кибербезопасности. Данная архитектура, фактически с момента появления, стала стандартной для атомной отрасли в международном масштабе. Она с небольшими вариациями повторена в документах МАГАТЭ и МЭК. Основные изменения относятся к числу уровней в системе и рекомендациям по менее строгому применению однонаправленных связей между активами на разных уровнях системы. Наличие различных вариантов обусловлено большой сложностью АСУТП АЭС как системы систем и сложившейся практикой работы.

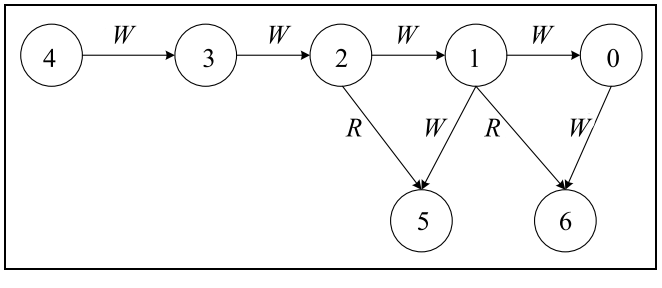

Рис. 4. Упрощенная информационная модель архитектуры безопасности RG 5.71: узлы графа *0—4* соответствуют субъектам; узлы *5* и *6* — объектам

Для архитектуры вводится 5 уровней компьютерной безопасности: уровни нумеруются с 4 по 0. Самый высокий (значимый) — 4, самый низкий — 0. Без ограничений поток данных разрешен с верхнего на более низкий уровень безопасности, передача данных с нижнего уровня на высший разрешена только для двух первых уровней кибербезопасности. Основная цель архитектуры кибербезопасности состоит в сохранении целостности данных и предотвращении модификации информации системами нижнего уровня кибербезопасности в системах верхнего уровня. Для достижения данной цели реализуется модель Биба для двух высших уровней кибербезопасности. Для низших уровней модель реализуется в ограниченном масштабе. Вводится запрет инициации соединения для нижнего уровня.

На рис. 4 приведена возможная информационная модель архитектуры типа RG 5.71. В модели для упрощения на каждом из уровней выделен единственный актив-субъект. Поток данных от верхнего уровня к нижнему определяется наличием доступа на запись (w) от субъекта, принадлежащего более высокому уровню, к низкому. Для безопасного доступа субъектов с уровней 0 и 1 к субъектам на более высоких уровнях 1 и 2 соответственно, применяется однонаправленный доступ по чтению (r) через буферные активы-объекты 5 и 6 соответственно. Применение буферных активов необходимо для того чтобы запретить возможность инициации доступа с нижнего уровня на верхний.

Особенность архитектуры RG 5.71 заключается в наличии рекомендаций по формированию зональной модели, позволяющей группировать системы по важности для физической безопасности и безопасности объекта. При использовании зональной модели рекомендуется соблюдать рекомендации:

— каждая зона включает в себя системы, имеющие одинаковую или сопоставимую важность для физической безопасности и безопасности установки;

— системы, относящиеся к одной зоне, имеют аналогичные потребности в отношении защитных мер;

— различные компьютерные системы, принадлежащие одной зоне, образуют область надежной связи для внутренней коммуникации в пределах этой зоны;

— зональные границы требуют механизмов развязки для потоков данных на основе политики, зависящей от конкретной зоны;

— в целях улучшения конфигурации зоны могут быть разделены на субзоны.

В целом архитектура RG 5-71 представляет собой разумное сочетание сложившейся практики построения АСУТП АЭС с требованиями по кибербезопасности.

ЗАКЛЮЧЕНИЕ

Рассмотрены вопросы, связанные с процессом управления кибербезопасностью АСУТП АЭС. Анализируются практические вопросы оценки риска, методики назначения уровней кибербезопасности, меры защиты и построения архитектуры кибербезопасности. Обосновано утверждение, что основная цель киберзащиты АСУТП АЭС состоит в недопущении нарушения норм ядерной безопасности, и это определяет сильную связь классификации систем АСУТП АЭС по ядерной и кибербезопасности.

Сформулированы основные задачи обеспечения кибербезопасности АСУТП АЭС. Обозначены принципы построения архитектуры кибербезопасности. Рассмотрена связь между уровнями кибербезопасности и классическими уровнями доступа, известными из практики информационной безопасности. Приведен пример практической реализации пятиуровневой архитектуры кибербезопасности на основе модели Биба с разбиением уровней на отдельные зоны безопасности и предложена возможная информационная модель данной архитектуры.

ЛИТЕРАТУРА

1. *Менгазетдинов Н.Э., Бывайков М.Е., Зуенков М.А.* и др. Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУТП для АЭС «Бушер» на основе отечественных информационных технологий. — М.: ИПУ РАН, 2013.
2. *Федеральные* нормы и правила в области использования атомной энергии «Требования к управляющим системам, важным для безопасности атомных станций» НП-026-16. Зарегистрировано в Минюсте России 14 декабря 2016 г., № 44712.
3. *ГОСТ* Р МЭК 61508-4. Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения. 2012.
4. *Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г.* Концепция обеспечения защиты от несанкционированного доступа АСУТП АЭС «Бушер-1» // Автоматизация в промышленности». — 2005. — № 5. — С. 3—5.
5. *Промыслов В.Г., Полетыкин А.Г.* Методы борьбы с киберугрозами АСУТП современного предприятия // Information Security / Информационная безопасность. — 2016. — № 1.
6. *Харченко В., Скляр В., Брежнев Е.* Безопасность информационно-управляющих систем и инфраструктур ISBN: 978-3-8473-9859-2 // Pa marium academic publishing, 2013.
7. *Промыслов В.Г., Полетыкин А.Г.* Формальная иерархическая модель безопасности верхнего уровня АСУТП АЭС // Ядерные измерительно-информационные технологии. — 2012. — Т. 4 (44). — С. 39—53.
8. *IEC* 62645 ed 1. Атомные электростанции. Системы контроля и управления. Требования к программам обеспечения безопасности для компьютерных систем. — 2014.
9. *IEC* 62859. Атомная электростанция. Приборы и системы управления. Требования к координации безопасности и кибербезопасности. — 2016.
10. *Computer* Security at Nuclear Facilities Technical Guidance Reference Manual IAEA Nuclear Security Series. — 2011. — N 17.
11. *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.
12. *NST055* Handbook on the design of physical protection systems for nuclear material and nuclear facilities, (Draft) August, 2017.
13. *РФ* Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации».
14. *ISO* 13335-1 2004. Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационных и телекоммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационных и телекоммуникационных технологий.
15. *ISO/IEC* 27005 Международный Стандарт. Информационная технология. Методы защиты. Менеджмент рисков информационной безопасности.
16. *Постановление* Госатомнадзора РФ от 14.11.1997 № 9 «Об утверждении и введении в действие нормативного документа ПНАЭ Г-01-011-97 «Общие положения обеспечения безопасности атомных станций. ОПБ-88/97».
17. *IEC* 6155134. Атомные электростанции. Системы контроля и управления, важные для безопасности. Общие требования.
18. *IEC/TS* 62443-1-1 Терминология, концепции и модели. — 2009.
19. *US.* Nuclear regulatory commission. Research regulatory guide 5.71 Cyber security programs for nuclear facilities, January 2010.
20. *Девянин П.Н.* Модели безопасности компьютерных систем. — М.: Academia, 2005. — 144 с.

Статья представлена к публикации членом редколлегии В.Г. Лебедевым.

Бабаев Денис Игоревич — нач. отдела,
АО «НИИ по эксплуатации атомных электростанций»,
г. Москва, ✉ dibabaev@vniiaes.ru,

Полетыкин Алексей Григорьевич — д-р техн. наук,
зав. лабораторией, Институт проблем управления
им. В.А. Трапезникова РАН, г. Москва, ✉ poletik@ipu.ru,

Промыслов Виталий Георгиевич — канд. физ.-мат.,
вед. науч. сотрудник, Институт проблем управления
им. В.А. Трапезникова РАН, г. Москва, ✉ v1925@mail.ru,

Тимофеев Михаил Юрьевич — инженер-программист,
Институт проблем управления им. В.А. Трапезникова РАН,
г. Москва, ✉ timof-1964@mail.ru.