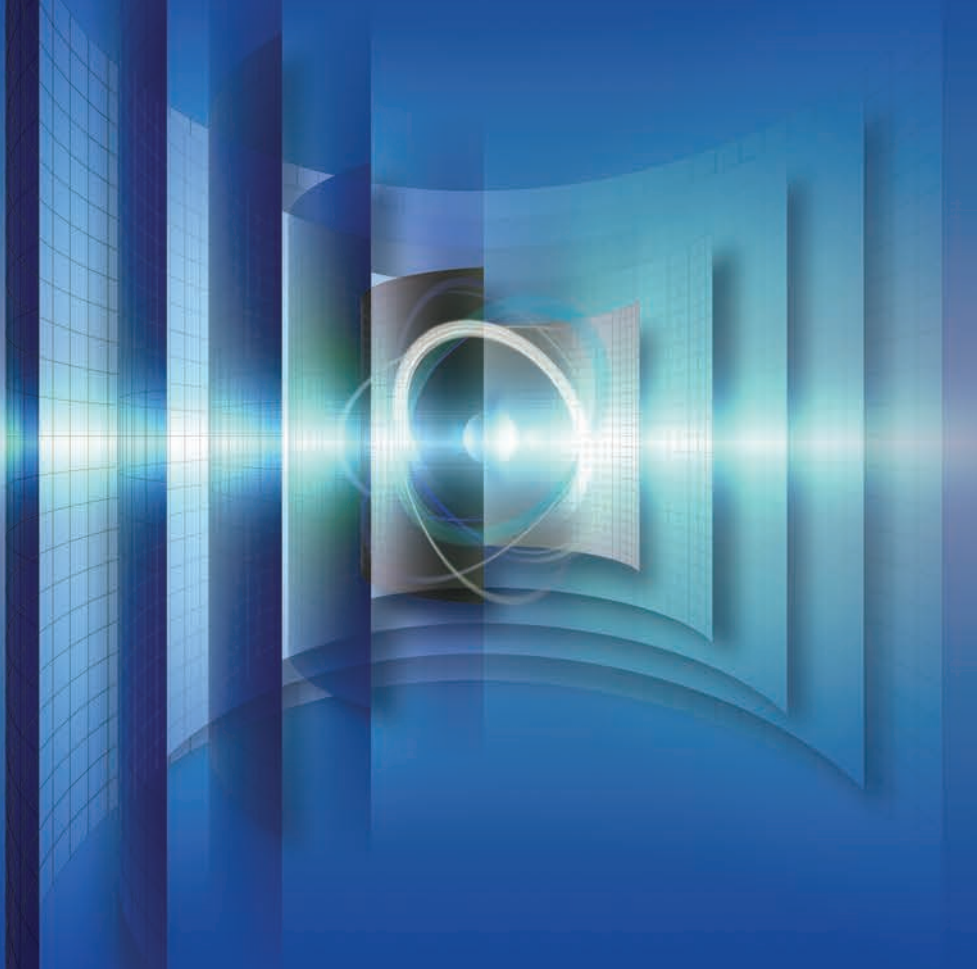
Серия изданий МАГАТЭ по физической ядерной безопасности, № 33-Т

Технические руководящие материалы

Компьютерная безопасность систем контроля и управления на ядерных установках



IAEA
Международное агентство по атомной энергии

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

В **Серии изданий МАГАТЭ по физической ядерной безопасности** освещаются вопросы физической ядерной безопасности, касающиеся предупреждения и обнаружения преступных или преднамеренных несанкционированных действий, которые совершаются в отношении ядерного материала, другого радиоактивного материала, соответствующих установок или соответствующей деятельности, а также реагирования на подобные действия. Эти публикации соответствуют положениям международно-правовых документов по физической ядерной безопасности, таких как Конвенция о физической защите ядерного материала и поправка к ней, Международная конвенция о борьбе с актами ядерного терроризма, резолюции 1373 и 1540 Совета Безопасности Организации Объединенных Наций и Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников, и служат дополнением к ним.

КАТЕГОРИИ ПУБЛИКАЦИЙ В СЕРИИ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

Публикации Серии изданий МАГАТЭ по физической ядерной безопасности выпускаются в следующих категориях:

- **«Основы физической ядерной безопасности»** — в них формулируется цель государственного режима физической ядерной безопасности и описываются основные элементы такого режима. Они служат основой для рекомендаций по физической ядерной безопасности;
- **«Рекомендации по физической ядерной безопасности»** — в них излагаются меры, которые следует принимать государствам для создания и обеспечения функционирования эффективного национального режима физической ядерной безопасности в соответствии с «Основами физической ядерной безопасности»;
- **«Практические руководства»** — в них даются руководящие указания относительно средств, при помощи которых государства могли бы осуществлять меры, изложенные в рекомендациях по физической ядерной безопасности. По существу, в них рассматриваются пути выполнения рекомендаций, касающихся общих направлений деятельности в сфере физической ядерной безопасности;
- **«Технические руководящие материалы»** — в них в дополнение к указаниям, содержащимся в практических руководствах, даются руководящие указания по конкретным техническим вопросам. В них подробно разбирается порядок действий по осуществлению необходимых мер.

СОСТАВЛЕНИЕ И РЕЦЕНЗИРОВАНИЕ

В подготовке и рецензировании публикаций Серии изданий по физической ядерной безопасности участвуют Секретариат МАГАТЭ, эксперты из государств-членов (помогающие Секретариату в составлении публикаций) и Комитет по руководящим материалам по физической ядерной безопасности (КРМФЯБ), отвечающий за рецензирование и одобрение проектов публикаций. При необходимости в период работы над публикацией также проводятся технические совещания открытого состава, чтобы специалисты из государств-членов и соответствующих международных организаций могли рассмотреть и обсудить проект текста. Кроме того, для обеспечения международного рецензирования и достижения консенсуса на высоком уровне Секретариат представляет проекты текстов всем государствам-членам на официальное рассмотрение в течение 120-дневного срока.

Для каждой публикации Секретариат готовит следующие документы, которые поэтапно одобряются КРМФЯБ в процессе подготовки и рецензирования:

- набросок и план работы с описанием предполагаемой новой или пересмотренной публикации, ее предполагаемой цели, сферы применения и содержания;
- проект публикации для представления на отзыв государствам-членам в течение 120-дневного периода консультаций;
- окончательный проект публикации, в котором учтены замечания государств-членов.

В процессе подготовки и рецензирования публикаций Серии изданий МАГАТЭ по физической ядерной безопасности принимаются во внимание соображения конфиденциальности и учитывается тот факт, что вопросы физической ядерной безопасности неразрывно связаны с общими и конкретными интересами национальной безопасности.

Одним из основополагающих моментов является необходимость учета в техническом содержании публикаций соответствующих норм безопасности МАГАТЭ и деятельности по гарантиям. В частности, публикации Серии изданий по физической ядерной безопасности, посвященные вопросам, которые пересекаются с вопросами безопасности, — известные как документы по взаимосвязанной тематике — на каждом из вышеуказанных этапов рецензируются соответствующими комитетами по нормам безопасности, а также КРМФЯБ.

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ НА ЯДЕРНЫХ УСТАНОВКАХ

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ
АВСТРИЯ
АЗЕРБАЙДЖАН
АЛБАНИЯ
АЛЖИР
АНГОЛА
АНТИГУА И БАРБУДА
АРГЕНТИНА
АРМЕНИЯ
АФГАНИСТАН
БАГАМСКИЕ ОСТРОВА
БАНГЛАДЕШ
БАРБАДОС
БАХРЕЙН
БЕЛАРУСЬ
БЕЛИЗ
БЕЛЬГИЯ
БЕНИН
БОЛГАРИЯ
БОЛИВИЯ, МНОГОНАЦИОНАЛЬНОЕ ГОСУДАРСТВО
БОСНИЯ И ГЕРЦЕГОВИНА
БОТСВАНА
БРАЗИЛИЯ
БРУНЕЙ-ДАРУССАЛАМ
БУРКИНА-ФАСО
БУРУНДИ
ВАНУАТУ
ВЕНГРИЯ
ВЕНЕСУЭЛА, БОЛИВАРИАНСКАЯ РЕСПУБЛИКА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАЙАНА
ГАМБИЯ
ГАНА
ГВАТЕМАЛА
ГВИНЕЯ
ГЕРМАНИЯ
ГОНДУРАС
ГРЕНАДА
ГРЕЦИЯ
ГРУЗИЯ
ДАНИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО
ДЖИБУТИ
ДОМИНИКА
ДОМИНИКАНСКАЯ РЕСПУБЛИКА
ЕГИПЕТ
ЗАМБИЯ
ЗИМБАБВЕ
ИЗРАИЛЬ
ИНДИЯ
ИНДОНЕЗИЯ
ИОРДАНИЯ
ИРАК
ИРАН, ИСЛАМСКАЯ РЕСПУБЛИКА
ИРЛАНДИЯ
ИСЛАНДИЯ
ИСПАНИЯ
ИТАЛИЯ
ЙЕМЕН
КАБО-ВЕРДЕ
КАЗАХСТАН
КАМБОДЖА
КАМЕРУН
КАНАДА
КАТАР
КЕНИЯ
КИПР
КИТАЙ
КОЛУМБИЯ
КОМОРСКИЕ ОСТРОВА
КОНГО
КОРЕЯ, РЕСПУБЛИКА
КОСТА-РИКА
КОТ-Д'ИВУАР
КУБА
КУВЕЙТ
КЫРГЫЗСТАН
ЛАОССКАЯ НАРОДНО-ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА
ЛАТВИЯ
ЛЕСОТО
ЛИБЕРИЯ
ЛИВАН
ЛИВИЯ
ЛИТВА
ЛИХТЕНШТЕЙН
ЛЮКСЕМБУРГ
МАВРИКИЙ
МАВРИТАНИЯ
МАДАГАСКАР
МАЛАВИ
МАЛАЙЗИЯ
МАЛИ
МАЛЬТА
МАРОККО
МАРШАЛЛОВЫ ОСТРОВА
МЕКСИКА
МОЗАМБИК
МОНАКО
МОНГОЛИЯ
МЬЯНМА
НАМИБИЯ
НЕПАЛ
НИГЕР
НИГЕРИЯ
НИДЕРЛАНДОВ, КОРОЛЕВСТВО
НИКАРАГУА
НОВАЯ ЗЕЛАНДИЯ
НОРВЕГИЯ
ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ
ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ
ОМАН
ПАКИСТАН
ПАЛАУ
ПАНАМА
ПАПУА — НОВАЯ ГВИНЕЯ
ПАРАГВАЙ
ПЕРУ
ПОЛЬША
ПОРТУГАЛИЯ
РЕСПУБЛИКА МОЛДОВА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
РУАНДА
РУМЫНИЯ
САЛЬВАДОР
САМОА
САН-МАРИНО
САУДОВСКАЯ АРАВИЯ
СВЯТОЙ ПРЕСТОЛ
СЕВЕРНАЯ МАКЕДОНИЯ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СЕНЕГАЛ
СЕНТ-ВИНСЕНТ И ГРЕНАДИНЫ
СЕНТ-КИТС И НЕВИС
СЕНТ-ЛЮСИЯ
СЕРБИЯ
СИНГАПУР
СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
СЛОВАКИЯ
СЛОВЕНИЯ
СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
СУДАН
СЬЕРРА-ЛЕОНЕ
ТАДЖИКИСТАН
ТАИЛАНД
ТОГО
ТОНГА
ТРИНИДАД И ТОБАГО
ТУНИС
ТУРКМЕНИСТАН
ТУРЦИЯ
УГАНДА
УЗБЕКИСТАН
УКРАИНА
УРУГВАЙ
ФИДЖИ
ФИЛИППИНЫ
ФИНЛЯНДИЯ
ФРАНЦИЯ
ХОРВАТИЯ
ЦЕНТРАЛЬНОАФРИКАНСКАЯ РЕСПУБЛИКА
ЧАД
ЧЕРНОГОРИЯ
ЧЕШСКАЯ РЕСПУБЛИКА
ЧИЛИ
ШВЕЙЦАРИЯ
ШВЕЦИЯ
ШРИ-ЛАНКА
ЭКВАДОР
ЭРИТРЕЯ
ЭСВАТИНИ
ЭСТОНИЯ
ЭФИОПИЯ
ЮЖНАЯ АФРИКА
ЯМАЙКА
ЯПОНИЯ

Устав Агентства был утвержден 23 октября 1956 года на Конференции по выработке Устава МАГАТЭ, которая состоялась в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке. Устав вступил в силу 29 июля 1957 года. Центральные учреждения Агентства находятся в Вене. Главной целью Агентства является достижение «более скорого и широкого использования атомной энергии для поддержания мира, здоровья и благосостояния во всем мире».

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ, № 33-Т

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ НА ЯДЕРНЫХ УСТАНОВКАХ

ТЕХНИЧЕСКИЕ РУКОВОДЯЩИЕ МАТЕРИАЛЫ

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2024 ГОД

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Отпечатано МАГАТЭ в Австрии
Июль 2024 года
STI/PUB/1787

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ
НА ЯДЕРНЫХ УСТАНОВКАХ
МАГАТЭ, ВЕНА 2024 ГОД
STI/PUB/1787
ISBN 978-92-0-408024-7 (печатный формат)
ISBN 978-92-0-407924-1 (формат pdf)
ISSN 2788-8959

ПРЕДИСЛОВИЕ

Согласно Уставу, главной целью МАГАТЭ является достижение «более скорого и широкого использования атомной энергии для поддержания мира, здоровья и благосостояния во всем мире». Наша работа заключается как в предотвращении распространения ядерного оружия, так и в обеспечении доступа к ядерным технологиям в мирных целях в таких областях, как здравоохранение и сельское хозяйство. Крайне важно обеспечить безопасное обращение со всеми ядерными и другими радиоактивными материалами и установками, на которых они находятся, и их надлежащую защиту от преступных или преднамеренных несанкционированных действий.

Ответственность за обеспечение физической ядерной безопасности возлагается на каждое государство в отдельности, однако созданию и поддержанию эффективных режимов физической ядерной безопасности в немалой степени способствует международное сотрудничество. Центральная роль, которую МАГАТЭ играет в содействии такому сотрудничеству и оказании помощи государствам, широко признана. Эта роль МАГАТЭ находит воплощение в многочисленном членском составе организации, ее уставном мандате, уникальном экспертном потенциале и многолетнем опыте в области предоставления технической помощи и подготовки специальных практических руководящих материалов для государств.

Начиная с 2006 года МАГАТЭ выпускает Серию изданий по физической ядерной безопасности, предназначенную для оказания помощи государствам в создании эффективных национальных режимов физической ядерной безопасности. Эти публикации дополняют положения международно-правовых документов по физической ядерной безопасности, таких как Конвенция о физической защите ядерного материала и поправка к ней, Международная конвенция о борьбе с актами ядерного терроризма, резолюции 1373 и 1540 Совета Безопасности Организации Объединенных Наций и Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников.

Разработка руководящих материалов осуществляется при активном участии экспертов из государств — членов МАГАТЭ, благодаря которому в этих материалах находит отражение консенсус в отношении надлежащей практики обеспечения физической ядерной безопасности. Комитет МАГАТЭ по руководящим материалам по физической ядерной безопасности, учрежденный в марте 2012 года и состоящий из представителей государств-членов, занимается рассмотрением и одобрением проектов публикаций Серии изданий по физической ядерной безопасности по мере их подготовки.

МАГАТЭ вместе со своими государствами-членами будет и далее продолжать деятельность, направленную на то, чтобы блага от мирного применения ядерных технологий были доступны для целей улучшения здоровья, повышения благосостояния и процветания людей во всем мире.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Руководящие материалы, опубликованные в Серии изданий МАГАТЭ по физической ядерной безопасности, не являются обязывающими документами для государств, однако государства могут использовать эти руководящие материалы в качестве документов, помогающих им выполнять свои обязательства, вытекающие из международно-правовых документов, а также осуществлять свои обязанности по обеспечению физической ядерной безопасности внутри государства. В тексте руководящих материалов используется формулировка «следует», отражающая международную надлежащую практику и указывающая на международный консенсус в отношении необходимости принятия государствами рекомендуемых или эквивалентных альтернативных мер.

Термины из области физической безопасности должны пониматься так, как они определены в публикации, в которой они используются, или в руководящих материалах более высокого уровня, которые данная публикация дополняет. В остальных случаях слова и выражения употребляются в своем общепринятом значении.

Дополнение рассматривается в качестве неотъемлемой части публикации. Материал, содержащийся в дополнении, имеет тот же статус, что и основной текст. Приложения используются для включения в публикацию практических примеров, дополнительной информации или пояснений. Приложения не являются неотъемлемой частью основного текста.

Для обеспечения точности информации, содержащейся в настоящей публикации, были приложены большие усилия, однако ни МАГАТЭ, ни его государства-члены не несут ответственности за последствия, которые могут возникнуть в результате использования этой информации.

Использование тех или иных названий стран или территорий не является выражением какого-либо суждения со стороны издателя, в роли которого выступает МАГАТЭ, относительно правового статуса таких стран или территорий, их органов и учреждений, либо относительно делимитации их границ.

Упоминание названий конкретных компаний или продуктов (независимо от того, указаны они как зарегистрированные или нет) не подразумевает какого-либо намерения нарушить права собственности и не должно толковаться как одобрение или рекомендация со стороны МАГАТЭ.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1. Системы контроля и управления (СКУ) играют крайне важную роль в обеспечении безопасной эксплуатации ядерных установок. По мере того, как цифровые технологии продолжают развиваться, а их возможности расширяются, они все чаще включаются в СКУ и интегрируются с ними[1]. На новых ядерных установках и в современных проектах ядерных установок используются высокоинтегрированные цифровые СКУ для эффективной и одновременной обработки огромного количества технологических данных, и при этом они требуют меньшей степени участия и вмешательства человека, чем прежние СКУ. Кроме того, цифровые технологии часто внедряются в СКУ при модернизации существующих установок. Однако применение цифровых технологий в СКУ сделало эти системы уязвимыми для кибератак.

1.2. Кибератака — это злоумышленное действие со стороны отдельных лиц или организаций, направленное на чувствительную информацию или чувствительные информационные активы с целью хищения, изменения, предотвращения доступа или уничтожения конкретной цели посредством несанкционированного доступа к уязвимой системе (или действий внутри нее). К чувствительным информационным активам относятся системы управления, сети, информационные системы и любые другие электронные или физические носители. Злоумышленники предпринимали успешные кибератаки, направленные на СКУ, такие как кибератака с помощью вирусной программы Stuxnet, которая привела к выводу из строя оборудования на ядерной установке [1].

1.3. Кибератаки на СКУ могут поставить под угрозу ядерную и физическую безопасность ядерных установок. Они могут способствовать саботажу (диверсии) или облегчить несанкционированное изъятие ядерного материала. С точки зрения ядерной безопасности кибератаки на СКУ могут повлечь за собой самые разнообразные последствия, такие как временная потеря управления технологическим процессом или неприемлемые

[1] Термин «СКУ» используется по всему дальнейшему тексту настоящей публикации для обозначения тех систем контроля и управления, которые работают на основе цифровых технологий, опираются на них или функционирование которых обеспечивается такими технологиями.

радиологические последствия. То обстоятельство, что обществу известно о кибератаках, затрагивающих СКУ, может также поколебать уверенность в ядерной и физической безопасности ядерных установок.

1.4. Необходимость защиты компьютерных систем (включая СКУ) определена в п. 4.10 «Рекомендаций по физической ядерной безопасности, касающихся физической защиты ядерных материалов и ядерных установок» (INFCIRC/225/Revision 5) [2], который гласит:

> «Компьютеризированные системы, используемые для обеспечения физической защиты, ядерной безопасности, а также учета и контроля ядерных материалов, следует защищать от компрометации (например, кибератак, манипуляции или фальсификации) в соответствии с *оценкой угроз* или *проектной угрозой*».

1.5. В публикации Серии изданий МАГАТЭ по физической ядерной безопасности № 17 «Компьютерная безопасность на ядерных установках» [3] содержатся руководящие указания по реализации программы компьютерной безопасности применительно к ядерным установкам, которые подкрепляют рекомендации, приведенные в [2]. В [3] также приводятся сведения о ключевых терминах, таких как «компьютерная безопасность», «безопасность ИТ» и «кибербезопасность». Для целей настоящей публикации термины «безопасность ИТ» и «кибербезопасность» считаются синонимами компьютерной безопасности и использоваться не будут.

1.6. Компьютерная безопасность должна явным образом учитываться на каждой стадии жизненного цикла СКУ. Термин «жизненный цикл» (в отличие от срока службы) подразумевает, что жизнь системы действительно циклична (как в случае с рециклированием или переработкой) и, в частности, что элементы старой системы используются в новой системе. В [4] содержится список типичных видов деятельности в рамках жизненного цикла СКУ.

1.7. Так исторически сложилось, что при проектировании СКУ на ядерных установках компьютерной безопасности уделялось не слишком много внимания, поскольку считалось, что проводные или аналоговые системы неуязвимы для кибератак в силу их «жесткой» реализации, изолированности и разъединенности систем, а также практически полного отсутствия интерактивной коммуникации, особенно с внешними сетями или

системами. Переход к цифровым технологиям изменил характер СКУ на ядерных установках, обеспечив взаимосвязь между перепрограммируемыми (дистанционно или локально) и функционально неодинаковыми СКУ.

1.8. Более широкое использование универсальных программируемых цифровых компонентов и устройств привело к тому, что СКУ стали более однотипными. Это включает использование общих элементов и подходов в различных промышленных областях (например, протоколов связи). Злоумышленные действия[2], направленные против этих обычных для других отраслей технологий, могут затронуть и ядерную установку.

1.9. Уполномоченные лица на площадке или в некоем удаленном месте, которые имеют логический или физический доступ к СКУ, могут как инсайдеры представлять угрозу ядерной и физической безопасности ядерной установки. Такими инсайдерами могут быть работники установки или персонал, нанятый продавцами, подрядчиками или поставщиками, которые могут воспользоваться своим правом доступа для совершения злоумышленных действий. Необходимость защиты компьютерных систем от инсайдерских угроз признана в [5].

ЦЕЛЬ

1.10. Цель настоящей публикации — дать руководящие указания по компьютерной безопасности для защиты СКУ на ядерных установках от злоумышленных действий, которые могут помешать таким системам выполнять функции, связанные с обеспечением ядерной и физической безопасности. Хотя главное внимание в ней уделено безопасной эксплуатации этих систем, применение данного руководства может также способствовать улучшению ядерной безопасности и эксплуатационных характеристик ядерных установок.

1.11. Настоящая публикация предназначена для компетентных органов, включая регулирующие органы, а также для руководящего, эксплуатационного, технического и инженерного персонала ядерных установок, продавцов, подрядчиков и поставщиков СКУ, проектировщиков СКУ, исследовательских лабораторий и других организаций, занимающихся вопросами ядерной и физической безопасности ядерных установок.

---

[2] Злоумышленные действия не включают события, вызванные ошибкой человека или случайными отказами оборудования или компонентов.

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.12. Область применения настоящей публикации — применение мер компьютерной безопасности к СКУ, обеспечивающим ядерную безопасность, физическую безопасность[3] или выполнение вспомогательных функций на ядерных установках. Эти меры предназначены для защиты СКУ от злоумышленных действий, совершаемых отдельными лицами или организациями. В настоящей публикации также рассматривается применение таких мер к средам разработки, моделирования и технического обслуживания этих систем.

1.13. Руководство, приведенное в данной публикации, применимо к СКУ на новых[4] ядерных установках и к новым СКУ на существующих установках. Ожидается, что данное руководство будет в максимально возможной степени применено к устаревшим СКУ на существующих установках, включая те, на которых не используются цифровые технологии.

1.14. Хотя другие сопряженные системы и системы информационно-коммуникационных технологий (ИКТ), такие как системы контроля выполнения работ и связи, в данной публикации специально не рассматриваются, они также могут создать риски для СКУ. Эти риски необходимо принимать во внимание при разработке и применении мер компьютерной безопасности СКУ на установке. Меры компьютерной безопасности для этих систем могут отличаться от тех, которые применяются для СКУ, и должны быть оценены и адаптированы соответствующим образом.

1.15. В настоящей публикации нет исчерпывающих руководящих указаний по всем моментам, связанным с ядерной безопасностью СКУ. Такие указания можно найти в [4, 6]. Кроме того, в настоящей публикации не определяются и не изменяются технические термины, используемые в нормах безопасности МАГАТЭ и других публикациях МАГАТЭ, посвященных ядерной безопасности. В тексте данной публикации эти термины выделены, а их определения можно найти в Глоссарии МАГАТЭ по вопросам безопасности [7].

---

[3] Системы, выполняющие функции физической безопасности, включают системы, используемые для физической защиты и учета и контроля ядерного материала.

[4] Новая установка — это установка, которая еще не прошла стадию ввода в эксплуатацию.

СТРУКТУРА

1.16. В настоящей публикации за введением следуют четыре раздела. В разделе 2 рассказывается об СКУ, используемых на ядерных установках, и о роли компьютерной безопасности в защите этих систем от кибератак. В разделе 3 описывается взаимосвязь между компьютерной безопасностью и ядерной безопасностью СКУ. В разделе 4 приводятся руководящие указания по компьютерной безопасности, которые должны применяться на различных стадиях жизненного цикла СКУ, в том числе при выводе установки из эксплуатации.

2. КЛЮЧЕВЫЕ КОНЦЕПЦИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ СКУ

2.1. На ядерных установках СКУ используются для мониторинга процессов и оборудования и управления ими. К этим системам относятся:

a) системы SCADA (диспетчерского управления и сбора данных);
b) распределенные системы управления;
c) централизованные цифровые системы управления;
d) системы управления, состоящие из программируемых логических контроллеров;
e) микроконтроллеры и «умные» устройства;
f) системы, использующие программируемые логические устройства (например, программируемые пользователем вентильные матрицы, сложные устройства с программируемой логикой и интегральные схемы отдельных приложений).

Подобные системы, управляющие работой промышленных предприятий, часто называют «промышленными системами управления».

2.2. СКУ призваны обеспечивать безопасное, надежное, безотказное и детерминированное поведение ядерной установки как при нормальной эксплуатации, так и при нарушении нормальной эксплуатации[5].

[5] Нарушение нормальной эксплуатации упоминается в Глоссарии МАГАТЭ по вопросам безопасности [7] как синоним «ожидаемого при эксплуатации события». Для целей настоящей публикации более понятным считается первый термин.

Проектные соображения и меры, имеющие целью повышение ядерной безопасности, могут также дать преимущества с точки зрения физической безопасности. Например, такие проектные меры, как детерминированное функционирование, предотвращение сбоев, обнаружение сбоев, методы обеспечения отказоустойчивости, управление конфигурацией, независимая верификация и валидация, а также другие современные методы тестирования могут обеспечить определенную защиту от злоумышленных попыток изменить поведение СКУ.

2.3. При проектировании общей архитектуры СКУ на ядерных установках используются концепции, которые могут способствовать повышению компьютерной безопасности, смягчив последствия возникновения преднамеренных или случайных неисправностей[6], такие как независимость, резервирование, глубокоэшелонированная защита для целей безопасности и неодинаковость[7]. Термин «глубокоэшелонированная защита для целей безопасности» используется в настоящей публикации для обозначения глубокоэшелонированной защиты, как она определена в Глоссарии МАГАТЭ по вопросам безопасности [7], чтобы отличать его от применения аналогичной, но ориентированной на физическую безопасность концепции «глубокоэшелонированной защиты» (как она определена в Основах физической ядерной безопасности [8]) при осуществлении мер компьютерной безопасности, описанных в разделе 4.

2.4. Следует оценить реализацию этих концепций в общей архитектуре СКУ установки и других проектных мерах, чтобы понять, какую роль они играют в обеспечении компьютерной безопасности. Например, неодинаковость проекта или технологий, скорее всего, снизит общие уязвимости ключевых систем безопасности или управления, но может привнести уязвимости, свойственные каждой отдельной системе.

2.5. Руководящие указания, содержащиеся в настоящей публикации, относятся ко всем СКУ, связанным с ядерной установкой, если не указано иное.

---

[6] Термин «неисправность» используется в настоящем тексте для обозначения ситуаций, которые не были учтены ранее (т.е. не являются ожидаемыми при эксплуатации событиями), но в которых СКУ не срабатывает так, как ожидается.

[7] Независимость, резервирование, глубокоэшелонированная защита для целей безопасности и неодинаковость относятся здесь к конкретным понятиям, которые используются в Глоссарии МАГАТЭ по вопросам безопасности [7].

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ СКУ

2.6. В [2], п. 2.2, говорится следующее:

«Следует добиваться, чтобы государственный *режим физической защиты*[8] обеспечивал достижение этих целей путем:

— предупреждения *злоумышленных действий* посредством сдерживания и защиты чувствительной информации;
— пресечения попыток *злоумышленных действий* или *злоумышленных действий* посредством интегрированной системы *обнаружения*, задержки проникновения (продвижения) и реагирования;
— смягчения последствий *злоумышленного действия*».

2.7. Ниже приводятся примеры того, как предотвращение, пресечение и смягчение последствий могут быть применены к компьютерной безопасности СКУ.

— Предотвращение: установка отказоустойчивых устройств, блокирующих несанкционированную передачу данных с целью уменьшить вероятность сетевой кибератаки, которая может негативно повлиять на СКУ.
— Пресечение, включая обнаружение, задержку и реагирование: благодаря проверке файлов регистрации системных событий оператор может обнаружить события-предшественники и предпринять защитные меры до начала злоумышленного действия, которое может негативно повлиять на ядерную или физическую безопасность установки.
— Смягчение последствий и восстановление: если обнаружится, что СКУ заражена вредоносной программой, то после того, как распространение вредоносной программы будет остановлено, оператор определит, необходимы ли компенсирующие меры контроля (например, обновление сигнатур вирусов, установка или усовершенствование систем предотвращения или обнаружения вторжений или и то, и другое) для предотвращения повторного заражения, проведет перестройку системы, проверит эффективность

[8] Ранее для выражения концепции, которая теперь именуется физической ядерной безопасностью ядерных материалов и ядерных установок, использовался термин «физическая защита».

компенсирующих мер контроля, восстановит систему и вернет ее в рабочее состояние после проведения детального анализа ядерной безопасности и проверки целостности системы, если это необходимо.

2.8. Защита СКУ от компрометации иногда основывается на предположении, что достаточно принять только одну превентивную меру, например изолировать системы от других сетей. Однако такое предположение, по всей вероятности, станет причиной недостаточного применения мер противодействия и смягчения последствий, так что неэффективность этой единственной меры компьютерной безопасности может повлечь за собой компрометацию защищаемой системы.

2.9. Для общих систем ИКТ разработано множество различных подходов, методов, методик, стандартов и рекомендаций по компьютерной безопасности. Некоторые из них нельзя напрямую применить к СКУ на ядерных установках, которые имеют специфические требования компьютерной безопасности, не пересекающиеся с системами ИКТ.

2.10. Тем не менее, поскольку компьютерную безопасность СКУ невозможно полностью отделить от компьютерной безопасности систем ИКТ, операторы и регулирующие органы должны разрабатывать политику, требования, меры и методы обеспечения компьютерной безопасности, основанные на комплексном подходе к СКУ и системам ИКТ.

2.11. Жизненный цикл многих СКУ исчисляется десятилетиями, включая периоды, в течение которых поддержка поставщика может отсутствовать или быть недостаточной для выполнения требований компьютерной безопасности[9], предъявляемых к этим системам. Сюда относится поддержка, предоставляемая первоначальным поставщиком и связанными с ним третьими сторонами. Например, со временем антивирусные программы могут не обеспечить достаточной защиты от злоумышленного использования уязвимостей в СКУ из-за потери совместимости с аппаратным или программным обеспечением или невозможности дальнейшего обновления сигнатур вирусов.

[9] В настоящей публикации под «требованиями компьютерной безопасности» понимаются конкретные требования, установленные в письменном виде соответствующим компетентным органом или оператором для соблюдения регулирующих требований.

2.12. В большинстве случаев СКУ работают в режиме реального времени, и действия СКУ выполняются в строгих временных интервалах. К примерам таких действий СКУ на ядерных установках относится управление нормальной эксплуатацией, защитные действия, действия по ограничению и срабатывание аварийной сигнализации для операторов. Меры компьютерной безопасности не должны затруднять выполнение необходимых эксплуатационных действий или действий по обеспечению ядерной безопасности, препятствовать им или задерживать их выполнение. Меры компьютерной безопасности для современных СКУ могут быть использованы для предотвращения, обнаружения, задержки и реагирования на злоумышленные действия и для смягчения их последствий, однако необходимо позаботиться о том, чтобы эти меры реагирования не препятствовали выполнению заданных функций ядерной безопасности и не выводили систему за рамки ее проектных основ[10].

2.13. Меры компьютерной безопасности, применяемые задним числом или реализованные неудовлетворительным образом, могут дополнительно усложнить конструкцию СКУ, что может увеличить вероятность отказа СКУ или возникновения неисправности в ней.

2.14. В основном элементе 9 Основ физической ядерной безопасности [8] предусмотрено применение риск-ориентированных подходов при выделении ресурсов и при проведении мероприятий, связанных с физической ядерной безопасностью. Проект, разрабатываемый с использованием риск-ориентированного подхода для учета соображений безопасности с самого начала процесса проектирования, может быть сделан более простым и надежным за счет интеграции средств защиты, исключения ненужного функционала (например, удаленного доступа) или усиления системы.

---

[10] В проектных основах узлов, важных для ядерной безопасности, должны быть указаны требуемые возможности, надежность и функциональность в соответствующих эксплуатационных состояниях, аварийных условиях и условиях, возникающих вследствие внутренних и внешних опасностей, чтобы обеспечить удовлетворение конкретных критериев приемлемости в течение срока службы ядерной установки. Более подробное определение проектных основ приведено в Глоссарии МАГАТЭ по вопросам безопасности [7]. Проектные основы СКУ более детально описаны в [4], раздел 3.

МЕРЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

2.15. Меры компьютерной безопасности используются для предотвращения, обнаружения, задержки злоумышленных действий и реагирования на них, а также для смягчения последствий таких действий. Меры компьютерной безопасности также используются для того, чтобы действия, не содержащие в себе злого умысла, не снижали уровень безопасности и не увеличивали уязвимость компьютерных систем для злоумышленных действий.

2.16. Меры компьютерной безопасности, направленные на устранение уязвимостей в системе или создание эшелонов защиты, можно отнести к одной из трех категорий: меры технического контроля, меры физического контроля или меры административного контроля. При разработке средств интегрированной компьютерной безопасности СКУ должны быть рассмотрены все три категории и выбрана соответствующая комбинация.

2.17. Меры технического контроля — это аппаратные средства и/или ПО, используемые для предотвращения, обнаружения, смягчения последствий и восстановления после вторжения или другого злоумышленного действия. При оценке эффективности мер технического контроля в сравнении с мерами физического или административного контроля должна учитываться их способность выполнять непрерывные и автоматические защитные действия.

2.18. Меры физического контроля — это физические барьеры, которые защищают приборы, компьютерные системы и дополнительное оборудование от физического повреждения и несанкционированного физического доступа. Меры физического контроля включают в себя замки, защитные корпуса, устройства индикации вмешательства, изолированные помещения, контрольно-пропускные пункты и охрану.

2.19. Меры административного контроля — это политика, процедуры и практика, направленные на защиту компьютерных систем путем инструктирования сотрудников и персонала сторонних организаций относительно необходимых действий. Меры административного контроля определяют разрешенные, необходимые и запрещенные действия сотрудников и стороннего персонала. Меры административного контроля для ядерных установок включают меры эксплуатационного и управленческого контроля.

ПРИМЕНЕНИЕ ДИФФЕРЕНЦИРОВАННОГО ПОДХОДА

2.20. Оператор должен устанавливать требования компьютерной безопасности на основе риск-ориентированного, дифференцированного подхода, в котором учитывается следующее:

— значимость функций СКУ как для ядерной безопасности (т.е. классификация по безопасности), так и для физической безопасности;
— выявленные и оцененные угрозы для установки;
— привлекательность СКУ для потенциальных злоумышленников;
— уязвимости СКУ;
— условия эксплуатации;
— потенциальные последствия, которые могут стать прямым или косвенным результатом компрометации системы.

Такой подход может основываться на результатах оценки рисков компьютерной безопасности.

2.21. При дифференцированном подходе требования компьютерной безопасности устанавливаются таким образом, чтобы они были соразмерными потенциальным последствиям атаки. Потенциальные последствия компрометации функции СКУ можно выстроить в следующем порядке (от худшего к лучшему сценарию):

— функция находится в неопределенном состоянии — последствия компрометации приводят к изменению конструкции или функции системы, которое не поддается наблюдению;
— неожиданное поведение или действия функции, которые наблюдаются оператором;
— функция отказывает;
— функция работает как положено, т.е. компрометация не оказывает негативного влияния на работу системы (т.е. система является отказоустойчивой).

2.22. Для применения дифференцированного подхода к компьютерной безопасности СКУ должны присваиваться уровни компьютерной защиты, описанные в настоящей публикации.

2.23. Пример применения дифференцированного подхода с использованием уровней защиты[11] приведен в [3]. Иной пример — применения дифференцированного подхода для обеспечения ядерной безопасности — приведен в [9].

УРОВНИ КОМПЬЮТЕРНОЙ ЗАЩИТЫ

2.24. Уровни компьютерной защиты и классы безопасности — это разные, но взаимосвязанные понятия. Классификация по безопасности узла, важного для безопасности, основывается на значимости его функции для безопасности, а также на потенциальных последствиях его отказа.

2.25. Каждой функции СКУ, связанной с установкой, обычно присваивается уровень компьютерной защиты, указывающий на степень защиты средствами компьютерной безопасности, в которой эта функция нуждается. Для каждого уровня потребуются разные наборы мер компьютерной безопасности, удовлетворяющие соответствующим требованиям компьютерной безопасности. Уровни защиты часто определяются на основе целей организации в области безопасности. В [10] приводится дополнительная информация о применении уровней защиты и контуров безопасности.

2.26. Определяются подсистемы и компоненты СКУ, неисправность которых может повлиять на ядерную безопасность (включая смягчение последствий аварий), физическую ядерную безопасность и учет и контроль ядерного материала, и им присваиваются уровни защиты в зависимости от их роли в функционировании СКУ.

2.27. Оператор присваивает уровень защиты системе, подсистеме или компоненту СКУ исходя из потенциальных последствий ее отказа или неисправности, включая неисправность, отличающуюся от предусмотренного проектом или допустимого типа отказа, который может быть определен в ходе анализа безопасности установки. Уровень компьютерной защиты, присвоенный системе, подсистеме или компоненту СКУ, относится именно к этой системе, подсистеме или компоненту и не зависит от ее окружения.

---

[11] «Уровни защиты» и «контуры безопасности» по всему тексту настоящей публикации означают уровни компьютерной защиты и контуры компьютерной безопасности.

КОНТУРЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

2.28. Понятие контура безопасности предполагает логическое и/или физическое объединение компьютерных систем, которые имеют общие требования компьютерной безопасности, обусловленные изначальными свойствами этих систем или их связями с другими системами. Все системы, находящиеся в пределах одного контура, защищаются на одном уровне защиты — на том, который присвоен функции СКУ с наиболее строгим уровнем защиты в пределах данного контура. Объединение СКУ в контуры безопасности может упростить применение мер компьютерной безопасности и управление этим процессом.

2.29. При выделении контуров безопасности необходимо учитывать следующие соображения:

— системы, принадлежащие к одному и тому же контуру, имеют схожие потребности в мерах компьютерной безопасности;
— системы, принадлежащие к одному контуру, образуют доверенную область для внутренней коммуникации между этими системами (т.е. внутреннюю доверенную область контура);
— каждый контур включает в себя системы, которые имеют одинаковую или сопоставимую значимость с точки зрения ядерной и физической безопасности установки либо принадлежат к внутренней доверенной области контура;
— соблюдаются требования к архитектуре безопасности системы (например, резервирование, неодинаковость, географическое и электрическое разделение, критерий единичного отказа);
— на границах контуров реализуются меры технического контроля для ограничения потока данных и коммуникации между системами, находящимися в разных контурах (например, в удаленном месте) или отнесенными к разным уровням защиты;
— съемные носители, мобильные устройства и другое временное оборудование, которому необходим логический или физический доступ к системе, используются только в пределах одного контура или оговоренного набора контуров;
— для улучшения конфигурации контуры могут быть разделены на сегменты.

2.30. Когда на установке выделяются контуры безопасности, некоторые системы или компоненты СКУ могут быть отнесены к контуру с более высоким уровнем защиты, чем тот, который был присвоен им изначально.

Например, коммуникационному устройству, выполняющему только функции ядерной или физической безопасности более низкого уровня, может быть присвоен тот же уровень защиты, что и системе защиты реактора, если оно расположено в контуре безопасности системы защиты реактора. Это обусловлено потенциальной возможностью злоумышленного использования данного устройства для компрометации компонентов системы защиты реактора, которые крайне важны с точки зрения безопасности. Более того, использование контура безопасности, охватывающего систему защиты реактора, позволяет создать в этом контуре внутреннюю доверенную область, тем самым гарантируя, что между компонентами системы защиты реактора и коммуникационным устройством не потребуется устанавливать дополнительные средства компьютерной безопасности.

3. РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ СКУ

3.1. Риск-ориентированный подход к обеспечению компьютерной безопасности СКУ может предполагать использование оценки рисков для определения уязвимостей установки для кибератак, связанных с этими системами, и определение последствий, которые могут возникнуть в результате успешного использования этих уязвимостей. Затем на основе результатов оценок рисков могут быть выбраны меры компьютерной безопасности.

3.2. Поскольку СКУ часто имеют ключевое значение для безопасности установки, знание вопросов ядерной безопасности может помочь в оценке риска, разработке мер компьютерной безопасности для СКУ, оценке потенциальных противоречий между ядерной и физической безопасностью, а также в изучении того, как эти противоречия могут быть преодолены. Например, злоумышленники могут совершить саботаж (диверсию) на установке в форме кибератаки на СКУ установки, которая может иметь потенциальные последствия для ядерной и физической безопасности. Такие атаки могут привести к сбоям в работе СКУ или заставить СКУ работать не так, как они вели бы себя в случае предполагаемого поведения или при тех типах отказа, которые были заранее просчитаны. Злоумышленные действия могут затронуть как одну СКУ, так и несколько таких систем. Например, злоумышленник может обойти несколько уровней глубокоэшелонированной

защиты для целей безопасности или вызвать их одновременный отказ[12]. Злоумышленные действия могут также сочетать в себе кибератаки с элементами физического нападения.

3.3. Неадекватное обеспечение компьютерной безопасности или компрометация какой-либо СКУ могут поставить под угрозу ядерную безопасность установки. Например, при компрометации СКУ злоумышленник может получить данные, содержащие важнейшую информацию, необходимую для планирования атаки, или модифицировать данные, чтобы создать условия для совершения саботажа (диверсии) в отношении систем установки или несанкционированного изъятия ядерных материалов. В иных случаях кибератака, ведущая к саботажу (диверсии), может спровоцировать аварию или снизить эффективность выполнения функции ядерной безопасности. Такая атака может также привести к тому, что система станет недоступной.

3.4. Кроме того, кибератаки на СКУ могут повлечь за собой последствия, дающие возможность несанкционированного изъятия ядерного материала с установки. СКУ, выполняющие функции физической защиты или учета и контроля ядерного материала, могут подвергнуться кибератакам, в результате которых установка может быть приведена в состояние, не предусмотренное в плане обеспечения безопасности площадки. Злоумышленное действие может также сочетать в себе кибератаку на эти системы с элементами физического нападения с целью несанкционированного изъятия ядерного материала.

3.5. Таким образом, меры компьютерной безопасности СКУ должны быть направлены как на кибератаки, напрямую ведущие к саботажу (диверсии), так и на кибератаки, позволяющие собрать информацию, которая может способствовать саботажу (диверсии) на ядерной установке или несанкционированному изъятию ядерного материала.

---

[12] Пять уровней глубокоэшелонированной защиты для целей ядерной безопасности подробно описаны в [7].

ВЗАИМОСВЯЗЬ С ПРОЦЕССОМ УПРАВЛЕНИЯ РИСКАМИ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ УСТАНОВКИ

3.6. Для применения мер компьютерной безопасности с целью защиты функций, выполняемых СКУ, у оператора должен быть налажен процесс управления рисками в области компьютерной безопасности (УРКБ) установки. Этот процесс используется для выявления уязвимостей установки[13] для кибератак и определения последствий успешной компрометации одной или нескольких функций, выполняемых СКУ (что может включать злоумышленное использование уязвимостей).

3.7. К результатам процессов УРКБ установки должна относиться идентификация функций установки, выполняемых СКУ, в том числе вспомогательными и дополнительными системами, которые в случае их компрометации могут негативно повлиять на ядерную безопасность, физическую безопасность ядерного материала или управление авариями. В качестве исходных данных для УРКБ установки могут быть использованы данные анализа безопасности установки, но одного анализа безопасности недостаточно, поскольку в нем не учитываются все неисправности. Неисправности, вызванные кибератаками, могут привести установку в состояние, которое не было учтено в анализе безопасности.

3.8. По итогам процессов УРКБ установки должны быть определены потенциальные последствия компрометации системы вследствие кибератаки на СКУ, связанные с ядерной безопасностью, физической ядерной безопасностью, учетом и контролем ядерного материала. При анализе последствий атаки на ту или иную СКУ следует учитывать возможность того, что эта атака может быть частью более крупной атаки, затрагивающей несколько СКУ, или комбинации кибератаки и физического нападения. Затем этот анализ может быть использован для присвоения отдельным системам и компонентам СКУ соответствующих уровней защиты исходя из потенциальных последствий их отказа или неисправности.

3.9. Уровни защиты, присваиваемые СКУ, могут быть увязаны с иерархическим перечнем потенциальных последствий для ядерной или физической безопасности. Например, могут быть использованы состояния

---

[13] Иерархия и определения состояний станции приведены в Глоссарии по вопросам безопасности [7], если не указано иное.

станции, последствия саботажа (диверсии), иерархические уровни категоризации ядерных материалов или их сочетание, как показано в примерах, приведенных в пп. 3.10–3.13 и 3.15.

3.10. Исходя из соображений безопасности для обозначения потенциальных последствий кибератаки на СКУ для ядерной безопасности могут быть использованы состояния станции. Например, состояния станции могут быть увязаны с уровнями защиты СКУ так, как указано ниже (ситуации перечислены в порядке увеличения тяжести последствий).

1) Нормальная эксплуатация: кибератака на СКУ не может вывести работу установки за пределы и условия, предусмотренные для нормальной эксплуатации.
2) Ожидаемое при эксплуатации событие: кибератака на СКУ может привести к такому отклонению состояния станции от нормального режима эксплуатации, которого можно ожидать, но которое, с учетом соответствующих проектных положений, не вызовет значительного повреждения узлов, важных для безопасности, и не приведет к возникновению аварийных ситуаций.
3) Проектная авария[14]: кибератака на СКУ может вызвать аварийные условия, которые остаются в пределах проектных основ установки и для которых повреждение ядерного материала (или другого радиоактивного материала) и выброс радиоактивного материала удерживаются в разрешенных пределах.
4) Запроектные условия: кибератака на СКУ может вызвать аварийные условия, которые не учтены в проектных авариях, но учтены в процессе проектирования установки в соответствии с методологией улучшенной оценки и при которых выбросы радиоактивного материала удерживаются в допустимых пределах. Запроектные условия могут включать условия тяжелых аварий.

3.11. Последствия саботажа (диверсии) в отношении функций, выполняемых СКУ, также могут быть связаны с уровнями защиты. Такой подход предполагает установление государством предела неприемлемых радиологических последствий (НРП), как это рекомендовано в [2], п. 3.44. Определение предела НРП может основываться на количественных или качественных критериях, которые могут быть выражены показателями выбросов радионуклидов (например, выброс, превышающий некоторое

[14] Иерархия и сопроводительный текст для проектной аварии и запроектных условий взяты из [7].

определенное количество), доз (например, выброс, приводящий к облучению человека, находящегося в некоторой определенной точке, обычно за пределами площадки, в дозе, превышающей некоторое определенное значение) или состояния установки (например, саботаж (диверсия), который может привести к значительному повреждению активной зоны реактора). Как указывается в [11], пп. 3.94 и 95:

> «...цели, саботаж (диверсия) в отношении которых может привести к существенному радиологическому выбросу, серьезно влияющему на население и окружающую среду вне границ ядерной установки, требуют наиболее высокого уровня защиты. Такое экстремальное событие, согласно... [ссылка на [2]], влечет за собой серьезные радиологические последствия.
>
> Следовательно, государство должно также определить предел серьезных радиологических последствий».

3.12. В [11] приведен пример иерархического списка потенциальных последствий саботажа (диверсии), который для функций СКУ представлен в обобщенном виде ниже, в порядке возрастания тяжести последствий.

— Радиологические последствия ниже предела НРП. Цели, порождающие столь малые последствия, нуждаются в соответственно низком уровне защиты.
— НРП можно разделить на три категории, по возрастанию тяжести последствий:
  - последствия уровня С: саботаж (диверсия), который может привести к облучению лиц на площадке в дозах, требующих принятия срочных защитных мер для минимизации последствий для здоровья персонала на площадке;
  - последствия уровня В: саботаж (диверсия), который может привести к облучению или загрязнению за пределами площадки, требующим принятия срочных защитных мер для минимизации последствий для здоровья за пределами площадки (также могут считаться радиологическими последствиями высокого уровня);
  - последствия уровня А: саботаж (диверсия), который может привести к возникновению серьезного детерминированного эффекта для здоровья за пределами площадки (вероятно, также будет считаться радиологическими последствиями высокого уровня).

3.13. Уровни защиты также могут быть увязаны с возможностью несанкционированного изъятия ядерного материала. Потенциальные последствия кибератак на СКУ, выполняющие функции физической защиты или учета и контроля ядерного материала, могут быть увязаны с уровнями защиты на основе категории материала, который может подвергнуться несанкционированному изъятию. В [2], таблица I, указаны критерии категоризации ядерного материала и далее приведены рекомендации по физической защите, основанные на этой категоризации.

3.14. В настоящее время на международном уровне не существует согласованной модели, которая отображала бы полностью интегрированную иерархию всех последствий для ядерной и физической безопасности, порождаемых авариями и событиями в области физической ядерной безопасности, возникающими в результате кибератак. Однако оператор или государство должны разработать такую иерархию на национальном уровне.

3.15. При оценке совокупных последствий кибератаки на СКУ установки могут быть учтены и другие последствия, такие как потеря репутации. Перечень возможных последствий приведен в [12].

3.16. Тактика и методы действий злоумышленников постоянно меняются, и на ядерных установках должна быть сформирована культура физической ядерной безопасности, предполагающая постоянный анализ рисков в области компьютерной безопасности и позволяющая адаптировать программу компьютерной безопасности установки. О культуре физической ядерной безопасности более подробно говорится в [13].

3.17. Следует проанализировать конфигурацию системы и деятельность, связанную с СКУ, оснащенными цифровым оборудованием, в целях выявления изменений в путях логического и физического доступа, которые могут открыть лазейки для использования злоумышленником. Эта деятельность, связанная с СКУ, включает в себя временное техническое обслуживание, процессы закупок, поддержку со стороны поставщиков, связь с полевыми устройствами и обновление ПО в ручном режиме.

3.18. УРКБ установки — это многократно повторяющийся и циклический процесс, который может включать первоначальный анализ, идентификацию и оценку угроз, определение уровней защиты, периодический обзор и анализ актуализированных данных. Следует наладить четкий процесс согласования для изучения и проверки результатов нового или актуализированного анализа.

3.19. Для новых установок УРКБ установки должно выполняться как часть процесса проектирования, а его результаты должны согласовываться до завершения стадии первоначального ввода в эксплуатацию.

3.20. Для существующих установок исходные данные для нового или актуализированного УРКБ установки могут включать анализ безопасности, детали архитектуры безопасности и технологического процесса, а также ранее согласованные результаты УРКБ установки.

ВЗАИМОСВЯЗЬ С УРКБ СИСТЕМЫ

3.21. В процессе УРКБ системы должны использоваться результаты УРКБ установки (если таковые имеются) и проектные документы СКУ в качестве исходного материала для определения риска безопасности, связанного с кибератаками на одну или несколько систем, подсистем или компонентов СКУ. Оцененный риск для компьютерной безопасности СКУ должен быть проанализирован и зафиксирован документально.

3.22. Оператор должен распределить роли и обязанности по оценке рисков в области компьютерной безопасности СКУ и управлению этими рисками на протяжении всего жизненного цикла СКУ. Обеспечение компьютерной безопасности требует целенаправленных усилий со стороны многопрофильных организаций и групп. Например, оператором могут быть образованы рабочие группы, отвечающие за управление процессами и действиями по обеспечению компьютерной безопасности, а также за получение разрешений.

3.23. Оператору следует вести инвентарный перечень СКУ, включая ПО, подсистемы и компоненты, который корректируется и актуализируется на протяжении всего жизненного цикла системы. Этот инвентарный перечень должен использоваться оператором при осуществлении УРКБ системы.

3.24. Компоненты СКУ должны быть оценены и отнесены к соответствующему уровню защиты на основе УРКБ системы. Для этих компонентов следует определить последствия для ядерной и физической безопасности, которые могут возникнуть в результате неисправности или компрометации. Если на установке выделены контуры безопасности, то следует определить такой контур и отнести к нему соответствующий компонент.

3.25. При осуществлении УРКБ системы оператору следует учесть возможность совершения кибератаки на каждом этапе жизненного цикла СКУ. При оценке оператору следует также учесть, что кибератаки могут затрагивать отдельную систему или несколько систем и могут использоваться в сочетании с другими формами злоумышленных действий, причиняющими физический ущерб. В процессе УРКБ системы следует также учесть злоумышленные действия, которые могут внести изменения в технологическую сигнализацию, данные конфигурации оборудования или ПО.

3.26. Кроме того, в процессе УРКБ системы должны быть приняты во внимание все векторы атаки, которые могут быть использованы для внедрения в СКУ вредоносного кода или данных. Например, вредоносный код может быть внедрен в СКУ через коммуникационные соединения, поставляемые продукты и услуги или портативные устройства, временно подключенные к целевому оборудованию.

3.27. В ходе УРКБ системы должна быть определена вероятность наступления каждого потенциального последствия, связанного с СКУ, путем использования в качестве исходных данных следующего: наличия конкретных векторов атаки, которые могут быть использованы для внедрения в СКУ вредоносного кода или данных; применения и эффективности мер компьютерной безопасности; возможностей, которые дает угроза; другой соответствующей информации.

3.28. УРКБ системы — это многократно повторяющийся и циклический процесс, который, как и УРКБ установки, включает в себя первоначальный анализ, применение мер компьютерной безопасности, периодический обзор и анализ актуализированных данных. О повторном проведении УРКБ системы следует задуматься, когда происходит одно из следующих событий:

— пересматривается УРКБ установки или анализ безопасности установки;
— производится модификация системы;
— происходят соответствующие события или инциденты в области физической безопасности;
— выявляются новые или изменившиеся угрозы или уязвимости.

3.29. В процессе УРКБ системы должны быть выявлены действия или отсутствие действий со стороны человека, которые могут негативно повлиять на физическую безопасность.

ВЫБОР МЕР КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

3.30. Руководящие указания, приведенные в пп. 3.31–3.34, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

3.31. Каждой системе, подсистеме или компоненту СКУ должен быть присвоен уровень защиты сообразно потенциальным последствиям ее отказа или неисправности как для ядерной, так и для физической безопасности.

3.32. Применение мер компьютерной безопасности к каждой СКУ должно определяться присвоенным ей уровнем защиты либо уровнем защиты того контура безопасности, в котором она находится — в зависимости от того, какой из этих уровней выше.

3.33. Для каждого уровня защиты должны быть идентифицированы и определены требования компьютерной безопасности. Следует оценить эффективность мер по выполнению этих требований, чтобы убедиться, что для СКУ, отнесенных к каждому уровню защиты, обеспечена достаточная защита.

3.34. Если меры компьютерной безопасности не могут обеспечить достаточной защиты СКУ на каждом уровне защиты, следует задуматься о принятии дополнительных или альтернативных мер, например о применении средств физической защиты на уровне установки, независимых электронных функций, мер по перепроектированию системы или административных мер, позволяющих устранить конкретные уязвимости или уменьшить последствия неисправности.

ВЗАИМОСВЯЗЬ МЕЖДУ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ И ФИЗИЧЕСКОЙ БЕЗОПАСНОСТЬЮ

3.35. В [8], п. 1.2, говорится следующее:

> «Обеспечение физической ядерной безопасности и обеспечение ядерной безопасности преследуют общую цель — это защита людей, имущества, общества и окружающей среды. Меры по обеспечению физической безопасности и меры по обеспечению безопасности

должны разрабатываться и осуществляться в комплексе, чтобы добиться синергии между этими двумя областями деятельности, а также таким образом, чтобы меры по обеспечению физической ядерной безопасности не ставили под угрозу безопасность, а меры по обеспечению безопасности не ставили под угрозу физическую безопасность».

Дополнительные руководящие указания по вопросам ядерной безопасности СКУ можно найти в [4, 6].

3.36. Целесообразность применения той или иной меры компьютерной безопасности будет определяться соображениями ядерной безопасности, физической безопасности и эксплуатации. Выбор мер компьютерной безопасности для СКУ требует участия персонала, отвечающего за ядерную безопасность, физическую безопасность и эксплуатацию. Меры компьютерной безопасности не могут существовать в отрыве от соображений ядерной безопасности, а средства ядерной безопасности — в отрыве от соображений физической безопасности. Например, по соображениям ядерной безопасности определенные функции физической безопасности (такие как сбор учетных документов аудита или срабатывание охранной сигнализации) могут быть реализованы в отдельных системах, которые могут контролировать СКУ, но не оказывают негативного влияния на способность системы выполнять свои основные функции. В иных случаях активное использование досмотровых сканеров только тогда, когда СКУ не работают, может решать задачи обеспечения физической безопасности, ограничивая при этом воздействие на рабочие системы.

3.37. Неправильно спланированные меры компьютерной безопасности могут создать возможность для определенных типов отказа системы, повысить вероятность ложных срабатываний и подорвать способность системы надежно выполнять свою функцию ядерной безопасности. Например, неправильно спланированная реализация в СКУ системы обнаружения вредоносных программ или вирусов может усложнить СКУ, увеличить время отклика системы и привести к тому, что СКУ станет уязвимой для злоумышленного использования. Вместе с тем грамотно разработанная мера технического контроля, гарантирующая, что на СКУ будет установлено только проверенное и одобренное ПО, может улучшить способность этой системы надежно выполнять свою функцию ядерной безопасности, дав при этом значительный эффект с точки зрения физической безопасности.

3.38. Многие функции, заложенные в СКУ из соображений ядерной безопасности, могут также иметь преимущества с точки зрения физической безопасности. Одним из примеров является проверка полученных данных на достоверность, аутентичность и целостность, прежде чем они будут использоваться в какой-либо функции СКУ.

3.39. Могут быть ситуации, когда та или иная мера компьютерной безопасности не может быть реализована в соответствии с уровнем защиты, присвоенным СКУ, например из-за конфликта с основными функциями ядерной безопасности, но такие исключения должны быть тщательно проанализированы и обоснованы.

3.40. Весь комплекс мер компьютерной безопасности СКУ должен работать слаженно и не допускать возникновения единых точек отказа (или сам не создавать таких точек).

3.41. Стратегия обеспечения ядерной безопасности может негативно повлиять на физическую безопасность. Например, проектирование для нужд ядерной безопасности часто предполагает распределение функций между разными подсистемами (или процессорами), чтобы изолировать последствия отказа, а также обеспечение резервирования и неодинаковости систем, чтобы единичные отказы не ставили под угрозу выполнение важных функций. Эти стратегии приводят к росту количества подсистем в СКУ, что, в свою очередь, увеличивает количество целей для кибератаки. В этой связи необходимо принять меры для снижения риска того, что в результате кибератаки будут подорваны принципы неодинаковости или резервирования систем. Меры компьютерной безопасности не должны привносить новых уязвимостей, которые могут привести к отказам по общей причине этих резервных и разнородных систем.

СООБРАЖЕНИЯ ЯДЕРНОЙ БЕЗОПАСНОСТИ ПРИ ПРИНЯТИИ МЕР КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

3.42. Руководящие указания, содержащиеся в пп. 3.43–3.52, применимы ко всем СКУ, важным для ядерной безопасности.

3.43. Реализация мер компьютерной безопасности не должна отрицательно влиять на основные функции ядерной безопасности и эффективность работы СКУ.

3.44. Ни нормальное, ни неисправное функционирование какого бы то ни было средства компьютерной безопасности не должно негативно влиять на способность СКУ выполнять свою функцию ядерной безопасности.

3.45. Оператор должен определить, зафиксировать и учесть в анализе системных опасностей типы отказа мер компьютерной безопасности и то, как эти типы отказа отразятся на функциях СКУ.

3.46. Меры компьютерной безопасности, нацеленные на защиту человеко-системного интерфейса, не должны отрицательно влиять на способность оператора поддерживать ядерную безопасность установки. Оператор также должен учитывать негативные последствия таких действий, как перехват и модификация технологических данных, передаваемых на человеко-системный интерфейс (например, спуфинг), чтобы не дать оператору задействовать какую-либо функцию ядерной безопасности (например, ручное отключение) либо задержать выполнение этой функции.

3.47. Меры компьютерной безопасности, которые по практическим соображениям не могут быть интегрированы в СКУ, должны быть реализованы отдельно от СКУ. Для использования и технического обслуживания этих отдельных устройств могут потребоваться дополнительные меры административного контроля.

3.48. Меры компьютерной безопасности, интегрируемые в СКУ, должны разрабатываться в соответствии с руководящими указаниями по системам менеджмента, приведенными в [14], или эквивалентной альтернативной системой менеджмента и сертифицироваться на том же уровне, что и система, в которую эти меры интегрированы.

3.49. При возникновении коллизии между ядерной безопасностью и физической безопасностью следует оставить в силе проектные решения по обеспечению ядерной безопасности при условии, что оператором будет найдено совместимое техническое решение для удовлетворения требований компьютерной безопасности. Для снижения риска до приемлемого уровня должны быть реализованы компенсационные меры компьютерной безопасности, подкрепленные всесторонним обоснованием и анализом рисков безопасности. Реализуемые меры не должны долгое время оставаться исключительно мерами административного контроля. Отсутствие технического решения по обеспечению физической безопасности никогда не следует воспринимать как норму.

3.50. Оператор должен четко определить, кто несет основную ответственность за разработку, выбор и реализацию мер компьютерной безопасности, но эта работа должна вестись на совместной основе персоналом, отвечающим за деятельность по проектированию, обслуживанию, обеспечению ядерной и физической безопасности СКУ.

3.51. Анализ проекта СКУ должен показывать, что меры компьютерной безопасности, интегрированные в СКУ, и меры, реализованные в виде отдельных устройств, не окажут негативного влияния на выполнение заданных функций ядерной безопасности систем и компонентов, важных для ядерной безопасности.

3.52. Мероприятия по техническому обслуживанию средств компьютерной безопасности не должны отрицательно влиять на доступность СКУ.

4. КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ В ТЕЧЕНИЕ ЖИЗНЕННОГО ЦИКЛА СКУ

4.1. Проектирование СКУ для ядерных установок должно осуществляться в рамках интегрированной системы менеджмента установки[15] с целью обеспечить учет и реализацию всех требований компьютерной безопасности на всех стадиях жизненного цикла СКУ, а также соблюдение этих требований компьютерной безопасности в окончательном проекте. В [14] установлены общие требования безопасности для систем менеджмента ядерных установок. Кроме того, в [8], п. 3.12(a), говорится о важности интегрированных систем менеджмента для физической ядерной безопасности. В [3] более подробно рассматривается общая взаимосвязь между системами менеджмента и компьютерной безопасностью.

---

[15] Согласно [7], система менеджмента (управления) — это «ряд взаимосвязанных или взаимодействующих элементов (система) для установления политики и целей и обеспечения эффективного и результативного выполнения поставленных задач». В данной публикации это включает в себя организационную структуру, организационную культуру, политику и процессы, в том числе те, которые имеют целью поиск и выделение ресурсов (например, персонала, оборудования, инфраструктуры и рабочей среды) на разработку СКУ.

4.2. В [4], п. 2.13, говорится следующее:

> «В цифровых СКУ соответствие конечного продукта его целевому назначению главным образом, но не исключительно, обусловлено применением высококачественных процессов разработки, предусматривающих строгое регламентирование и применение проектных требований».

В п. 2.14 добавляется, что

> «в атомной энергетике, а также в других областях с особыми требованиями к обеспечению безопасности, таких как аэрокосмическая промышленность, применяются процессы разработки, как правило, представляемые в виде моделей жизненного цикла, описывающих процессы разработки электронных систем и взаимосвязь между этими процессами. <...> Как правило, процессы, имеющие отношение к определенному этапу разработки, объединяются в группу одной стадии жизненного цикла».

Вопросы компьютерной безопасности должны приниматься во внимание на всех стадиях жизненного цикла СКУ.

4.3. В [4], п. 2.17, указывается:

> «Для описания разработки СКУ необходимо применять три базовых уровня жизненных циклов:
>
> — жизненный цикл общей архитектуры СКУ[16];
> — жизненные циклы одной или нескольких отдельных СКУ;
> — жизненные циклы одного или нескольких отдельных компонентов СКУ: управление жизненными циклами компонентов, как правило, осуществляется в рамках процесса разработки платформы, и эти циклы не зависят от уровня общей архитектуры, а также от жизненных циклов на уровне отдельных систем. Жизненные циклы компонентов цифровых систем обычно подразделяются на отдельные жизненные циклы разработки программных и аппаратных (технических) средств».

---

[16] Как определено в [4], п. 3.10, «общая архитектура СКУ представляет собой организационную структуру отдельных СКУ станции».

4.4. Модели жизненного цикла и действия, отнесенные к каждой стадии жизненного цикла, обычно определяются разработчиками и операторами системы, но такое определение и реализация должны представлять собой междисциплинарную деятельность, охватывающую многие другие области, в том числе компьютерную безопасность. Как правило, разработчики несут основную ответственность за СКУ до тех пор, пока системы не будут переданы эксплуатирующей организации для монтажа, интеграции и ввода в эксплуатацию.

4.5. Поскольку жизненный цикл СКУ может охватывать несколько десятилетий, роль разработчиков или другие роли в течение жизненного цикла системы могут играть разные организации. Например, нередко бывает так, что поставщик выполняет первоначальную разработку, а покупатель позднее производит модификацию, особенно если эти модификации незначительны. Тот факт, что эти модификации производятся разными организациями, не отменяет необходимости применения мер компьютерной безопасности на всех стадиях жизненного цикла СКУ.

4.6. При первой же возможности меры компьютерной безопасности должны быть последовательно спланированы для всех жизненных циклов архитектуры, системы и компонентов СКУ. В ходе этого планирования следует уточнять, какие меры компьютерной безопасности будут применяться на каждой стадии для защиты архитектуры, систем и компонентов СКУ от кибератак, которые могут поставить под угрозу функции, важные для ядерной безопасности. Следует учитывать, что функции ядерной безопасности или меры компьютерной безопасности могут измениться на более поздних стадиях.

4.7. Процесс разработки СКУ должен быть направлен на минимизацию потенциальных уязвимостей и слабых мест в компьютерной безопасности и выявление потенциальных остаточных уязвимостей и слабых мест на каждой стадии жизненного цикла СКУ.

4.8. Хотя модели жизненного цикла могут быть организованы по-разному, в данной публикации в качестве основы для изложения соображений, относящихся к компьютерной безопасности, в течение жизненного цикла СКУ используются следующие условные стадии жизненного цикла:

— планирование процесса;
— разработка проектных основ;
— разработка общей архитектуры СКУ и распределение функций;

— установление требований к СКУ;
— подбор ранее разработанных изделий;
— детальное проектирование и реализация;
— интеграция системы;
— валидация системы;
— монтаж, интеграция и ввод в эксплуатацию;
— эксплуатация и техническое обслуживание;
— модификация;
— вывод из эксплуатации.

4.9. Помимо этих стадий, жизненный цикл СКУ также включает многие виды деятельности, которые являются общими для всех стадий жизненного цикла. Этими общими видами деятельности, важными с точки зрения компьютерной безопасности, являются:

— обеспечение качества;
— управление конфигурацией;
— верификация и валидация[17];
— оценка физической безопасности;
— документирование.

4.10. Требования и действия по обеспечению компьютерной безопасности для каждой стадии жизненного цикла должны быть соразмерны последствиям несанкционированного или ненадлежащего доступа, использования, раскрытия информации, манипулирования, нарушения работы или вывода из строя СКУ. Следует также учесть возможность компрометации любой системы, вспомогательной системы или информации, которая может негативно повлиять на ядерную или физическую безопасность.

4.11. Оставшаяся часть настоящего раздела разбита на подразделы, в которых приведены общие руководящие указания по компьютерной безопасности, применимые ко всем стадиям жизненного цикла, и

---

[17] В Глоссарии МАГАТЭ по вопросам безопасности [7] даются определения как верификации, так и валидации. Верификация компьютерной системы — это «*процесс*, имеющий целью обеспечить, чтобы данный этап в жизненном цикле *системы* удовлетворял требованиям, введенным на предыдущем этапе». Валидация компьютерной системы — это «*процесс* испытаний и оценки интегрированной компьютерной *системы* (аппаратные средства и программное обеспечение) с целью обеспечения соблюдения функциональных, эксплуатационных и интерфейсных требований».

руководящие указания по физической безопасности, относящиеся к отдельным стадиям жизненного цикла. При этом стадии рассматриваются только один раз, но руководящие указания следует применять ко всем жизненным циклам, в которых присутствует данная стадия.

ОБЩИЕ РУКОВОДЯЩИЕ УКАЗАНИЯ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

4.12. В политике обеспечения компьютерной безопасности ядерной установки определяются общие цели компьютерной безопасности этой установки. При планировании мер компьютерной безопасности установки и системы эти цели указываются в данной политике в ясной, конкретной и, по возможности, поддающейся измерению форме. Цели на уровне установки преобразуются в цели на уровне системы. В [3] содержатся дополнительные руководящие указания по обеспечению компьютерной безопасности на ядерных установках.

4.13. Политика обеспечения компьютерной безопасности должна включать элементы, касающиеся физической безопасности СКУ, и поэтому она должна применяться к любой организации, которая отвечает за деятельность в рамках жизненного цикла СКУ. Эти организации включают операторов, продавцов, подрядчиков и поставщиков, которые разрабатывают, внедряют и закупают СКУ, ПО и компоненты.

4.14. Каждая организация, ответственная за деятельность в рамках жизненного цикла СКУ, должна определить и задокументировать стандарты и протоколы, соответствующие применимой политике безопасности, чтобы свести к минимуму присутствие в аппаратных средствах, ПО и встроенном ПО недокументированного кода (например, программных закладок), вредоносного кода (например, средств проникновения в сеть, вирусов, червей, «троянских коней» и логических «бомб») и других нежелательных, ненужных или недокументированных функций или приложений с целью минимизации числа возможных путей, по которым может быть совершена кибератака.

4.15. Политика, программа, соответствующие стандарты и применимые протоколы в области компьютерной безопасности должны учитывать особенности каждой отдельной стадии жизненного цикла СКУ, чтобы защитить СКУ установки от компрометации.

4.16. Политика, программа, стандарты и протоколы в области компьютерной безопасности, а также все меры компьютерной безопасности должны соответствовать регулирующим требованиям и требованиям компьютерной безопасности.

4.17. Политика, стандарты и протоколы в области компьютерной безопасности могут быть предусмотрены в программе обеспечения физической безопасности СКУ организации либо включены в планы, относящиеся к жизненному циклу СКУ. На практике часто применяется смешанный подход.

АСПЕКТЫ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ, ОТНОСЯЩИЕСЯ К СКУ

4.18. В политике обеспечения компьютерной безопасности ядерных установок должен быть описан порядок применения дифференцированного подхода к реализации мер компьютерной безопасности СКУ. Дифференцированный подход должен применяться сообразно значимости для ядерной и физической безопасности каждой функции СКУ (например, в соответствии с уровнем защиты, присвоенным каждой системе). Руководство должно установить четкие цели политики обеспечения компьютерной безопасности, согласующиеся с общими целями ядерной и физической безопасности установки, и следить за их достижением, а также уделить особое внимание физической безопасности СКУ. Подробнее об общих соображениях в отношении политики и программы обеспечения компьютерной безопасности говорится в [3].

4.19. В политике обеспечения компьютерной безопасности должны учитываться следующие соображения, имеющие значение для СКУ:

— контроль доступа — как физического, так и логического — и использование наименьших привилегий;
— управление конфигурацией и активами, включая управление паролями, управление внесением исправлений, использование систем, усиление систем, контроль конфигурации, установление ограничений на использование мобильных устройств и съемных носителей, беспроводные устройства и сети, а также удаленный доступ;
— действия по проверке целостности систем и компонентов;
— процессы закупок;

— менеджмент рисков и угроз, включая процессы сбора, анализа, документирования данных и обмена данными с другими лицами, которые обязаны получать информацию об уязвимостях, слабых местах и угрозах и принимать соответствующие меры;
— реагирование на инциденты и восстановление;
— аудит и оценки.

4.20. В политике обеспечения компьютерной безопасности должны быть установлены роли и обязанности организаций или лиц, которые выполняют действия в рамках жизненного цикла СКУ.

ПРОГРАММА КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

4.21. Каждая организация, отвечающая за деятельность в рамках жизненного цикла СКУ, должна разработать и ввести в действие интегрированную или отдельную программу компьютерной безопасности, относящуюся к СКУ.

4.22. В программе компьютерной безопасности должны быть определены роли и обязанности для каждой стадии жизненного цикла каждой СКУ.

4.23. В программе компьютерной безопасности должно быть указано, что ответственные организации применяют концепцию глубокоэшелонированной защиты и определяют применимые меры компьютерной безопасности СКУ в соответствии с присвоенным им уровнем защиты.

4.24. В программе компьютерной безопасности должно быть определено, какие меры компьютерной безопасности будут применяться для защиты от злоумышленных действий, совершаемых инсайдерами, и от манипулирования СКУ (включая ее целостность) на каждой стадии жизненного цикла СКУ.

4.25. В программе компьютерной безопасности должно уточняться, что доступ к СКУ, компонентам, ПО, конфигурационным данным и инструментам контролируется на всех стадиях жизненного цикла СКУ. К примерам того, как на практике организуется контроль доступа, относятся принцип наименьших привилегий и предоставление информации исходя из служебной необходимости.

4.26. В программе компьютерной безопасности должны затрагиваться вопросы конфиденциальности мер компьютерной безопасности, включая защиту соответствующей документации сообразно уровню защиты СКУ, к которым относится эта документация.

4.27. В программе компьютерной безопасности должны учитываться потенциальные уязвимости и слабые места в компьютерной безопасности на каждой стадии жизненного цикла СКУ.

4.28. В программе компьютерной безопасности должен быть установлен процесс, посредством которого информация о безопасности СКУ, такая как данные об уязвимостях, обнаруженных в СКУ установки, или о конкретных средствах защиты, используемых для защиты этих систем, засекречивается как чувствительная информация и дробится[18]. В [8] чувствительная информация определяется как «информация в любой форме, включая программное обеспечение, несанкционированное раскрытие, корректировка, изменение, уничтожение или неиспользование которой могут поставить под угрозу физическую ядерную безопасность».

4.29. Ядерным установкам и связанным с ними организациям настоятельно рекомендуется обмениваться прочей нечувствительной информацией об уязвимостях, чтобы установки были лучше подготовлены к ситуациям, когда информация об уязвимостях СКУ будет распространена и передана потенциальным злоумышленникам. Руководящие указания по защите ядерной информации (включая ее засекречивание) приведены в [15].

4.30. В программе компьютерной безопасности СКУ должно быть предусмотрено проведение и документирование периодического анализа и оценки компьютерной безопасности на каждой стадии жизненного цикла.

4.31. В программе компьютерной безопасности должны быть указаны меры компьютерной безопасности, обеспечивающие создание безопасной среды, в которой может вестись деятельность по разработке.

4.32. В случае устаревших СКУ можно в большей степени полагаться на меры административного контроля и изоляцию, чем в случае современных систем. В программе компьютерной безопасности должны быть определены

---

[18] Дробление означает разделение информации на отдельно контролируемые блоки, чтобы не дать возможности инсайдерам собрать всю информацию, необходимую для совершения попытки злоумышленного действия.

и закреплены дополнительные компенсационные меры компьютерной безопасности, необходимые для обеспечения компьютерной безопасности устаревших СКУ.

БЕЗОПАСНАЯ СРЕДА РАЗРАБОТКИ

4.33. Руководящие указания, приведенные в пп. 4.34–4.40, относятся к разработке всех систем, подсистем и компонентов СКУ, к которым применяется дифференцированный подход к компьютерной безопасности в соответствии с присвоенным им уровнем защиты.

4.34. СКУ должны разрабатываться в безопасной среде разработки. Это относится как к внутренним, так и к внешним сайтам. При присвоении уровня защиты этой среде следует учитывать уровень защиты системы в целевой среде, уровень защиты других систем, разрабатываемых или хранящихся в общей среде разработки, а также средств разработки. Меры компьютерной безопасности среды должны быть оценены на предмет соответствия требованиям присвоенного уровня защиты.

4.35. Безопасная среда разработки должна включать меры административного контроля, такие как контроль конфигурации и управление активами.

4.36. Для контроля доступа к безопасным средам разработки должны использоваться меры физического контроля.

4.37. Тестовое и вспомогательное оборудование, используемое в средах разработки СКУ, должно быть проверено с целью убедиться в том, что использование этого оборудования не открывает путей для внедрения в безопасную среду разработки вредоносного кода или данных.

4.38. Меры компьютерной безопасности должны обеспечивать контроль перемещения данных и устройств на всех этапах разработки, чтобы гарантировать, что вредоносный код или данные не будут внедрены в безопасную среду разработки, и защитить чувствительную информацию, связанную с СКУ. Эти меры компьютерной безопасности должны включать в себя меры административного и технического контроля, такие как ограничения на использование и процедуры контроля съемных

носителей и мобильных устройств. Безопасная среда разработки должна рассматриваться как отдельная среда, которая физически и логически отделена от операционной и корпоративной бизнес-среды.

4.39. Должны быть введены меры компьютерной безопасности для защиты целостности безопасной среды разработки, а также входных и выходных данных разработки (например, данных, конфигурационных файлов, обновлений ПО и патчей к нему) во время передачи данных между безопасной средой разработки и целевой средой. Эти меры могут включать в себя автоматизированные системы конфигурирования активов, где польза с точки зрения защиты безопасной среды разработки и целевой среды подтверждена аналитически.

4.40. Инструменты сторонних производителей или поставщиков, используемые для разработки СКУ, должны быть протестированы, проверены и защищены сообразно уровню защиты, присвоенному среде разработки.

ПЛАНЫ ЧРЕЗВЫЧАЙНЫХ МЕР

4.41. Организации, выполняющие одно или несколько действий в рамках жизненного цикла СКУ, должны разработать планы и процедуры чрезвычайных мер для недопущения продолжения и эскалации аномального поведения, а также для восстановления системы после инцидентов, связанных с компьютерной безопасностью. Эти планы и процедуры чрезвычайных мер должны изучаться, периодически отрабатываться и актуализироваться при обнаружении недоработок.

4.42. Оператору следует разработать план реагирования на инциденты в области компьютерной безопасности, состоящий из процедур, которые позволяют выявить, идентифицировать возможные аномальные или подозрительные формы поведения, обнаруженные в СКУ и связанных с ними системах, и отреагировать на них.

4.43. В плане реагирования на инциденты в области компьютерной безопасности должны быть учтены требования к сбору информации и юридические требования для того, чтобы во время событий, связанных с безопасностью, могли сохраняться доказательства, необходимые для проведения расследования.

4.44. План реагирования на инциденты в области компьютерной безопасности должен предусматривать назначение персонала в группу реагирования на инциденты, связанные с компьютерной безопасностью установки. Эта группа должна быть создана на установке для реагирования на все выявляемые инциденты в области компьютерной безопасности. В число назначенных сотрудников могут входить те, кто обладает экспертными знаниями в области конкретных СКУ или компьютерной безопасности.

4.45. Копии файлов для резервного копирования и восстановления СКУ, имеющие важное значение для планов и процедур чрезвычайных мер, должны включать ПО, основные данные и конфигурационные файлы. Эти копии должны храниться в некоем месте, физически отделенном от места расположения источника, для защиты от отказов по общей причине. Для защиты этих копий от хищения, манипуляций, а также удаления или уничтожения следует использовать меры компьютерной безопасности.

ПРОДАВЦЫ, ПОДРЯДЧИКИ И ПОСТАВЩИКИ СКУ

4.46. В пп. 4.47–4.53 «продавцы», «подрядчики» и «поставщики» означают тех, кто поставляет на ядерную установку цифровое оборудование, ПО и услуги для СКУ, к которым применяется дифференцированный подход к компьютерной безопасности в соответствии с присвоенным системе уровнем защиты. Оператор должен контролировать применение руководящих указаний, содержащихся в пп. 4.47–4.53, посредством заключения договора с соответствующими продавцами, подрядчиками или поставщиками.

4.47. У организаций, заключающих подрядные и субподрядные договора о поставках, должны иметься надежные и поддающиеся проверке процессы обеспечения компьютерной безопасности.

4.48. Продавцы, подрядчики и поставщики должны отвечать всем применимым требованиям компьютерной безопасности. Это предполагает применение мер компьютерной безопасности, указанных оператором, в ходе технической поддержки, предоставляемой на месте или на предприятии продавца, подрядчика или поставщика, а также во время любой транзитной перевозки или хранения приобретенных товаров.

4.49. У продавца, подрядчика или поставщика должен быть налажен процесс управления компьютерной безопасностью.

4.50. Применимые требования компьютерной безопасности на объектах, где продавец, подрядчик или поставщик выполняет определенные действия с СКУ, должны быть четко определены оператором в договоре в зависимости от уровня защиты, присвоенного системе, подсистеме или компоненту.

4.51. Должен существовать процесс, позволяющий оператору и продавцу, подрядчику или поставщику информировать друг друга об уязвимостях и координировать усилия по реагированию и смягчению последствий.

4.52. Продавец, подрядчик или поставщик должен доказать, что у него имеется надежный механизм приема сообщений об уязвимостях, их оценки и информирования о них ядерной установки в течение всего периода предоставления услуг по договору. Это требование может выходить за рамки обычного гарантийного срока и действовать на протяжении жизненного цикла установленного оборудования. В этих случаях данный механизм должен быть включен на увеличенный период времени в договорные обязательства, согласованные продавцами, подрядчиками или поставщиками.

4.53. Необходимо проводить аудиты и оценку работы продавцов, подрядчиков или поставщиков, ответственных за проектирование, разработку, интеграцию и техническое обслуживание СКУ, и сообщать о результатах оператору.

ОБУЧЕНИЕ ПО ВОПРОСАМ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

4.54. Весь персонал, работающий с СКУ, в том числе с чувствительной информацией, связанной с этими системами, должен периодически проходить обучение по основам и процедурам обеспечения компьютерной безопасности.

4.55. Весь персонал, имеющий физический или логический доступ к СКУ, должен иметь квалификацию, соответствующую его обязанностям в области компьютерной безопасности, и проходить специальное обучение по вопросам безопасности СКУ в соответствии с его ролями и обязанностями для поддержания своей квалификации.

4.56. Все сотрудники, имеющие физический или логический доступ к СКУ, должны повысить свою компетентность до уровня, соответствующего их роли, чтобы уметь решать задачи компьютерной безопасности и распознавать потенциальные инциденты в области компьютерной безопасности. Эти лица могут быть проинформированы о влиянии изменений, внесенных либо в СКУ, либо в связанные с ней меры компьютерной безопасности, к которым они имеют доступ.

4.57. Сотрудники, включенные в группу реагирования на инциденты в области компьютерной безопасности, должен пройти обучение по вопросам выявления инцидентов в области компьютерной безопасности и реагирования на них. Это может предполагать использование испытательного стенда СКУ в качестве компонента учебной программы по безопасности СКУ.

4.58. Инженерно-технический, эксплуатационный и обслуживающий персонал должен быть обучен выполнению функций СКУ, связанных как с ядерной, так и с физической безопасностью.

4.59. Персонал, занимающийся проектированием СКУ, должен пройти обучение по безопасному проектированию и программированию СКУ для ядерных установок (например, как учитывать соображения безопасности при разработке ПО).

ОБЩИЕ ЭЛЕМЕНТЫ ВСЕХ СТАДИЙ ЖИЗНЕННОГО ЦИКЛА

4.60. В большинстве случаев требования безопасности к системе менеджмента [14] и общие руководящие указания, содержащиеся в соответствующих руководствах по безопасности [16, 17], содержат достаточно рекомендаций в отношении деятельности системы менеджмента, связанной с компьютерной безопасностью, на всех стадиях жизненного цикла СКУ. Однако есть несколько областей, в которых требуется более конкретные рекомендации.

Системы менеджмента

4.61. Руководящие указания, приведенные в пп. 4.62–4.70, относятся ко всем организациям, выполняющим одно или несколько действий в рамках жизненного цикла СКУ, к которым применяется дифференцированный подход к компьютерной безопасности в соответствии с присвоенным системе уровнем защиты.

4.62. Требования безопасности 6–8 для систем менеджмента, приведенные в [14], пп. 4.8–4.20, следует использовать при разработке регулирующих требований и/или требований компьютерной безопасности, относящихся к системам менеджмента.

4.63. Каждая организация, отвечающая за разработку, установку, эксплуатацию, техническое обслуживание или вывод из эксплуатации систем или компонентов СКУ, должна учитывать вопросы компьютерной безопасности СКУ в своей интегрированной системе менеджмента.

4.64. Интегрированная система менеджмента установки должна поддерживать процессы и процедуры обеспечения компьютерной безопасности.

4.65. Деятельность на протяжении жизненного цикла должна вестись в рамках системы менеджмента, предусматривающей адекватные меры по обеспечению физической безопасности систем и компонентов СКУ.

4.66. Должны существовать поддающиеся аудиторской проверке процессы и процедуры, подтверждающие, что системы, подсистемы и компоненты СКУ, важные для поддержания компьютерной безопасности, продолжают выполнять свои функции безопасности на протяжении всего срока службы.

4.67. Должны быть предусмотрены проверки СКУ на предмет безопасности (например, проверки конфигурации) в течение всего жизненного цикла СКУ, показывающие, что процедуры безопасности соблюдаются, а требуемый стандарт качества изготовления достигнут (например, не было добавлено лишних компонентов).

4.68. Следует проводить независимые[19] инспекции для подтверждения того, что процессы и процедуры обеспечения компьютерной безопасности выполняются так, как описано в плане обеспечения качества оператора.

4.69. Следует подготавливать подробные учетные документы о деятельности в рамках жизненного цикла, которые должны храниться таким образом, чтобы их можно было в любой момент просмотреть и сравнить с требованиями компьютерной безопасности. В этих документах должны описываться все инциденты, связанные с компьютерной безопасностью, а также меры реагирования или чрезвычайные меры, принятые по следам этих инцидентов.

4.70. Уполномоченные лица, имеющие привилегированный логический или физический доступ к СКУ, должны проверяться на благонадежность, проходить обучение по вопросам компьютерной безопасности, а также быть объектами наблюдения за поведением в соответствии с программой уменьшения инсайдерской угрозы на установке или эквивалентной программой (см. [5]).

Анализ и аудит компьютерной безопасности

4.71. Руководящие указания, приведенные в пп. 4.72–4.77, относятся ко всем организациям, выполняющим одно или несколько действий в рамках жизненного цикла СКУ, к которым применяется дифференцированный подход к компьютерной безопасности в соответствии с присвоенным им уровнем защиты.

4.72. Следует на регулярной основе проводить анализ и аудит компьютерной безопасности СКУ и связанной с ними деятельности, чтобы удостовериться в соблюдении регулирующих положений, политики обеспечения компьютерной безопасности, а также в учете передового опыта обеспечения безопасности СКУ.

4.73. Анализ компьютерной безопасности СКУ должен быть независимым и выполняться квалифицированными внутренними и/или внешними экспертами.

---

[19] «Независимая» означает, что инспекция проводится лицом или организацией, посторонними по отношению к объекту проверки.

4.74. Должны быть определены и задокументированы правила и процедуры проведения такого анализа, включающие описание ролей и обязанностей.

4.75. В ходе анализа компьютерной безопасности СКУ должно проверяться выполнение связанных с ними мер компьютерной безопасности и их эффективность.

4.76. Работающие СКУ не должны тестироваться методами интрузивной оценки. Тесты методами интрузивной оценки предполагают попытку использования какой-либо уязвимости (например, как при проведении тестов на проникновение), которая может изменить условия эксплуатации или конфигурацию СКУ, выведя их за рамки проектных основ. Оператору следует рассмотреть возможность использования контролируемых методов для проведения тестов без полезной нагрузки, когда установка находится в состоянии, при котором предотвращаются НРП: например, когда установка находится в состоянии останова или при выгруженном топливе. Проведение и выполнение этих тестов должно регламентироваться правилами и процедурами установки. Эти тесты должны быть разработаны по отдельности для каждой системы. В тестах методами интрузивной оценки должна участвовать группа реагирования на инциденты в области компьютерной безопасности.

4.77. Учетные документы по анализу компьютерной безопасности и соответствующие аналитические данные должны архивироваться, актуализироваться и сохраняться на протяжении всего жизненного цикла СКУ.

Управление конфигурацией для нужд компьютерной безопасности

4.78. Руководящие указания, приведенные в пп. 4.79–4.87, относятся ко всем системам, подсистемам и компонентам СКУ, которым присвоен тот или иной уровень защиты.

4.79. Действия по контролю конфигурации ПО могут помочь в предотвращении и обнаружении инцидентов в области компьютерной безопасности, хотя главной целью этих действий не является решение конкретных задач физической ядерной безопасности. Выгода с точки зрения компьютерной безопасности, полученная в результате выполнения этих действий, должна быть проанализирована и подтверждена, прежде чем будет признано, что данную выгоду принесли именно эти действия. Например, при помощи этих действий может быть обнаружен инцидент

в области компьютерной безопасности, но время начала реагирования на обнаруженный инцидент, скорее всего, будет недостаточным для защиты системы по сравнению с временем реагирования в системе компьютерной безопасности, предусматривающей меры эшелонированной компьютерной защиты с элементами автоматического реагирования.

4.80. Неуправляемые изменения конфигурации ПО являются серьезным источником новых уязвимостей и непредсказуемых ситуаций. Как правило, система управления конфигурацией, используемая в СКУ, представляет собой типовую систему, которая также управляет многими другими типами систем. Тем не менее систему управления конфигурацией следует использовать таким образом, чтобы она включала в себя знания как об СКУ, так и о мерах по обеспечению их компьютерной безопасности.

4.81. Управление конфигурацией зависит от управления изменениями, которое представляет собой процесс, призванный обеспечить, чтобы при изменении компьютерной системы применялись утвержденные процессы проектирования и выполнялась соответствующая верификация и валидация. Оно также включает в себя контроль документов, которыми подкрепляются эти процессы. В п. 5.26 публикации «Применение системы управления для установок и деятельности», Серия норм безопасности МАГАТЭ, № GS-G-3.1 [16], говорится следующее:

> «Типы документов, которые подлежат контролю, должны включать в себя, но не должны ограничиваться следующим перечнем: документы, которые определяют систему управления; требования по безопасности; инструкции по выполнению работ; отчеты по проведенным оценкам; чертежи; файлы данных; технические требования; машинные коды; заказы на поставку и связанные с этим документы; и документы поставщика».

4.82. Меры компьютерной безопасности СКУ, основанные на процессе управления конфигурацией установки, должны соответствовать требованиям контроля конфигурации установки, применимым к соответствующей СКУ.

4.83. Управление конфигурацией для принятия мер компьютерной безопасности, связанных с СКУ, должно быть обеспечено на протяжении всего жизненного цикла СКУ.

4.84. В управление конфигурацией для принятия мер компьютерной безопасности, связанных с СКУ, должны быть включены методы и процедуры анализа последствий изменений конфигурации, утверждения изменений конфигурации, обеспечения корректного объединения версий ПО, выпуска проектной документации и выдачи разрешений на использование ПО, а также организации и ведения учета изменений конфигурации в хронологическом порядке (например, того, какие версии ПО применяются на определенном этапе проектирования).

4.85. Процедуры идентификации, хранения и выдачи разрешений на использование компонентов СКУ и связанных с ними мер технического контроля должны быть защищены от компрометации.

4.86. Конфигурационные документы по мерам компьютерной безопасности, связанным с СКУ, должны храниться и защищаться от несанкционированного доступа или компрометации. Эта информация должна быть засекречена как чувствительная информация, и доступ к ней должен предоставляться исходя из служебной необходимости.

4.87. К ПО и конфигурационным файлам в процессе разработки, транспортировки, установки и использования должны применяться меры технического контроля, ограничивающие доступ к ним и обеспечивающие их целостность.

Верификация и валидация

4.88. Руководящие указания, приведенные в пп. 4.89–4.94, относятся ко всем системам, подсистемам и компонентам СКУ, которым присвоен тот или иной уровень защиты.

4.89. На каждой стадии процесса разработки СКУ используется информация, полученная на более ранних стадиях, и получаются результаты, которые будут играть роль исходных данных на более поздних стадиях. Верификация должна проводиться после завершения одной фазы процесса разработки и перед переходом к следующей фазе процесса разработки и должна включать оценку мер компьютерной безопасности.

4.90. Перед завершением этапа процесса разработки СКУ, на котором система вводится в эксплуатацию, должна быть выполнена валидация СКУ с целью удостовериться в том, что требования компьютерной безопасности выполнены и что при этом система продолжает

соответствовать функциональным, эксплуатационным и интерфейсным требованиям. Это должно обеспечить высокую степень уверенности в том, что система будет выполнять свою функцию надлежащим образом. Валидация мер компьютерной безопасности должна выполняться коллективами, отдельными специалистами или группами, не зависящими от проектировщиков и разработчиков. Например, объем независимой валидации и степень независимости должны быть соразмерны уровню защиты, присвоенному соответствующей системе или компоненту — независимо от того, выполняется ли валидация персоналом продавца, подрядчика или поставщика либо внешними экспертами, посторонними по отношению к продавцу, подрядчику или поставщику.

4.91. Мероприятия по верификации и валидации должны показывать, что СКУ удовлетворяет соответствующим требованиям компьютерной безопасности.

4.92. Оператор должен проводить верификацию и валидацию каждой меры технического контроля, чтобы убедиться в том, что она обеспечивает защиту СКУ на заданном уровне и не снижает надежности ее функций, связанных с ядерной или физической безопасностью.

4.93. Объем усилий по верификации и валидации мер компьютерной безопасности должен быть соразмерен уровню защиты, присвоенному соответствующей СКУ, либо классификации СКУ по безопасности — в зависимости от того, какой из критериев является более строгим.

4.94. При верификации и валидации должны выявляться, регистрироваться и документироваться обнаруженные уязвимости, слабые места или другие аномалии и меры по их устранению. С учетом размера и сложности большинства современных компьютерных систем гарантировать полноту результатов этих действий или их успешность в плане выявления всех аномалий может быть трудно. Например, автоматизированные инструменты для анализа программного кода зависят от используемой платформы и языка программирования и могут быть успешными лишь частично. Кроме того, может оказаться невозможным просканировать определенные операционные системы, машинный код и функции вызываемых библиотек, в которых могут содержаться уязвимости, которые могут быть использованы злоумышленником.

Оценки компьютерной безопасности

4.95. Руководящие указания, приведенные в пп. 4.96–4.100, относятся ко всем системам, подсистемам и компонентам СКУ, которым присвоен тот или иной уровень защиты.

4.96. На каждой стадии жизненного цикла СКУ должны выполняться оценки компьютерной безопасности в целях выявления потенциальных угроз, а также уязвимостей и слабых мест.

4.97. Необходимо отслеживать публичную информацию или информацию из открытых источников, а также информацию от продавцов, подрядчиков или поставщиков и из экспертных источников, чтобы своевременно выявлять изменения в общей картине угроз и новые уязвимости.

4.98. Новые или изменившиеся угрозы и уязвимости должны оцениваться на предмет их потенциального влияния на компьютерную безопасность СКУ. Если эти изменения могут привести к потенциальным нарушениям безопасности или создать неприемлемые риски для установки, должны быть приняты корректирующие меры (например, внесены изменения в средства защиты).

4.99. Каждая организация, отвечающая за разработку, установку, эксплуатацию, техническое обслуживание или вывод из эксплуатации систем или компонентов СКУ, должна периодически проводить оценку и аудит компьютерной безопасности.

4.100. Результаты оценок компьютерной безопасности должны использоваться для актуализации УРКБ системы.

Документирование

4.101. Руководящие указания, приведенные в пп. 4.102–4.106, относятся ко всем системам, подсистемам и компонентам СКУ, которым присвоен тот или иной уровень защиты.

4.102. Документация по компьютерной безопасности СКУ помогает избежать двусмысленностей и облегчает корректную и безошибочную эксплуатацию, наблюдение, поиск и устранение неисправностей,

техническое обслуживание, будущую модификацию и модернизацию системы, а также обучение сотрудников установки и персонала технической поддержки.

4.103. Должна составляться документация для регистрации достаточного объема информации, относящейся к компьютерной безопасности СКУ, чтобы демонстрировать, что меры компьютерной безопасности разрабатываются, вводятся и применяются таким образом, чтобы обеспечивать требуемую степень защиты, соответствующую присвоенному уровню защиты.

4.104. Для деятельности на каждой стадии жизненного цикла СКУ должны быть определены исходные и итоговые документы по компьютерной безопасности.

4.105. Документация должна обеспечивать прослеживаемость требований компьютерной безопасности во всей деятельности, охватываемой жизненным циклом СКУ. Добавление, модификация и исключение мер компьютерной безопасности СКУ должны фиксироваться.

4.106. Документация должна быть защищена от несанкционированного раскрытия, фальсификации и удаления, а также уничтожения сообразно уровню защиты, присвоенному соответствующей СКУ.

Проектные основы

4.107. Руководящие указания, приведенные в пп. 4.108–4.114, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

4.108. В [4], п. 3.11, говорится, что «проектная основа определяет функции, состояния и требования общей структуры СКУ и каждой отдельной системы СКУ». Затем эта информация используется для применения требований компьютерной безопасности к каждой СКУ и к вспомогательным системам безопасности. Проектные основы также используются для определения технических условий, касающихся проектирования, реализации, строительства, тестирования и эффективности мер компьютерной безопасности.

4.109. Проектные основы общей архитектуры СКУ и каждой СКУ в отдельности должны использоваться для обоснования проектирования мер компьютерной безопасности, которые должны быть реализованы для выполнения нормативных требований компьютерной безопасности (включая проектную угрозу или оценку угроз). Дополнительные руководящие указания по проектной угрозе (включая оценки угроз и альтернативные заключения об угрозах) приведены в [18].

4.110. В проектных основах должны излагаться соображения и делаться допущения, связанные с проектированием мер компьютерной безопасности СКУ и вспомогательных систем безопасности.

4.111. В проектных основах должна быть определена степень защиты, применяемая к каждой СКУ в соответствии с уровнем защиты, присвоенным ей в процессе УРКБ установки и системы.

4.112. В проектных основах должны уточняться требования к мерам компьютерной безопасности, в том числе к мерам технического, физического и административного контроля.

4.113. В проектных основах должны определяться требования ядерной безопасности, позволяющие проводить эффективную валидацию, чтобы не допустить негативного влияния мер компьютерной безопасности на показатели ядерной безопасности СКУ.

4.114. Проектные основы должны периодически актуализироваться с учетом изменений в нормативных требованиях компьютерной безопасности или рисках.

Контроль доступа

4.115. Руководящие указания, приведенные в пп. 4.116–4.120, относятся ко всем системам, подсистемам и компонентам СКУ, к которым применяется дифференцированный подход к компьютерной безопасности в соответствии с присвоенным им уровнем защиты.

4.116. Для предотвращения несанкционированного доступа к СКУ должен контролироваться физический и логический доступ к этим системам. Привилегированный доступ к СКУ должен строго контролироваться, чтобы только уполномоченный персонал имел право доступа к существующей конфигурации, ПО и аппаратным средствам и мог вносить изменения в них.

Этот доступ может быть ограничен выполнением рабочих обязанностей уполномоченным персоналом — как по продолжительности, так и по количеству систем, к которым возможен доступ.

4.117. Количество точек доступа к сетям и устройствам должно быть сокращено до минимально возможного, чтобы минимизировать число потенциальных векторов атаки.

4.118. Каналы цифровой коммуникации должны использоваться только в разрешенных целях и контролироваться на предмет аномальной активности. При обнаружении аномальной активности должны приниматься соответствующие меры.

4.119. Для СКУ, которым присвоен самый строгий уровень защиты, следует рассмотреть возможность применения методов многофакторной аутентификации, если такие методы совместимы с требованием оперативного взаимодействия между персоналом установки и СКУ.

4.120. Должны быть разработаны и периодически актуализироваться протоколы определения функций и прав доступа для системных и пользовательских учетных записей и управления ими. В этих протоколах должен учитываться принцип наименьших привилегий. Этот процесс может быть упомянут в виде ссылки в программе компьютерной безопасности установки и интегрированной системе менеджмента установки либо интегрирован в них.

Защита конфиденциальности информации

4.121. Руководящие указания, приведенные в пп. 4.122–4.125, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

4.122. При применении недостаточных мер физической защиты и компьютерной безопасности для защиты конфиденциальности информации может произойти несанкционированное раскрытие информации, которое

может привести к ослаблению физической защиты или компьютерной безопасности системы или установки. В публикации № 23-G Серии изданий МАГАТЭ по физической ядерной безопасности [15] говорится следующее:

> «Информация — это знания, независимо от формы их существования или выражения. К ней относятся идеи, концепции, события, процессы, мысли, факты и закономерности. Информация может записываться на физические носители, например на бумагу, пленку, магнитные или оптические носители, либо храниться в электронных системах».

4.123. Информация, связанная с СКУ, должна быть идентифицирована (например, соответствующие базы данных, файлы и документация; изменяемые компоненты; имитаторы) и при необходимости засекречена как чувствительная информация и защищена при помощи соответствующих мер. В [12, 15] содержится дополнительная информация о рекомендациях по защите конфиденциальной информации.

4.124. Меры компьютерной безопасности должны использоваться для защиты конфиденциальности информации, связанной с СКУ, которая может включать информацию о проектировании, производстве, установке и эксплуатации СКУ и связанного с ними оборудования.

4.125. Оператору следует применять меры технического, физического и административного контроля для предотвращения и обнаружения несанкционированного раскрытия или утечки чувствительной информации, связанной с СКУ, и реагирования на них.

Мониторинг безопасности

4.126. Руководящие указания, приведенные в пп. 4.127–4.130, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

4.127. Требования компьютерной безопасности для мониторинга безопасности СКУ должны быть установлены сообразно присвоенным системам уровням защиты.

4.128. При мониторинге СКУ, требующих наивысшего или высокого уровня защиты, меры компьютерной безопасности, применяемые для обнаружения компрометации или неисправностей, должны базироваться

на принципах независимости[20] или неодинаковости. В соответствующих местах должны быть установлены пользовательские интерфейсы для мониторинга безопасности и индикации компрометации, регистрирующие приборы и устройства сигнализации, которые должны быть подходящими и достаточными для эффективного мониторинга компьютерной безопасности во всех состояниях станции.

4.129. Для того чтобы облегчить выполнение всех необходимых действий по обеспечению ядерной и физической безопасности, должны быть установлены требования к мониторингу состояния мер технического или физического контроля.

4.130. Следует на постоянной основе вести мониторинг СКУ и регистрацию связанных с ними мер компьютерной безопасности. При помощи анализа должны выявляться случаи несанкционированного доступа или внесения несанкционированных изменений. Необходимо заботиться о защите целостности этих учетных данных.

Соображения по поводу общей защитной архитектуры компьютерной безопасности

4.131. Руководящие указания, приведенные в пп. 4.132–4.140, относятся ко всем системам, подсистемам и компонентам СКУ, которым присвоен тот или иной уровень защиты.

4.132. Оператор должен определить общую защитную архитектуру компьютерной безопасности СКУ, в которой всем СКУ присваивается уровень защиты и они ставятся под защиту в соответствии с применимыми требованиями.

4.133. Защитная архитектура должна использоваться для поддержания и укрепления способности СКУ к предотвращению, обнаружению, задержке, смягчению последствий кибератак и восстановлению системы после них. Среди прочего, защитная архитектура включает в себя формальные логические или физические границы, такие как контуры безопасности, в

[20] Примером независимости может служить отделение систем мониторинга от СКУ, что дает возможность разделения обязанностей.

которых применяются защитные меры[21]. При внедрении такой архитектуры операторам следует задуматься об ограничении динамических элементов как у составных сетей, так и у входящих в них отдельных систем, чтобы сделать их поведение более детерминированным. Такое повышение детерминированности может облегчить применение эффективных мер компьютерной безопасности для обнаружения потенциальных инцидентов в области компьютерной безопасности.

4.134. Между системами, подсистемами и компонентами СКУ, имеющими разные уровни защиты и защищенными при помощи разных мер компьютерной безопасности, должны быть установлены границы компьютерной безопасности. Границы компьютерной безопасности — это логические и физические границы системы или набора систем, которые находятся на одном уровне защиты и поэтому могут быть защищены путем применения общих защитных мер (например, контуры компьютерной безопасности).

4.135. Для того чтобы защитная архитектура оставалась эффективной, следует контролировать поток данных между контурами безопасности, отнесенными к разным уровням защиты, и между отдельными СКУ, находящимися на одном уровне защиты, на основе риск-ориентированного подхода.

4.136. СКУ, требующие наивысшей степени защиты (т.е. самого строгого уровня защиты), должны соединяться с системами, требующими более низкой степени защиты (т.е. менее строгого уровня защиты), только через отказоустойчивые, детерминированные, однонаправленные каналы передачи данных[22]. Направление этих каналов должно быть ограничено передачей данных от устройств, требующих наиболее строгого уровня защиты, к устройствам, которым присвоены менее строгие уровни защиты. Крайне не рекомендуется делать исключения из этого правила, которые

[21] Примером такой защитной архитектуры может служить архитектура, включающая серию концентрических уровней защиты с постепенным возрастанием степени безопасности и охватывающая как аппаратные, так и программные компоненты.

[22] Удаленный доступ к системам с наиболее строгим уровнем защиты не может быть реализован из-за однонаправленного ограничения на исходящий трафик из СКУ.

могут допускаться только на сугубо индивидуальной основе и при условии подготовки полного обоснования и проведения анализа рисков, связанных с физической безопасностью[23].

4.137. Цифровые устройства или коммуникационные сети, используемые для мониторинга, технического обслуживания и восстановления данных, не должны освобождаться от мер технического контроля, применяемых для защиты каналов передачи данных между устройствами, имеющими разные уровни защиты.

4.138. Системы, которым присвоен наиболее строгий уровень защиты, должны быть размещены в границах наиболее защищенного контура. Реализация функций беспроводной связи в СКУ, которым присвоен наиболее строгий уровень защиты, проблематична из-за трудностей с обеспечением безопасных границ для таких коммуникаций.

4.139. Обмен данными между СКУ установки и центром аварийного реагирования (на площадке или за ее пределами) должен быть защищен и контролироваться при помощи мер компьютерной безопасности.

4.140. Меры технического контроля, реализованные в каждом контуре безопасности или на границе контура безопасности, должны базироваться на технологиях, отличных от тех, которые применяются на соседних уровнях защиты или границах безопасности. Это позволит обеспечить использование неодинаковых технологий для защиты СКУ.

Глубокоэшелонированная защита от компрометации

4.141. Руководящие указания, приведенные в пп. 4.142–4.151, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

4.142. Глубокоэшелонированная защита от компрометации подразумевает выстраивание мер компьютерной безопасности в виде нескольких эшелонов защиты, которые должны дать сбой или быть обойдены, чтобы кибератака могла продолжиться и причинить вред СКУ. Таким образом, глубокоэшелонированная защита достигается не только за счет создания

[23] Некоторые государства-члены убеждены в том, что исключения из этого правила недопустимы ни при каких обстоятельствах.

нескольких эшелонов защиты (например, контуров безопасности в рамках защитной архитектуры компьютерной безопасности), но и за счет введения и реализации тщательно продуманной программы мер компьютерной безопасности, которые дают возможность оценки, предотвращения, обнаружения атаки на СКУ, защиты от нее и реагирования на нее, а также смягчения ее последствий и восстановления системы после такой атаки. Например, если произойдет сбой в системе предотвращения (например, нарушение политики) или если механизмы защиты будут обойдены (например, новым вирусом, который еще не идентифицирован как кибератака), другие механизмы будут по-прежнему готовы к тому, чтобы обнаружить несанкционированное изменение в затронутой СКУ и отреагировать на него.

4.143. Никакой сбой внутри эшелонов защиты или на их границах не должен сделать общую компьютерную безопасность СКУ несуществующей или неэффективной. Например, злоумышленное использование критической уязвимости в общем устройстве сетевой защиты, используемом в двух логически связанных, но физически разобщенных местах, может способствовать совершению атаки в обход нескольких эшелонов мер компьютерной безопасности.

4.144. СКУ и соответствующие цифровые компоненты должны разрабатываться и эксплуатироваться в соответствии с концепцией глубокоэшелонированной защиты от компрометации.

4.145. Следует назначить персонал для выполнения защитных действий, которые дополняют меры технического контроля. Следует проанализировать и обосновать соотношение между действиями человека и мерами технического контроля.

4.146. Необходимо применять системный подход к выявлению и документированию действий человека, которые могут негативно повлиять на безопасность СКУ на каждом этапе жизненного цикла СКУ.

4.147. Для определения надлежащего порядка обеспечения безопасности СКУ следует использовать риск-ориентированный подход, включая реализацию мер технического контроля и глубокоэшелонированную защиту от компрометации. Эшелоны мер компьютерной безопасности, используемые для организации глубокоэшелонированной защиты от компрометации, должны создаваться в рамках процесса УРКБ установки и системы.

4.148. Каждый эшелон защиты должен быть защищен от кибератак, исходящих из соседних эшелонов.

4.149. Механизмы защиты, используемые для изоляции эшелонов защиты друг от друга, должны смягчать последствия отказов по общей причине.

4.150. Эшелоны защиты и соответствующие контрмеры должны предотвращать атаки или задерживать процесс их совершения.

4.151. Эшелоны защиты должны быть эффективны на протяжении всего жизненного цикла СКУ и должны учитываться при проектировании, определении конфигурации, модификации и задании параметров компонентам системы.

КОНКРЕТНАЯ ДЕЯТЕЛЬНОСТЬ В РАМКАХ ЖИЗНЕННОГО ЦИКЛА

Спецификация требований компьютерной безопасности

4.152. Должны быть установлены и задокументированы требования компьютерной безопасности для защитной архитектуры и для отдельных систем и компонентов СКУ. Эти требования к защитной архитектуре должны быть выведены из проектных основ СКУ.

4.153. Требования компьютерной безопасности систем, подсистем и компонентов СКУ должны охватывать функциональные и эксплуатационные требования, конфигурацию системы, квалификацию, учет человеческого фактора, определение и передачу данных, документацию, установку и ввод в эксплуатацию, эксплуатацию и техническое обслуживание.

4.154. При разработке требований компьютерной безопасности СКУ следует принимать во внимание УРКБ установки и системы. Требования компьютерной безопасности должны рассматриваться и актуализироваться в зависимости от изменений в результатах УРКБ установки и системы.

4.155. Сочетание требований компьютерной безопасности защитной архитектуры и отдельных СКУ должно соответствовать проектным основам, установленным для всей архитектуры СКУ.

Подбор ранее разработанных изделий

4.156. Руководящие указания, приведенные в пп. 4.157–4.164, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход.

4.157. К ранее разработанным изделиям могут относиться электронные устройства, ранее разработанное программное обеспечение (РПО), готовые коммерческие продукты (ГКП), цифровые устройства, состоящие из аппаратного и программного обеспечения (включая встроенное ПО), аппаратные устройства, сконфигурированные с помощью языка описания аппаратуры или ранее разработанных функциональных блоков.

4.158. Ранее разработанные изделия могут включать в себя аппаратное и программное обеспечение (включая встроенное ПО), ранее разработанное организациями, у которых не имеется надлежащей программы компьютерной безопасности или которые не желают делиться подробной информацией о своей программе компьютерной безопасности. В таких случаях необходимо проанализировать характеристики компьютерной безопасности данных изделий и обосновать их использование в составе либо СКУ, либо вспомогательных систем.

4.159. Скорее всего, РПО и ГКП будут являться собственностью компании, и в большинстве случаев их исходный код будет недоступен для проведения обстоятельной проверки. Следовательно, вполне вероятно, что у оператора не будет иметься надежного метода для всесторонней оценки уязвимостей в системе безопасности этих продуктов. В таких случаях, если эти продукты не будут модифицированы разработчиком приложения, потребуется принять компенсирующие меры компьютерной безопасности.

4.160. Следует применять меры компьютерной безопасности для недопущения того, чтобы функции РПО и ГКП стали причиной несоответствия СКУ требованиям компьютерной безопасности. Например, могут быть даны рекомендации по уменьшению объема выполняемого кода, закрытию доступа к точкам входа для неавторизованных пользователей и исключению ненужного функционала и минимизации тем самым площади атаки (т.е. усиление системы). Впрочем, применение этих мер компьютерной безопасности может обеспечить лишь ограниченную защиту, и оператору следует применять дополнительные компенсирующие меры компьютерной безопасности.

4.161. Ранее разработанные компоненты или ПО должны быть выбраны и сконфигурированы при помощи процедуры квалификационного тестирования на безопасность сообразно уровню защиты СКУ.

4.162. Использование РПО и ГКП должно быть проверено на соответствие этих продуктов требованиям компьютерной безопасности СКУ.

4.163. Оператор должен определить документацию, необходимую для квалификационного тестирования РПО. Не следует полагаться на меры технического контроля, эффективность которых не может быть доказана.

4.164. Ненужные функции или сервисы в конфигурируемом РПО или ГКП должны быть исключены.

Проектирование и внедрение СКУ

4.165. Руководящие указания, приведенные в пп. 4.166–4.174, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

4.166. На этапе внедрения СКУ (интегрированного аппаратного и программного обеспечения) проект системы преобразуется в код, структуры баз данных и соответствующие машинно-исполняемые формы. Внедрение предполагает конфигурирование и настройку аппаратных средств, кодирование и тестирование ПО, а также конфигурирование и настройку коммуникаций (включая, при необходимости, установку повторно используемого ПО и ГКП).

4.167. На этапах жизненного цикла СКУ, связанных с проектированием и внедрением, должны быть определены требования к компьютерной безопасности СКУ и проверено их выполнение.

4.168. Требования, определенные в спецификации СКУ, должны быть преобразованы в конкретные элементы конструкции в описании конструкции системы. Эти конкретные элементы конструкции должны включать требования, которые должны быть реализованы в конструкции СКУ или с помощью мер компьютерной безопасности, реализуемых вне СКУ.

4.169. Конструктивные элементы системы компьютерной безопасности СКУ должны иметь отношение к контролю физического и логического доступа к функциям системы, использованию сервисов СКУ и обмену данными с другими системами.

4.170. Физический и логический доступ к СКУ должен контролироваться в зависимости от уровня защиты, присвоенного СКУ. Например, к системам, отнесенным к наиболее строгому уровню защиты, должны предъявляться такие требования компьютерной безопасности, как многофакторный контроль доступа, например контроль доступа, требующий комбинации знаний (например, пароль), физических средств (например, ключ, карта с микропроцессором) и персональных характеристик (например, отпечатки пальцев).

4.171. СКУ следует проектировать таким образом, чтобы в них были предусмотрены функции, обеспечивающие устойчивость к компрометации или защиту от нее.

4.172. При проектировании должна обеспечиваться достаточная уверенность в том, что безопасность системы, которой присвоен данный уровень защиты, не будет снижена в результате ее подключения к системам, отнесенным к более низким уровням защиты.

4.173. Для того чтобы СКУ была менее подвержена кибератакам, должны быть разработаны надлежащие комбинации мер административного контроля (например, программа компьютерной безопасности) и мер физического контроля.

4.174. Компоненты СКУ должны быть размещены и смонтированы в тех местах установки, которые обеспечивают физическую сохранность оборудования и его сетевых коммуникаций с другими системами; например, все устройства передачи данных между системами и компонентами должны быть помещены в защитные корпуса.

Интеграция СКУ

4.175. Руководящие указания, приведенные в пп. 4.176–4.178, относятся ко всем системам, подсистемам и компонентам СКУ.

4.176. Интеграция СКУ — это процесс объединения аппаратных и программных средств СКУ (включая встроенное ПО) в единую систему. Часто продавцы, подрядчики или поставщики выполняют интеграционное тестирование каждой отдельной системы, которую они производят, а также комбинации систем, к которым они имеют доступ, перед их отправкой на установку. Цель этого тестирования — удостовериться в том, что исполнение программных компонентов и интерфейс между компонентами СКУ соответствуют требованиям.

4.177. На этапе жизненного цикла СКУ, когда происходит системная интеграция, перед началом тестирования должны быть введены в действие и сконфигурированы в соответствии со спецификациями интегрированные меры технического контроля.

4.178. В ходе интеграционного тестирования продавец, подрядчик или поставщик должен подтвердить, что интегрированные меры компьютерной безопасности работают в штатном режиме и не оказывают негативного влияния на способность СКУ выполнять свои основные функции.

Валидация систем

4.179. Руководящие указания, приведенные в пп. 4.180–4.185, относятся ко всем системам, подсистемам и компонентам СКУ, которым присвоен тот или иной уровень защиты.

4.180. Мероприятия по валидации системы обычно проводятся параллельно с другими стадиями жизненного цикла. После завершения интеграции системы обычно выполняется частичная валидация системы, например путем использования смоделированных входных данных. Работы по валидации обычно продолжаются на стадиях установки, интеграции и ввода в эксплуатацию СКУ. Валидация считается завершенной, когда система переходит в режим нормальной эксплуатации.

4.181. Во время валидации каждой системы, подсистемы и компонента СКУ должно быть продемонстрировано выполнение требований компьютерной безопасности и действий по конфигурированию. Цель тестирования функций безопасности — обеспечить валидацию требований компьютерной безопасности СКУ путем проведения интеграционных, системных и приемочных испытаний, когда это практически целесообразно и необходимо.

4.182. При помощи мероприятий по валидации системы должна быть подтверждена эффективность мер компьютерной безопасности и проверено их потенциальное воздействие, прямое или косвенное, на функции ядерной безопасности.

4.183. Следует продемонстрировать, что каждая мера технического контроля, реализованная в СКУ, работает в штатном режиме, не увеличивает риск появления уязвимостей в системе безопасности и не снижает надежность функций ядерной безопасности.

4.184. Валидация мер компьютерной безопасности СКУ должна включать оценку конфигурации системы (в том числе всех внешних соединений), квалификационное тестирование ПО, квалификационное тестирование системы и заводские приемочные испытания системы. Валидация этих мер компьютерной безопасности может быть подкреплена системными тестами СКУ, дающими возможность выявить потенциальные уязвимости или охарактеризовать неожиданное поведение или действия.

4.185. Тестирование системы в целях ее валидации должно проводиться в безопасной среде. Например, устройства для тестирования, такие как имитаторы или эмуляторы, должны быть защищены с помощью мер компьютерной безопасности. Строгость мер компьютерной безопасности должна быть соизмерима с уровнем защиты, присвоенным СКУ.

Установка, общая интеграция и ввод в эксплуатацию СКУ

4.186. Во время установки и ввода в эксплуатацию оператор должен выполнить приемочную проверку адекватности мер физического и технического контроля в целевой среде, приняв во внимание общую интеграцию СКУ[24].

4.187. Установка СКУ, общая интеграция и ввод в эксплуатацию СКУ должны проводиться в безопасной среде. При установлении уровня защиты для этой среды следует учитывать уровень защиты системы в целевой среде и уровень защиты инструментов, используемых при установке и вводе в эксплуатацию.

---

[24] В настоящей публикации «общая интеграция СКУ» означает интеграцию всех СКУ на установке и отличается от «интеграции СКУ», о которой говорилось выше.

4.188. Безопасная среда должна быть защищена при помощи мер компьютерной безопасности, соразмерных уровню защиты, присвоенному СКУ, и процедур обеспечения безопасности, выполняемых при установке и вводе в эксплуатацию. В некоторых случаях следует предусмотреть компенсирующие меры административного и физического контроля для контроля доступа к защищенной среде, а также к соответствующему оборудованию и источникам данных.

4.189. Оборудование, используемое в защищенной среде, должно быть проверено с целью убедиться в том, что его использование не открывает путей для внедрения вредоносного кода или данных в среду или компоненты СКУ.

4.190. Должны быть предусмотрены меры компьютерной безопасности для контроля и мониторинга перемещения данных и цифровых активов в защищенную среду и из нее.

Эксплуатация и техническое обслуживание

4.191. Руководящие указания, приведенные в пп. 4.192–4.205, относятся ко всем системам, подсистемам и компонентам СКУ, к которым может быть применен дифференцированный подход в соответствии с присвоенным им уровнем защиты.

4.192. Деятельность по эксплуатации и техническому обслуживанию продолжается на протяжении всего жизненного цикла СКУ и уже рассматривалась в предыдущих разделах, посвященных планированию процессов и деятельности, общей для всех стадий жизненного цикла. Эксплуатирующая организация должна взять на себя всю полноту ответственности за компьютерную безопасность при проведении текущих мероприятий по эксплуатации и техническому обслуживанию, когда система вступит в стадию эксплуатации и технического обслуживания.

4.193. Мероприятия по техническому обслуживанию — это действия, необходимые оператору для поддержания систем или компонентов в надлежащем рабочем состоянии. Этими мероприятиями по техническому обслуживанию должны быть охвачены меры технического и физического контроля, обеспечивающие компьютерную безопасность СКУ, и они могут включать:

— периодическое профилактическое техническое обслуживание или тестирование;
— действия, направленные на обнаружение ухудшения состояния компонентов, его недопущение или смягчение его последствий;
— действия по диагностике, ремонту, капитальному ремонту отказавших компонентов или их замене на идентичные компоненты.

4.194. При проведении мероприятий по эксплуатации и техническому обслуживанию должны применяться меры компьютерной безопасности с целью гарантировать, что компоненты и системы не подвергнутся компрометации.

4.195. Стадия эксплуатации предполагает использование СКУ оператором в заданной эксплуатационной среде. На этапе эксплуатации оператор должен:

— удостоверяться в том, что безопасность СКУ не нарушена, используя такие методы, как периодическое тестирование и мониторинг, просмотр системных журналов и мониторинг в режиме реального времени, когда это возможно;
— оценивать влияние изменений в СКУ, происходящих в эксплуатационной среде, на безопасность СКУ;
— оценивать влияние всех предлагаемых изменений на безопасность СКУ;
— оценивать эксплуатационные регламенты на соответствие их предполагаемому назначению;
— анализировать риски для безопасности, влияющие на оператора и систему;
— оценивать новые ограничения в системе, обусловленные безопасностью;
— оценивать эксплуатационные регламенты на предмет правильности и удобства использования;
— выполнять периодические самооценки и аудиты безопасности компьютерных систем, которые являются ключевыми составляющими эффективной программы безопасности;
— оценивать имеющиеся сообщения об инцидентах, в которых говорится о новых угрозах и уязвимостях.

4.196. Деятельность по эксплуатации и техническому обслуживанию должна анализироваться с целью убедиться в принятии мер компьютерной безопасности для предотвращения внедрения в СКУ вредоносного ПО.

4.197. Мероприятия по техническому обслуживанию должны соответствовать действующим требованиям компьютерной безопасности СКУ, если только эти требования не будут изменены в ходе работ по техническому обслуживанию. В некоторых случаях для выполнения необходимых задач по техническому обслуживанию может потребоваться временно отменить меры компьютерной безопасности или приостановить их действие. В период, когда меры компьютерной безопасности недоступны, система подвергается большему риску, и необходимо принять компенсирующие меры.

4.198. Работы по калибровке, тестированию и техническому обслуживанию могут предполагать использование съемных носителей и мобильных устройств, которые временно подключаются к цифровым системам и компонентам СКУ. Меры компьютерной безопасности при этих видах деятельности должны включать:

— применение эффективных мер административного и технического контроля при безопасном и надежном обращении с цифровыми устройствами;
— проверку целостности всех уставок систем управления с целью предотвращения нежелательных изменений и защиты от них;
— использование квалифицированного персонала (в том числе сторонних организаций), обученного выполнению этих действий на основе требований компьютерной безопасности.

4.199. Интерфейсы, когда они не требуются или не используются, должны быть отключены либо к ним должен быть ограничен доступ (например, подключение обслуживающих или инструментальных компьютеров).

4.200. Должны быть предусмотрены меры компьютерной безопасности для предотвращения ненужного или несанкционированного доступа.

4.201. Должны существовать процессы мониторинга или приложения для сравнения текущей конфигурации ПО с известными конфигурациями.

4.202. Удаленный доступ должен быть по возможности ограничен. Если возникает необходимость в удаленном доступе, следует учитывать риск таких соединений и применять дополнительные меры компьютерной безопасности. Такое соединение должно поддерживаться ровно столько, сколько это необходимо для его конкретной задачи.

4.203. Деятельность по эксплуатации и техническому обслуживанию должна тщательно контролироваться с помощью формальных процессов выдачи нарядов на выполнение работ и регламентов технического обслуживания. Например, при выполнении таких задач, как внесение изменений в конфигурацию работающих СКУ, следует применять принцип сдержек и противовесов, например правило двух лиц.

4.204. Эксплуатационная деятельность не должна требовать внесения изменений в меры компьютерной безопасности СКУ.

4.205. Средства эксплуатации и обслуживания системы, которые могут быть использованы для компрометации СКУ, должны быть защищены соразмерно уровню защиты соответствующей СКУ. Например, средства, используемые в системе, отнесенной к более строгому уровню защиты, не должны применяться в системе, отнесенной к более низкому уровню защиты.

Модификация СКУ

4.206. Применение мер компьютерной безопасности к устаревшим СКУ на действующей ядерной установке не всегда бывает простым делом. Например, могут возникнуть следующие трудности:

— изменение архитектуры устаревших СКУ может оказаться невозможным без изменения детерминированного поведения устаревших СКУ;
— существующие технологии, используемые для хранения программ или данных, организации интерфейса или связи, могут не поддаваться модификации;
— существующие сооружения и планировка установки могут не давать возможности для принятия достаточных мер физической защиты;
— современные меры технического контроля, выполняющие функции мониторинга безопасности, могут быть несовместимы с технологиями, реализованными в устаревших СКУ.

4.207. При модернизации ядерной установки, предполагающей замену устаревших СКУ на современные, оператор должен учитывать возможность того, что может потребоваться сохранение устаревших интерфейсов с первоначальными системами установки и другими системами, а также возможность появления новых уязвимостей и слабых мест вместе с новой технологией или конструкцией.

4.208. Модификации СКУ приводят к изменению самой системы или документации к ней. Эти изменения можно разбить на следующие категории:

— изменения или усовершенствования (корректирующие или адаптивные);
— миграция (т.е. перенос системы в новую операционную среду);
— замена (т.е. прекращение активной поддержки со стороны ремонтно-эксплуатационной организации, частичная или полная замена на новую систему или установка модернизированной системы).

4.209. Модификации СКУ могут быть продиктованы установленными требованиями либо выполняться для исправления ошибок (корректирующие), адаптации к изменившимся условиям эксплуатации (адаптивные) или реагирования на дополнительные запросы оператора или внесенные им усовершенствования.

4.210. При внесении модификаций в СКУ следует предусмотреть оценку безопасности модифицированной СКУ, например путем актуализации УРКБ системы.

4.211. Компьютерная безопасность должна рассматриваться как часть процесса управления изменениями. Сюда относятся изменения в программном и аппаратном обеспечении СКУ.

4.212. Чтобы убедиться в том, что в результате модификаций в среду установки не были привнесены уязвимости, оператор должен оценить предлагаемые изменения в СКУ, в том числе их влияние на программу компьютерной безопасности и существующий уровень безопасности СКУ, оценить аномалии, обнаруженные в процессе эксплуатации, оценить потребности в миграции и оценить внесенные модификации, включая проведение мероприятий по валидации и верификации.

4.213. Меры компьютерной безопасности должны быть подвергнуты оценке, как описано в пп. 4.206–4.212 выше, и при необходимости пересмотрены с учетом требований компьютерной безопасности, возникших в результате процесса модификации.

4.214. Во время модификации существующие требования компьютерной безопасности СКУ должны оставаться в силе, если только их не требуется изменить в рамках работ по модификации.

4.215. В отношении мер компьютерной безопасности должно быть предусмотрено управление конфигурацией, чтобы не допустить внедрения в СКУ несанкционированного ПО.

4.216. При проведении работ по миграции систем оператор должен убедиться, что переносимые системы соответствуют требованиям компьютерной безопасности, предъявляемым к СКУ.

4.217. Перед сдачей в эксплуатацию из системы и ее конфигурационных файлов должны быть удалены артефакты разработки, установки и тестирования.

4.218. Модификации СКУ должны рассматриваться как процессы разработки и проходить верификацию и валидацию.

4.219. В ходе всех модификаций СКУ и ее компонентов, включая ПО, аппаратные средства и конфигурацию системы, должны приниматься в расчет потенциальные уязвимости и угрозы безопасности, которые могут возникнуть не только во время выполнения этих действий, но и как результат модификаций.

4.220. Многие цифровые активы и связанные с ними компоненты, включая съемные носители, обладают способностью сохранять цифровые данные после удаления из системы. Эти цифровые данные могут включать в себя запрограммированную последовательность операций или остаточные данные системы, такие как показания датчиков, сигналы управления, аналитические данные и данные о сетевом трафике. Эти данные могут быть извлечены из компонентов, которые более не используются.

4.221. Должны быть предусмотрены меры административного и технического контроля, гарантирующие, что остаточные данные на неиспользуемых компонентах не послужат целям разработки компьютерного эксплойта. Следует либо уничтожить компоненты, либо полностью удалить с них данные, если только не будет доказано, что остаточные данные на компонентах, использование которых прекращается, не несут в себе риска с точки зрения нарушения безопасности.

4.222. В случае модификаций, связанных с заменой СКУ, оператор должен провести такие мероприятия, как очистка данных, уничтожение диска или полная перезапись, чтобы гарантировать невозможность восстановления данных из замененной СКУ после ее вывода из эксплуатации.

ВЫВОД ИЗ ЭКСПЛУАТАЦИИ

4.223. На стадии вывода из эксплуатации, прежде чем ядерные материалы, другие радиоактивные материалы и чувствительные информационные активы будут удалены с установки, оператор должен оценить последствия замены существующих функций безопасности СКУ или их удаления из операционной среды.

4.224. В ходе этой оценки оператор должен проанализировать последствия удаления функций физической безопасности системы для системных интерфейсов, связанных и не связанных с обеспечением ядерной безопасности.

4.225. Оператор должен задокументировать методы, при помощи которых будут смягчены последствия изменения функций безопасности СКУ (например, замена функций физической безопасности, изоляция от других систем ядерной безопасности и от взаимодействий этих систем с оператором или отключение функций интерфейса с СКУ).

4.226. До завершения вывода установки из эксплуатации в протоколах безопасности должны сохраняться элементы, обеспечивающие очистку оборудования и данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] ALBRIGHT, D., BRANNAN, P., WALROND, C., Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report (2011), http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8.

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок, (INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по физической ядерной безопасности, № 13, МАГАТЭ, Вена (2012).

[3] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Компьютерная безопасность на ядерных установках, Серия изданий МАГАТЭ по физической ядерной безопасности, № 17, МАГАТЭ, Вена (2012).

[4] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Проектирование систем контроля и управления для атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-39, МАГАТЭ, Вена (2018).

[5] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя, Серия изданий МАГАТЭ по физической ядерной безопасности, № 8, МАГАТЭ, Вена (2009).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems and Software Important to Safety for Research Reactors, IAEA Safety Standards Series No. SSG-37, IAEA, Vienna (2015).

[7] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Глоссарий МАГАТЭ по вопросам безопасности: терминология, используемая в области ядерной безопасности и радиационной защиты (издание 2018 года), МАГАТЭ, Вена (2023).

[8] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Цель и основные элементы государственного режима физической ядерной безопасности, Серия изданий МАГАТЭ по физической ядерной безопасности, № 20, МАГАТЭ, Вена (2014).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of a Graded Approach in the Application of the Safety Requirements for Research Reactors, IAEA Safety Standards Series No. SSG-22, IAEA, Vienna (2012).

[10] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants - Instrumentation and Control Systems - Requirements for Security Programmes for Computer-based Systems, IEC 62645:2014, IEC, Geneva (2014).

[11] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Физическая защита ядерного материала и ядерных установок (практическое применение рекомендаций INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по физической ядерной безопасности, № 27-G, МАГАТЭ, Вена (2022).

[12] INTERNATIONAL STANDARDS ORGANIZATION, Information Technology – Security Techniques – Information Security Risk Management, ISO/IEC:27005:2011, ISO, Geneva (2011).

[13] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Культура физической ядерной безопасности, Серия изданий МАГАТЭ по физической ядерной безопасности, № 7, МАГАТЭ, Вена (2022).
[14] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Лидерство и менеджмент для обеспечения безопасности, Серия норм безопасности МАГАТЭ, № GSR Part 2, МАГАТЭ, Вена (2017).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[16] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Применение системы управления для установок и деятельности, Серия норм безопасности МАГАТЭ, № GS-G-3.1, МАГАТЭ, Вена (2009).
[17] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Система управления для ядерных установок, Серия норм безопасности МАГАТЭ, № GS-G-3.5, МАГАТЭ, Вена (2014).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

ЗАКАЗ В СТРАНАХ

Платные публикации МАГАТЭ могут быть приобретены у перечисленных ниже поставщиков или в крупных книжных магазинах.

Заказы на бесплатные публикации следует направлять непосредственно в МАГАТЭ. Контактная информация приводится в конце настоящего перечня.

СЕВЕРНАЯ АМЕРИКА

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Тел.: +1 800 462 6420 • Факс: +1 800 338 4550
Эл.почта: orders@rowman.com • Сайт: http://www.rowman.com/bernan

ОСТАЛЬНЫЕ СТРАНЫ

Просьба связаться с местным поставщиком по вашему выбору или с вашим основным дистрибьютером:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Торговые заказы и справочная информация:
Тел: +44 (0) 1767604972 • Факс: +44 (0) 1767601640
Эл.почта: eurospan@turpin-distribution.com

Индивидуальные заказы:
www.eurospanbookstore.com/iaea

Дополнительная информация:
Тел: +44 (0) 2072400856 • Факс: +44 (0) 2073790609
Эл.почта: info@eurospangroup.com • Сайт: www.eurospangroup.com

Заказы на платные и бесплатные публикации можно направлять напрямую по адресу:

Группа маркетинга и сбыта (Marketing and Sales Unit)
Международное агентство по атомной энергии
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Телефон: +43 1 2600 22529 или 22530 • Факс: +43 1 26007 22529
Эл.почта: sales.publications@iaea.org • Сайт: https://www.iaea.org/ru/publikacii

Компьютерная безопасность — это сложная область с возрастающим числом угроз, которым со всех сторон подвергается динамично развивающаяся технологическая среда. Обеспечение компьютерной безопасности на ядерных установках становится еще более сложным делом ввиду интеграции в систему менеджмента компьютерной безопасности систем контроля и управления (СКУ). В настоящей публикации даются руководящие указания по решению задачи применения мер компьютерной безопасности к СКУ на ядерных установках, включая технические основы и методологии применения мер компьютерной безопасности к СКУ, обеспечивающим ядерную безопасность, физическую безопасность или выполнение вспомогательных функций на ядерных установках. Эти меры предназначены для защиты систем СКУ от злоумышленных действий, совершаемых отдельными лицами или организациями. В настоящей публикации также рассматривается применение таких мер к средам разработки, моделирования и технического обслуживания этих систем.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА