ПРОВЕДЕНИЕ ОЦЕНОК КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ НА ЯДЕРНЫХ УСТАНОВКАХ

IAEA
Международное агентство по атомной энергии

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.

ПРОВЕДЕНИЕ ОЦЕНОК КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ 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
БЫВШАЯ ЮГОСЛ. РЕСП. МАКЕДОНИЯ
ВАНУАТУ
ВЕНГРИЯ
ВЕНЕСУЭЛА, БОЛИВАРИАНСКАЯ РЕСПУБЛИКА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАЙАНА
ГАНА
ГВАТЕМАЛА
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
КАЗАХСТАН
КАМБОДЖА
КАМЕРУН
КАНАДА
КАТАР
КЕНИЯ
КИПР
КИТАЙ
КОЛУМБИЯ
КОНГО
КОРЕЯ, РЕСПУБЛИКА
КОСТА-РИКА
КОТ-Д'ИВУАР
КУБА
КУВЕЙТ
КЫРГЫЗСТАН
ЛАТВИЯ
ЛАОССКАЯ НАРОДНО-ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА
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
НИДЕРЛАНДЫ
НИКАРАГУА
НОВАЯ ЗЕЛАНДИЯ
НОРВЕГИЯ
ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ
ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ
ОМАН
ПАКИСТАН
ПАЛАУ
ПАНАМА
ПАРАГВАЙ
ПАПУА-НОВАЯ ГВИНЕЯ
ПЕРУ
ПОЛЬША
ПОРТУГАЛИЯ
РЕСПУБЛИКА МОЛДОВА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
РУАНДА
РУМЫНИЯ
САЛЬВАДОР
САН-МАРИНО
САУДОВСКАЯ АРАВИЯ
СВАЗИЛЕНД
СВЯТОЙ ПРЕСТОЛ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СЕНЕГАЛ
СЕНТ-ВИНСЕНТ И ГРЕНАДИНЫ
СЕРБИЯ
СИНГАПУР
СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
СЛОВАКИЯ
СЛОВЕНИЯ
СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
СУДАН
СЬЕРРА-ЛЕОНЕ
ТАДЖИКИСТАН
ТАИЛАНД
ТОГО
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
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».

ПРОВЕДЕНИЕ ОЦЕНОК КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ НА ЯДЕРНЫХ УСТАНОВКАХ

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2018

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

За дополнительной информацией просьба обращаться по адресу:
Секция управления информацией
Международное агентство по атомной энергии
Венский международный центр
а/я 100
1400 Вена, Австрия
эл. почта: Official.Mail@iaea.org

ПРОВЕДЕНИЕ ОЦЕНОК КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ
НА ЯДЕРНЫХ УСТАНОВКАХ

IAEA-TDL-006
ISBN 978-92-0-408317-0

Напечатано МАГАТЭ в Австрии, январь 20118 года

ПРЕДИСЛОВИЕ

Цель физической ядерной безопасности заключается в предотвращении, обнаружении и реагировании на злоумышленные действия в отношении ядерного материала, других радиоактивных материалов или связанных с ними установок и деятельности. Компьютеры, компьютерные системы и цифровые компоненты играют все более важную роль в управлении чувствительной информацией, ядерной безопасностью, физической ядерной безопасностью, а также учетом и контролем материала на этих объектах. Компрометация компьютерных систем может оказать негативное воздействие на физическую ядерную безопасность как напрямую, так и опосредованно, и может способствовать совершению злоумышленных действий.

В Серии изданий МАГАТЭ по физической ядерной безопасности рассматриваются вопросы физической ядерной безопасности, касающиеся предотвращения и обнаружения, а также реагирования в отношении злоумышленных действий, связанных с ядерным материалом, другими радиоактивными материалами или связанными с ними установками, включая кражи, саботаж (диверсии), несанкционированный доступ и незаконную передачу. В дополнение к основанным на международном консенсусе руководящим материалам, выпущенным в Серии изданий МАГАТЭ по физической ядерной безопасности, МАГАТЭ издает также другие публикации, содержащие дополнительные рекомендации экспертов по конкретным темам.

Публикация Серии изданий МАГАТЭ по физической ядерной безопасности, № 17, "Компьютерная безопасность на ядерных установках" содержит руководство по разработке и применению программы по компьютерной безопасности на ядерной или радиологической установке. На основе руководства, представленного в публикации в Серии изданий МАГАТЭ по физической ядерной безопасности, № 17, в настоящей публикации излагается методология проведения оценки компьютерной безопасности на ядерных установках. Периодическое проведение таких оценок и безотлагательное осуществление корректирующих мер имеет чрезвычайно важное значение для защиты компьютеров и компьютерных активов. Методология, описанная в настоящей публикации, может применяться в случае проведения как внутренних самооценок, так и внешних оценок. Настоящая публикация предназначена для использования экспертами по оценке при планировании и проведении индивидуализированных оценок на конкретных установках и в конкретных организациях.

В подготовке настоящей публикации приняли участие более тридцати экспертов, которые провели три консультативных совещания, а также ряд дополнительных совещаний экспертов, и от более чем десяти государств-членов были получены соответствующие материалы.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Настоящая публикация подготовлена на основе оригинального материала, представленного соавторами, и не редактировалась редакционным персоналом МАГАТЭ. Ответственность за выраженные в ней мнения несут соавторы, и эти мнения необязательно отражают точку зрения МАГАТЭ или его государств-членов.

Ни МАГАТЭ, ни его государства-члены не несут ответственности за последствия, которые могут возникнуть в результате использования настоящей публикации. В настоящей публикации не затрагиваются вопросы ответственности – юридической или иного рода – за действия или бездействие со стороны какого-либо лица.

Использование тех или иных названий стран или территорий не означает какого-либо суждения со стороны издателя – МАГАТЭ – относительно правового статуса таких стран или территорий, их органов и учреждений либо относительно определения их границ.

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

Термины из области физической безопасности должны пониматься так, как они определены в публикации, в которой они применяются, или в руководящих материалах, на которые опирается эта публикация. Во всех остальных случаях слова употребляются в их общепринятом значении.

Дополнение считается неотъемлемой частью публикации. Материал, приведенный в дополнении, имеет тот же статус, что и основной текст. Приложения используются для представления практических примеров, дополнительной информации или пояснений. Приложения являются неотъемлемой частью основного текста.

МАГАТЭ не несет ответственности за постоянство и точность приводимых в настоящей публикации адресов веб-сайтов внешних или третьих сторон и не гарантирует того, что информационное наполнение таких веб-сайтов является или останется точным и релевантным.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. ОБЩИЕ СВЕДЕНИЯ

Физическая компьютерная безопасность все шире признается в качестве ключевого компонента в физической ядерной безопасности. Ожидается, что по мере развития технологий использование компьютеров и вычислительных систем во всех аспектах эксплуатации установки, в том числе систем безопасности и физической безопасности, будет расти. В публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 20, "Цель и основные элементы государственного режима физической ядерной безопасности" подчеркивается важность деятельности по обеспечению кибербезопасности, которая позволяет определять и устранять проблемы и факторы, могущие повлиять на возможности обеспечивать адекватную физическую ядерную безопасность [1]. Эти вопросы рассматриваются в публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 13, "Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок" (INFCIRC/225/Revision 5) [2], в которой указано следующее;

> "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." ([2], пункты 4.10/5.19)

Процесс строгой, всесторонней оценки может помочь в деле повышения эффективности программы обеспечения компьютерной безопасности установки (и на государственном уровне). Публикация в Серии изданий МАГАТЭ по физической ядерной безопасности, № 17, "Компьютерная безопасность на ядерных установках" [3] содержит руководство по разработке и применению такой программы. Многие другие публикации посвящены вопросам информационной и компьютерной безопасности и проведения аудитов/оценок; к таким публикациям относятся:

- серия стандартов ISO/IEC 27000 [4-8] по вопросам менеджмента информационной безопасности;
- стандарт ISO 19011:2011 [9], содержащий руководство по аудиту систем менеджмента;
- NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment (Специальная публикация 800-115 НИСТ "Техническое руководство по тестированию и оценке информационной безопасности") [10].

Настоящая публикация была подготовлена с целью удовлетворения потребности в конкретных руководящих материалах для ядерной области, соответствующих международным стандартам, руководствам Международного агентства по атомной энергии (МАГАТЭ) и признанным методам надлежащей практики.

1.2. НАЗНАЧЕНИЕ

В настоящей публикации излагается методология проведения оценок компьютерной безопасности на ядерных установках. Эта методология может быть легко адаптирована для проведения оценок на объектах с другими радиоактивными материалами.

Руководящие материалы были разработаны для применения в различных контекстах, включая:

— миссии специализированной консультативной службы по компьютерной безопасности, организуемые МАГАТЭ по просьбе государств-членов;

— целевой модуль по компьютерной безопасности в других организуемых МАГАТЭ миссиях, например, миссиях Международной консультативной службы по физической защите (ИППАС), в которых физическая защита является объектом оценивания;

— оценки, проводимые национальным компетентным органом на площадках и установках в государстве;

— самооценки, проводимые на установке или на уровне организации;

— оценку компьютерной безопасности у поставщиков и третьих сторон, которые обеспечивают поддержку ядерных установок.

Методология предназначена для проведения оценки применяемой на установке практической деятельности с целью укрепления организации и ее процедур и практики. В ней учитываются руководящие материалы МАГАТЭ по физической ядерной безопасности, международные стандарты, нормы и методы надлежащей практики, получившие одобрение международного сообщества. Она построена как рассмотрение высокого уровня структуры компьютерной безопасности, включая анализ на функциональном уровне мер и процедур, применяемых на объекте для обеспечения функционирования этой структуры, с уделением особого внимания всем функциям физической ядерной безопасности и безопасности, обеспечиваемых компьютерными системами.

Каждая оценка может требовать индивидуализации и четкого разграничения ожидаемых итогов. Например, ожидаемым итогом оценки, проводимой компетентным органом (КО), может быть отчет о том, как оператор выполнил свои нормативно-правовые обязательства. Этот отчет, по-видимому, не будет включать предложения в отношении путей решения выявленных проблем, однако в нем могут указываться действия, которые должны быть предприняты в соответствии с приоритетностью, установленной КО и в последующей оценке. В то же время консультативной группе, проводящей оценку, может быть адресована просьба представить рекомендации по возможным решениям, а также перечень своих выводов. Консультативные группы также могут рассмотреть вопрос о приоритетах и последующей деятельности; в структуре оценки может быть предусмотрено сотрудничество между группой оценки и принимающей стороной при проведении анализа и разработке плана действий.

Важно, чтобы цели и ожидаемые итоги оценки были четко сформулированы и согласованы в ходе подготовительного совещания.

Основное внимание в настоящей публикации уделяется оказанию помощи группе оценки в разработке плана проведения индивидуализированных оценок на конкретной установке. Она не предназначена служить в качестве всеобъемлющего контрольного перечня как такового, а вместо этого рассчитана на то, что группа оценки будет руководствоваться своим опытом при использовании данного руководства, обеспечивая, чтобы осуществляемая ими работа носила комплексный характер и проводилась в соответствии с целями оценки и имеющимися ресурсами.

1.3. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая публикация посвящена оценке практики обеспечения компьютерной безопасности на ядерных установках любого типа, в том числе на атомных электростанциях, установках ядерного топливного цикла, исследовательских реакторах и т.д. Хотя обращение с другими радиоактивными материалами, перевозка и связанные с этим операции конкретно не рассматриваются в настоящей публикации, принципы и процессы, описанные здесь, могут быть легко адаптированы для целей оценивания такой деятельности.

Настоящая публикация конкретно ориентирована только на аспекты информационной безопасности, относящиеся к компьютерам. Например, в ней не рассматриваются требования, предъявляемые к классификации, маркировке информации и обращению с ней.

Оценка основывается на результатах анализа, собеседований и обследований и, как правило, не включает тестирование системы в активном режиме. В частности, оценка, детально описываемая в настоящей публикации, не включает в себя тестирование на проникновение или подключение тестовых устройств к системе. Члены группы оценки не осуществляют работу на оборудовании объекта, на котором проводится оценка, но группа может запросить для изучения текущие журналы систем или конфигурационные файлы действующей производственной системы. При необходимости и в рамках оценки группа оценки просит установку выполнить конкретные операционные задачи, и активное тестирование может проводиться в рамках самооценки или с помощью услуг, предоставляемых по запросу сторонней организацией. Особая осторожность необходима при проведении активного тестирования на любой действующей производственной системе.

Методология, описанная в настоящей публикации, была разработана для идеальной ситуации: группа состоит из трех-четырех экспертов по оценке, которые будут находиться 1-2 недели на объекте с целью проведения оценки. В то же время предусматривается также возможность адаптирования этой методологии в случаях, когда временные и ресурсные ограничения не позволяют обеспечить такой объем работы.

1.4. СТРУКТУРА

Настоящая публикация состоит из обзора методологии с подробным руководством для различных этапов оценки. Она содержит следующие разделы:

— раздел 2 – обзор методологии оценки с описанием основных этапов и шагов, которых можно придерживаться;

— раздел 3 – более подробное описание подготовительных работ, которые могут быть выполнены перед проведением оценки;

— раздел 4 – описание методологии оценки;

— раздел 5 – подробное руководство по проведению оценки, включая примеры задаваемых вопросов и информации, рассматриваемой в ходе процесса оценки;

— раздел 6 – описание действий, которые обычно осуществляются в конце оценки и в качестве последующих мероприятий по итогам оценки;

— приложение I, которое содержит подсказки и информацию по надлежащей практике проведения оценок, касающихся промышленных систем управления;

— приложение II, в котором приводится предназначенный для членов группы шаблон для записей о работах, выполняемых на местах;

— приложение III – шаблон для итогового отчета;

— приложение IV, в котором приводятся вопросы, касающиеся учета принимающей организацией изложенных в отчете результатов.

На рисунке 1 показаны основные этапы планирования оценки и предполагаемые сроки.

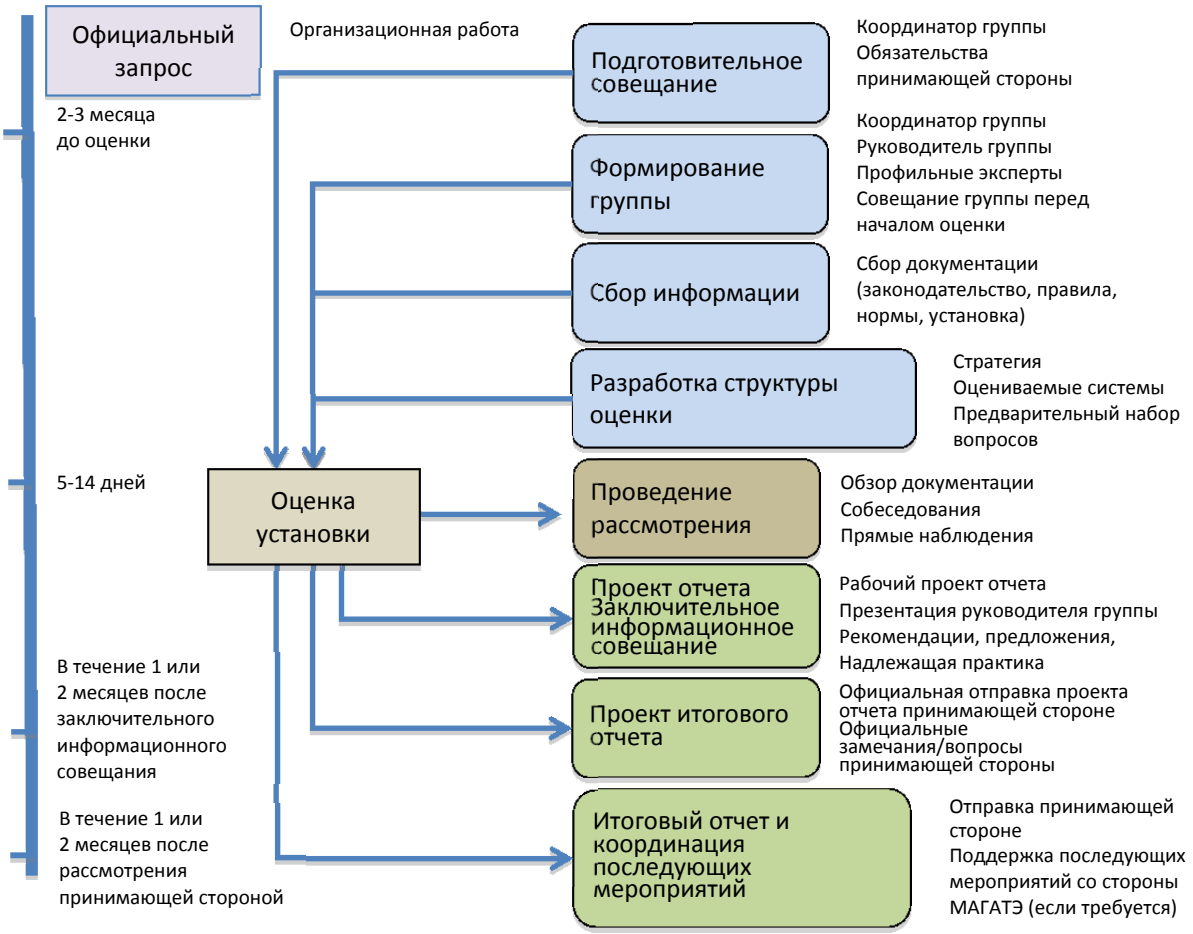

РИС. 1. Этапы и сроки оценки. Сроки могут быть скорректированы в соответствии с имеющимися ресурсами и временными ограничениями.

2. ОБЗОР МЕТОДОЛОГИИ И ПРОЦЕССА ОЦЕНКИ

2.1. ЦЕЛИ

Цель методологии оценки заключается в оказании помощи государствам-членам и операторам в разработке, внедрении, поддержании и – в случае необходимости – укреплении структуры обеспечения компьютерной безопасности на их установках, а также помощи их компетентным органам в оценивании эффективности принятых мер. Настоящая публикация представляет собой руководящий документ высокого уровня, предназначенный для применения при разработке и проведении оценки на ядерных установках или на других установках с радиоактивным материалом, но не должен использоваться в качестве исчерпывающего контрольного перечня для проведения оценки. Ее основная цель заключается в предоставлении рекомендаций в отношении некоторых или всех из указанных ниже действий:

— для операторов установки – как их программа обеспечения компьютерной безопасности может устранять соответствующие киберугрозы и быть структурированной для адаптации к их эволюции;

— для национальных компетентных органов – как транслировать международные рекомендации в конкретные требования к системе компьютерной безопасности государства на объектах с ядерными и другими радиоактивными материалами;

— для операторов установки – какие выбрать различные методы, с помощью которых могут быть выполнены международные рекомендации и требования надлежащей практики;

— для национальных компетентных органов и операторов установки – как проводить объективную оценку состояния имеющейся структуры компьютерной безопасности и выполнения международных руководящих рекомендаций и требований надлежащей практики;

— для ключевых сотрудников национальных компетентных органов и операторов установки – предоставление возможности обсудить применяемую ими практику с экспертами, имеющими опыт применения соответствующей практики в аналогичной области на других объектах;

— для специалистов по компьютерной безопасности из государств-членов – предоставление этим специалистам возможности обогатить свой опыт и знания в области своей специализации.

Кроме того, оценка может использоваться для выявления надлежащей практики, о которой затем могут быть информированы другие установки и/или государства-члены для реализации ими долгосрочных усовершенствований.

2.2. АСПЕКТЫ РЕГУЛИРОВАНИЯ

Настоящая публикация может использоваться как справочное руководство компетентными органами при проведении оценок компьютерной безопасности на объекте. Кроме того, компетентный орган может поручить установке проведение самооценки или же может потребовать, чтобы самооценки проводились на периодической основе. Компетентный орган может потребовать, чтобы оценка объекта проводилась независимой или третьей стороной.

Подготовительный процесс предусматривает определение конкретных норм и регулирующих положений, которые должны использоваться при составлении выводов,

рекомендаций и предложений. Компетентный орган может запрашивать следующую информацию, полученную в ходе проведения оценки и включаемую в итоговый отчет:

— перечень выводов;
— план действий на установке по реализации выводов, включая принимаемые меры и сроки;
— данные системы контроля, используемой для мониторинга и отслеживания реализации отдельных выводов;
— периодические отчеты, когда это необходимо, о ходе реализации конкретных выводов.

Компетентный орган может использовать эти результаты проверок в качестве основы для проведения будущих инспекций.

2.3. ПРОЦЕСС ОЦЕНКИ

Элементы и схема процесса проведения оценки представлены на рис. 2. Этот процесс будет рассмотрен подробно ниже.

Настоящая публикация содержит руководство и рекомендации в отношении того, как планировать оценку и формировать группу оценки. Условиями проведения эффективной оценки является наличие достаточных ресурсов, квалифицированной группы оценки и тесного сотрудничества со стороны установки.

Кроме того, она позволяет определить сферы репрезентативной оценки и руководство по сбору информации на основе концепции функциональных доменов и доменов физической безопасности. Группа оценки разрабатывает структуру оценки – систематический план оценивания установки – с учетом целей планирования, руководящих материалов МАГАТЭ, отраслевых стандартов, нормативных руководств, надлежащей практики и т.п. Конкретный контрольный список для этого не приводится, так как каждая оценка уникальна в своем роде и требует индивидуального подхода.

В зависимости от характера оценки и временных ограничений члены группы оценки могут корректировать масштабы оценки с учетом конкретной ситуации и конкретных потребностей, связанных с данной установкой. Необходимо предусматривать всесторонний анализ всех аспектов компьютерной безопасности в рамках проводимой оценки для вынесения информированного суждения о текущем состоянии программы обеспечения компьютерной безопасности.

При проведении оценки группа должна собрать достаточное количество информации, необходимой для оценки практики обеспечения компьютерной безопасности на установке на соответствующем уровне. Представленное руководство содержит подсказки по сбору информации и рекомендации по ключевым пунктам.

Группе оценки необходимо применять метод критического суждения при оценивании структуры обеспечения компьютерной безопасности на установке и основывать свое суждение на обоснованных результатах обследований, а не на предположениях. Группа может также выносить рекомендации и представлять предложения по улучшению и применению надлежащей практики на установке. Важно, чтобы группа сознавала, что приемлемыми могут быть различные подходы к реализации физической безопасности (за исключением случаев, когда компетентный орган выбирает конкретный подход).

Результатом проведения оценки являются итоговый отчет и, как правило, заключительное информационное совещание. Помимо представления выводов, полученных в ходе проведения оценки, в отчете об оценке приводятся рекомендации

или предложения, которые могут обеспечить совершенствование рассматриваемых систем или процессов. В отчете могут быть также рассмотрены последствия выводов для физической безопасности и безопасности установки в целом. Рекомендуется выявлять надлежащую практику и доводить информацию о ней до сведения других установок и/или государств-членов.

В ходе заключительного информационного совещания руководитель группы представляет полученные в результате проведения оценки выводы и, в частности, рекомендации и предложения. Важно, чтобы руководитель группы также устанавливал соответствующий контекст для выводов и любой актуальной информации. Рекомендуется, чтобы результаты и особенно "отчеты, подготовленные в соответствии с дифференцированным подходом", всегда представлялись в рамках соответствующего контекста и с должным обоснованием.

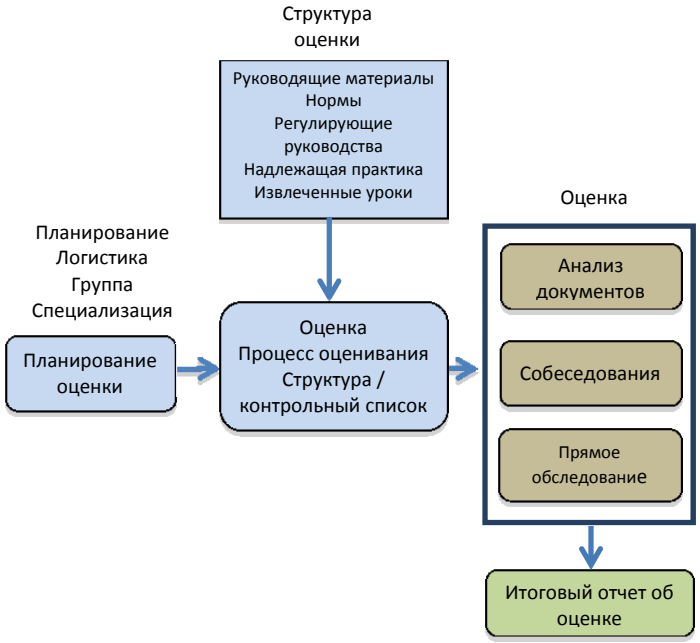

РИС.2. Элементы оценки.

2.4. ДОМЕНЫ ОЦЕНКИ

Подход к оценке компьютерной безопасности состоит из двух основных элементов: анализа общей программы обеспечения физической компьютерной безопасности и анализа одного или нескольких уровней систем. Оценка позволяет получить представление о состоянии компьютерной безопасности на установке. Концепция, использованная в настоящей публикации, обеспечивает рассмотрение в рамках различных доменов как функциональных операций, так и компьютерной безопасности на установке. Она обеспечивает охват процессов и систем, выполняющих основные функции, включая операции, бизнес-процессы, безопасность, физическую безопасность и реагирование на чрезвычайные ситуации.

2.4.1. Функциональные домены

В целом компьютерные системы на ядерных установках могут быть отнесены к одной или нескольким из пяти функциональных доменов, описанных в данном разделе. Оценка может быть спланирована так, чтобы она охватывала один или несколько этих функциональных доменов (см. подраздел 2.6 "Масштабируемость", в котором приводится дополнительная информация). Полная оценка компьютерной безопасности охватывает все пять доменов:

i. Домен операций: компьютерные системы, используемые для обеспечения функционирования объекта, являющегося предметом оценки. К ним относятся системы контроля и управления и сбора данных. Другими системами, подлежащими рассмотрению, являются системы, которые необходимы для обеспечения эксплуатации самой установки, например, системы отопления, охлаждения, вентиляции, освещения и лифтового хозяйства.

ii. Домен бизнес-процессов: компьютерные системы, используемые в менеджменте и операциях, ориентированных на бизнес-процессы (организационно-административную деятельность) объекта. Типичным примером является система разрешений на выполнение работ (допусков). Системы домена бизнес-процессов, как правило, имеют соединения с внешними сетями, которые могут иметь отношение к другим доменам.

iii. Домен безопасности: компьютерные системы, которые имеют чрезвычайно важное значение для безопасности установок и обеспечения защиты людей и окружающей среды от радиационных рисков и видов деятельности, могущих привести к таким рискам. К ним относятся, например, системы предотвращения и защиты, используемые для останова установки атомной электростанции.

iv. Домен физической защиты: компьютерные системы, используемые для защиты и контроля ядерных и радиологических материалов на объекте. К ним относятся системы контроля доступа и системы физической защиты для контроля периметра, а также системы учета и контроля ядерного материала.

v. Домен реагирования на чрезвычайные ситуации: компьютерные системы, используемые для обнаружения, реагирования на возникновение и минимизации последствий чрезвычайных ситуаций, угрожающих общественной безопасности, здоровью и окружающей среды. Например, компьютерные системы могут использоваться для мониторинга излучения и окружающей среды, пожарной сигнализации и пожаротушения и связи в случае чрезвычайных ситуаций.

2.4.2. Домены физической безопасности

Домены физической безопасности представляют собой целевые области высокого уровня, в которых проводится анализ компьютерной безопасности. Они позволяют группе оценки, осуществляющей оценивание функционального домена, определить комплексную цель для анализа практики обеспечения физической безопасности. Эти домены являются адаптированными вариантами, описанными в стандарте IEC/ISO 27002 [6]. Они включают:

i. менеджмент физической безопасности;

ii. менеджмент компьютерной безопасности;

iii. менеджмент активов;

iv. безопасность людских ресурсов (персонала);

v. физическую защиту;

vi. менеджмент коммуникации и операций;

vii. контроль доступа к компьютерам;

viii. приобретение, развитие и обслуживание компьютерных систем;

ix. менеджмент инцидентов, связанных с компьютерной безопасностью;

x. менеджмент непрерывности функционирования;

xi. обеспечение соответствия требованиям.

Публикация Серии изданий МАГАТЭ по физической ядерной безопасности, № 17, "Компьютерная безопасность на ядерных установках" [3] и стандарты серии ISO/IEC 27000 [4-8] вместе образуют исходный базис для оценивания. Стандарты на промышленные системы управления, методы надлежащей практики и накопленный опыт также могут рассматриваться группой оценкой при разработке плана проведения оценки (возможно, контрольного перечня оценивания). В разделе 5 более подробно описывается каждый домен физической безопасности и приводится руководство по оценке в рамках каждого домена. В приложении I приводятся примеры уроков, извлеченных из оценивания промышленных систем управления.

2.5. МЕТОДЫ ОЦЕНИВАНИЯ

Группа оценки использует все или некоторые из следующих методов для получения информации, необходимой для выработки своих выводов и рекомендаций:

— анализ документов и записей, например законодательства, регулирующих положений, установки;

— проведение собеседований с персоналом соответствующих организаций, таким как персонал компетентного органа, операторы установки и представители других организаций;

— проведение прямых обследований организации, ее практики и систем и осуществления мер по обеспечению компьютерной безопасности.

2.5.1. Анализ документов и записей

Процесс сбора информации включает в себя обзор, изучение или анализ документов и записей установки, предоставленных установкой или собранных на ней. Задача заключается в том, чтобы:

— провести оценку соответствия мероприятий и мер по обеспечению компьютерной безопасности внутренним процедурам;

— провести оценку соблюдения национального законодательства, стратегий, регулирующих требований и руководящих материалов;

— определить согласованность с соответствующими международными руководящими рекомендациями, например руководящими материалами МАГАТЭ, стандартами ИСО/МЭК и методами надлежащей практики;

— определить соответствие применяемых механизмов и мер по обеспечению компьютерной безопасности установленной международной и национальной надлежащей практике;

— оценить соответствие нынешней ситуации в плане имеющихся угроз (например, проектной угрозы);

— определить процессы и/или системы для детальной оценки на объекте в выбранных/соответствующих функциональных доменах.

К документам может относиться (не ограничиваясь перечисленным) любой из следующих документов:

— документ с изложением политики;
— процедуры;
— учредительные документы компании;
— регулирующие руководящие материалы/законы;
— предыдущие отчеты об оценке (внешние оценки, самооценки и т.п.);
— записи (например, о тренировках, инспекциях и т.п.);
— веб-страницы (Интернет и Интранет);
— учебные материалы (для новых работников, по компьютерной безопасности и т.п.);
— инвентарные списки компьютеров;
— списки контроля доступа;
— конфигурационные файлы;
— схемы сетей;
— схемы установки;
— операционные журналы;
— наборы правил (например, брандмауэры, СОВ, маршрутизаторы и т.п.).

В разделе 5 перечислены рекомендованные документы и записи для рассмотрения в рамках каждого домена физической безопасности и приводятся подсказки, обеспечивающие понимание конкретных вопросов, которые следует рассматривать при анализе документов на предмет соответствия надлежащей практике.

2.5.2. Собеседования

Собеседования и беседы с отдельными лицами или группами на установке и/или в соответствующем компетентном органе обеспечивают дополнительный объем информации для оценки. Действительно, в случае надлежащего проведения эти собеседования, возможно, представляют собой наиболее важную часть оценки. После рассмотрения соответствующих письменных документов с персоналом установки могут быть проведены собеседования с целью:

— получения дополнительной информации;
— проверки того, что письменные процедуры понимаются и исполняются так, как они письменно изложены;
— выявления связанных с оценкой вопросов, появившихся после осуществления предыдущих действий или проведения инструктажей;
— выявления индивидуальных мнений;
— формирования суждения о базе знаний, профессиональной подготовке и ресурсах оцениваемого объекта;
— обоснования, подтверждения или оспаривания результатов обследований, проведенных в ходе изучения на объекте принятых мер обеспечения компьютерной безопасности;
— определения информационных потоков и фактических процессов в организации.

Собеседования также позволяют обмениваться важной информацией между членами группы оценки и персоналом установки. Обсуждение в виде дружеского обмена мнениями – это, как правило, наилучший метод проведения собеседований. Конфронтационный подход не может быть продуктивным. При необходимости можно пользоваться услугами переводчика во избежание взаимного недопонимания. Необходимо тщательно отбирать соответствующих респондентов из числа персонала для собеседований с целью обеспечения надлежащего уровня обмена информацией. Например, руководящий состав не всегда будет способен ответить на вопросы, связанные с технической стороной осуществления процессов. В круг сотрудников, рекомендуемых для приглашения к собеседованиям, входят (без ограничения перечисленным):

i. Административное руководство:
   - руководитель объекта;
   - руководитель(и) установки(ок);
   - руководитель службы физической безопасности;
   - начальник службы безопасности;
   - руководитель(и) информационной/ компьютерной/ИТ-безопасности;
   - руководитель отдела информационных технологий;
   - руководитель отдела людских ресурсов (кадров);
   - руководитель операций в чрезвычайных ситуациях;
   - другие сотрудники руководящего звена в случае необходимости.

ii. Технические специалисты:
   - системные администраторы;
   - ответственный за обслуживание СКУ;
   - системный инженер (для каждой отдельной системы);
   - технические операторы.

iii. Прочий персонал:
   - персонал, ответственный за обеспечение качества;
   - операторы пультов.

До начала собеседований группа оценки должна подготовить набор первоначальных вопросов или тем. Хорошо сформулированные вопросы могут помочь в оценивании:

- политики и процедур обеспечения осведомленности и соблюдения требований;
- эффективности подготовки кадров и обеспечения физической безопасности;
- подготовки и осведомленности по вопросам обеспечения физической безопасности;
- восприятия угроз и рисков;
- потенциала реагирования на инциденты;
- ясности функций и обязанностей;
- эффективности культуры безопасности;
- выявления проблем и подготовки отчетных материалов;
- мер обеспечения конфиденциальности;
- применения надлежащей практики;
- выбора технических мер и решений для реализации.

В частности, эффективный опрос позволит:

— прояснить вопросы, возникшие при изучении собранных документов;

— убедиться в том, что сотрудники, которым поручено или которые несут ответственность за осуществление процедур, хорошо понимают политику в области физической безопасности, имеющую отношение к их реализации;

— убедиться в том, что эти сотрудники хорошо понимают процедуры осуществления и имеют должную подготовку и квалификацию для выполнения своих должностных функций и/или соответствующей деятельности.

Собеседования предлагается проводить в открытой и динамичной манере, оставляя место для спонтанных вопросов и обмена информацией помимо постановки стандартных вопросов.

В разделе 5 приводятся примеры вопросов для каждого домена физической безопасности, которые группа оценки может использовать и адаптировать в зависимости от конкретных потребностей.

2.5.3. Прямые обследования

Прямые обследования применения мер по обеспечению компьютерной безопасности и осуществления процедур на установке являются важным аспектом процесса оценки. Проведению обследований практического применения этих мер и процедур может быть посвящена значительная часть общего времени проводимой на объекте оценки. Предполагается, что обследования будут охватывать применение процедур, планов, инструкций, подготовку регулярных и специальных отчетов и осуществление мер по контролю качества на объекте.

Деятельность на объекте, которая рекомендуется для обследования во время проведения оценки, включает (не ограничиваясь перечисленным):

— менеджмент конфигурации и активов;
— усиление защиты систем;
— процессы обеспечения физической безопасности;
— физический и логический контроль доступа;
— разграничение индивидуальных обязанностей;
— безопасность персонала;
— мониторинг и регистрацию событий;
— формирование архитектуры сети;
— применение надлежащей практики;
— осмотры/проверки систем.

Важно также рассмотреть любое применение компенсационных средств контроля, когда элемент контроля физической безопасности не может быть установлен на место, а вместо этого он замещается другим элементом для реализации той же самой цели обеспечения физической безопасности. Рассматриваемые действия могут обследоваться на предмет соответствия действующим на установке процедурам или правилам, руководствам и отраслевой надлежащей практике. Результаты обследований, полученные группой, затем могут использоваться для оценивания реальных возможностей осуществления на установке программы обеспечения компьютерной безопасности.

В разделе 5 перечислены соответствующие действия, выполняемые при проведении обследований в рамках каждого домена физической безопасности.

2.6. МАСШТАБИРУЕМОСТЬ

Характер конкретной оценки может обусловливать целесообразность или желательность ограничения масштабов оценки лишь некоторыми функциональными областями, о которых говорится в настоящем руководстве. Руководство, представленное в настоящей публикации, является гибким и может быть масштабировано с учетом различных подходов и сроков в зависимости от уровня оценки.

2.7. УЧЕТ АСПЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При проведении оценки исследуется защита чувствительной информации и активов чувствительной информации. Отчеты и рабочие документы могут содержать чувствительную информацию, несанкционированное раскрытие которой может скомпрометировать физическую ядерную безопасность и привести к серьезным последствиям. Поэтому важно, чтобы подготовительные материалы, технические записки, проекты отчетов и итоговый отчет были надлежащим образом классифицированы, маркированы, и обращение с ними, их хранение, передача и уничтожение осуществляются согласно соответствующим процедурам, установленным для чувствительной информации на принимающей установке. Методы обращения с такой информацией и обеспечения ее физической безопасности (защищенности) должны быть обсуждены в ходе подготовительного совещания и определены до начала оценки.

Члены группы, передающие свои технические записки другим членам группы для обсуждения, должны принимать специальные меры предосторожности для обеспечения безопасности чувствительной информации. До проведения оценки необходимо также уделить внимание типам электронных устройств или носителям данных, которые будут использоваться для составления индивидуальных заметок и проектов и окончательного варианта отчета.

Рекомендуется, чтобы обеспечение безопасности этих материалов было основано на принципе "необходимо знать", т.е. когда доступ к материалам ограничивается лицами, чья благонадежность и необходимость знать в отношении которых были проверены.

В зависимости от контекста оценки может требоваться, чтобы члены группы оценки подписывали соглашение о конфиденциальности или неразглашении.

3. ПОДГОТОВИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

3.1. СФЕРА ОХВАТА РАССМОТРЕНИЯ

Ввиду большого количества компьютерных систем на ядерных установках и масштабов функциональных доменов и доменов физической безопасности, подлежащих оценке, проведение всеобъемлющего рассмотрения всей программы обеспечения компьютерной безопасности в рамках одной оценки может оказаться невозможным. Первым шагом поэтому является определение принимающей стороной масштабов и целей оценки и при необходимости их разъяснение координатору группы или руководителю группы. В разделе 4 представлена концепция модульных компонентов конкретных функциональных доменов установки. Такой подход позволяет экспертам, планирующим оценку, определять приоритетные компоненты для проведения оценки с учетом конкретных условий.

3.2. ПОДГОТОВИТЕЛЬНОЕ СОВЕЩАНИЕ

Подготовительное совещание с участием координатора и руководителя группы и представителей всех соответствующих сторон обычно проводится на принимающей установке примерно за два-три месяца до проведения оценки. Желательным итогом этого совещания является выработка четкого понимания процесса и методологии оценки, включая подготовительную работу, механизмы проведения оценки и работу по составлению отчета по завершению оценки. По окончании совещания может быть распространен протокол совещания.

На совещании рассматриваются следующие вопросы:

- основные особенности программы оценки;
- цель и масштабы оценки;
- ожидаемый формат и содержание отчета;
- масштабы и уровень анализа, включаемого в отчет;
- требования по обращению с информацией и информационной безопасности применительно к отчету и техническим запискам;
- подготовка оценки, включая перечень требующихся документов;
- подготовка пакета предварительной информации для группы оценки;
- необходимая логистическая поддержка, например предоставление рабочего помещения для группы, принтера, копировального устройства и организация местных перевозок;
- предоставление услуг по письменному и устному переводу;
- обращение с конфиденциальными документами оцениваемой установки;
- процедуры, которых должна придерживаться группа оценки, включая соответствующие принимаемые действия и уведомляемое контактное лицо в принимающей организации, в случае обнаружения любого из указанных ниже событий:
  - фактическое или потенциальное нарушение безопасности системы,
  - умышленная халатность,
  - серьезная проблема безопасности,
  - серьезная проблема физической безопасности;
- завершение составления графика проведения оценки;

— возможный состав группы оценки;
— возможные последующие мероприятия.

3.3. ОБЯЗАТЕЛЬСТВА ПРИНИМАЮЩЕЙ СТОРОНЫ

Считается, что принимающая сторона должна финансировать проводимые работы. Принимающей стороной может быть руководство установки или государственное ведомство, отвечающее за проведение рассмотрения на установке, или государственное учреждение, если деятельность по оценке осуществляется в рамках рассмотрения на государственном уровне. В процессе подготовительного совещания координатор группы и руководитель группы договариваются с принимающей страны в отношении предоставления помещений и вспомогательных услуг, необходимых для работы на месте проведения оценки. В случае международной миссии оценка компьютерной безопасности обычно проводится на английском языке. Принимающая сторона должна обеспечивать предоставление услуг по устному переводу, необходимых членам группы для выполнения своей работы.

Важно, чтобы принимающая сторона предоставляла группе оценки в исключительное пользование безопасное помещение для совещаний на весь период проведения оценки. Это безопасное помещение для совещаний должно иметь достаточные размеры для работы группы и проведения обсуждений в условиях разумной конфиденциальности. Желательным также может быть предоставление доступа в Интернет, однако этот вопрос необходимо обсудить на первоначальном подготовительном совещании. Рекомендуется предоставлять в распоряжение членам группы компьютерный принтер и копировальный аппарат. Соответствующие документы, которые будут обсуждаться на подготовительном совещании, предоставляются на языке, согласованном между принимающей стороной и группой оценки. Для группы оценки на период проведения оценки требуется контейнер, шкаф или помещение с дополнительными мерами физической защиты для обеспечения безопасного хранения документов или активов, которые могут содержать конфиденциальные сведения или чувствительную информацию.

В целях экономии времени в процессе проведения оценки и формирования у членов группы хорошего понимания контекста оценки и регулирующих требований желательно, чтобы принимающая сторона предоставила соответствующие документы для распространения среди членов группы по меньшей мере за два месяца до прибытия группы на объект, учитывая при этом то, что некоторые документы могут быть предоставлены только непосредственно на объекте. Со всеми документами, полученными от принимающей стороны, необходимо обращаться в соответствии с соглашением, достигнутым между принимающей стороной и группой оценки.

В зависимости от масштабов оценки в число этих документов могут входить;

i. национальное законодательство:
   — закон(ы), регулирующий(е) компьютерную безопасность ядерных установок; краткое изложение функций и структуры (с указанием соответствующих отделов) различных государственных организаций, в чью компетенцию входят вопросы компьютерной безопасности, и как они взаимосвязаны друг с другом;
   — регулирующие положения по компьютерной безопасности ядерных установок;
   — соответствующие руководящие документы по регулированию, действующие в отношении ядерных установок;
   — параметры проектной угрозы.

ii. Организации и процедуры регулирующих органов:

— структура, организация и укомплектование персоналом; описание процедур лицензирования в соответствующих случаях;

— практика инспектирования;

— перечень применимых регулирующих положений, регулирующих руководств, кодексов и норм.

iii. Описание, организационная структура установки и процедуры обеспечения компьютерной безопасности:

— общая политика обеспечения физической безопасности (или ее соответствующие разделы);

— планы обеспечения компьютерной безопасности;

— функции и обязанности по обеспечению физической безопасности;

— программы подготовки и повышения осведомленности по вопросам обеспечения физической безопасности;

— инвентарные списки цифровых активов и описание того, каким образом и почему цифровые активы включены в программу обеспечения компьютерной безопасности установки;

— участие третьих сторон;

— оценка риска, включая описание того, как выбираются средства контроля физической безопасности;

— категоризация систем безопасности;

— процедуры обеспечения безопасности, имеющие отношение к физической безопасности;

— построение архитектуры сети;

— пограничные устройства между доменами сети, включая политику контроля потоков данных для этих устройств;

— техническая документация систем;

— имеющиеся отчеты об оценке (составленные самой установкой или третьей стороной);

— процедуры реагирования на инциденты, связанные с компьютерной безопасностью, и соответствующие записи;

— отчеты об инцидентах, связанных с компьютерной безопасностью, и корректирующие меры;

— документация по менеджменту конфигурации, включая анализ физической безопасности, связанный с изменениями конфигурации.

3.4. ФОРМИРОВАНИЕ ГРУППЫ

3.4.1. Состав группы

Группа может состоять из координатора группы, руководителя группы (при необходимости), трех или более экспертов и, возможно, редактора технической документации для помощи группе в составлении технических записок и итогового отчета об оценке. Состав группы может изменяться в соответствии с масштабами оценки.

Координатор группы или руководитель группы оценки отбирает экспертов для группы с согласия принимающей стороны. Эти эксперты должны иметь подтвержденные глубокие знания и богатый опыт в области компьютерной безопасности, а также специализацию в одной или нескольких областях эксплуатации, безопасности, физической безопасности установки, информационных технологий и технических средств на установке для оказания поддержки в оценивании функциональных доменов. Члены группы должны располагать необходимым временем для подготовки оценки, ее проведения и составления итогового отчета о ней. Знакомство по крайней мере одного из членов группы с конструкцией установок, эксплуатируемых принимающей стороной, будет способствовать проведению оценки.

Кроме того, рекомендуется, чтобы члены группы подбирались таким образом, чтобы охватывались различные национальные подходы к регулированию и реализации, включая соответствующее законодательство, регулирование ядерной деятельности, эксплуатацию установок и анализа систем компьютерной безопасности. Желательно, чтобы все эксперты в дополнение к их конкретной специализации были знакомы с другими национальными подходами и располагали знаниями в других соответствующих областях. Это позволит выполнить наилучшую возможную оценку компьютерной безопасности и выработать соответствующие рекомендации.

Для участия в совместном с группой проведении оценки может быть приглашен наблюдатель от принимающей стороны. Это может оказаться целесообразным с точки зрения облегчения обмена информацией.

3.4.2. Координатор группы

Координатор группы работает совместно с группой на протяжении всей оценки, координируя работу группы с партнерами в принимающей организации и обеспечивая логистическую и другую поддержку, которая может потребоваться. В случае миссии МАГАТЭ по оказанию консультативных услуг координатор группы распространяет последние варианты соответствующих документов и любых других применимых материалов, помимо предварительных материалов, предоставленных принимающей стороной, среди всех членов группы, с тем чтобы они могли ознакомиться с документами, которыми они будут пользоваться в ходе осуществления миссии.

Координатор группы несет общую ответственность за координацию оценки и предоставление итогового отчета об оценке.

Обязанности включают:

— координацию подготовительной работы и принятие необходимых мер для проведения оценки;

— установление контактов с соответствующими коллегами принимающей организации, которые будут основными контактными лицами для группы оценки в ходе осуществления миссии;

— назначение, совместно с принимающей организацией, если это необходимо, эксперта по компьютерной безопасности в качестве руководителя группы для проведения оценки;

— организацию, совместно с руководителем группы, подготовительного совещания с участием принимающей стороны;

— подбор, с одобрения принимающей организации, членов группы;

— координацию логистической поддержки группы оценки, включая предоставление соответствующих информационных документов;

— знание соответствующих правил, действующих на установке в отношении безопасности, физической безопасности, безопасности персонала, а также любых других применимых требований и распространение этой информации в группе оценки.

3.4.3. Руководитель группы

Роль руководителя группы особенно важна в обеспечении успешного проведения оценки. Кандидаты, назначаемые руководителями группы, должны обладать признанными лидерскими качествами и весьма богатым опытом во всем спектре вопросов, связанных с проведением рассмотрения, с которыми группе оценки придется иметь дело. В идеальном случае руководитель группы должен иметь опыт проведения оценок компьютерной безопасности на ядерных установках.

На руководителя группы, как правило, в целом возлагаются обязанности:

— представлять группу во взаимодействии с коллегой принимающей организации;

— руководить проведением подготовительного, начального и заключительного информационного совещаний;

— определять правила взаимодействия всех членов группы;

— проводить инструктаж членов группы по вопросам проведения оценки, включая изложение ее целей и процессов;

— обеспечивать наличие у членов группы необходимой информации, должным образом подготовленной для оценки;

— руководить разработкой детальных планов и графиков проведения оценки;

— осуществлять координацию и руководить работой группы по проведению рассмотрения, включая проведение ежедневных совещаний группы, обеспечение соблюдения графиков, информирование коллег принимающей организации, урегулирование вопросов, требующих решения, и подготовку к заключительному совещанию;

— осуществлять координацию анализа всех технических записок;

— координировать подготовку проекта отчета;

— представлять результаты оценки на заключительном информационном совещании;

— осуществлять подготовку итогового отчета;

— обеспечивать, чтобы члены группы были осведомлены по вопросам конфиденциальности и соответственно правил обращения с информацией;

— обеспечивать, чтобы члены группы были осведомлены и подготовлены по вопросам применения соответствующих правил на установке, касающихся безопасности, физической безопасности, безопасности персонала, и других применимых требований.

3.4.4. Члены группы

Члены группы проводят оценку, сбор информации, оценивание результатов и участие в составлении итогового отчета. Они обладают экспертными знаниями в области компьютерной безопасности и дополнительными знаниями, касающимися работы организации или установки.

Обязанности членов группы включают:

— проведение анализа документов и записей;

— участие в совещаниях и дискуссиях со своими коллегами в принимающей организации, в соответствующих случаях;

— участие в совещаниях группы и в разработке мероприятий по оценке;

— сравнение заключений/выводов с результатами, полученными другими членами группы;

— составление технических записок по реализации мер обеспечения компьютерной безопасности на установках принимающей стороны на основе докладов, документации, результатов собеседований и прямых обследований организации и применяемой ею практики;

— оценивание систем в функциональных доменах с учетом средств контроля в домене физической безопасности;

— осведомленность о соглашении о конфиденциальности с организацией и соответственно о правилах обращения со всей информацией;

— осведомленность по вопросам применения и соблюдение на установке соответствующих правил, касающихся безопасности, физической безопасности, безопасности персонала, и других применимых требований.

3.4.5. Редактор технической документации

Редактор технической документации может быть полезен в группе в плане оказания помощи в своевременной подготовке отчета по оценке, а также помощи членам группы в составлении технических записок. Редактор технической документации присутствует на всех совещаниях, информационных брифингах и собеседованиях и ведет записи в дополнение к информации, собранной группой. В ходе проведения оценки редактор технической документации собирает письменные материалы, подготовленные группой, и форматирует и при необходимости редактирует эти материалы. Обязанности включают:

— участие в работе группы;

— ведение детальных записей и/или оказание помощи членам группы в подготовке к проведению обследований и собеседований;

— подготовку отчета об оценке вместе с группой и руководителем группы;

— поддержание осведомленности о соглашении о конфиденциальности с принимающей организацией и соответственно о правилах обращения со всей информацией;

— поддержание осведомленности по вопросам применения и соблюдение на установке соответствующих правил, касающихся безопасности, физической безопасности, безопасности персонала, и других применимых требований.

3.5. СОВЕЩАНИЕ ГРУППЫ ПЕРЕД ПРОВЕДЕНИЕМ ОЦЕНКИ

До начала оценки рекомендуется провести совещание группы с целью обеспечения координации действий в группе. Это особенно важно, если группа ранее не работала вместе, как в случае проведения международных миссий с участием экспертов из разных стран. Даже если группа регулярно работает вместе, также целесообразно организовывать совещание группы перед проведением оценки для обсуждения и уточнения конкретных деталей данной конкретной оценки.

В зависимости от характера миссии или оценки это совещание может организовываться за несколько месяцев до начала оценки или непосредственно перед ней.

Совещание проводится координатором и руководителем группы. Повестка дня может включать следующие пункты:

i. представление членов группы;

ii. справочная информация об оценке:

   a) масштабы оценки;
   b) график и сроки проведения оценки;

iii. опыт членов группы:

   a) квалификация и знания членов группы;
   b) ожидания членов группы;

iv. обсуждение факторов, являющихся специфичными для данной оценки и рассматриваемых ядерных установок;

v. обсуждение процесса оценки в деталях;

vi. определение и подробное описание функций, обязанностей и специализации каждого члена группы.

3.6. ГРАФИК ПРОВЕДЕНИЯ ОЦЕНКИ

График проведения оценки будет во многом зависеть от следующих факторов: проводится ли она на одной или нескольких площадках, является ли она специализированной оценкой или модулем в рамках другой оценки, миссии или консультативных услуг. В таблице 1 представлен примерный график проведения специализированной оценки компьютерной безопасности, при осуществлении которой большинство рабочий дней проводится на объекте и редактор технической документации ежедневно дополняет проект доклада.

ТАБЛИЦА 1. ПРИМЕРНЫЙ ГРАФИК ПРОВЕДЕНИЯ ОЦЕНКИ

1-й день
Группа оценки проводит совещание группы перед началом оценки и ориентационное совещание
2-й день
Группа получает необходимый инструктаж по входу на принимающую установку
Начальное совещание с представителями принимающей установки
Начало оценки
Совещание по заслушиванию итогов и подготовка к следующему дню
Редактор технической документации готовит ежедневный отчет по результатам заслушивания итогов
Руководитель группы при необходимости знакомит с результатами представителя принимающей организации
3-й день – последний день-2
Начало оценки
Совещание по заслушиванию итогов и подготовка к следующему дню
Редактор технической документации готовит ежедневный отчет по результатам заслушивания итогов и составляет обзор собранных ежедневные записок и отчетов
Руководитель группы при необходимости знакомит с результатами представителя принимающей организации
Последний день-1
Члены группы обсуждают и готовят итоговое резюме оценки
Редактор технической документации составляет заключительный отчет для рассмотрения членами группы
Руководитель группы готовит презентацию для заключительного информационного совещания
Руководитель группы при необходимости знакомит с результатами представителя принимающей организации
Последний день
Заключительное информационное совещание – ознакомление принимающей организации с результатами оценки

3.6.1. Совещания группы

Ежедневные совещания группы, обычно организуемые в конце дня, позволяют проводить обзор работы, выполненной за день, оценивать достигнутый прогресс, обсуждать выводы/заключения, подготовленные членами группы, и обеспечивать наличие у редактора технической документации необходимой информации, полученной в результате выполнения работы в течение дня.

Это совещание также может быть использовано для подготовки к работе на следующий день, например, включающей:

- рассмотрение соответствующих разделов руководящих принципов оценки и/или подготовительных материалов;
- составление перечня вопросов по каждой теме;
- планирование мероприятий по обследованиям на местах;
- определение основных вопросов для рассмотрения в приоритетном порядке на следующий день.

4. МЕТОДОЛОГИЯ ОЦЕНКИ

4.1. ОБЗОР МЕТОДОЛОГИИ

Типичным началом оценки является общий анализ практики обеспечения компьютерной безопасности на установке. Затем может проводиться более детальный анализ отдельных процессов и систем в соответствии с подходом, описанным в подразделе 4.3.1. Он основывается на разделении практики обеспечения компьютерной безопасности на функциональные домены и домены физической безопасности. Такой процесс позволяет улучшить оценивание эффективности и качества всей программы обеспечения компьютерной безопасности.

4.2. ОЦЕНКА ОБЩЕЙ ПРОГРАММЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

На этапе сбора информации оценка общей программы обеспечения безопасности включает в себя анализ соответствующей политики, планов, процедур, реализации и организационных схем. Собеседования и обследования на местах помогут в проведении дальнейшей оценки практики обеспечения компьютерной безопасности. Четырьмя аспектами общей исследуемой картины являются: подход к менеджменту, процессы обеспечения компьютерной безопасности, менеджмент угроз и последствий и менеджмент рисков.

В следующих разделах излагаются ориентировочные критерии для каждого из этих аспектов, на которых может основываться оценка.

4.2.1. Подход к менеджменту

Одним из ключевых элементов успешной программы обеспечения компьютерной безопасности является принятие политики компьютерной безопасности на всех уровнях менеджмента и операций и ее реализации на практике. Программа обеспечения компьютерной безопасности не будет успешной без решительной приверженности этому процессу со стороны руководства. Примерными критериями являются:

i. Приверженность руководства, демонстрируемая на всех уровнях.

ii. Четко определенные цели компьютерной безопасности.

iii. Четко установленные функции и обязанности для достижения того, чтобы процессы обеспечения компьютерной безопасности, в том числе конкретные функции и обязанности:

   a) распространялись на все функциональные домены;
   b) устанавливались с применением координированного подхода в соответствующих функциональных доменах;
   c) обеспечивали надлежащую организационную структуру (включая отдельную должность ответственного за компьютерную безопасность или эквивалентного ему специалиста).

iv. Менеджмент обеспечивает доступ к адекватным ресурсам (людским, финансовым, временным, экспертным и т.д.).

v. Процессы менеджмента включают проведение внутренних оценок и осуществление мер по обеспечению качества.

vi. Обеспечение соответствия нормативной (регулирующей) базе.

4.2.2. Процессы обеспечения компьютерной безопасности

Они представляют собой применение мер по обеспечению компьютерной безопасности при реализации политики обеспечения компьютерной безопасности. Сюда входит применение средств технического контроля, средств административного контроля и средств физического контроля для предотвращения, обнаружения событий, связанных с компьютерной безопасностью, и реагирования на эти события. Примерными критериями являются:

- наличие политики и программы обеспечения компьютерной безопасности;
- наличие структурированного, формализованного, задокументированного набора процессов, обеспечивающих компьютерную безопасность;
- применяются процессы, обеспечивающие непрерывный анализ и совершенствование, например периодическое проведение рассмотрений, аудитов, осуществление четких процедур по обслуживанию, выполнение самооценки и т.п.;
- процессы являются упреждающими в максимально возможной степени и не носят реактивный характер.

4.2.3. Менеджмент угроз и последствий

На основании источников достоверной информации соответствующие государственные органы и в соответствующих случаях сами объекты определяют угрозы и соответствующий потенциал путем оценки угроз и, в надлежащих случаях, проектной угрозы. При рассмотрении угроз проводится анализ возможных нарушителей с потенциалом совершения кибератак. Рекомендуется непрерывно проводить анализ и оценку угроз для выявления изменений, способных повлиять на компьютерную безопасность организации или установки. Ниже перечислены примерные критерии и вопросы.

- В организации внедрен зрелый процесс менеджмента, направленный на устранение угроз, уязвимостей и потенциальных последствий.
- Какие справочные материалы и методологии используются?
- Каковы масштабы анализа угроз (например, на уровне организации, части организации, системы и т.д.)?
- Как был выполнен, задокументирован и использован анализ применительно к базовым средствам контроля физической безопасности.
- Потенциальные цели были установлены и оценены для определения необходимости их защиты от угроз физической ядерной безопасности.
- Оценки включают в себя анализ потенциальных последствий, связанных с кибератаками целей.
- Применительно к оцениванию угроз – как часто проводится регулярный анализ и вносятся корректировки?
- Поддерживаются ли процессы минимизации, обеспечения непрерывности и восстановления, предусмотренные для борьбы с компрометацией компьютерных систем, в программе реагирования на инциденты?

4.2.4. Менеджмент риска и соблюдение основополагающих принципов обеспечения физической безопасности

Государства и установка должны обеспечивать, чтобы программа обеспечения компьютерной безопасности была способна ограничивать и удерживать риск компрометации компьютеров на приемлемом уровне посредством менеджмента рисков. В программе обеспечения компьютерной безопасности должно быть, кроме того, подробно регламентировано применение основополагающих принципов обеспечения физической безопасности, включая применение дифференцированного подхода и глубокоэшелонированной защиты, с целью обеспечения защиты активов от событий, связанных с физической ядерной безопасностью, с учетом уровня последствий или воздействия, к которым могут привести эти события. Ниже перечислены примерные критерии и вопросы.

— Меры по обеспечению компьютерной безопасности основаны на дифференцированном подходе. В частности, были установлены уровни физической безопасности в соответствии с четко определенными процессами или правилами (например, с учетом безопасности, проектной угрозы, анализа потенциальных последствий и т.п.). Применяются ли эти процессы или правила на практике?

— Как реализуется глубокоэшелонированная защита в компьютерных компонентах и системах?

— Как оценки риска влияют на дифференцированный подход?

— Обеспечивает ли дифференцированный подход охват всех вопросов, определенных в оценке рисков?

4.3. МАТРИЦА ОЦЕНКИ

4.3.1. Введение

Ключевым элементом данной методологии оценки является оценивание функциональных доменов и доменов физической безопасности (представленных в подразделе 2.4). В таблице 2 представлена матрица, предназначенная для фиксирования данных по обоим типам доменов оценки, что обеспечивает достаточный по глубине охват в оценке вопросов, представляющих прямой интерес. В матрицу оценки включены:

— пять основных функциональных доменов, сгруппированных в столбец;

— домены физической безопасности (адаптированные области, предусмотренные в стандарте ISO 27000), которые представлены в виде строк.

Эта матрица помогает:

— определить масштабы оценки;

— структурировать итоги анализа и обследований как на стадии сбора информации, так и в процессе работы на местах;

— группе оценки проводить достаточно широкий анализ, позволяющий выносить информированные оценки;

— наглядно видеть результаты оценки.

4.3.2. Функциональные домены

Глобальная оценка включает оценивание пяти функциональных доменов: операции, бизнес-процессы, безопасность, физическая защита и реагирование на чрезвычайные ситуации. В некоторых случаях возможно проведение оценки в более ограниченном масштабе, сосредоточенной на определенном наборе этих доменов (например, при проведении типовой миссии ИППАС будет оцениваться только физическая защита).

Ниже приводится примерный перечень групп систем или функций для оценивания в рамках каждого из пяти функциональных доменов. Этот перечень может быть изменен с учетом конкретных особенностей установки, на которой проводится оценка. Он также может быть скорректирован с учетом масштабов оценки и типа объекта. При необходимости этот набор может изменяться в ходе оценки и включать дополнительные элементы, выявленные при осуществлении работы на местах. Ниже приведены примеры систем или функций в каждом домене.

Домен операций

- Системы управления процессами: системы контроля и управления (СКУ) для управления установкой.
- СКУ помещения щита управления, включая системы аварийной сигнализации.
- Компьютерные системы управления процессами для сбора и подготовки информации, предназначенной для помещения щита управления.
- СКУ для обращения с топливом и его хранения.
- Менеджмент конфигурации/обслуживание.
- Дистанционный доступ и виртуальные частные сети (ВЧС) для создания рабочей среды.
- Инфраструктура речевой связи и передачи данных.
- Инфраструктурные системы эксплуатации и управления.
- Среда тестирования и разработки для систем домена операций.

Домен бизнес-процессов

- Инфраструктура речевой связи и передачи данных.
- Системы менеджмента людских ресурсов и хранилища данных.
- Инженерно-технические системы.
- Системы выдачи рабочих заданий и разрешений на выполнение работ.
- Системы закупок.
- Офисные системы.

Домен безопасности

- Системы защиты: СКУ, используемые для автоматически инициируемых действий по защите реактора и станции.
- Системы обслуживания устройств безопасности: СКУ, выполняющие действия по обеспечению безопасности, инициируемые системами защиты и ручным приводом.
- Вспомогательные средства системы безопасности: системы аварийного энергоснабжения для СКУ.

Домен физической защиты

- Мониторинг периметра/обнаружение проникновения.
- Системы контроля доступа.
- Системы учета и инвентарного контроля (помимо ядерных материалов).
- Системы учета и контроля ядерного материала.
- Инфраструктура речевой связи и передачи данных.
- Системы предупредительной сигнализации.
- База данных по допускам к работам и информации, используемая для обеспечения наличия у персонала надлежащих разрешений.

Домен реагирования на чрезвычайные ситуации

- Мониторинг окружающей среды.
- Радиационный мониторинг.
- Противопожарные системы.
- Инфраструктура речевой связи и передачи данных.

В итоговом отчете указывается, какие системы и функции были оценены и какие системы и функции не были предметом рассмотрения.

4.3.3. Домены физической безопасности

В отличие от функциональных доменов оценка может охватывать полный набор из одиннадцати доменов физической безопасности для обеспечения достаточно широкого масштаба рассмотрения. Как отмечалось ранее, эти одиннадцать доменов (областей) физической безопасности заимствованы в адаптированном виде из стандартов серии ISO/IEC 27000 [4-8]. Они были скорректированы для применения при проведении оценки компьютерной безопасности на ядерных установках. Раздел 5 содержит конкретное руководство по оцениванию каждого из этих доменов применительно к физической ядерной безопасности. Это – примерный, а не директивный перечень.

В таблице 2 представлена перекрестная матрица доменов физической безопасности и функциональных доменов, которая может быть использована для отслеживания степени выполнения оценки и обеспечения всеобъемлющего исследования выбранных областей рассмотрения. Использование такой матрицы – на усмотрение группы оценки. В дополнение к контролю степени выполнения оценки матрица позволяет наглядно видеть результаты обследований в рамках разных доменов, что может помочь в определении тенденций или пробелов в обеспечении физической безопасности.

ТАБЛИЦА 2. МАТРИЦА ОХВАТА ДОМЕНОВ.

Функциональные домены Домены физической безопасности	Операции	Бизнес-процессы	Безопасность	Физическая защита	Реагирование на чрезвычайные ситуации
Политика обеспечения физической безопасности					
Менеджмент компьютерной безопасности					
Менеджмент активов					
Безопасность людских ресурсов (персонала)					
Физическая защита					
Менеджмент коммуникации и операций					
Контроль доступа					
Приобретение, развитие и обслуживание					
Менеджмент инцидентов, связанных с компьютерной безопасностью					
Менеджмент непрерывности					
Обеспечение соответствия требованиям					

5. РУКОВОДЯЩИЕ ПРИНЦИПЫ ОЦЕНКИ ПО ДОМЕНАМ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

5.1. ОБЩИЙ ОБЗОР

В данном разделе излагаются руководящие принципы и надлежащая практика, относящиеся к каждому из одиннадцати доменов физической безопасности, для применения в качестве возможных критериев оценивания при проведении оценки. Указанные руководящие принципы не предназначены для использования непосредственно в качестве контрольного списка, но могут быть применены для составления плана оценки с учетом конкретных условий. Члены группы в ходе оценки должны уделять внимание не только отдельным доменам, но и их интеграции и воздействию на общую программу обеспечения компьютерной безопасности.

5.2. ПОЛИТИКА ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

5.2.1. Описание домена физической безопасности

Этот домен обеспечивает директивное руководство и поддержку в обеспечении компьютерной безопасности в соответствии с требованиями в отношении ядерной безопасности и физической безопасности, а также соответствующими законами, регулирующими положениями, правилами и требованиями, предъявляемыми к бизнес-процессам.

Административное руководство должно установить четкое направление политики в соответствии с требованиями обеспечения ядерной безопасности и физической безопасности и продемонстрировать свою поддержку и приверженность компьютерной безопасности путем ввода в действие и поддержания политики обеспечения компьютерной безопасности во всей организации.

Политика обеспечения компьютерной безопасности должна быть определена, доводиться до сведения соответствующих лиц, документироваться и периодически рассматриваться. Рекомендуется, чтобы в политике учитывались все пять ядерных функциональных доменов: операции, бизнес-процессы, безопасность, физическая защита и реагирование на чрезвычайные ситуации.

Требуемые документы и записи

- Политика/план обеспечения компьютерной безопасности.
- Политика/план обеспечения физической безопасности установки.
- Доведение политики обеспечения компьютерной безопасности до сведения персонала.
- Протоколы аудитов компьютерной безопасности.
- Протоколы пересмотра и обновлений политики обеспечения компьютерной безопасности.
- Протоколы тренировок в области обеспечения компьютерной безопасности.

Подсказки для анализа документов и записей

- Определена ли политика обеспечения физической безопасности?
- Согласуется ли эта политика с другой политикой, применяемой на установке?

— Как политика обеспечения безопасности доводится до сведения персонала?
— Как проявляется приверженность руководства этой политике?
— Как часто проводится рассмотрение политики с целью внесения в нее изменений? Имеются ли записи, фиксирующие результаты таких рассмотрений?
— Как руководство проводит оценки эффективности политики?
— Учтены ли в политике обеспечения безопасности все пять ядерных функциональных доменов?
— Существуют ли исключения в политике обеспечения безопасности, задокументированы ли они?
— Доведена ли политика обеспечения безопасности до сведения третьих сторон (субподрядчиков и т.п.)?
— Учитывает ли политика рекомендации по имеющейся надлежащей практике?
— Устанавливает ли политика четкие цели физической безопасности?
— Определены ли четко обязанности и назначен ли соответствующий ответственный орган?

Примерные вопросы для собеседований

— Обеспечена ли осведомленность респондентов о политике обеспечения физической безопасности?
— Понимают ли респонденты установленные функции и обязанности (в том числе свои)?
— Имеют ли они доступ к реализации политики обеспечения физической безопасности?
— Как политика обеспечения физической безопасности воплощена в конкретных руководствах или инструкциях, относящихся к выполняемой ими работе?

Пункты в плане проведения обследований

— Конкретные процессы, связанные с реализацией политики.
— В соответствующих случаях проверить согласованность политики.

Подсказки для анализа на местах

— Задавать одинаковые вопросы сотрудникам из разных подразделений на различных уровнях в организации.

5.3. МЕНЕДЖМЕНТ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Описание домена физической безопасности

В организации должна быть сформирована система менеджмента для обеспечения компьютерной безопасности.

Руководство должно утвердить политику обеспечения компьютерной безопасности, распределить функции и обязанности и рассматривать ход осуществления компьютерной безопасности в организации. Это может быть составным элементом более широкой политики обеспечения физической безопасности. Во всех подразделениях организации (например, ИТ и СКУ/инженерно-технические системы) рекомендуется применять многодисциплинарный подход.

Требуемые документы и записи

- Политика/план обеспечения компьютерной безопасности.
- Организационные схемы и описания должностей.
- Политика и процедуры, в которых подробно описывается организационная структура.
- Перечень лиц, ответственных за компьютерную безопасность, и членов группы обеспечения компьютерной безопасности.
- Описание процесса утверждения изменений (модификаций) в политике/процедурах обеспечения компьютерной безопасности.
- Процедуры и процесс выдачи разрешений на закупку нового оборудования для обработки информации.
- Учебная программа, политика и записи.

Подсказки для анализа документов и записей

- Каковы цели компьютерной безопасности?
- Где в организационной иерархии предусматривается выполнение обязанностей по обеспечению компьютерной безопасности?
- Какова структура группы компьютерной безопасности?
- Все функциональные домены входят в компетенцию лица, ответственного за компьютерную безопасность (ОКБ). Если в штате предусмотрен не одна должность ОКБ, должны быть четко установлены должностные обязанности, ответственность и порядок коммуникации. Необходимо наличие четко определенных линий взаимодействия между функциями и обязанностями.
- Предусматривается ли в процедурах модификации обеспечение компьютерной безопасности?
- Обеспечивается ли специальная подготовка для персонала, которому поручены функции обеспечения физической безопасности?
- Кто должен проходить подготовку, как часто проводилось обучение и какой процент персонала получил необходимую подготовку?

Примерные вопросы для собеседований

- Знаете ли вы своего ответственного за компьютерную безопасность и как контактировать с ним?
- Каковы базовые процедуры обеспечения компьютерной безопасности?
- Проводит ли группа компьютерной безопасности регулярные совещания? Составляются ли протоколы совещаний? Каков процесс уведомления группы компьютерной безопасности о событиях и инцидентах или изменениях, которые могут привести к компрометации безопасности?
- Каков процесс (т.е. инструменты или процедуры) защиты чувствительной информации?
- Какую подготовку по вопросам компьютерной безопасности получили сотрудники? Проводится ли эта подготовка на непрерывной основе?
- Был ли проведен анализ квалификации внутри организации с целью выявления пробелов в профессиональной подготовке? Как устранялись эти пробелы?

Вопросы для проведения обследований

— Получили ли специалисты по компьютерной безопасности соответствующую внешнюю подготовку по вопросам обеспечения компьютерной безопасности?

— Каким образом отслеживается выполнение задач по обеспечению компьютерной безопасности и принятие последующих мер (например, на основе рекомендаций в протоколах совещаний)?

— Назначено ли лицо, ответственное за проведение аудитов/оценок компьютерной безопасности? Включаются ли аудиты/оценки в ежегодное планирование?

Подсказки для анализа на местах

— Членам группы компьютерной безопасности рекомендуется участвовать в проведении оценки.

— Является ли компьютерная безопасность заметной на всех уровнях руководства и персонала?

5.4. МЕНЕДЖМЕНТ АКТИВОВ

Описание домена физической безопасности

Цель этого домена – защита активов организации. Сюда входит ответственность за менеджмент активов, ведение инвентарных списков санкционированных аппаратных средств и программного обеспечения, списка несанкционированных аппаратных средств и программного обеспечения, а также классификацию компьютеров (систем важных для безопасности и/или физической безопасности).

Все активы должны иметь определенного владельца, отвечающего за применение надлежащих средств контроля.

Требуемые документы и записи

— Политика и процедуры, в которых подробно описывается система менеджмента активов.

— Инвентарный список активов (компьютерных систем, сетевого оборудования, программного обеспечения, версий).

— Процедуры и критерии определения компьютеров, включенных в программу обеспечения компьютерной безопасности, если это применимо.

— Перечень/схема физического расположения активов, включенных в инвентарный список.

— Процедуры ведения инвентарного учета, включая периодичность и регистрацию обновлений инвентарных списков.

— Функциональная схема систем и связанных с ними компьютерных активов.

— Схема зональной модели (если это применимо).

— Политика и процедура классификации чувствительной информации.

Подсказки для анализа документов и записей

— Менеджмент активов должен охватывать полный жизненный цикл активов.

— Какое подразделение организации занималось составлением инвентарных списков?
— Кто ведет инвентарные списки?
— Кто имеет доступ к ним?
— Прослеживаемость изменений.
— Защита инвентарных списков (включая резервные копии).
— Как проводится классификации активов? Документируется ли она? Каково качество?
— Привязываются ли активы к определенной зоне и управляются ли они в соответствии с зональной моделью?
— Определены ли "уровни физической безопасности"? Каковы меры обеспечения физической безопасности, предусмотренные для каждого уровня?
— Привязаны ли уровни физической безопасности к конкретным зонам? На каком основании делается такая привязка?
— Соответствуют ли физическое расположение инвентарному списку?
— Насколько зональная модель соответствует физическому расположению системы (или ее части)?
— Как активы маркированы в соответствии с классификацией по функциональному домену?
— Как классификация транслируется в логические зоны (ср. дифференцированный подход)?
— Проверить, не подключено ли оборудование к более чем одной зоне.
— Были ли оценены меры физической защиты с точки зрения компьютерной безопасности?
— Какова зависимость мер физической защиты от компьютерных и/или сетевых систем?

Примерные вопросы для собеседований

— Каковы меры обеспечения физической безопасности для обследуемого уровня?
— Имеется ли у вас или можете ли вы получить доступ к инвентарному списку активов?
— Разрешается ли использование внешних или частных устройств, и если да, то при каких обстоятельствах? (Спросить о применяемых средствах контроля безопасности)
— Как решаются вопросы, связанные со сроком службы (как подбирается и содержится новое оборудование и каков процесс замены)?
— Как происходит обращение с оборудованием, принадлежащим третьим сторонам?

Вопросы для проведения обследований

— Проверить по схеме сети наличие конкретных устройств.
— Подключен ли этот компьютер к соответствующей сети?
— Правильно ли маркировано данное устройство в соответствии с действующей политикой?
— Применяются ли меры обеспечения физической безопасности в отношении данного актива?

— Проверить соответствие между инвентарным списком и установленным оборудованием на местах (например, на основе выборочной проверки).

— Проверить менеджмент версий, а также менеджмент конфигурации параметров.

— Как осуществляется менеджмент конфиденциальности активов и инвентарных списков?

— Откуда и как осуществляются администрирование и обслуживание подключенных к сети активов?

Подсказки для анализа на местах

— Соответствует ли физическое расположение инвентарному списку?

— Соответствует ли зональная модель физическому расположению системы (или ее части)?

— Как активы маркированы в соответствии с классификацией по функциональному домену?

— Как классификация транслируется в логические зоны или уровни физической безопасности (ср. дифференцированный подход)?

— Проверить, не подключено ли оборудование к более чем одной зоне.

5.5. БЕЗОПАСНОСТЬ ЛЮДСКИХ РЕСУРСОВ (ПЕРСОНАЛА)

Описание домена физической безопасности

Цель заключается в обеспечении того, чтобы персонал, подрядчики и пользователи, являющиеся третьими сторонами, т.е. все сотрудники, наделенные обязанностями в рамках организации, понимали свои функции и обязанности в отношении использования компьютеров и компьютерной безопасности. Обязанности по обеспечению безопасности должны быть определены еще до приема сотрудника на работу и изложены в условиях найма и доводиться до сведения сотрудника в течение всего его срока найма или действия его контракта.

Оценивание благонадежности сотрудников (также называемое проверкой персонала) рекомендуется проводить в случае каждого кандидата для приема на работу, подрядчика и пользователя, являющегося третьей стороной, на предмет соответствия уровню доступа к чувствительным данным и системам. Сотрудникам, подрядчикам и сторонним пользователям систем обработки информации также рекомендуется подписывать соглашение о возложении на них функций и обязанностей в области обеспечения безопасности и принимать участие в программах подготовки кадров, соответствующих их обязанностям. Это может быть отражено в соответствующих национальных законах, которые должны при этом учитываться.

Программа повышения осведомленности по вопросам обеспечения компьютерной безопасности – это непрерывный процесс, осуществляемый при поддержке руководства объекта.

Требуемые документы и записи

— Политика и процедуры, касающиеся использования компьютеров и безопасности, предназначенные для персонала, подрядчиков и субподрядчиков.

— Записи по менеджменту персонала, относящиеся к использованию компьютеров и безопасности.

— Какие меры принимаются для контроля соответствия между привилегиями (полномочиями) и статусом сотрудника (менеджмент права доступа согласно функции)?

— Политика и процедуры по подготовке персонала (подготовка ориентационная, по функциям, переподготовка).

— Документация по сертификации/аттестации и должностные требования сотрудников группы компьютерной безопасности.

Подсказки для анализа документов и записей

— Как часто персонал проходит подготовку по осведомленности в вопросах компьютерной безопасности?

— Какова процедура получения доступа к компьютерам, приложениям и данным?

— Каков процесс получения доступа к конфиденциальным данным и приложениям?

— Как оценивается эффективность культуры компьютерной безопасности?

— Публикуется ли справочник по персоналу в интернете? В каком формате, с какой информацией?

— Какова политика компании в отношении использования социальных сетей?

— Для какого персонала требуется проверка благонадежности?

— Каковы будут последствия, если кто-либо нарушает процедуры обеспечения безопасности?

— Являются ли санкции за нарушения достаточными и правильно ли они применяются? Поощряется ли надлежащим образом "хорошее поведение"?

— Применяется ли "Уведомление о соглашении об использовании" или "Политика допустимого использования технологии"? Они могут быть в виде заставки на экране компьютера, появляющейся при входе в аккаунт (учетную запись).

— Используется ли на компьютерах в соответствующих случаях защищенная паролем экранная заставка (скринсейвер)? Каково время задержки при ее включении?

Примерные вопросы для собеседований

— Как часто персонал проходит подготовку по осведомленности в вопросах компьютерной безопасности?

— Какова процедура получения доступа к компьютерам, приложениям и данным?

— Каков процесс получения доступа к конфиденциальным данным и приложениям?

— Каким является процесс представления рапорта о потенциальном инциденте в области компьютерной безопасности?

— Как поощряется сообщение сотрудниками по собственной инициативе информации о потенциальных инцидентах в области компьютерной безопасности?

— Каковы будут последствия, если кто-либо нарушает процедуры обеспечения безопасности?

Вопросы для проведения обследований

— Проверить соглашение о доступе к компьютерам/политику пользователей компьютеров.

— Проверить сертификаты/документацию по регистрации обучения по вопросам компьютерной безопасности.

— Проверить состояние аккаунтов (учетных записей) согласно должностям методом случайной выборки сотрудников/подрядчиков (например, проверить наличие официальных разрешений у сотрудников, охваченных системой безопасности).

— Проверить состояние аккаунтов (учетных записей) сотрудников, недавно уволенных из организации.

— Являются ли санкции за нарушения достаточными и правильно ли они применяются? Поощряется ли надлежащим образом "хорошее поведение"?

— Появляется ли на компьютерах заставка "Уведомление о соглашении об использовании" или "Политика допустимого использования технологии" при входе в компьютерную систему?

— Используется ли на компьютерах в соответствующих случаях защищенная паролем экранная заставка (скринсейвер)? Каково время задержки при ее включении?

Подсказки для анализа на местах

— Может ли один человек или несколько лиц создавать риск единой точки отказа в процессе?

— Как осуществляется менеджмент прав доступа переведенных на другую работу или уволенных лиц?

— Как организация содействует формированию активной культуры компьютерной безопасности в компании? Распространяется ли она на поведение вне рабочей среды, например, на использование социальных сетей?

5.6. ФИЗИЧЕСКАЯ ЗАЩИТА

Описание домена систем

Цель этого домена заключается в обеспечении физической защиты компьютерных активов. Она предназначена для предотвращения несанкционированного физического доступа к системам, саботаж (диверсия) в отношении которых может привести к нарушению или блокированию услуг или потока информации. Контроль предотвращения и физической безопасности должен основываться на оценке риска и реализовываться в соответствии с дифференцированным подходом. Должное внимание необходимо уделять минимизации инсайдерской угрозы (угрозы, исходящей от внутреннего нарушителя).

В случае СКУ осуществление физического контроля часто является единственным способом обеспечения контроля доступа; средства технического контроля могут вообще отсутствовать или они могут быть неприменимыми для этих систем.

Требуемые документы и записи

— Политика/план обеспечения физической безопасности (или защиты) установки.

— Политика/план обеспечения компьютерной безопасности.

— Функциональная схема систем и связанных с ними компьютерных активов.

— Схема физического расположения установок.

— Перечень/схема физического расположения активов, включенных в инвентарный список.
— Схема/перечень физических средств контроля.
— Схемы разводки кабелей/проводов физической сети.
— Процедуры для соответствующих процессов контроля физического доступа и менеджмента списков доступа.
— Журналы контроля физического доступа в помещения и к оборудованию.
— Организационные схемы и описания должностей.

Подсказки для анализа документов и записей

— Согласованность между средствами технического контроля, административного контроля и физического контроля.
— Соответствие между чувствительностью функции и физической защитой соответствующих систем/компонентов.
— Надлежащая компьютерная безопасность систем, обеспечивающих физическую защиту.
— Надлежащая компьютерная безопасность систем, ответственных за контроль среды.
— Проверка надлежащего физического разделения сетей/компонентов/ оборудования с различными уровнями физической безопасности.
— Определены ли характеристики угрозы и являются ли реализованные средства контроля адекватными?
— Определить ограничения доступа, основанные исключительно на процедурах (т.е. средствах административного контроля).

Примерные вопросы для собеседований

— Каковы обозначенные контролируемые/чувствительные зоны?
— Описать технические и процедурные механизмы контроля доступа, применяемые для каждой контролируемой/чувствительной зоны.
— Адекватны ли меры физической защиты, применяемые для рассматриваемых компьютерных систем?
— Каковы предполагаемые физические угрозы в организации (в том числе с учетом ресурсов и мотивов и включая инсайдерскую угрозу)?
— Какова политика предоставления доступа или обеспечения сопровождения для третьих сторон, работающих в контролируемых зонах?
— Какова политика, применяемая в отношении использования портативных носителей и наладонных электронных устройств в контролируемых зонах?
— Каким является процесс утилизации вышедшего из строя или замененного компьютерного оборудования?
— Каков процесс уничтожения электронных носителей?
— Какова процедура выноса компьютерного оборудования и носителей с объекта (например, процедура выноса ноутбука для работы дома)?

— Какова процедура использования стороннего (т.е. не принадлежащего объекту) оборудования для работы на объекте, такого как ноутбук, флеш-накопитель и т.п.?

— Каковы средства физического и административного контроля, связанные с защитой компьютерной среды?

Вопросы для проведения обследований

— Провести обследование средств и процедур обеспечения контроля доступа в действии.

— Проверить, чтобы число сотрудников, имеющих разрешение на физический доступ, было сведено к минимуму. Должен вестись и предоставляться сотрудникам службы безопасности список контроля доступа, в котором указаны лица, имеющие право доступа.

— Провести обследование защиты кабелей и проводки, шкафов, стоек, коммутационных панелей и как кабели связаны друг с другом. Следует иметь в виду, что сетевое оборудование может быть размещено в многоцелевых зонах, а не только в серверных помещениях. Находится ли оборудование в защищенной зоне? Кто имеет доступ?

— Какие устройства применяется для обеспечения физической безопасности оборудования, например, устройства для обнаружения вмешательства, устройства физической блокировки, сигнализации, видеонаблюдения и т.п.?

— Провести обследование применения процедурных мер защиты (пропуска-карточки, сопровождение, разметка, которую нельзя переступать, обеспечение соблюдения правила двух человек и т.п.).

— Провести обследование использования личных ИТ-устройств, таких как смарт-телефоны, ноутбуки, планшетные компьютеры, портативные носители и т.п.

— Провести обследование размещения компьютерных терминалов: обеспечивает ли их расположение предотвращение несанкционированного просмотра экранов и клавиатур?

— Остаются ли компьютерные носители на столе без присмотра?

— Какие меры обеспечения физической безопасности применяются во вспомогательной инфраструктуре, предназначенной для компьютерной инфраструктуры (т.е. средства контроля физической безопасности для систем вентиляции и охлаждения, основного и резервного питания и т.п.)?

— Как маркируются, инвентаризируются и отслеживаются отдельные единицы оборудования?

Подсказки для анализа на местах

— Провести анализ средств физического контроля и административного контроля в совокупности.

— Рассмотреть инсайдерскую угрозу и что может быть сделано в отношении физического доступа к компьютерным ресурсам.

— Провести обследование по вопросу об использовании на работе личных компьютерных устройств, таких как смарт-телефоны, ноутбуки, планшетные компьютеры, портативные носители и т.п.

— Провести проверку согласованности между логическим и физическим контролем доступа.
— Проверить, охвачен ли физический доступ к (отдельным) СКУ предупредительной сигнализацией. Куда передается предупредительный сигнал? Каковы нормальные действия в случае предупредительного сигнала?

5.7. МЕНЕДЖМЕНТ КОММУНИКАЦИИ И КОМПЬЮТЕРНЫХ ОПЕРАЦИЙ

Описание домена физической безопасности

Основная цель этого домена физической безопасности – обеспечить контроль эксфильтрации и инфильтрации данных в компьютерных системах в рамках программы обеспечения компьютерной безопасности в целях защиты от ввода новых уязвимостей и контроля операционных процедур, обеспечивающие работу и защитные функции систем в штатном режиме. Еще одна цель заключается в том, чтобы обеспечить защиту целостности компьютеров и коммуникации.

Требуемые документы и записи

— Схемы потоков данных для выявления взаимосвязей между сетями и потоками данных.
— Политика и процедура для менеджмента конфигурации.
— Схема архитектуры сети.
— Политика и процедура для переконфигурации компьютеров/сетей.
— Политика и процедура для усиления защиты компьютерных систем.
— Политика и процедура для носителей: доступ к носителям, их маркировка, хранение, транспортировка и обезличивание.
— Политика и процедуры верификации и валидации средств контроля физической безопасности на компьютерах и в сетях в рамках программ обеспечения компьютерной безопасности.
— Документация по квалификации/сертификации лиц, проводящих верификацию и валидацию.
— Политика и процедура внешнего распространения/публикации информации (например, на корпоративном сайте).
— Политика и процедура обращения с общедоступной информацией.
— Политика и процедура менеджмента предоставления услуг третьими сторонами для всех классов компьютеров и сетей в рамках программы обеспечения компьютерной безопасности.
— Соглашения с третьими сторонами о сетях на установке, к которым может иметь доступ третья сторона, и о решениях по обеспечению безопасности для третьих сторон.
— Политика и процедура работы с подрядчиками, являющимися третьими сторонами.
— Политика и процедура постоянного мониторинга и оценки программы обеспечения компьютерной безопасности.

— Политика и процедура цифрового обмена информацией на объекте и с внешними объектами.

— Политика, процедура изъятий из программы обеспечения компьютерной безопасности, включая документацию по ним.

— Политика и процедура использования беспроводных устройств, мобильных устройств или съемных носителей.

— Политика и процедура введения ограничений на использование и применение беспроводных технологий.

— Политика и процедура проведения сканирования несанкционированных беспроводных подключений и точек беспроводного доступа.

— Политика и процедура действий в случае обнаружения несанкционированных беспроводных подключений или точек доступа.

— Политика и процедура использования портативных компьютерных устройств, включая мобильные телефоны.

— Политика и процедура постоянного мониторинга и оценки небезопасных и неавторизованных сетевых подключений.

— Политика и процедура применения и описание методов, используемых для обнаружения несанкционированного использования систем или сетей или доступ к ним.

— Полезным также может быть проведение поиска по открытым источникам информации с целью оценки общедоступной информации об объекте или организации, которая потенциально может представлять риск для компьютерной безопасности.

Подсказки для анализа документов и записей

— Провести анализ утвержденных процедур, выполняемых операционным и обслуживающим персоналом, на предмет определения внутренне присущей безопасности и согласованности с политикой и планом обеспечения физической безопасности.

— Применяются ли процедуры обеспечения безопасности к различным режимам работы установки с целью решения разных проблем, связанных с ними?

— Охватывают ли рассматриваемые процедуры обеспечения безопасности проблемы, от которых они должны обеспечивать защиту?

— Проведен ли на принимающей установке эффективный анализ для обеспечения того, чтобы эти средства контроля безопасности действовали и обеспечивали защиту так, как они должны делать это?

— Проведена ли на принимающей установке оценка воздействия успешного вывода из строя средств контроля безопасности в пределах домена менеджмента коммуникации и операций?

— Проведена ли на принимающей установке оценка воздействия успешного вывода из строя средств контроля безопасности, связанных с удаленной деятельностью или деятельностью третьих сторон (включая обслуживание)?

— Проведено ли конфигурирование компьютеров на принимающей установке с целью устранения известных на данный момент уязвимостей?

— Применяется ли концепция "наименьших привилегий"?

— Применяется ли на принимающей установке анализ безопасности и программа тестирования (включая анализ уязвимости, тестирование на проникновение или другие средства) для выявления потенциальных известных и неизвестных уязвимостей? Каковы масштабы программы тестирования?

— Существуют ли требования в отношении применения подрядчиками и субподрядчиками политики обеспечения компьютерной безопасности?

Примерные вопросы для собеседований

— Какова процедура выноса компьютерного оборудования и носителей с объекта (например, процедура выноса ноутбука для работы дома)?

— Какова процедура использования стороннего (т.е. не принадлежащего объекту) оборудования в работе на объекте, такого как ноутбук, флеш-накопитель и т.п.?

Вопросы для проведения обследований

— Убедиться в том, что компьютеры на установке отконфигурированы для поддержки принципа наименьших привилегий и применяется процесс анализа и смягчения известных в настоящее время уязвимостей.

— Провести обследование выполнения процедур.

— Проверить наличие признаков внешних структур или подключений (например, для резервирования или мониторинга).

— Провести выборочные проверки на наличие ноутбуков/мобильных устройств и уточнить данные об их использовании.

— Провести проверку соответствия между зарегистрированными в документации системами, приложениями, сетевой архитектурой и т.п. и фактическим положением дел.

Подсказки для анализа на местах

— Выяснить, является ли анализ рисков достаточно полным для выявления рисков, связанных с сетевыми коммуникациями и мобильными устройствами.

— Рассмотреть вопрос: что является самой большой остающейся проблемой?

5.8. КОНТРОЛЬ ДОСТУПА К КОМПЬЮТЕРАМ

Описание домена физической безопасности

Целью является контроль логического доступа (средствами технического и административного контроля) к компьютерным системам или электронной информации.

Этот домен включает требования по контролю доступа, менеджменту доступа пользователей, обязанностям пользователей, контролю доступа к сети, контролю доступа к операционным системам, контролю доступа к приложениям и информации и мобильным компьютерным устройствам и методам телеработы.

Доступ к компьютерным системам (СКУ, контрольным системам, техническим системам, системам обеспечения физической безопасности и бизнес-системам) контролируется на основе плана обеспечения компьютерной безопасности.

Правила логического контроля доступа к компьютерам и сетям устанавливаются посредством процесса выдачи официальных разрешений.

Требуемые документы и записи

- План обеспечения компьютерной безопасности.
- Политика и процедура контроля доступа к компьютерам (менеджмент прав, менеджмент аккаунтов).
- Документация, содержащая результаты аудитов контроля доступа.
- Политика и процедура пересмотра авторизации доступа к системам, включая привилегии.
- Организационная структура для менеджмента прав администратора компьютеров.
- Политика и процедуры использования паролей (сложность, длина и политика блокировки аккаунтов).
- Политика и процедура, касающиеся порядка предоставления и документирования привилегий.
- Описание применяемых механизмов аутентификации.
- Документация по регистрации и мониторингу контроля доступа.
- Политика и процедура авторизации и учета аккаунтов.
- Политика доступа к сети – средства контроля безопасности коммутаторов, не подсоединенные гнезда и т.п.
- Политики доступа к сети – использование виртуальных локальных сетей.
- Топология сетей и трафика.
- Политика, касающаяся шлюза безопасности – списки контроля доступа к маршрутизаторам, правила брандмауэра.
- Схема/список точек беспроводного доступа.
- Политика и процедура предоставления удаленного доступа (кому, когда, зачем, какие сервисы).
- Политика и процедура использования и обеспечения физической безопасности модемов.
- Политика и процедура открытия аккаунтов с правами администратора/высоким уровнем привилегий.

Подсказки для анализа документов и записей

- В случаях, когда необходимые меры технического контроля доступа (например, пароли) не могут быть реализованы в рамках некоторых компонентов СКУ по причинам технического или операционного характера, проверить, чтобы применялись корректирующие меры (например, адаптированные процедуры, меры по повышению физической безопасности, безопасности персонала, обнаружению проникновения и аудиту) в соответствии с уровнем физической безопасности для СКУ.
- Проверить согласованность между средствами технического контроля, административного контроля и физического контроля.
- В отношении СКУ уделить особое внимание методам и случаям удаленного доступа, когда были применены беспроводные и мобильные технологии.

— В отношении беспроводных технологий выяснить, существует ли политика по использованию доступа и имеется ли программа оценки для обеспечения соблюдения этой политики?

— Проверить применение принципов "разделения обязанностей" и "наименьших привилегий" в техническом или административном плане. В частности, в случае СКУ и важных старых систем проверить наличие корректирующих мер, если они не применяются.

Примерные вопросы для собеседований

— К каким системам имеет доступ персонал, выполняющий конкретные должностные функции?

— К каким из этих систем осуществляется удаленный доступ? С какой частотой? Почему к этим системам осуществляется удаленный доступ?

— Проверить, практикуется ли делегирование или предоставление прав доступа вне установленной процедуры.

— Какое существует мнение в отношении политики контроля доступа: слишком строгая, слишком слабая и т.д.? Соответствует ли она операционным потребностям?

— Определить регулярно возникающие вопросы/проблемы, касающиеся контроля доступа, которые не решаются должным образом (т.е. в отношении которых применяются временные решения).

— Каким является процесс предоставления/получения доступа к компьютеру? Какие применяются процессы для аннулирования и возобновления?

— Выяснить, не практикуется ли обход средств контроля доступа для повышения операционной эффективности (или удобства) в некоторых случаях.

— Какие инциденты или даже анекдотические случаи зафиксированы в прошлом в связи с контролем доступа?

— Имеет ли администратор две учетные записи (администратора/пользователя)?

— Как в организации регистрируются кадровые изменения, касающиеся персонала (например, смена подразделения, изменение обязанностей и т.п.)?

Вопросы для проведения обследований

— Попросить продемонстрировать средства и процедуры обеспечения контроля доступа.

— Проверить, практикуется ли делегирование или предоставление прав доступа вне установленной процедуры.

— Проверить списки логического контроля доступа, с тем чтобы обеспечить уменьшение числа лиц с правом доступа до минимума.

— Проверить доступ через модемы и точки беспроводного доступа.

— Провести мониторинг активности беспроводной сети.

— Проверить доступные порты подключения.

— Выяснить существование возможных точек подключения для пассивного мониторинга.

— Проверить наличие не заблокированных систем и рабочих станций.

— Проверить наличие систем, не защищенных паролем, с дефолтными (созданными по умолчанию) аккаунтами (учетными записями) или с очевидным паролем.

— Проверить наличие баннеров, информирующих пользователей о санкционированных видах использования.

— Проверить, как обеспечивается сетевое разделение (логически, физически, отключением от сети).

— Проверить сетевую архитектуру и особенно интерфейсы между доменами физической безопасности.

— Выяснить наличие возможных путей компрометации критических систем (безопасности, контроля) через бизнес- или корпоративные сети или иными способами.

— Определить регулярно возникающие вопросы/проблемы, касающиеся контроля доступа, которые не решаются должным образом (применяются временные решения).

— Проверить наличие механизмов аутентификации без документирования.

— Проверить процедуры входа в систему; существует ли механизм аутентификации открытого текста?

— Практикуется ли совместное использование сотрудниками аккаунтов (учетных записей) и паролей; используются ли групповые аккаунты (учетные записи)?

— Запросить график работ, намеченных для выполнения во время оценки, и выбрать некоторые работы для обследования, например внесение исправлений (патчей), параметризация, установка программного обеспечения и т.п.

Подсказки для анализа на местах

— Сколько различных паролей сотруднику необходимо использовать в повседневных операциях? В ходе специальных операций? (Использование слишком большого числа паролей может привести к применению стикеров-напоминалок и т.п.)

— Практикует ли персонал выход из системы/блокировку аккаунта (учетной записи) при оставлении своего компьютера, если это применимо?

— Как обеспечивается отслеживаемость в случае использования групповых/общих аккаунтов (учетных записей)?

— Как обеспечивается сложность пароля?

— Какова согласованность между средствами логического и физического контроля доступа?

5.9. ПРИОБРЕТЕНИЕ, РАЗВИТИЕ И ОБСЛУЖИВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ

Описание домена физической безопасности

Цель этого домена физической безопасности заключается в обеспечении безопасности и целостности приобретаемых компьютерных систем и работ по обслуживанию, выполняемых поставщиком после вводы системы в эксплуатацию. Средства контроля физической безопасности, входящие в этот домен физической безопасности, включают защиту цепи поставок, обеспечение правильности программного обеспечения, интеграцию потенциала обеспечения безопасности, производственные испытания и приемочное тестирование.

Особое внимание необходимо уделить работам по обслуживанию компьютерных систем. Такие работы необходимо оценивать, с тем чтобы убедиться в том, что предусмотрены достаточные средства контроля для защиты от уязвимостей или вредоносных программ. Кроме того, рекомендуется проводить оценку мер по обслуживанию в целях обеспечения компьютерной безопасности, таких как патч-менеджмент, на предмет их своевременности и эффективности.

Требуемые документы и записи

- Политика и процедура для приобретения систем и услуг, включая разработку требований безопасности к приобретенным или разработанным системам.
- Описание требований, предусматривающих принятие мер по обеспечению безопасности для защиты от внесения уязвимостей и угроз через цепи поставок.
- Описание требований, предъявляемых к поставщикам в отношении применения методов проверки качества и валидации программного обеспечения с целью сведения к минимуму появления дефектного или некорректного программного обеспечения.
- Описание или подтверждение того, как на установке обеспечивается наличие в случае вновь приобретенных систем достаточной проектной информации по безопасности, а также способности выполнять и поддерживать функции средств контроля безопасности.
- Описание или подтверждение наличия требований по физической безопасности, касающихся разработки, реализации и документирования тестов на безопасность и планов оценивания безопасности с целью обеспечения соответствия приобретенных изделий всем установленным требованиям по физической безопасности.
- Описание и подтверждение наличия требования безопасности, касающегося поддержания целостности приобретенной системы до момента поставки изделия на объект. Описание того, как на установке проводится верификация и проверка того, что программа обеспечения безопасности, реализованная до поставки, обеспечивает по меньшей мере тот же уровень безопасности, что и программа, применяемая к компьютерной системе, находящейся в эксплуатации.
- План и результаты тестирования для верификации и валидации кода на предмет соответствия требованиям проектирования и конфигурирования с учетом обеспечения безопасности.
- Процедуры приемочных испытаний компьютерного/электронного оборудования.
- Документ с изложением требований по реализации и поддержанию мер по обеспечению компьютерной безопасности.
- План проведения валидационного тестирования и результаты оценки эффективности реализованных мер по обеспечению компьютерной безопасности.
- Структура и методология компьютерной безопасности с описанием проектных средств обеспечения безопасности, предусмотренных для удовлетворения требований безопасности, установленных для компьютеров.
- Документация по проведению обслуживания компьютерных систем.
- Графики проведения обслуживания, отражающие приоритизированные работы, связанные с обеспечением компьютерной безопасности.

Подсказки для анализа документов и записей

— Проверить, чтобы компьютерная безопасность надлежащим образом обеспечивалась третьими сторонами.

— Проверить обеспечение безопасности в цепи приобретения и развития с учетом возможного наличия многих подрядчиков, субподрядчиков и т.д.

Примерные вопросы для собеседований

— Какие средства контроля применяются на объекте на оборудовании до и во время его монтажа?

— Какое тестирование выполняется на предприятии поставщика и после монтажа для оценивания функций безопасности?

— Какие средства контроля применяются для того, чтобы исключить внесение компьютерных уязвимостей или инструментов эксплуатации уязвимости, таких как вредоносные программы, в систему во время работ по обслуживанию?

— Каким образом контролируются работы по обслуживанию, выполняемые третьими сторонами на объекте?

— Документация по подтверждению проведения инспекций физической безопасности на предприятии поставщика и по обеспечению соблюдения требований безопасности.

Вопросы для проведения обследований

— Какие средства контроля применяются на объекте на оборудовании до и во время его монтажа?

— Как осуществляется передача чувствительной информации между поставщиком и установкой?

Примечание. Это трудно поддается обследованию на объекте, так как относится главным образом к третьим сторонам и происходит до поставки систем на объект.

Подсказки для анализа на местах

— Провести обследование работ по поддержанию компьютерной безопасности, выполняемых внутренним персоналом или сторонними подрядчиками.

5.10. МЕНЕДЖМЕНТ ИНЦИДЕНТОВ, СВЯЗАННЫХ С КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТЬЮ

Описание домена физической безопасности

Несмотря на все усилия, предпринимаемые организацией, инциденты, связанные с компьютерной безопасностью, могут иметь место. Цель этого домена физической безопасности заключается в обеспечении применения процессов для эффективной минимизации потенциальных последствий и эффективной коммуникации в случае инцидентов, связанных с компьютерной безопасностью.

Согласно публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 17 [3], инцидент, связанный с компьютерной безопасностью, – это событие, в случае которого фактически или потенциально подвергаются опасности конфиденциальность, целостность или доступность компьютерных, сетевых или цифровых информационных

систем или доступность информации, которую система обрабатывает, хранит или передает, или которое представляет собой нарушение или создает неизбежный риск нарушения политики безопасности, процедур безопасности или приемлемых правил пользования.

Требуемые документы и записи

- Политика и процедура для менеджмента инцидентов.
- План коммуникации в случае инцидентов.
- Обращения в службу ИТ-поддержки (зарегистрированные заявки).
- Подтверждение проведения оценок незапланированных отключений установки или систем (оценок корневых причин).
- Образцы или шаблоны отчетов об инцидентах (предпочтительным является фактический отчет).
- Процедура/вопросы, касающиеся перекрестного воздействия в рамках различных доменов мер реагирования на инцидент (например, действия, предпринимаемые в отношении ИТ-системы для бизнес-процессов после инцидента, связанного с безопасностью, могут быть неприемлемыми в условиях среды СКУ).
- План и процедуры реагирования на инциденты.
- Документация и последующие действия по результатам проведения тренировок с целью оценки эффективности плана реагирования на инциденты.

Подсказки для анализа документов и записей

- Учитываются ли в должной мере в менеджменте инцидентов, связанных с компьютерной безопасностью, внешние и внутренние (т.е. инсайдерские) угрозы?
- Имеется ли четкая классификация для характеризации инцидентов?
- Имеется ли четкое определение процедуры иерархической эскалации (критерии, контактные лица)?
- Процесс коммуникации предусматривает внутреннюю коммуникацию (в том числе с лицами, отвечающими за общий менеджмент инцидентов на установке) и внешнюю коммуникацию (с группами быстрого реагирования на нарушения компьютерной безопасности (ГБРКБ), национальными и международными органами).
- Были ли разработаны и адаптированы процедуры по криминалистической экспертизе, сохранению следов и т.п. для поддержки процесса расследования?
- Оценить процесс восстановления, а также определение и применение корректирующих мер.
- Проверить согласованность между менеджментом инцидентов и менеджментом непрерывности.
- Проверить связь между менеджментом инцидентов, связанных с компьютерной безопасностью, и общим менеджментом инцидентов на установке.
- Проводились ли на установке тренировки по исполнению планов и процедур реагирования в рамках самооценки (т.е. теоретические или имитационные тренировки)?

— Участвовала ли установка в каких-либо координированных тренировках по отработке действий в случае инцидентов, связанных с компьютерной безопасностью, с участием внешних организаций?

— Включены ли требования по сохранению доказательств и обеспечению цепи сохранности в план и процедуры реагирования на инциденты, связанные с компьютерной безопасностью?

Примерные вопросы для собеседований

— Провести проверку знания процедуры и, в частности, координат контактных лиц у работников и подрядчиков на случай возникновении инцидента, связанного с безопасностью.

— Описать, что можно считать инцидентом, связанным с безопасностью. Как классифицируются инциденты, связанные с безопасностью?

— Когда и при каких обстоятельствах следует сообщать об инциденте? Кому за пределами объекта направляется сообщение об инциденте?

— Какую процедуру следует применять в случае обнаружения работником или подрядчиком отклонения в функционировании средств контроля безопасности?

— Были ли на объекте какие-либо инциденты, связанные с безопасностью (компьютерной)?

— Может ли быть описано, что было сделано или изменено после недавнего инцидента, связанного с компьютерной безопасностью?

— Считаются ли применяемые процессы эффективными? Какие, если таковые имеются, проблемы по-прежнему остаются?

— Каким образом и как часто проводятся тренировки по отработке планов и процедур реагирования?

— Участвовал ли объект в каких-либо координированных тренировках по отработке действий в случае инцидентов, связанных с компьютерной безопасностью, на уровне установки, государства или на международном уровне?

Вопросы для проведения обследований

— Попросить провести демонстрацию работы конкретной управляющей системы отслеживания инцидентов (на бумажном носителе или в виде программного приложения).

Подсказки для анализа на местах

— Оценить достаточность подготовки персонала по применению процедуры.

5.11. МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ ФУНКЦИОНИРОВАНИЯ

Описание домена физической безопасности

Общей целью этого домена физической безопасности является обеспечение непрерывности и восстановления критически важных функций установки после серьезных сбоев в работе обычных компьютерных систем и процессах. Это включает в себя сбои, вызванные опасными природными явлениями, человеческими ошибками и действиями со злым умыслом.

Следует иметь в виду, что раздел по менеджменту инцидентов, связанных с компьютерной безопасностью, касается первоначального реагирования и минимизации последствий инцидента, тогда как в рамках данного домена основное внимание уделяется вопросам обеспечения непрерывности и процессам восстановления.

Требуемые документы и записи

- Политика и процедуры для менеджмента непрерывности.
- Список приложений и систем, которые охвачены менеджментом непрерывности, и перечень их владельцев/обязанностей.
- Записи, фиксирующие подготовку по вопросам обеспечения непрерывности операций (включая отчеты о тренировочных мероприятиях).
- План по обеспечению непрерывности операций.

Подсказки для анализа документов и записей

- Проверить, как менеджмент непрерывности функционирования в отношении компьютерной безопасности интегрирован в существующие программы обеспечения непрерывности операций (например, с помощью плана обеспечения непрерывности операций на объекте).
- Следует иметь в виду, что требования менеджмента непрерывности учитываются в базовом проекте и технических спецификациях систем безопасности и операционных систем СКУ. Рекомендуется, чтобы эти спецификации принимались во внимание при оценивании менеджмента непрерывности для систем безопасности и операционных систем СКУ. Это может быть не так в случае других функциональных доменов. Для СКУ, выполняющих важные функции обеспечения безопасности или физической безопасности, средняя наработка на отказ и средняя наработка до ремонта являются двумя ключевыми проектными характеристиками, которые необходимо учитывать при определении действия по менеджменту непрерывности.
- Определены ли важные подсистемы и взаимозависимости? Достаточны ли контрактные соглашения для достижения целей обеспечения непрерывности?
- Для важных систем и функций предусматривается соответствующий уровень диверсификации и резервирования.
- Учитывается ли надлежащим образом фактор злоумышленных действий (соотношение умышленной атаки к случайному отказу) в менеджменте непрерывности?
- Проверить согласованность между менеджментом инцидентов и менеджментом непрерывности.

Примерные вопросы для собеседований

- Проверить, известны ли, проверены и проанализированы ли планы тестирования непрерывности функционирования и восстановления компьютерных систем, а также процедуры восстановления (например, восстановления и актуализации данных в период между выключением и перезапуском).
- Получили ли сотрудники подготовку по восстановлению систем и менеджменту непрерывности функционирования? Кто прошел обучение? Как в менеджменте непрерывности учитывается приоритетность доступа и ресурсов в период операционной деградации?

— Проводили ли на установке тренировочные мероприятия, направленные на отработку действий по восстановлению систем и менеджменту непрерывности функционирования в случае киберсобытия?

— Имеются ли резервные системы для управления важными компьютерными функциями в случае инцидента/аварии?

— Какие средства контроля физической безопасности применяются в отношении резервных систем?

— Какова архитектурная связь с резервными системами?

— Существуют ли процедуры для продолжения работы после потери компьютерных функций?

Вопросы для проведения обследований

— Проверить, имеют ли сотрудники доступ к соответствующим процедурам обеспечения непрерывности функционирования.

— В оценке для анализа может быть выбрана совокупность средств контроля менеджмента непрерывности, например процедур резервирования и восстановления, средств альтернативной коммуникации (в частности, при реагировании на чрезвычайные ситуации) и соглашений с подрядчиками о приоритетности.

— Запросить последний отчет о тренировках.

— Провести обследование альтернативных и резервных средств контроля, если таковые имеются.

Подсказки для анализа на местах

— Провести обследование выполнения процедуры восстановления, либо в рамках системы, в лаборатории разработок, либо с помощью "бумажного" процесса.

— Является ли информация о конфигурации установки актуализированной? С помощью какого механизма/процесса?

— Провести оценку значения приоритетности доступа и ресурсов во время ухудшения функционирования применительно к общим целям на объекте.

5.12. ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

Описание домена физической безопасности

Если оценка проводится компетентным органом или это самооценка, обеспечение соблюдения соответствующих правовых, установленных законом, нормативных или договорных обязательств, связанных с обеспечением компьютерной безопасности, может быть предметом рассмотрения в рамках оценки.

Цель этого домена физической безопасности заключается в проверке того, что программа обеспечения компьютерной безопасности согласуется с этими соответствующими правовыми, установленными законом, нормативными или договорными обязательствами.

Следует иметь в виду, что этот домен может не применяться в некоторых контекстах; вопрос о его применении можно рассматривать при планировании масштабов оценки.

Требуемые документы и записи

- Документы по правовым, установленным законом, нормативным или договорным обязательствам, которые имеют отношение к вопросам обеспечения компьютерной безопасности.
- Отчеты по обеспечению соблюдения регулирующих требований (внутренние или внешних организаций).
- Процедуры/процесс сертификации, если они применяются в отношении компьютерной безопасности.
- Описание компонента компьютерной безопасности в проектной угрозе.
- Руководящие документы по конструкции и модификациям систем (разделы, которые касаются ограничений в обеспечении соблюдения требований).

Подсказки для анализа документов и записей

- Каждый функциональный домен может иметь разные критерии и ограничения, касающиеся обеспечении соблюдения требований.
- Кроме того, в зависимости от страны и типа объектов, могут одновременно применяться несколько систем регулирующих требований, подлежащих соблюдению, которые вводятся в действие на уровне разных государственных учреждений (например, регулирующим орган по вопросам безопасности и учреждением, занимающимся вопросами физической безопасности).
- Вопросы обеспечения компьютерной безопасности могут быть отражены в документах с более широкой сферой применения; например, это могут быть специальные разделы, посвященные вопросам компьютерной безопасности, в действующих стандартах или нормах безопасности.
- Как правовые и регулирующие требования интегрированы в политику обеспечения физической безопасности, организацию и процедуры?
- Имеются ли в политике обеспечения физической безопасности четкие ссылки на соответствующие документы или их перечни?
- Обычно для СКУ предусматриваются специальные руководящие документы по конструкции и модификациям, однако группа оценки может проводить анализ этих аспектов применительно к другим доменам (например, системам, связанным с учетом ядерного материала, реагированием на чрезвычайные ситуации).

Примерные вопросы для собеседований

- Как определяется применение, проводится отслеживание применения и осуществляется выполнение регулирующих требований?
- Кто отвечает за выполнение таких задач (определение, отслеживание и выполнение)?
- Получить объяснение, как проводится валидация модификаций на местах на предмет определения их влияния на соблюдение правовых, установленных законом, нормативных и договорных обязательств.

Вопросы для проведения обследований

— В оценке для валидации выполнения на местах может быть выбрана совокупность требований компьютерной безопасности, вытекающих из правовых, законодательных, нормативных и договорных обязательств.

Подсказки для анализа на местах

— Начинать следует с небольшой репрезентативной выборки; если будет выявлено несколько несоответствий; выборка может быть исследована вновь с изучением дополнительных элементов.

6. ИТОГОВЫЙ ОТЧЕТ И ДЕЯТЕЛЬНОСТЬ ПОСЛЕ ОЦЕНКИ

6.1. ПОДГОТОВКА ИТОГОВОГО ОТЧЕТА

Одним из наиболее важных аспектов оценки является обсуждение результатов обследований, определение выводов, рекомендаций и предложений, представляемых принимающей организации. Эта информация отражается в итоговом отчете и сообщается представителям принимающей установки или организации на заключительном информационном совещании.

Формат и содержание отчета может изменяться в зависимости от целей оценки, но он должен содержать определенные последовательные разделы, такие как резюме, введение, результаты и выводы. В приложении III приводится примерный план отчета об оценке. На рис. 3 представлен процесс подготовки и составления отчета.

РИС. 3. Анализ в процессе оценки

Компонент сбора данных в оценке состоит из регистрации представляющих интерес данных обследований, полученных на этапах анализа документов/записей, собеседований и прямых обследований. Результаты обследований сами по себе являются значимыми, но они могут также выступать в роли коллективного индикатора тенденций на уровне объекта или организации, в отношении которых может требоваться принятие мер. В ходе анализа заметок, сделанных на местах, аналогичные результаты обследований могут быть объединены в группы для иллюстрации тенденций или повторяющихся случаев.

Результаты обследований затем анализируются на предмет соблюдения требований, содержащихся в таких документах, как национальные регулирующие положения, применяемые в организации процедуры и/или международные стандарты (нормы) в

соответствующих случаях. В случае выявления несоответствий или отклонений от соблюдения регулирующих положений или внутренней процедуры составляется вывод. Базис для составления вывода должен быть четко определен и согласован на предварительных совещаниях по планированию.

Важно также понимать, что перечень выводов представляет собой общее отражение состояния объекта, полученное на основании ряда обследований, проведенных группой оценки. При анализе результатов обследований и составлении выводов необходимо принимать во внимание несколько факторов, включая:

- глубину и широту оценки;
- компетенцию и опыт группы оценки;
- уровень доступа, предоставленного группе оценки;
- уровень ресурсов, обеспеченных для оценки, например, время и количество экспертов по оценке.

Составленные в оценке выводы таким образом представляют собой избирательную выборку, а не исчерпывающее отображение практики обеспечения компьютерной безопасности в организации. Полученный вывод подтверждает наличие проблемы, однако отсутствие выводов не означает, что проблемы, связанные с обеспечением компьютерной безопасностью, отсутствуют.

Результаты обследований не всегда приводят к выводам, и не все выводы носят отрицательный характер. Дополнительным итогом является выявление "надлежащей практики", т.е. организационного процесса или процедуры, обеспечивающей новый и эффективный метод достижения целей безопасности. Необходимо выявлять такую практику и сообщать о ней в качестве примера для использования другими организациями в целях улучшения их программ по обеспечению безопасности.

Помимо выводов и надлежащей практики группа оценки может также включать в отчет с выводами дополнительные руководящие материалы, рекомендации и предложения.

В рекомендациях указываются руководящие принципы обеспечения соответствия правовым и регулирующим требованиям (национальных законам/нормативным актам) и/или международным нормам в соответствующих случаях. Рекомендации, как правило, не содержат информации о том, как следует устранять проблему, а лишь указывают на то, что проблема должна быть устранена.

В предложениях приводится дополнительная информация, касающаяся выводов, включая корректирующие меры или стратегии минимизации. Такая информация не обязательно базируется на регулирующих (нормативных) руководящих материалах, при ее представлении скорее следует использовать технические стандарты и примеры надлежащей практики в данной отрасли.

Предложения могут включать, например, следующие меры:

- модификация оборудования и установка дополнительных устройств и средств для повышения уровня безопасности;
- усовершенствование процедур и административных мер;
- разработка дополнительных проверок и средств контроля;
- устранение недостатков, выявленных в операционных процедурах;
- устранение недостатков в политических документах;
- обучение персонала по вопросам исполнения как общих, так и конкретных должностных функций;

— внесение изменений в рабочую среду;

— внесение изменений в планирование и график работы и/или в список лиц, которым поручается выполнение конкретных обязанностей.

6.1.1. Анализ значимости

При проведении оценки одно лишь составление вывода часто является недостаточным; в конечном счете необходимо выяснить воздействие или возможные последствия вывода. Принимающая организация должна рассмотреть последствия или значимость данного вывода для физической безопасности и безопасности. Анализ воздействия может проводиться на различных уровнях. На первом уровне рассматриваются последствия данного вывода с уделением особого внимания воздействию или значимости в соответствии с триадой КЦД (конфиденциальность, целостность и доступность). На втором уровне проводится систематическое изучение и выполняется анализ всей совокупности выводов и их общего воздействия на объект или организацию. Выполнение такого анализа является непростой задачей, и необходимо наличие многопрофильной группы для исследования всей совокупности последствий для безопасности, физической безопасности, операций и т.д.

Анализ такого уровня, как правило, не проводится группой оценки, осуществляющей рассмотрение вопросов регулирования, в котором выполнение анализа поручается принимающей организации. Вместе с тем такой анализ может выполняться совместно с группой оценки, работающей в рамках осуществления самооценки или технических консультативных миссий, проводимых третьими сторонами. Для проведения таких оценок требуются значительные ресурсы и время.

6.2. ЭЛЕМЕНТЫ ОТЧЕТА

В зависимости от плана оценки отчеты могут составляться в процессе оценки, например, это может быть составление проекта отчета для заключительного информационного совещания или представляемые впоследствии документы.

При определении содержания отчета должны учитываться следующие соображения:

— члены группы должны быть объективными, основывать свои выводы на анализе соответствующих документов, результатах собеседований с ключевыми сотрудниками и прямых обследованиях;

— члены группы должны консультироваться с коллегами принимающей организации с целью уточнения конкретных вопросов и подтверждения того, что эти вопросы правильно понимаются;

— члены группы должны консультироваться друг с другом и в особенности с руководителем группы и обмениваться результатами своих выводов во избежание дублирования, непоследовательности и появления вопросов, которые могут вступать в противоречие с другими выводами;

— заключения членов групп, в частности содержащиеся в рекомендациях, предложениях и констатации надлежащей практики, необходимо четко документировать с обоснованием, подтверждающим справедливость конкретных рекомендаций, предложений или надлежащей практики;

— необходимо учитывать чувствительность с точки зрения безопасности (конфиденциальности) итогового отчета, исходя из чувствительности его содержания, уязвимостей, которые оно может раскрыть (и потенциальных последствий этого), и применимой национальной или действующей на уровне

организации политики в области защиты чувствительной информации. Конфиденциальность отчета должна быть указана на документе, и обращение с отчетом должно осуществляться соответствующим образом.

При формулировании вывода в отчете должны быть по возможности ясно и четко указаны:

- соответствующая функция и домены физической безопасности (задействовано может быть несколько доменов);
- руководящие материалы и надлежащая практика, используемые для оценивания (со ссылками на руководящие материалы);
- сам вывод;
- потенциальное воздействие вывода (оно может быть классифицировано по шкале серьезности последствий, например, административный уровень, незначительные, значительные, серьезные и т.д.);
- рекомендуемое решение или корректирующие меры.

Выводы могут быть дополнительно сгруппированы по функциям и доменам физической безопасности в целях общей классификации или для оценивания объединённых областей.

Отчет отражает уровень уверенности группы в том, что оценка была достаточно полной для обеспечения объективного оценивания установки.

Должны быть идентифицированы области, не попавшие в оценку.

В отношении формата и стиля отчета полезными могут быть следующие соображения:

- начальное резюме с изложением общих впечатлений группы, полученных в ходе проведения оценки, может помочь в проведении дальнейшего, более детального обсуждения отдельных областей;
- язык должен быть простым, ясным, кратким, объективным и безличным;
- в соответствующие разделы могут быть вставлены графики и фотографии. Особенно полезными являются иллюстрации, касающиеся правительства или организации, и диаграммы или фотографии, иллюстрирующие конкретный недостаток или надлежащую практику;
- для указания подразделений, должностей и систем организации должны использоваться официальные названия (или официальные переводы);
- сокращения должны расшифровываться при первом употреблении, и для удобства также в отдельной таблице должен быть приведен их перечень с определениями.

6.3. ЗАКЛЮЧИТЕЛЬНОЕ ИНФОРМАЦИОННОЕ СОВЕЩАНИЕ

Участниками заключительного информационного совещания являются сотрудники объекта, на котором проводится оценка, а также в их число могут входить другие стороны. В случае необходимости руководитель группы оценки проводит консультации с оцениваемой организацией по любым вопросам, возникающим в ходе проведения оценки, которые могут влиять на доверие к заключениям оценки. Совещание по оценке является официальным, и поэтому должен вестись протокол и составляться список присутствующих.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

[1] 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).

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок, 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] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems – Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Information Security Management Systems – Requirements, ISO/IEC 27001:2005, ISO, Geneva (2005).

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Geneva (2005).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2008).

[8] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Guidelines for auditing management systems, ISO 19011:2011, ISO, Geneva (2011).

[10] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800–115, Gaithersburg, Maryland, USA (2008).

ГЛОССАРИЙ

Ниже приведены определения терминов, используемых в настоящей публикации. Определения, если они уже имеются, заимствованы из публикаций МАГАТЭ или международных стандартов и норм. В этом случае определение содержит ссылку на первоначальную публикацию (включенную в перечень раздела "Справочные материалы" в конце основного документа).

Вывод. Результат обследований, свидетельствующий о расхождении между тем, как что-то осуществляется, и тем, как это должно осуществляться в соответствии с регулирующим требованием, стандартом, нормой или надлежащей практикой.

Компьютерная безопасность. Конкретный аспект информационной безопасности, относящийся к компьютерным системам, сетям и цифровым системам [3].

В настоящей публикации термин "компьютерная безопасность" относится к физической безопасности всех компьютеров, согласно определению, приведенному здесь, и всех взаимосвязанных систем и сетей. (Термины "безопасность ИТ" и "кибербезопасность" считаются синонимами, но не употребляются здесь).

Компьютеры и компьютерные системы. Вычислительные, коммуникационные устройства, а также системы контроля и управления, составляющие функциональные элементы ядерной установки. К ним относятся не только настольные компьютеры, мейнфреймовые системы, серверы и сетевые устройства, но и компоненты более низкого уровня, такие как встроенные системы и ПЛК (программируемые логические контроллеры). В случае промышленных установок такие компьютерные системы могут называться промышленными системами управления (ПСУ), а на атомных электростанциях – системами контроля и управления (СКУ) атомных станций.

Надлежащая практика. Надлежащая практика представляет собой программу, деятельность, способ применения оборудования и т.п., которые признаются передовыми и вносят вклад прямо или косвенно в повышение эксплуатационной безопасности или физической безопасности, а также обеспечивают устойчивые хорошие показатели эффективности работы. Надлежащая практика заметно превосходит ожидаемый уровень исполнения и не представляет собой только соблюдение текущих требований.

Оценка. Методология, описанная в настоящей публикации, является деятельностью, которая для простоты и последовательности называется "оценкой". Но, как уже отмечалось выше, эта методика может применяться в различных контекстах, и в таких случаях могут быть уместными другие описания деятельности, такие как "консультация или консультационные услуги", "миссия или визит экспертов", "аудит" или "самооценка". Термин "оценка" не должен толковаться как наделение МАГАТЭ или какой-либо другой организации, проводящей оценку, какими-либо дополнительными полномочиями или обязанностями.

Предложение. Предлагаемая мера или усовершенствование, которые могут быть реализованы на оцениваемой ядерный установке.

Предложение может служить дополнением к рекомендации или может иметь самостоятельный характер. Оно может косвенно способствовать повышению физической безопасности при эксплуатации, но, прежде всего, предложение

преследует цели повышения эффективности хороших показателей работы, определения направления полезного расширения существующей программы и указания возможного наилучшего альтернативного варианта осуществления работы. В целом предложение предназначается для стимулирования административного руководства и персонала установки (станции) к продолжению поиска путей повышения показателей работы.

Результат обследований. То, что было установлено как результат анализа документов, собеседования или прямого обследования.

Рекомендация. Мера, повышающая физическую безопасность ядерной установки (при проведении оценки в принимающей организации); обязательная мера по обеспечению соблюдения, выполнение которой необходимо для реализации вывода (например, сделанного государственным регулирующим органом).

Рекомендация представляет собой указание, которое настоятельно рекомендуется выполнить в отношении деятельности или программы, оцениваемой в целях повышения операционной физической безопасности. Она основывается на руководящих материалах Серии изданий МАГАТЭ по физической ядерной безопасности, национальных регулирующих положениях, стандартах, нормах или международной апробированной надлежащей практике и направлена на устранение коренных причин возникновения данной проблемы, а не только ее симптомов. Часто рекомендация включает апробированный метод достижения уровня совершенства, выходящего за рамки минимальных требований. Она должна быть конкретной, реалистичной и направленной на обеспечение ощутимых результатов усовершенствования.

Употребление термина "рекомендация" в настоящей публикации не следует путать с его значением в руководящих материалах в рамках серии изданий по физической ядерной безопасности.

Требование. Базис для конкретной оценки, т.е. правила, регулирующие положения, стандарты и нормы, которые необходимо соблюдать.

ПРИЛОЖЕНИЕ I
ПОДСКАЗКИ ДЛЯ ОЦЕНКИ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

ОБЗОР СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

В контексте настоящей публикации термины "компьютеры" и "компьютерные системы" относятся к вычислительным, коммуникационным устройствам, а также системам контроля и управления, составляющим функциональные элементы ядерной установки. К ним относятся не только настольные компьютеры, мейнфреймовые системы, серверы и сетевые устройства, но и компоненты более низкого уровня, такие как встроенные системы и ПЛК (программируемые логические контроллеры). Часть этих компьютерных систем включает в себя цифровые системы контроля и управления и средства контроля. Оценивание этих систем и средств в процессе проведения оценки является особенно важным, поскольку их компрометация может иметь серьезные последствия как для физической безопасности, так и безопасности.

Система контроля и управления (СКУ) служит в качестве эксплуатационной стержневой системы для процессов на установке. В публикации Серии изданий МАГАТЭ по ядерной энергии, № NP–T–3.12 ([I-1], с. 2-3) подробно излагаются три основные функции, выполнение которых обеспечивает СКУ в отношении процессов на установке (станции). Первая функция – это функционирование датчиков или детекторов (например, для измерения и наблюдения), необходимое для поддержки таких функций, как мониторинг и контроль, и позволяющее персоналу установки оценивать ее состояние. Таким образом, СКУ, такие как датчики и детекторы, являются прямыми средства сопряжения с физическими процессами на атомной электростанции, и их сигналы передаются оператору по коммуникационным системам, а также поступают в предназначенные для принятия решений системы (аналоговые или компьютерные).

Вторая функция обеспечивает автоматическое управление как для основной установки, так и для многих вспомогательных систем. Третья функция СКУ – это реагирование на отказы/сбои и отклонения от нормального режима работы, обеспечивающее при этом безопасность и защиту установки от последствий любого нарушения функционирования или отклонения в работе систем установки или в результате ошибочных действий в ручном режиме.

Эти вычислительные и связанные с ними системы (СКУ), используемые в реализации операционных функций атомной электростанции, установки топливного цикла или хранилища, обеспечивают поддержку различных функций и имеют разные наименования в промышленных отраслях. Здесь термин "промышленные системы управления" (ПСУ) используется для описания этих систем, которые включают в себя: системы диспетчерского управления и сбора данных (SCADA), распределенные системы управления, а также другие системы управления конфигурациями, такие как блочно монтируемые программируемые логические контроллеры [I -2].

Элементы управления в ПСУ могут включать ([I-2], с. 2–4):

— удаленные терминальные устройства, предназначенные для поддержки контроля и мониторинга удаленных устройств;

— программируемые логические контроллеры, которые представляют собой небольшие компьютеры, часто используемые для управления промышленными процессами;

— интеллектуальные электронные устройства, которые представляют собой интеллектуальные датчики/ исполнительные устройства для локального сбора данных, коммуникации и локального управления;

— человеко-машинный интерфейс/человеко-системный интерфейс, обеспечивающий средство сопряжения для операторов для целей мониторинга технологических процессов на установке и управления ими.

Эти системы используются в рамках сети ПСУ, содержащей также стандартные и специализированные сетевые компоненты, такие как маршрутизаторы, брандмауэры, серверы, модемы и удаленные точки доступа.

Управляющая сеть далее взаимодействует с компонентами более низкого уровня, такими как датчики и исполнительные устройства, для контроля и/или мониторинга процессов на установке, как показано на рис. I-1.

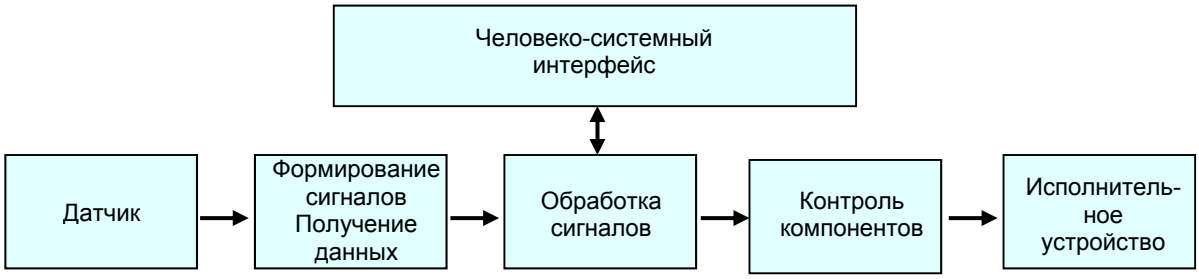

РИС. I-1. Блок-схема типичной функции СКУ [I-1].

Одна сеть может обеспечивать управление несколькими идентичными процессами. С другой стороны, управление процессами может осуществляться посредством полностью отдельных сетей. В управляющей сети каждый из этих отдельных компонентов представляет собой потенциальное уязвимое место системы и, следовательно, должен рассматриваться на определенном уровне в рамках проводимой оценки. Проблема может заключаться в том, что эти компоненты не обязательно были разработаны с учетом требований компьютерной безопасности.

ОБЩИЕ УЯЗВИМОСТИ СИСТЕМ КОНТРОЛЯ

Ниже перечислены общие уязвимости, определенные Министерством национальной безопасности США [I-3], которые могут рассматриваться при разработке и проведении оценки ПСУ и СКУ установки. Один компонент не может и не должен сам по себе быть единственным предметом рассмотрения при анализе проблем, напротив несколько отдельных компонентов должны рассматриваться вместе в общем контексте оценки. Компенсационные средства контроля или гнездовые защитные механизмы могли быть уже ранее задействованы с целью устранения этих возможных проблем.

Контроль доступа

— Доступ не ограничивается объектами, для которых он требуется.

— Протокол ПСУ позволял системным хостам ПСУ считывать или перезаписывать файлы на других хостах, без какой-либо регистрации.

— Документация и информация о конфигурации находилась в свободном пользовании (доступ только для чтения).

— Общие ресурсы доступны на множественных системах.

— Отсутствует ролевая аутентификация для коммуникации с компонентами ПСУ.

— Удаленный пользователь может загрузить файл в любое место на целевом компьютере.
— Произвольная загрузка файла допускается на хостах ПСУ.
— Произвольная выгрузка файлов разрешена на хостах ПСУ.
— Удаленный клиент может запустить любой процесс.
— Сервис ПСУ допускает анонимный доступ.
— Нераскрытые обходные ("бэкдор") аккаунты (учетные записи) с правами администратора для обеспечения доступа поставщику в будущем для выполнения работ по обслуживанию, установке обновлений или обучения.
— Злоупотребление аккаунтом (учетной записью) менеджера.
— Удаленная эксплуатация сервисов приложений ПСУ разрешала доступ на корневом уровне на хостах ПСУ.
— Сервис базы данных работает как администратор.
— Аутентификация не требуется для считывания конфигурационного файла системы, содержащего детали аккаунтов (учетных записей) пользователей, включая пароли.
— Отсутствие разделения обязанностей посредством авторизации присвоенных прав доступа.
— Отсутствие принудительной системы блокировки в случае неудачных попыток входа в систему.

Пароли

— Некоторые хосты ПСУ имели очень слабые трехсимвольные административные пароли.
— Слабые пароли были восстановлены и разрешают доступ на корневом уровне ко всем ресурсам системы.
— Было обнаружено несколько слабых паролей.
— Дефолтный (создаваемый по умолчанию) пароль не был изменен.
— Используются дефолтные (создаваемые по умолчанию) имена пользователей и пароли на уровне администратора.
— Дефолтные (создаваемые по умолчанию) учетные данные присвоены нескольким предопределенным аккаунтам (учетным записям) пользователей на устройстве, включая административную учетную запись пользователя.
— Компонент ПСУ прямо доступен из Интернета с использованием дефолтных (создаваемых по умолчанию) имени пользователя и пароля.
— Длина, надежность и сложность паролей принудительно не обеспечиваются.
— Многие аккаунты (учетные записи), в том числе аккаунт (учетная запись) администратора, не имеют даты истечения срока действия пароля.
— Политика блокировки аккаунтов (учетных записей) не определена.
— Функция сложности пароля была отключена.
— История паролей установлена на ноль запоминаемых предыдущих паролей.

Кодовые артефакты

Хранение ПСУ, например исходного кода и конфигурация системы в общей файловой системе, создает значительный потенциал для "добычи" информации злоумышленниками. В составе многих ПСУ предусматриваются открытые сетевые ресурсы на хостах ПСУ. Ниже приведены примеры выводов оценки, связанных с этой уязвимостью:

- наличие общедоступных сетевых ресурсов на хостах ПСУ. Два общих ресурса обнаружены на рабочей станции и серверных компьютерах;
- общие ресурсы (папки) на множественных системах;
- к файлам имеется доступ для чтения;
- утечка информации через общие каталоги;
- наличие большого количества общедоступных сетевых ресурсов на хостах ПСУ;
- исходный код для ПСУ совместно используется на хостах ПСУ. Исходный код можно скачать и использовать для отыскания уязвимостей.

Патч-менеджмент

Обнаружены неисправленные (с помощью патчей) или старые версии приложений в программном обеспечении ПСУ, включая следующее:

- наличие уязвимой версии базы данных;
- наличие уязвимой версии веб-сервера;
- технология связывания и внедрения объектов для управления технологическими процессами OPC использует удаленный вызов процедур (RPC) и распределённую модель компонентных объектов (DCOM); без обновленных патчей технология OPC подвержена воздействию известных уязвимостей RPC/DCOM;
- наличие уязвимых (неисправленных с помощью патчей) библиотек SSL.

Планирование/политика/процедуры

- Отсутствие официальной документации.
- Неудовлетворительное ведение документации по физической безопасности.
- Отсутствие предусмотренного в организационной структуре подразделения по компьютерной безопасности.
- Отсутствие политики в области аварийного восстановления.
- Отсутствие понимания процедур восстановления.
- Слабые возможности резервного копирования и восстановления.

Недостатки в построении сети

Общие недостатки

- Не определен периметр безопасности.
- Сетевые устройства неправильно отконфигурированы.
- Безопасность портов не обеспечена на сетевых устройствах.

Отсутствие сетевого сегментирования

- Управляющие сети используются для неуправляемого трафика.

— Сервисы управляющей сети не находятся в управляющей сети.

— Отсутствует внутреннее сегментирование производственной сети ПСУ: серверы протокола внутренней передачи данных между центрами управления (ICCP) не находятся в DMZ.

— Отсутствует внутреннее сегментирование производственной сети ПСУ: хост с выделенным последовательным каналом для передачи данных с использованием высокорискового приложения не находится в DMZ.

— Системы, связанные управлением, доступны в корпоративной локальной сети.

— Реагирование на инциденты и оценка с применением CSET на местах позволили выявить наличие указанных ниже проблем на множественных сайтах.

— Управляющие сети используются для неуправляемого трафика.

— Сервисы управляющей сети не находятся в управляющей сети.

Брандмауэры/DMZ

— Брандмауэры отсутствуют.

— Отсутствует функциональная DMZ.

— Физические кабели, подключенные непосредственно к локальной сети ПСУ, идут в обход брандмауэра.

— SSH-сервер соединяет корпоративную локальную сеть и локальную сеть ПСУ в обход брандмауэра.

— Третья сетевая карта на сервере ICCP подключена напрямую к локальной сети ПСУ.

— Доступ к конкретным портам на хосте не ограничивается требуемыми IP-адресами.

— Списки доступа определены, но не применяются. Нет фильтрации входящих пакетов.

— Списки доступа не соответствуют требуемым портам.

— Доступ к сетевым принтерным сервисам в корпоративной локальной сети не ограничен защитой паролем или списком контроля доступа.

— Клиент электронной почты в DMZ имел доступ к корпоративной сети и Интернету.

— Недостаточные ограничения исходящего доступа.

— Правила брандмауэра не адаптированы к трафику ПСУ.

Аудит и отчетность

— Отсутствие аудитов/оценок безопасности;

— отсутствие регистрации или неудовлетворительная регистрация;

— сетевая архитектура не достаточно хорошо понимается;

— слабое исполнение политики удаленного входа в систему;

— слабый контроль входящих и исходящих потоков среды передачи;

— неудовлетворительный метод мониторинга событий в управляющей сети.

СПРАВОЧНЫЕ МАТЕРИАЛЫ К ПРИЛОЖЕНИЮ I

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

[I-2] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800–82, Gaithersburg, Maryland, USA (2011).

[I-3] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Common Cybersecurity Vulnerabilities in Industrial Control Systems, US Department of Homeland Security, (2011), available online at: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

ПРИЛОЖЕНИЕ II

ШАБЛОН ДЛЯ РЕЗУЛЬТАТОВ НАБЛЮДЕНИЙ

Помещенный ниже примерный шаблон предназначен для оказания помощи экспертам по оценке в сборе и анализе данных, используемых при проведении оценки.

Этот шаблон и таблица данных приводятся исключительно в качестве примеров и могут быть изменены в соответствии с потребностями группы оценки.

Результаты обследований используются при составлении итогового отчета об оценке.

Эксперт по оценке		**Номер**			
Дата и время					
Место расположения	Место проведения обследования				
Установка	если это применимо				
Система	если это применимо				
Домен физической безопасности	Согласно определению				
Функциональный домен	Согласно определению				
Уровень физической безопасности					
Обследования:	Описать результат обследования или что было выявлено				
Как было выявлено?	Анализ документов	Собеседование	Обследование	Открытый источник	Прочее:
Цель	Рекомендация	Предложение	Надлежащая практика	Прочее:	
Вывод*	Описать отклонения				
Основание*	Ссылка на руководящие материалы МАГАТЭ, надлежащую практику, стандарт, норму, регулирующие положения, известный вектор атак и т.п.				
Корневая причина*	Причина существования проблемы				
Эксплуатируемость уязвимости*	легкая	умеренная	сложная		
Доступность*	Внешняя угроза/инсайдерская угроза (знакомая или незнакомая)				
Потенциальные последствия*	Описание прямых и косвенных последствий выводов				
Уровень значимости*	Категоризация выводов на основе их потенциальных последствий (организации могут разрабатывать свою собственную шкалу значимости или последствий)				
Действие*	Внедрение надлежащей практики, применение стандартов, норм, регулирующих правил и положений, системы внесения патчей и т.п.				
ПРИМЕЧАНИЯ:					

* Это может быть не сразу определено во время проведения обследований, и допускается заполнение этих граф на более позднем этапе.

Условные обозначения для шаблона работ на местах

Функциональные домены

OP: Домен операций

BU: Домен бизнес-процессов

BU: Домен безопасности

PP: Домен физической защиты

ER: Домен реагирования на чрезвычайные ситуации

Домены физической безопасности

SP: Политика обеспечения физической безопасности

OI: Организация информационной безопасности

AM: Менеджмент активов

HR: Безопасность людских ресурсов (персонала)

PP: Физическая защита

CO: Менеджмент коммуникации и операций

CA: Контроль доступа к компьютерам

CM: Приобретение, развитие и обслуживание компьютерных систем

CI: Менеджмент инцидентов, связанных с компьютерной безопасностью

CM: Менеджмент непрерывности

CP: Обеспечение соответствия требованиям

Эксплуатируемость уязвимости

Легкая	Уязвимость общеизвестна; публичные инструменты эксплуатации уязвимости существуют
Умеренная	Некоторые детали известны; проверка концепции доступна
Сложная	Детальных данных нет

Возможные виды действий

Модификация оборудования и установка дополнительных устройств и средств для предотвращения повторения одних и тех же или подобных событий

Усовершенствование процедур и административных мер, а также дополнительные проверки и меры контроля

Устранение недостатков, выявленных в операционной документации (руководствах по эксплуатации)

Устранение недостатков в нормативных документах

Подготовка персонала по вопросам должного исполнения работы

Внесение изменений в рабочую среду

Внесение изменений в планирование и график работы и/или в список лиц, которым поручается выполнение конкретных обязанностей.

ПРИЛОЖЕНИЕ III

ШАБЛОН ИТОГОВОГО ОТЧЕТА

РЕЗЮМЕ

В резюме кратко и лаконично излагаются контекст, цели, методология и требования, основные рекомендации и методы надлежащей практики.

ВВЕДЕНИЕ

- Цели
- Круг вопросов
- Упрощенная карта сетевой архитектуры для обеспечения общего понимания пределов оценки группой оценки и принимающей организацией
- Методология
- Определения (при необходимости)

РЕЗУЛЬТАТЫ ОЦЕНКИ

Выводы

- Выводы получаются путем применения фильтров для требований к результатам обследований. Выводы должны быть перечислены.
- Документы с изложением требований, такие как регулирующие положения, процедуры, нормы, надлежащая практика и т.п., должны быть определены, и ссылки на них необходимо указывать в выводах.
- Результаты обследований можно, но не обязательно включать, но могут быть приведены ссылки в выводах (ссылки можно не приводить, если они уже были доведены до сведения представителей установки).

Рекомендации, предложения и надлежащая практика

- Рекомендации (по выводам) и предложения должны быть определены и снабжены ссылками на требования или руководящие документы.
- Если оценка проводится государством или регулирующим органом, рекомендации могут быть точно определены, как, например, директивы, предписания и т.п.
- Рекомендации могут быть ранжированы с применением дифференцированного подхода с учетом потенциального риска или последствий для установки. Критерии для ранжирования должны быть обсуждены и согласованы на совещании перед проведением оценки.

Стратегия минимизации (факультативно)

- Включение раздела о стратегии минимизации является вариантом, который может быть обсужден до проведения оценки.

— В случае включения в итоговый отчет стратегии минимизации содержание этого раздела должно быть обсуждено с персоналом установки.

Анализ последствий (факультативно)

— В отчет может быть включен анализ потенциальных последствий выводов для функциональных доменов на установке, таких как безопасность, физическая безопасность, радиационная защита и т.д. Этот анализ не является частью всех оценок, и уровень анализа должен быть обсужден и согласован на совещании по планированию.

ЗАКЛЮЧЕНИЕ

В этом разделе приводится обзор результатов оценки и повторяются основные рекомендации, предложения и примеры надлежащей практики в отношении соблюдения требований и анализа рисков на ядерной установке. В случае включения в итоговый отчет стратегии минимизации дополнительно может быть приведен план основных действий.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

Перечень соответствующих документов/ссылок, используемых для оценки и анализа:

— требования;
— регулирующие руководства;
— стандарты (нормы);
— используемые процедуры, любые другие документы и т.п.;
— собеседования с сотрудниками;
— должности лиц, с которыми проводятся собеседования (менеджер, инженер, техник и т.д.).

СОКРАЩЕНИЯ

ПРИЛОЖЕНИЕ

— График проведения оценки
— Формы обследований
— Формы выводов

ПРИЛОЖЕНИЕ IV

СООБРАЖЕНИЯ, КАСАЮЩИЕСЯ ПРИНЯТИЯ МЕР ПО РЕЗУЛЬТАТАМ ОТЧЕТА

В данном приложении указаны вопросы, которые принимающей организации следует учитывать при рассмотрении результатов, изложенных в итоговом отчете об оценке. В отчете излагаются в совокупности все выводы, результаты обследований, рекомендации и предложения. В каждой организации могут применяться свои собственные процессы разработки плана действий на основе этих результатов.

Рассмотрение отчета должно проводиться с участием сотрудников, представляющих несколько уровней управления, включая руководство высшего звена. Это важно для обеспечения того, чтобы при разработке плана действий были расставлены надлежащие акценты и использовались соответствующие ресурсы. Некоторые меры по исправлению или минимизации могут быть несложными, в то время как другие меры могут требовать детального анализа. Изложенные ниже соображения могут быть полезными при принятии решений в процессе разработки этого плана действий.

Последствия

- Каковы основные последствия отчета для организации?
- Как отчет может повлиять на общий профиль рисков в организации?

Меры по минимизации

- Какая дополнительная информация необходима для принятия решения?
- Какова эффективность предлагаемого решения? (Какова степень снижения риска?)
- Могут ли несколько выводов быть реализованы с помощью единого решения?
- Каковы последствия реализации рекомендуемого решения (например, связана ли реализация решения с нежелательными побочными эффектами, такими как недействительность сертификации, лицензирования или гарантий систем?).
- Приводит ли предлагаемое решение к дополнительным или иным рискам?
- Какие меры существуют в качестве альтернативы рекомендуемому решению?
- Как организация может проверить эффективность предлагаемой рекомендации?

Сроки осуществления мер по минимизации

- Каков срок выполнения рекомендации? Достаточен ли он для устранения угрозы?
- Какие особые условия необходимы для реализации решения (например, отключение/останов или период обслуживания)?
- Может ли вывод быть реализован путем применения промежуточных мер до осуществления более постоянных мер?
- Существуют ли организационные планы реализации будущих проектов, которые направлены на решение или изменение проблем или которые обеспечивают возможность устранения проблемы?

Затраты на осуществление мер по минимизации

- Располагает ли организация соответствующими специалистами и техническим экспертным потенциалом для реализации рекомендации?
- Что входит в расходы на предлагаемое решение?
  - расходы на приобретение;
  - затраты на реализацию;
  - коммуникационные расходы на новое решение;
  - затраты на обучение персонала;
  - затраты на обучение пользователей;
  - затраты на обеспечение производительности и удобств;
  - расходы на аудит и верификацию эффективности;
  - расходы по утилизации в конце жизненного цикла.

Коммуникация

- Представляется ли полезным информирование внешних организаций, например, поставщиков, партнеров отрасли или компетентных органов, о конкретных результатах, изложенных в отчете?
- Если оценка является частью процесса регулирования, компетентный орган может требовать отчетности, касающейся плана действий и последующих мероприятий.

Прочие соображения

- Является ли данный вывод повторяющимся, что может означать, что вопрос не был надлежащим образом решен или что предыдущая мера оказалась не эффективной?
- Свидетельствуют ли накопившиеся выводы о более значительной проблеме в организации?
- Как организация может предотвратить повторение этого или связанных с ним выводов в будущем?
- Как будет отслеживаться в рамках организации реализация изложенных в отчете результатов и плана действий?

ЗАКАЗ В СТРАНАХ

В указанных 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.

ГЕРМАНИЯ

Goethe Buchhandlung Teubig GmbH

Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Телефон: +49 (0) 211 49 874 015 • Факс: +49 (0) 211 49 874 28
Эл. почта: kundenbetreuung.goethe@schweitzer-online.de • Сайт: www.goethebuch.de

ИНДИЯ

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Телефон: +91 22 4212 6930/31/69 • Факс: +91 22 2261 7928
Эл. почта: alliedpl@vsnl.com • Сайт: www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Телефон: +91 11 2760 1283/4536
Эл. почта: bkwell@nde.vsnl.net.in • Сайт: www.bookwellindia.com

ИТАЛИЯ

Libreria Scientifica “AEIOU”

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Телефон: +39 02 48 95 45 52 • Факс: +39 02 48 95 45 48
Эл. почта: info@libreriaaeiou.eu • Сайт: www.libreriaaeiou.eu

КАНАДА

Renouf Publishing Co. Ltd

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Телефон: +1 613 745 2665 • Факс: +1 643 745 7660
Эл. почта: order@renoufbooks.com • Сайт: www.renoufbooks.com

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Тел: +1 800 462 6420 • Факс: +1 800 338 4550
Эл. почта: oorders@rowman.com Сайт: www.rowman.com/bernan

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Научно-технический центр по ядерной и радиационной безопасности

107140, Москва, Малая Красносельская ул, д. 2/8, кор. 5, РОССИЙСКАЯ ФЕДЕРАЦИЯ
Телефон: +7 499 264 00 03 • Факс: +7 499 264 28 59
Эл. почта: secnrs@secnrs.ru • Сайт: www.secnrs.ru

СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Тел: +1 800 462 6420 • Факс: +1 800 338 4550
Эл. почта: orders@rowman.com • Сайт: www.rowman.com/bernan

Renouf Publishing Co. Ltd

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Телефон: +1 888 551 7470 • Факс: +1 888 551 7471
Эл. почта: orders@renoufbooks.com • Сайт: www.renoufbooks.com

ФРАНЦИЯ

Form-Edit

5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Телефон: +33 1 42 01 49 49 • Факс: +33 1 42 01 90 90
Эл. почта: formedit@formedit.fr • Сайт: www.form-edit.com

ЧЕШСКАЯ РЕСПУБЛИКА

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Телефон: +420 242 459 205 • Факс: +420 284 821 646
Эл. почта: nakup@suweco.cz • Сайт: www.suweco.cz

ЯПОНИЯ

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Телефон: +81 3 4335 9312 • Факс: +81 3 4335 9364
Эл. почта: bookimport@maruzen.co.jp • Сайт: www.maruzen.co.jp

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

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Телефон: +43 1 2600 22529 или 22530 • Факс: +43 1 2600 29302 или +43 1 26007 22529
Эл. почта: sales.publications@iaea.org • Сайт: www.iaea.org/books

18-00579R

Международное агентство по атомной энергии
Вена
ISBN 978-92-0-408317-0