Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Серия изданий МАГАТЭ по физической ядерной безопасности, № 17

Технические руководящие материалы
Справочное руководство

Компьютерная безопасность на ядерных установках

IAEA
Международное агентство по атомной энергии

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

В публикациях **Серии изданий МАГАТЭ по физической ядерной безопасности** рассматриваются вопросы физической ядерной безопасности, касающиеся предотвращения и обнаружения хищения, саботажа, несанкционированного доступа, незаконной передачи или других злоумышленных действий в отношении ядерного материала, других радиоактивных веществ или связанных с ними установок и реагирования на такие действия. Эти публикации соответствуют таким международным договорно-правовым документам в области физической ядерной безопасности, как Конвенция о физической защите ядерного материала с внесенными в нее поправками, Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников, резолюции 1373 и 1540 Совета Безопасности Организации Объединенных Наций и Международная конвенция о борьбе с актами ядерного терроризма, а также дополняют их.

КАТЕГОРИИ ПУБЛИКАЦИЙ В СЕРИИ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

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

- **“Основы физической ядерной безопасности”,** которые содержат задачи, концепции и принципы физической ядерной безопасности и на основе которых составляются рекомендации в отношении физической безопасности.
- **“Рекомендации”,** где излагается передовой опыт, который следует использовать государствам-членам при осуществлении “Основ физической ядерной безопасности”.
- **“Практические руководства”,** в которых развиваются рекомендации по широким направлениям деятельности и предлагаются меры по их осуществлению.
- Публикации, относящиеся к **“Техническим руководящим материалам”,** включают: **“Справочные руководства”,** в которых подробно описываются меры и/или даются руководящие указания в отношении применения практических руководств в конкретных областях или видах деятельности; **“Учебные руководства”,** касающиеся учебных планов и/или учебных пособий для учебных курсов МАГАТЭ в области физической ядерной безопасности; **“Руководства по услугам”,** в которых даются руководящие указания в отношении проведения и масштабов консультативных миссий МАГАТЭ по физической ядерной безопасности.

ПОДГОТОВКА И РАССМОТРЕНИЕ

В подготовке этих публикаций Секретариату МАГАТЭ помогают международные эксперты. В отношении документов категорий “Основы физической ядерной безопасности”, “Рекомендации” и “Практические руководства” МАГАТЭ проводит технические совещания открытого состава, чтобы заинтересованные государства-члены и соответствующие международные организации имели надлежащую возможность рассмотреть проект текста. Кроме того, для обеспечения высокого уровня международного рассмотрения и достижения консенсуса Секретариат представляет проекты текстов всем государствам-членам на период в 120 дней на официальное рассмотрение. Это дает возможность государствам-членам в полной мере выразить свое мнение до опубликования текста.

Публикации категории “Технические руководящие материалы” готовятся в тесных консультациях с международными экспертами. Проведение технических совещаний не требуется, но они могут быть при необходимости организованы для ознакомления с широким спектром мнений.

В процессе подготовки и рассмотрения публикаций Серии МАГАТЭ по физической ядерной безопасности учитываются соображения конфиденциальности и признается, что вопросы физической ядерной безопасности неразрывно связаны с общими и конкретными задачами национальной безопасности. Одним из основополагающих факторов является необходимость учета в техническом содержании публикаций соответствующих норм безопасности МАГАТЭ и деятельности по гарантиям.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ НА ЯДЕРНЫХ УСТАНОВКАХ

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ
АВСТРИЯ
АЗЕРБАЙДЖАН
АЛБАНИЯ
АЛЖИР
АНГОЛА
АРГЕНТИНА
АРМЕНИЯ
АФГАНИСТАН
БАНГЛАДЕШ
БАХРЕЙН
БЕЛАРУСЬ
БЕЛИЗ
БЕЛЬГИЯ
БЕНИН
БОЛГАРИЯ
БОЛИВИЯ
БОСНИЯ И ГЕРЦЕГОВИНА
БОТСВАНА
БРАЗИЛИЯ
БУРКИНА-ФАСО
БУРУНДИ
БЫВШАЯ ЮГОСЛ. РЕСП. МАКЕДОНИЯ
ВЕНГРИЯ
ВЕНЕСУЭЛА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАНА
ГВАТЕМАЛА
ГЕРМАНИЯ
ГОНДУРАС
ГРЕЦИЯ
ГРУЗИЯ
ДАНИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО
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
САУДОВСКАЯ АРАВИЯ
СВЯТОЙ ПРЕСТОЛ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СЕНЕГАЛ
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
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”.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ, № 17

ТЕХНИЧЕСКИЕ РУКОВОДЯЩИЕ МАТЕРИАЛЫ

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ НА ЯДЕРНЫХ УСТАНОВКАХ

СПРАВОЧНОЕ РУКОВОДСТВО

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2012 ГОД

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Все научные и технические публикации МАГАТЭ защищены в соответствии с положениями Всемирной конвенции об авторском праве в том виде, как она была принята в 1952 году (Берн) и пересмотрена в 1972 году (Париж). Впоследствии авторские права были распространены Всемирной организацией интеллектуальной собственности (Женева) также на интеллектуальную собственность в электронной и виртуальной форме. Для полного или частичного использования текстов, содержащихся в печатных или электронных публикациях МАГАТЭ, должно быть получено разрешение, которое обычно является предметом соглашений о роялти. Предложения о некоммерческом воспроизведении и переводе приветствуются и рассматриваются в каждом отдельном случае. Вопросы следует направлять в Издательскую секцию МАГАТЭ по адресу:

Группа маркетинга и сбыта
Издательская секция
Международное агентство по атомной энергии
Vienna International Centre
PO Box 100
1400 Vienna, Austria
факс: +43 1 2600 29302
тел.: +43 1 2600 22417
эл. почта: sales.publications@iaea.org
веб-сайт: http://www.iaea.org/books

© МАГАТЭ, 2012

Напечатано МАГАТЭ в Австрии
Ноябрь 2012

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
НА ЯДЕРНЫХ УСТАНОВКАХ
МАГАТЭ, ВЕНА, 2012

STI/PUB/1527
ISBN 978–92–0–435510–9
ISSN 1816–9317

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

ПРЕДИСЛОВИЕ

В нынешней глобальной ситуации нельзя исключить вероятность того, что ядерный или другой радиоактивный материал может быть использован в злоумышленных целях. Государства реагируют на этот риск, принимая на себя коллективное обязательство по усилению защиты такого материала и его контроля и обеспечению эффективного реагирования на события, связанные с физической ядерной безопасностью. Государства приняли решение укрепить существующие договорно-правовые документы и разработали новые международные договорно-правовые документы с целью укрепления физической ядерной безопасности во всем мире. Физическая ядерная безопасность играет основополагающую роль в сфере управления ядерными технологиями и в тех применениях, в которых используется или транспортируется ядерный или другой радиоактивный материал.

Посредством своей Программы по физической ядерной безопасности МАГАТЭ оказывает государствам поддержку в деле установления, поддержания и обеспечения устойчивости эффективного режима физической ядерной безопасности. МАГАТЭ приняло комплексный подход к обеспечению физической ядерной безопасности. Он исходит из того, что эффективный национальный режим физической ядерной безопасности основывается на: соблюдении надлежащих международно-правовых документов; защите информации; физической защите; учете и контроле материала; обнаружении незаконного оборота такого материала и принятии соответствующих ответных мер; национальных планах реагирования; и на чрезвычайных мерах. Посредством своей серии изданий по физической ядерной безопасности МАГАТЭ стремится согласованно и комплексно оказывать государствам помощь в осуществлении такого режима и обеспечении его устойчивости.

В Серии изданий МАГАТЭ по физической ядерной безопасности выпускаются публикации следующих категорий: «Основы физической ядерной безопасности», излагающие цели и важнейшие элементы государственного режима физической ядерной безопасности; «Рекомендации»; «Практические руководства»; и «Технические руководящие материалы».

Каждое государство несет полную ответственность за физическую ядерную безопасность, а именно: обеспечение сохранности ядерного и другого радиоактивного материала и физической безопасности связанных с ним установок и видов деятельности; обеспечение сохранности такого материала при его использовании, хранении или транспортировке; борьбу с незаконным оборотом и непреднамеренным перемещением такого материала; и готовность к реагированию на событие, связанное с физической ядерной безопасностью.

Настоящая публикация относится к категории «Технические руководящие материалы» в серии изданий МАГАТЭ по физической ядерной безопасности, и

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

в ней рассматриваются вопросы компьютерной безопасности на ядерных установках. Она основана на национальном опыте и практике, а также на публикациях в сферах компьютерной безопасности и физической ядерной безопасности. Руководящие материалы предназначены для рассмотрения государствами, компетентными органами и операторами.

Подготовка данной публикации серии изданий МАГАТЭ по физической ядерной безопасности стала возможной благодаря вкладам, внесенным многими экспертами из государств-членов. Процесс широких консультаций со всеми государствами-членами включал совещания консультантов и технические совещания открытого состава. Затем проект документа был разослан всем государствам-членам, с тем чтобы они в течение 120 дней выработали дальнейшие замечания и предложения. Замечания, полученные от государств-членов, были рассмотрены и учтены в окончательном варианте данной публикации.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Настоящий документ не затрагивает вопросов ответственности – юридической или иного рода – за действия или бездействия со стороны какого-либо лица.

Хотя для обеспечения точности информации, содержащейся в данной публикации, были приложены большие усилия, ни МАГАТЭ, ни его государства-члены не принимают на себя ответственности за последствия, которые могут возникнуть в результате ее использования.

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

Упоминание названий конкретных компаний или продуктов (независимо от того, были они зарегистрированы или нет) не подразумевает какого-либо намерения нарушить права собственности, и его не следует рассматривать как одобрение или рекомендацию со стороны МАГАТЭ.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ 1

1.1. Общие сведения 1
1.2. Цель 2
1.2.1. Цели физической ядерной безопасности и компьютерной безопасности 2
1.2.2. Сфера применения 3
1.3. Условия, специфические для ядерных установок 3
1.4. Структура 4
1.5. Методология 4
1.6. Основная терминология 5

ЧАСТЬ I. РУКОВОДСТВО ДЛЯ МЕНЕДЖМЕНТА 7

2. СООБРАЖЕНИЯ, СВЯЗАННЫЕ С РЕГУЛИРОВАНИЕМ И МЕНЕДЖМЕНТОМ 9

2.1. Соображения законодательного характера 10
2.2. Соображения, связанные с регулированием 11
2.3. Основа физической безопасности площадки 12
2.3.1. Политика обеспечения компьютерной безопасности 13
2.3.2. Компьютерные системы на ядерных установках . . . 13
2.3.3. Глубокоэшелонированная защита 14
2.4. Оценка обстановки в плане угрозы 14

3. СИСТЕМЫ МЕНЕДЖМЕНТА 15

4. ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ 17

4.1. Полномочия и обязанности 17
4.1.1. Руководство 17
4.1.2. Сотрудник по компьютерной безопасности 18
4.1.3. Группа компьютерной безопасности 19
4.1.4. Другие обязанности руководства 20
4.1.5. Индивидуальные обязанности 20
4.2. Культура компьютерной безопасности 21

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

4.2.1. Программа обучения в области компьютерной безопасности 22

ЧАСТЬ II. ПРАКТИЧЕСКОЕ РУКОВОДСТВО 23

5. РЕАЛИЗАЦИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ 25

5.1. План и политика обеспечения компьютерной безопасности 25
5.1.1. Политика обеспечения компьютерной безопасности 25
5.1.2. План обеспечения компьютерной безопасности 26
5.1.3. Элементы ПОКБ 26
5.2. Взаимодействие с другими областями безопасности 27
5.2.1. Физическая безопасность 28
5.2.2. Кадровая безопасность 28
5.3. Анализ и менеджмент активов 28
5.4. Классификация компьютерных систем 29
5.4.1. Важность для безопасности 30
5.4.2. Системы физической безопасности или системы, связанные с физической безопасностью 32
5.5. Дифференцированный подход к компьютерной безопасности 33
5.5.1. Уровни физической безопасности 33
5.5.2. Зоны 34
5.5.3. Пример применения модели уровней физической безопасности 35
5.5.4. Зоны разделения 40

6. УГРОЗЫ, УЯЗВИМОСТИ И УПРАВЛЕНИЕ РИСКОМ 40

6.1. Основные понятия и взаимосвязи 41
6.2. Оценка риска и управление риском 41
6.3. Идентификация и определение характера угроз 43
6.3.1. Проектная угроза 44
6.3.2. Профили данных исполнителей атак 44
6.3.3. Сценарии атак 45
6.4. Упрощенные результаты оценки риска 50

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

7. ОСОБЫЕ СООБРАЖЕНИЯ, КАСАЮЩИЕСЯ ЯДЕРНЫХ УСТАНОВОК 50

7.1. Этапы жизненного цикла и режимы работы установок 50
7.2. Различия между системами ИТ и промышленными системами управления 52
7.3. Требования в отношении дополнительных возможностей подключения и связанные с этим последствия 53
7.4. Соображения, касающиеся обновлений программного обеспечения 55
7.5. Учет требований безопасности при проектировании и в спецификациях компьютерных систем 56
7.6. Процедура контроля доступа третьих сторон/поставщиков 57

СПРАВОЧНЫЕ МАТЕРИАЛЫ 59

БИБЛИОГРАФИЯ 61

ПРИЛОЖЕНИЕ I: СЦЕНАРИИ АТАК НА СИСТЕМЫ ЯДЕРНЫХ УСТАНОВОК 63

ПРИЛОЖЕНИЕ II: МЕТОДОЛОГИЯ ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ 69

ПРИЛОЖЕНИЕ III: РОЛЬ ОШИБКИ ЧЕЛОВЕКА В КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ 75

ОПРЕДЕЛЕНИЯ 79

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

1. ВВЕДЕНИЕ

1.1. ОБЩИЕ СВЕДЕНИЯ

В последнее десятилетие возросло внимание, уделяемое компьютерной безопасности, поскольку появились четкие и многочисленные свидетельства уязвимости компьютерных систем. Все более часто фиксировались случаи злоумышленного использования подобных уязвимостей, причем с все более серьезными последствиями. В ситуации, характеризуемой все более и более сложными угрозами, возможность возникновения кибертерроризма как средства совершения атак на критически важную инфраструктуру государства побудила ряд национальных компетентных органов заняться подготовкой мер защиты и выпуском новых регулирующих положений. Такие регулирующие положения устанавливают требования компьютерной безопасности, затрагивающие многие уровни и различные стадии эксплуатации ядерных установок. Параллельно этому быстрыми темпами развивалась сама информационная безопасность, что привело к появлению обширного набора различных видов международной образцовой практики и документов по стандартам, среди которых документы серии ИСО/МЭК 27000 [1–5] быстро завоевывают видное место.

МАГАТЭ, признавая базовую ценность серии документов ИСО 27000 и других стандартов для промышленности и бизнеса, хотело бы сосредоточить внимание на специфических условиях, влияющих на компьютерную безопасность на ядерных установках. Поэтому возникла необходимость разработки публикации, в которой были бы изложены и обобщены соответствующие руководящие материалы и надлежащие решения. В настоящей публикации сведены воедино знания и опыт специалистов, занимающихся применением, тестированием и рассмотрением руководящих материалов и стандартов по компьютерной безопасности на ядерных установках и в составе другой критически важной инфраструктуры. В ней собраны и изложены специальные положения, образцовая практика и извлеченные уроки в рамках ядерной дисциплины, причем они рассматриваются в контексте программы по физической безопасности, совместимой с другими руководящими материалами МАГАТЭ и соответствующими промышленными стандартами.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

1.2. ЦЕЛЬ

1.2.1. Цели физической ядерной безопасности и компьютерной безопасности

При обеспечении физической ядерной безопасности основное внимание уделяется мерам по предупреждению, обнаружению и реагированию, применяемым в сфере противодействия преступным или преднамеренным несанкционированным действиям, совершаемым в отношении *ядерного материала, других радиоактивных материалов, связанных с ними установок или связанной с ними деятельности* или направленным на них, и другим намеренным действиям, которые могли бы прямо или косвенно привести к вредным последствиям для людей, имущества, общества или окружающей среды.

Компьютерная безопасность играет все более важную роль в обеспечении достижения этих целей. Поэтому в настоящей публикации рассматривается создание и совершенствование программ по защите компьютерных систем, сетей и других цифровых систем, критически важных для безопасной и надежной эксплуатации установки и для предотвращения хищений, саботажа и других злоумышленных действий.

Все другие системы, необходимые для эксплуатации установки, или любая вспомогательная или бизнес-система, несанкционированная модификация или изменение которой может поставить под угрозу состояние средств обеспечения безопасности или работоспособность, будут охвачены путем распространения положений данной публикации на эти системы.

В этом контексте злоумышленные действия, совершаемые в отношении компьютерных систем и затрагивающие физическую ядерную безопасность, могут быть классифицированы следующим образом:

— атаки для сбора информации, совершаемые с целью планирования и выполнения дальнейших злоумышленных действий;
— атаки, направленные на отключение или ухудшение работы одного или нескольких компьютеров, критически важных для физической безопасности или безопасности установки;
— нарушение нормальной работы одного или нескольких компьютеров в сочетании с другими параллельными режимами атаки, такими как физическое вторжение в заданные места.

Цели компьютерной безопасности обычно определяют как защиту характеристик конфиденциальности, целостности и доступности электронных данных или готовности компьютерных систем и процессов. Идентифицируя и

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

защищая те атрибуты данных или систем, которые могут оказывать неблагоприятное воздействие на функции безопасности и физической безопасности на ядерных установках, можно добиться достижения целей безопасности.

1.2.2. Сфера применения

Основная цель настоящей публикации состоит в том, чтобы добиться понимания важности обеспечения компьютерной безопасности как основополагающей части общего плана по физической безопасности ядерных установок.

Еще одной целью данной публикации является предоставление специфических для ядерных установок руководящих материалов по осуществлению программы компьютерной безопасности. Это достигается посредством представления определенных предлагаемых подходов, структур и процедур осуществления, разработанных для ядерных установок. В совокупности они являются критически важными для достижения и поддержания уровня защиты, определенного в стратегии физической безопасности площадки, и обеспечения соответствия национальным целям физической ядерной безопасности.

Целью настоящего справочного руководства является также предоставление рекомендаций относительно оценки существующих программ, анализа критически важных цифровых активов и определения соответствующих мер по уменьшению риска.

1.3. УСЛОВИЯ, СПЕЦИФИЧЕСКИЕ ДЛЯ ЯДЕРНЫХ УСТАНОВОК

Необходимость наличия руководящих материалов по компьютерной безопасности на ядерных установках подкрепляется особыми условиями, характеризующими данную отрасль промышленности. Ниже перечислены некоторые из этих условий, которые будут полностью рассмотрены в настоящей публикации:

— на ядерных установках должны соблюдаться установленные национальными регулирующими органами требования, которые могут прямо или косвенно регламентировать компьютерные системы или содержать руководящие материалы;
— на ядерных установках может оказаться необходимой защита от дополнительных угроз, которые обычно не рассматриваются в других отраслях промышленности; Такие угрозы могут также возникать ввиду

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

того, что ядерная промышленность связана с чувствительной информацией;
— требования компьютерной безопасности на ядерных установках могут отличаться от требований на других предприятиях. При обычной производственной деятельности подлежат соблюдению требования лишь в ограниченном диапазоне. На ядерных установках необходимо принимать во внимание более широкую основу или совершенно иной набор соображений, чем, например, те, которые рассматриваются в сферах электронной коммерции, банковского дела или даже военных применений. Эти различия подробно изложены и объяснены в разделе 7.

1.4. СТРУКТУРА

Руководящие материалы в настоящей публикации предназначены для широкой аудитории, которая включает лиц, определяющих политику, сотрудников органов, занимающихся регулированием физической ядерной безопасности, руководящих работников установок, персонал, обязанности которого связаны с физической безопасностью, технический персонал, поставщиков и подрядчиков. Они применимы ко всем стадиям жизненного цикла систем установок, включая проектирование, разработку, эксплуатацию и обслуживание.

Настоящая публикация состоит из двух частей:

— часть I (разделы 2–4) разработана с целью оказания поддержки менеджерам при принятии ими сбалансированных заключений и обоснованных решений относительно политики, проектирования и менеджмента компьютерной безопасности на установках. Она содержит руководящие материалы, касающиеся регулирующих и административных положений по компьютерной безопасности;
— часть II (разделы 5–7) содержит технические и административные руководящие материалы по осуществлению всеобъемлющего плана обеспечения компьютерной безопасности.

1.5. МЕТОДОЛОГИЯ

Основная методология, используемая для обеспечения компьютерной безопасности, подобна методологиям, используемым для обеспечения физической ядерной безопасности и ядерной безопасности. Этим подчеркиваются необходимость и преимущество включения вопросов

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

компьютерной безопасности во всеобъемлющие планы обеспечения физической безопасности установки с самого начала.

Успешная защита компьютерных систем может быть обеспечена посредством адаптации методов и инструментальных средств образцовой практики, разработанных в рамках более широкого сообщества, занимающегося вопросами компьютерной безопасности, с учетом в то же время специфики ядерной промышленности.

Изложенный ниже логический процесс, подробно описанный в разделе 5, показывает, как может разрабатываться, осуществляться, поддерживаться и совершенствоваться компьютерная безопасность на ядерной установке:

— выполнять национальные юридические и регулирующие требования;
— изучить соответствующие руководящие материалы МАГАТЭ и другие международные руководящие материалы;
— обеспечить поддержку со стороны старшего руководства и наличие надлежащих ресурсов;
— определить периметр компьютерной безопасности;
— выявить взаимодействия между компьютерной безопасностью и эксплуатацией установки, ядерной безопасностью и другими аспектами физической безопасности площадки;
— разработать политику обеспечения компьютерной безопасности;
— выполнить оценку риска;
— выбрать, разработать и осуществить защитные меры компьютерной безопасности;
— интегрировать компьютерную безопасность в систему менеджмента установки;
— регулярно проводить аудит, рассмотрение и совершенствование системы.

В настоящей публикации будут более подробно рассмотрены те этапы методологии, в отношении которых существуют специфические положения для ядерных установок. Другие этапы методологии компьютерной безопасности могут быть осуществлены посредством прямых ссылок на существующие национальные и международные стандарты (см. справочные материалы в конце настоящей публикации).

1.6. ОСНОВНАЯ ТЕРМИНОЛОГИЯ

Поскольку в различных сообществах, осуществляющих практическую деятельность, термины могут иметь неодинаковые значения, в данном разделе

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

разъяснены значения некоторых важных терминов, используемых в настоящей публикации.

В контексте данной публикации **компьютеры** и **компьютерные системы** означают вычислительные, коммуникационные устройства, контрольно-измерительную аппаратуру и устройства управления, являющиеся функциональными элементами ядерной установки. К ним относятся не только настольные компьютеры, большие вычислительные системы, серверы, сетевые устройства, но также и компоненты более низкого уровня, такие как встраиваемые системы и ПЛК (программируемые логические контроллеры). По существу настоящая публикация затрагивает все компоненты, которые могут быть подвержены вредному электронному воздействию.

В настоящей публикации термин **компьютерная безопасность** будет использоваться для описания безопасности всех компьютеров, определенных выше, и всех взаимосвязанных систем и сетей, образованных суммой элементов. Термины **безопасность ИТ** (информационных технологий) и **кибербезопасность** для целей настоящей публикации считаются синонимами компьютерной безопасности и не будут использоваться в данной публикации.

Компьютерная безопасность, определенная здесь, является подмножеством понятия **информационная безопасность** (определенного, например, в документе ИСО/МЭК 27000 [1]), и у них являются общими многие цели, методология и терминология.

Определения других терминов, используемых в данной публикации, приведены в конце настоящего руководства.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Часть I

РУКОВОДСТВО ДЛЯ МЕНЕДЖМЕНТА

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

2. СООБРАЖЕНИЯ, СВЯЗАННЫЕ С РЕГУЛИРОВАНИЕМ И МЕНЕДЖМЕНТОМ

В данном разделе приведены сведения об основных компонентах структуры высокого уровня для обеспечения компьютерной безопасности на ядерных установках. В частности, в нем рассмотрены вопросы, имеющие отношение к законодательным и регулирующим органам, а также к менеджменту установок и стратегии обеспечения безопасности. На рис. 1 показана в наглядном упрощенном виде иерархия нормативных документов, имеющих отношение к учреждению и выполнению программы компьютерной безопасности на ядерной установке.

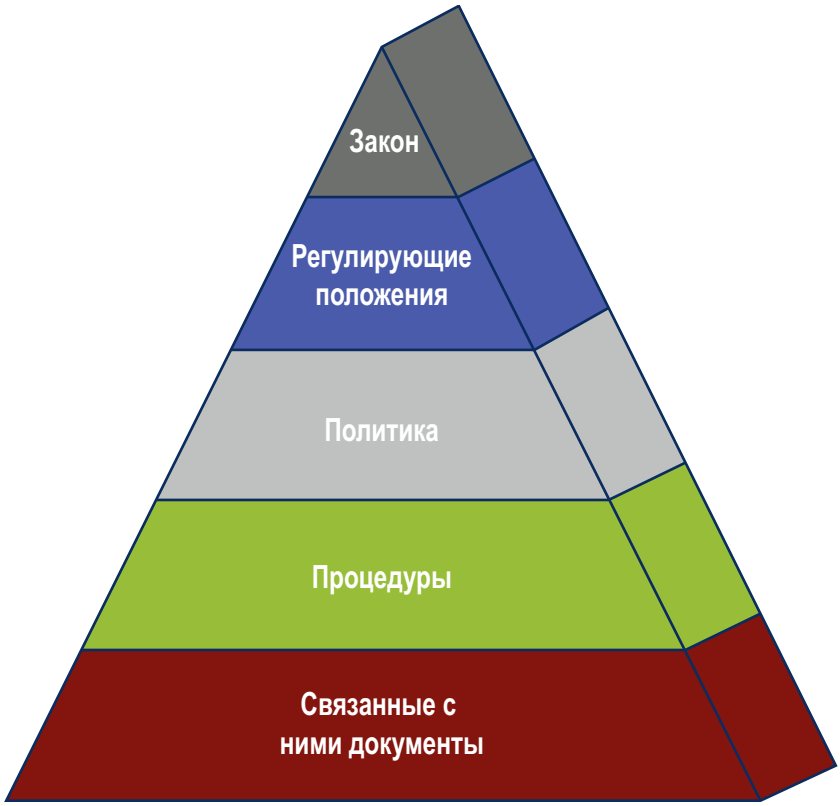


РИС. 1. Соответствующие нормативные документы.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

2.1. СООБРАЖЕНИЯ ЗАКОНОДАТЕЛЬНОГО ХАРАКТЕРА

Ключевая роль государства заключается в создании правовой основы для физической ядерной безопасности, а также для компьютерной безопасности в целом. При надлежащем осуществлении они оказывают значительное влияние на безопасность и физическую безопасность ядерных установок. Следует предусматривать, чтобы государственная юридическая система, по крайней мере, обеспечивала законодательную и регулирующую основу, охватывающую защиту чувствительной информации и распространяющуюся на любой вид деятельности, которая могла бы способствовать нарушениям физической ядерной безопасности.

Вследствие специфики ее проблем, компьютерная безопасность, возможно, нуждается в специальных законодательных положениях, позволяющих учитывать уникальный характер преступлений и режимов работы, связанных с компьютерными системами. Государствам следует тщательно рассматривать вопрос о том, охватывает ли их нынешнее законодательство надлежащим образом злоумышленные действия, которые могут быть совершены при помощи компьютеров. Наряду с прочим, к важным законам, которые могут повлиять на компьютерную безопасность и ее осуществление, относятся:

— законы о компьютерных преступлениях;
— законы о терроризме;
— законы о защите критической национальной инфраструктуры;
— законы, требующие раскрытия информации;
— законы о конфиденциальности и обращении с личными данными.

Важно, чтобы государственное законодательство постоянно пересматривалось и обновлялось таким образом, чтобы оно включало положения относительно новых и появляющихся видов преступной деятельности и других потенциальных угроз компьютерной безопасности.

Ввиду характера компьютерных сетей существует возможность того, что нарушители будут осуществлять злоумышленные действия в пределах государства, находясь вне его физических границ и потому будучи потенциально недосягаемы для государственной юридической системы. Во время подготовки настоящей публикации единственным актуальным международным договорно-правовым документом, посвященным регулированию международного сотрудничества в противодействии компьютерным преступлениям, являлась Конвенция о киберпреступности Совета Европы [6].

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

2.2. СООБРАЖЕНИЯ, СВЯЗАННЫЕ С РЕГУЛИРОВАНИЕМ

Регулирующему органу при осуществлении руководства следует принимать во внимание актуальное законодательство и предоставлять операторам инструментальные средства и способы для правильного толкования и выполнения юридических обязательств. Регулирующие органы могут также выбирать или указывать соответствующие эталонные руководящие материалы, такие как стандарты ИСО (Международной организации по стандартизации) или публикации МАГАТЭ.

Следует обеспечивать, чтобы при осуществлении деятельности регулирующих органов в сфере компьютерной безопасности четко признавалась цель защиты от хищения ядерного материала и от саботажа, приводящего к возможному радиоактивному выбросу. Поэтому при подготовке регулирующих положений по компьютерной безопасности следует также принимать во внимание регулирующие положения по физической ядерной безопасности и ядерной безопасности.

Желательно, что государственные регулирующие органы (в тех случаях, когда имеется более одного органа) сотрудничали между собой с целью достижения согласованности мнений относительно необходимых требований, которые будут введены.

Государственные регулирующие органы могут, как минимум, выпустить на высоком уровне заявление относительно регулирующих требований в сфере компьютерной безопасности. Более детализированные регулирующие требования могут также включать положения относительно:

— приверженности руководства обеспечению компьютерной безопасности (раздел 4);
— ответственности за программу по компьютерной безопасности, включая указание ролей сотрудника(ов) и группы(групп) по компьютерной безопасности (раздел 4);
— политики в сфере компьютерной безопасности, плана реализации и плана по обеспечению выполнения требований (раздел 5), включая:
  • установление периметра компьютерной безопасности;
  • определение рисков;
  • стратегию управления рисками;
  • программу по обучению и улучшению информированности в сфере компьютерной безопасности;
  • план бесперебойной эксплуатации;
— процесса аудита и рассмотрения - внутреннего, внешнего или осуществляемого непосредственно регулирующими органами.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

В требованиях не следует предписывать детальные технические решения, поскольку вследствие технического прогресса они могут быстро устаревать. Вместо этого требования могут концентрироваться на ожидаемых результатах, поскольку они могут быть изложены таким образом, чтобы они в меньшей степени зависели от технологии.

От установок может потребоваться продемонстрировать соответствие национальным требованиям физической безопасности в виде одобренного общего плана по физической безопасности площадки (ПФБП) или любого эквивалентного комплекта документов. **Государственным регулирующим органам следует выпускать требования к компьютерной безопасности в качестве части требований к ПФБП**.

2.3. ОСНОВА ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ПЛОЩАДКИ

Обеспечение физической безопасности площадки связано прежде всего с обязанностью руководства, и в частности старшего руководства, обеспечивать выполнение в полном объеме законодательных и регулирующих требований посредством осуществления ПФБП.

Все аспекты физической безопасности (в том числе кадровые, физические, информационные и компьютерные) взаимодействуют между собой и дополняют друг друга, формируя совокупность средств физической безопасности установки, которая может быть определена в ПФБП (см. рис. 2). Недостатки любого аспекта физической безопасности могут повлиять на другие области и приводить к дополнительным требованиям в отношении остальных аспектов физической безопасности. Компьютерная безопасность – это

РИС. 2. Взаимодействие различных областей физической безопасности.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

многопрофильная дисциплина, взаимодействующая со всеми другими областями физической безопасности на ядерной установке.

Все положения настоящей публикации следует осуществлять, постоянно учитывая более широкую основу ПФБП. Подобным же образом при разработке ПФБП следует с самого начала учитывать аспекты компьютерной безопасности.

Обязанностью руководства является также обеспечение надлежащей координации различных аспектов физической безопасности и интеграция компьютерной безопасности на соответствующем уровне.

2.3.1. Политика обеспечения компьютерной безопасности

Руководству следует осознавать, что компьютерная технология все более широко используется для реализации многих жизненно важных функций на ядерных установках. Это обстоятельство обусловливает многочисленные выгоды в плане эксплуатационной безопасности и эффективности. Вместе с тем, для того, чтобы обеспечить надлежащие функциональные возможности компьютерной системы, необходимо предусматривать адекватные и сбалансированные барьеры безопасности, обеспечивающие максимальную защиту от злоумышленных действий и в то же время излишне не препятствующие работе системы.

Поэтому на всех ядерных установках следует иметь политику обеспечения компьютерной безопасности, утвержденную и проводимую самым старшим руководителем на площадке. Эта политика определяет общие цели компьютерной безопасности на установке.

Следует обеспечивать, чтобы политика обеспечения компьютерной безопасности являлась частью общей политики обеспечения физической безопасности площадки и была согласована и скоординирована с другими соответствующими обязанностями в области физической безопасности. При разработке политики обеспечения компьютерной безопасности следует также учитывать ее влияние на юридические и человеческие ресурсы.

Политика обеспечения компьютерной безопасности и связанный с ней план обсуждены более детально в разделе 5.

2.3.2. Компьютерные системы на ядерных установках

С точки зрения требований к архитектуре, конфигурации или характеристикам, к компьютерным системам и сетям, поддерживающим функционирование ядерной установки, относятся многие нестандартные компьютерные системы на основе информационных технологий (ИТ). Эти системы могут включать специализированные промышленные системы

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

управления (ПСУ), системы контроля доступа, системы аварийной сигнализации и слежения и информационные системы, имеющие отношение к безопасности и физической безопасности и аварийному реагированию. Хотя эволюция ПСУ происходила от строго специализированных решений к более широкому использованию общепринятой архитектуры вычислительных систем, между ПСУ и стандартными системами на базе ИТ все еще имеются существенные различия, которые нужно учитывать при подготовке плана по физической безопасности площадки. Полное обсуждение уникального характера компьютерных систем, связанных с ядерными установками, приведено в разделе 7.

2.3.3. Глубокоэшелонированная защита

В требованиях к защите следует отразить концепцию нескольких эшелонов и методов защиты (конструкционных, технических, кадровых и организационных), которые требуется преодолеть или обойти нарушителям для достижения своих целей.

Главным средством предотвращения и смягчения последствий нарушений безопасности является "глубокоэшелонированная защита". Глубокоэшелонированная защита обеспечивается прежде всего за счет сочетания ряда последовательных и независимых уровней защиты, только после отказа или выхода из строя которых компьютерная система может подвергнуться вредному воздействию. Если происходит отказ одного уровня защиты или преодоление одного барьера, имеются последующие уровень или барьер. При надлежащей организации глубокоэшелонированная защита обеспечивает, что ни один одиночный технический, человеческий или организационный отказ не может привести к вредному воздействию на компьютерную систему и что сочетания отказов, способные привести к компьютерному инциденту, весьма маловероятны. Независимая эффективность разных уровней защиты – это необходимый элемент глубокоэшелонированной защиты.

2.4. ОЦЕНКА ОБСТАНОВКИ В ПЛАНЕ УГРОЗЫ

Обстановка в плане угроз компьютерной безопасности представляет собой быстро изменяющийся, развивающийся сценарий. В то время как хорошая программа обеспечения компьютерной безопасности будет обеспечивать ее собственную устойчивость, имеющиеся специальные средства противодействия наиболее распространенным угрозам, существующим в настоящее время, не гарантируют защиты от завтрашних угроз.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Ответственному государственному компетентному органу следует периодически проводить оценку угроз, включая угрозы безопасности компьютерных систем и информации по актуальным векторам атаки, связанным с безопасностью компьютерных систем, используемых на ядерных установках. Типичным инструментальным средством, используемым для определения уровней угрозы и в качестве основы для разработки средств обеспечения безопасности, является проектная угроза (ПУ, см. раздел 6.3.1).

Крайне важно, чтобы на установках постоянно проводилась активная и текущая оценка угрозы, результаты которой регулярно доводились бы до сведения руководства и эксплуатационного персонала.

В разделе 6 содержится детальное, но не исчерпывающее описание потенциальных источников атак и связанных с ними механизмов атаки применительно к ядерным установкам, а также методологий, используемых для оценки и идентификации угроз.

3. СИСТЕМЫ МЕНЕДЖМЕНТА

Система менеджмента несет ответственность за установление политики и целей и обеспечение возможности эффективного и результативного достижения этих целей. Системы менеджмента являются жизненно важным элементом поддержки культуры физической ядерной безопасности. Многими видами деятельности на ядерных установках управляют системы менеджмента. В идеальном случае они объединяют элементы физической безопасности, безопасности, охраны здоровья, экологические, качественные и экономические элементы в единое инструментальное средство управления или комплекс интегрированных и взаимно укрепляющих систем [7, 8].

Системы менеджмента должны подвергаться рассмотрению с целью обеспечения их полноты и соответствия политике обеспечения физической безопасности площадки. В более широком плане системы менеджмента являются по своей природе динамическими и должны адаптироваться к изменяющимся условиям на установке и в окружающей среде; они не могут быть осуществлены в качестве одноразовой меры, но нуждаются в непрерывной оценке и совершенствовании. Рис. 3 иллюстрирует жизненный цикл процессов менеджмента.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

РИС. 3. Жизненный цикл менеджмента безопасности.

Цель настоящего раздела - дополнить существующие руководящие материалы по системам менеджмента необходимыми подробными сведениями для менеджмента компьютерной безопасности. Ключевыми элементами, которые следует рассматривать или добавлять с целью интеграции необходимых положений по компьютерной безопасности, являются:

— идентификация и классификация информационных активов;
— формальный анализ риска;
— соблюдение законодательных и регулирующих требований;
— эксплуатационные требования предприятия;
— требования к компетентности ключевых работников;

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

— обеспечение устойчивости функционирования;
— управление доступом с использованием логических средств;
— безопасность жизненного цикла системы;
— управление конфигурацией;
— изменение и утверждение мер компьютерной безопасности;
— реализация установленных мер компьютерной безопасности;
— принятие осуществленных мер компьютерной безопасности;
— соблюдение утвержденных мер компьютерной безопасности;
— незамедлительный анализ инцидентов компьютерной безопасности и соответствующее информирование;
— регулярная отчетность о соблюдении требований;
— регулярные рассмотрения осуществленных мер безопасности (аудиты) силами внутренних и внешних экспертов;
— обучение с целью улучшения информированности;
— новые риски и изменения в выявленных рисках;
— изменения законодательных и регулирующих требований;
— среднесрочные планы обеспечения информационной безопасности.

Вышеуказанные процессы следует рассматривать как постоянно выполняемую деятельность, осуществляемую на всех этапах жизненного цикла системы. Специфические особенности реализации следует детально изложить в плане обеспечения компьютерной безопасности, обсужденном в разделе 5.

4. ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ

4.1. ПОЛНОМОЧИЯ И ОБЯЗАННОСТИ

В следующих ниже разделах подробно изложены минимальные требования к руководящим работникам и штату специалистов, необходимых для успешной организации и поддержания программы компьютерной безопасности.

4.1.1. Руководство

Старшее руководство установки организует работы по обеспечению компьютерной безопасности путем создания надлежащей организации, занимающейся вопросами разработки и поддержки. С этой целью руководству следует:

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

— принять на себя общую ответственность за все аспекты компьютерной безопасности;
— определить цели физической безопасности установки;
— обеспечить соблюдение законов и регулирующих положений;
— установить приемлемый уровень риска для установки;
— распределить в организации обязанности по обеспечению компьютерной безопасности;
— обеспечить надлежащую связь между различными аспектами физической безопасности;
— обеспечить введение осуществимой политики обеспечения компьютерной безопасности;
— предоставить надлежащие ресурсы для осуществления жизнеспособной программы обеспечения компьютерной безопасности;
— обеспечить проведение периодических аудитов и обновлений политики и процедур компьютерной безопасности;
— обеспечить поддержку программ обучения и информирования.

Обычно осуществление постоянного процесса обеспечения компьютерной безопасности поручают специалистам организации.

4.1.2. Сотрудник по компьютерной безопасности

Компьютерная безопасность связана почти со всеми видами деятельности на установке. Поэтому важно поручить общий надзор за обеспечением компьютерной безопасности одному четко определенному органу. В настоящей публикации используется название должности «сотрудник по компьютерной безопасности» (СКБ); в других случаях эта функция может называться «сотрудник по безопасности ИТ» или «сотрудник по информационной безопасности», или же ее выполнение может быть связано с рядом других обязанностей. Какой бы подход ни использовался, следует обеспечивать четкую координацию этой функции на установке; кроме того, она должна быть независима от подразделений, занимающихся осуществлением, и для нее следует предусмотреть четкие и доступные линии отчетности перед старшим руководством.

СКБ должен обладать глубокими знаниями в области компьютерной безопасности и хорошо знать другие аспекты физической безопасности на ядерных установках. Дальнейшие требования включают знание ядерной безопасности и управления проектами и способность объединять специалистов по различным дисциплинам в эффективную группу.

Типичные обязанности СКБ или эквивалентного сотрудника включают:

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— предоставление руководству компании консультаций по компьютерной безопасности;
— руководство группой компьютерной безопасности;
— координация и управление развитием деятельности по компьютерной безопасности (например, осуществление связанных с безопасностью политики, директив, процедур, руководящих принципов, мер);
— координация с физической безопасностью и другими дисциплинами, связанными с физической безопасностью и безопасностью с целью планирования мер безопасности и реагирования на инциденты, связанные с безопасностью;
— определение систем на установке, критических с точки зрения компьютерной безопасности (то есть, базиса компьютерной безопасности). Владельцев активов следует проинформировать относительно роли их оборудования в обеспечении компьютерной безопасности;
— проведение периодических оценок риска для компьютерной безопасности;
— проведение периодических инспекций, аудитов и рассмотрений базиса компьютерной безопасности и предоставление докладов о положении дел высшему руководству;
— разработка и осуществление обучения и оценки в области компьютерной безопасности;
— организация реагирования и руководство реагированием на инциденты в случае соответствующих связанных с компьютерной безопасностью аварийных ситуаций, включая координацию с соответствующими внутренними и внешними организациями;
— исследование инцидентов, связанных с компьютерной безопасностью, и разработка процедур действий после инцидентов и профилактических мер;
— участие в инициативах по оценке физической безопасности площадки;
— участие в анализе требований при приобретении/разработке новых систем.

4.1.3. Группа компьютерной безопасности

Весьма важно, чтобы СКБ имел доступ к соответствующим межотраслевым экспертным знаниям, связанным с компьютерной безопасностью, безопасностью установки и эксплуатацией установки, а также физической безопасностью и безопасностью персонала. Источником таких знаний может быть специализированная группа компьютерной безопасности или специальный доступ к конкретным экспертным знаниям в организации.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Цель этой группы состоит в том, чтобы оказывать СКБ поддержку в выполнении его/ее обязанностей.

4.1.4. Другие обязанности руководства

Руководящие работники различного уровня в организации должны обеспечивать надлежащий уровень компьютерной безопасности в областях своей ответственности. Типичные обязанности включают:

- работу с соблюдением руководящих материалов плана обеспечения компьютерной безопасности на площадке;
- предоставление СКБ эксплуатационных требований и ответных замечаний по вопросам компьютерной безопасности и урегулирование потенциальных конфликтов между эксплуатационными требованиями и требованиями, связанными с физической безопасностью и безопасностью;
- уведомление СКБ о любых условиях, которые могут приводить к изменениям в средствах обеспечения компьютерной безопасности, таких как изменения персонала, изменения оборудования или изменения процессов;
- обеспечение надлежащего обучения и инструктажа сотрудников по вопросам компьютерной безопасности, связанным с их обязанностями;
- обеспечение того, чтобы субподрядчики и сторонние поставщики, работающие на подразделение, занимающее заключением контрактов, действовали с учетом плана обеспечения физической безопасности площадки;
- отслеживание, мониторинг и информирование о событиях, имеющих отношение к безопасности;
- обеспечение соблюдения мер безопасности персонала.

4.1.5. Индивидуальные обязанности

Каждый сотрудник организации несет ответственность за выполнение плана обеспечения компьютерной безопасности. Конкретные обязанности включают:

- знание базовых процедур обеспечения компьютерной безопасности;
- знание процедур обеспечения компьютерной безопасности для конкретного рабочего места;
- работу в пределах параметров, задаваемых политикой компьютерной безопасности;

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— уведомление руководства о любых изменениях, которые могут привести к сокращению средств обеспечения компьютерной безопасности;
— уведомление руководства о любых инцидентах или возможных инцидентах, приводящих к ухудшению компьютерной безопасности;
— посещение на регулярной основе курсов начальной подготовки и переподготовки по безопасности.

4.2. КУЛЬТУРА КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Высокая культура компьютерной безопасности является существенным компонентом любого эффективного плана обеспечения безопасности. Важно, чтобы руководство обеспечивало полную интеграцию информированности о компьютерной безопасности в общую культуру физической безопасности площадки. Характеристиками культуры физической ядерной безопасности являются мнения, отношения, поведение и системы менеджмента, которые в совокупности приводят к более эффективной программе физической ядерной безопасности. В основе культуры физической ядерной безопасности лежит понимание теми, кто выполняет функции регулирования, управления или эксплуатации ядерных установок или деятельности, или даже теми, кого может затрагивать эта деятельность, существования реальной угрозы и важности физической ядерной безопасности. (Более подробная информация о культуре физической ядерной безопасности содержится в [9].) Культура компьютерной безопасности является частью общей культуры физической безопасности и основана на применении вышеупомянутых характеристик к сфере информированности о компьютерной безопасности.

Опыт показывает, что большинство инцидентов компьютерной безопасности связаны с действиями людей и что безопасность любой компьютерной системы в значительной степени зависит от поведения всех ее пользователей. В приложении III приведены примеры ошибок человека, которые могут приводить к снижению безопасности. Культура компьютерной безопасности развивается посредством осуществления многих видов деятельности, направленных на информирование персонала и улучшение понимания вопросов компьютерной безопасности (например, с помощью плакатов, напоминаний, обсуждений с руководством, обучения, проведения тестов и т.п.). Атрибуты культуры компьютерной безопасности следует периодически измерять, рассматривать и постоянно улучшать. Для оценки культуры компьютерной безопасности в организации могут использоваться приведенные ниже показатели:

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

— требования компьютерной безопасности четко документированы и хорошо понимаются персоналом;
— существуют ясные и эффективные процессы и протоколы эксплуатации компьютерных систем в рамках организации и за ее пределами;
— сотрудники понимают и сознают важность соблюдения мер контроля в рамках программы компьютерной безопасности;
— обслуживание компьютерных систем обеспечивает их защиту и эксплуатацию в соответствии с базовыми принципами и процедурами компьютерной безопасности;
— руководство полностью привержено осуществлению инициатив в области безопасности и поддерживает их.

4.2.1. Программа обучения в области компьютерной безопасности

Высококачественная программа обучения является одним из краеугольных камней культуры компьютерной безопасности. Крайне важно путем обучения убедить персонал, подрядчиков и сторонних поставщиков в важности соблюдения процедур безопасности и поддержания культуры безопасности.

Программа улучшения информированности должна включать следующие требования:

— необходимым условием доступа к компьютерным системам должно быть успешное завершение обучения в области компьютерной безопасности и/или программы улучшения информированности; характер обучения должен соответствовать уровням безопасности системы и ожидаемой роли пользователей;
— сотрудники, выполняющие важные обязанности по обеспечению безопасности (например, СКБ, группа компьютерной безопасности, руководители проектов, администраторы ИТ), должны проходить обучение повышенного уровня/получать повышенную квалификацию;
— обучение всего персонала следует периодически повторять с целью учета новых процедур и появляющихся угроз;
— от сотрудников следует требовать подтверждения того, что они понимают свои обязанности в области безопасности.

Программа обучения должна включать показатели, позволяющие оценить понимание вопросов компьютерной безопасности, эффективность обучения и процессы постоянного совершенствования или переподготовки кадров.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Часть II

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

5. РЕАЛИЗАЦИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

В настоящей публикации не устанавливаются минимальные стандарты приемлемого риска или определенный набор мер по смягчению последствий, которые могли бы использоваться. Любой набор конкретных стандартов быстро устарел бы ввиду изменения цифровых систем, появления новых угроз, разработки новых инструментальных средств смягчения последствий и изменения регулирующих требований. В части II настоящей публикации основное внимание уделяется представлению комплекса методологических и конкретных рекомендаций в поддержку и для руководства реализацией компьютерной безопасности на ядерных установках.

Эти рекомендации не являются директивными или окончательными, и их следует использовать в качестве руководящих материалов; в соответствующих случаях для обеспечения требуемой глубокоэшелонированной защиты и достижения других фундаментальных целей физической ядерной безопасности могут приниматься альтернативные меры [10–12].

5.1. ПЛАН И ПОЛИТИКА ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

5.1.1. Политика обеспечения компьютерной безопасности

Как указано в разделе 2.3.1, политика обеспечения компьютерной безопасности устанавливает в организации цели компьютерной безопасности высокого уровня. Эта политика должна соответствовать надлежащим регулирующим требованиям. Требования политики обеспечения компьютерной безопасности следует детально изложить в документах более низкого уровня, которые будут использоваться при осуществлении и контроле этой политики. Кроме того, эта политика должна быть:

— осуществимой;
— достижимой;
— допускающей аудит.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

5.1.2. План обеспечения компьютерной безопасности

План обеспечения компьютерной безопасности (ПОКБ) разрабатывается с целью осуществления этой политики в форме организационных ролей, обязанностей и процедур. В данном плане определяются и детально описываются средства достижения целей компьютерной безопасности на установке, и он является частью общего ПФБП (или связан с ним).

В плане должны быть изложены основные действия в терминах восприимчивости к уязвимостям, защитных мер, анализа последствий и мер по смягчению последствий с целью установления и сохранения на приемлемом уровне кибер-риска на ядерной установке и содействия возвращению в безопасный эксплуатационный режим.

5.1.3. Элементы ПОКБ

Каждый индивидуальный элемент плана нацелен на достижение конкретных целей и решение определенных задач в соответствии с установленной политикой обеспечения компьютерной безопасности. Минимальное содержание и разбивка по пунктам ПОКБ предлагаются в следующих ниже подразделах:

a) Организация и обязанности:
   1) организационные схемы;
   2) ответственные лица и обязанности по отчетности;
   3) процесс периодического рассмотрения и утверждения.

b) Управление активами:
   1) список всех компьютерных систем;
   2) список всех программ, установленных на компьютерных системах;
   3) схема сети, включая все соединения с внешними компьютерными системами.

c) Оценка риска, уязвимости и соблюдения требований:
   1) периодичность рассмотрения и повторной оценки плана обеспечения безопасности;
   2) самооценка (включая процедуры тестов на возможность проникновения в систему);
   3) процедуры аудита и выявления и устранения недостатков;
   4) соблюдение регулирующих и законодательных требований.

d) Проектирование с учетом требований безопасности и управление конфигурацией системы:
   1) основные принципы архитектуры и проектирования;
   2) требования, связанные с различными уровнями безопасности;

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

3) формализация требований компьютерной безопасности для поставщиков и производителей;
4) безопасность всего жизненного цикла системы;

e) Эксплуатационные процедуры обеспечения безопасности:
1) контроль доступа;
2) безопасность данных;
3) безопасность линий и каналов связи:
4) безопасность платформ и прикладных программ (например, усиление защиты);
5) мониторинг систем;
6) поддержание компьютерной безопасности;
7) действия в случае инцидентов;
8) обеспечение устойчивости функционирования;
9) резервное копирование системы.

f) Менеджмент персонала:
1) проверка;
2) обучение;
3) аттестация;
4) прекращение действия контракта/кадровый перевод.

Вышеизложенные данные составляют основу для разработки ПОКБ. В дополнение к этой основе имеются многочисленные справочные материалы, причем основными международными справочными материалами служат документы ИСО/МЭК 27001 [2] для систем менеджмента информационной безопасности и ИСО/МЭК 27002 [3] для рекомендаций по практической реализации.

В то время как большинство перечисленных выше элементов единообразно в планах обеспечения компьютерной безопасности для любых видов деятельности или отраслей промышленности, существуют определенные нюансы их практической реализации на ядерных установках. Эти элементы ПОКБ более подробно описаны в разделе 7. Вопросы оценки риска, уязвимостей и соблюдения требований изложены в разделе 6. Анализ активов более детально рассматривается в разделе 5.3.

5.2. ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ОБЛАСТЯМИ БЕЗОПАСНОСТИ

Как указано в разделе 2.3, функционирование и поддержание ПОКБ следует обеспечивать в рамках структуры общего плана защиты установки. План обеспечения компьютерной безопасности для конкретной установки следует разрабатывать в тесных консультациях со специалистами по

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

физической защите, безопасности, эксплуатации и ИТ. ПОКБ должен регулярно рассматриваться и обновляться, с тем чтобы он отражал связанные с безопасностью события в любой области безопасности и эксплуатационный опыт системы обеспечения физической безопасности площадки.

5.2.1. Физическая безопасность

План обеспечения физической безопасности и ПОКБ должны дополнять друг друга. Для компьютеризированных активов существуют требования в отношении физического контроля доступа, и подобным же образом, ухудшение электронных характеристик может привести к деградации или потере определенных функций физической защиты. Сценарии атак вполне могут включать координацию как электронной, так и физической атаки. Группам, отвечающим за план обеспечения физической безопасности и ПОКБ, следует информировать друг друга и координировать свои усилия с целью обеспечения согласованности планов в процессе их разработки и рассмотрения.

5.2.2. Кадровая безопасность

Помимо информированности и обучения, весьма важными для обеспечения надежной компьютерной безопасности являются также и другие аспекты безопасности, обычно рассматриваемые в области кадровой безопасности. Необходимые положения относительно организации соответствующего уровня проверки, обязательств в отношении конфиденциальности, процедур завершения действия контрактов и определения требуемой профессиональной компетентности должны быть скоординированы между руководством по компьютерным вопросам и руководством по вопросам кадровой безопасности. В частности для персонала, исполняющего важные обязанности в области безопасности (системные администраторы, группа безопасности), может потребоваться проверка более высокого уровня.

5.3. АНАЛИЗ И МЕНЕДЖМЕНТ АКТИВОВ

Взаимодействие между компьютерными системами на ядерных установках может косвенным образом повлиять на безопасность. Поэтому важно, чтобы в плане обеспечения безопасности были **указаны все активы** и он включал **более полный инвентарный список тех активов, которые критически важны для функций физической безопасности и безопасности**

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

установки. В этот инвентарный список могут быть включены данные, компьютерные системы, их интерфейсы и их владельцы.

Удовлетворить вышеупомянутые потребности позволяет приведенная ниже методология:

a) следует проводить сбор актуальной информации об имеющихся компьютерных системах с целью создания полного списка активов;
b) следует определить взаимосвязь между выявленными активами;
c) следует определить и оценить их значимость для функций безопасности и выявленных систем безопасности, связанных с безопасностью систем и систем физической безопасности.

Важным необходимым условием для выполнения последующих шагов является завершение каждого предыдущего шага.

Всесторонний анализ компьютерных систем на ядерной установке включает:

- определение функций/задач и эксплуатационных режимов всех имеющихся компьютеризированных систем;
- определение имеющихся соединений, включая источники питания;
- анализ потоков данных с целью определения связанных между собой объектов, характера и назначения их связей;
- установление процедур, инициирующих связь, частоты связи и протоколов связи;
- определение местонахождения компьютерных систем и оборудования;
- анализ групп пользователей;
- установление прав собственности (для данных и компьютеризированных систем);
- соответствующий уровень безопасности (см. раздел 5.5, дифференцированный подход).

По-видимому, большая часть необходимой для анализа информации уже будет иметься в наличии, однако ее следует систематизировать и организовать. Источники актуальной информации включают системные спецификации и документацию.

5.4. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Как указано в разделе 1.6, в контексте данной публикации компьютеры и компьютерные системы означают вычислительные, коммуникационные устройства, контрольно-измерительную аппаратуру и устройства управления,

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

являющиеся функциональными элементами ядерной установки. Компьютерными функциями, представляющими основной интерес, являются процессы управления и обработки данных, связанные с безопасностью и физической безопасностью. Другие компьютерные функции могут представлять интерес в связи с поддержкой этих функций и возможным ухудшением безопасности вследствие вторичных или косвенных эффектов или воздействия на общую производительность установки.

Ниже представлен далеко не исчерпывающий список компьютерных систем, которые могут иметься на ядерных установках и иметь отношение к целям настоящих руководящих материалов. Они классифицированы отдельно согласно их важности с точки зрения безопасности и физической безопасности. Обе эти классификации следует принимать во внимание при определении соответствующего применимого уровня безопасности (раздел 5.5) и при анализе с целью оценки риска (раздел 6.2). Следует также иметь в виду, что некоторые функции явно перекрываются в плане актуальности с точки зрения безопасности и физической безопасности.

5.4.1. Важность для безопасности

В нормах безопасности МАГАТЭ (например, [13–15]) оборудование ядерных установок подразделено на категории согласно его функциям, как показано на рис. 4.

Оборудование станции

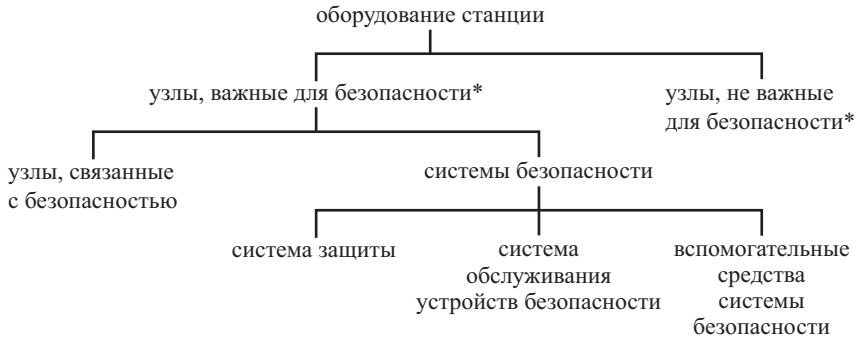
— Системы, важные для безопасности

• Системы безопасности

— системы защиты: контрольно-измерительные приборы и системы управления и защиты (КИП и СУЗ), которые используются для выполнения автоматически запускаемых действий по защите реактора и станции;
— системы обслуживания устройств безопасности: КИП и СУЗ, осуществляющие действия по обеспечению безопасности, инициированные системами защиты и ручными срабатываниями;
— вспомогательные средства системы безопасности: КИП и СУЗ для систем аварийного энергоснабжения.

• Системы, связанные с безопасностью

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).



*В данном контексте “узел” означает конструкцию, систему или элемент.

РИС. 4. Оборудование станции с точки зрения функций безопасности.

— системы управления технологическими процессами: КИП и СУЗ для управления работой станции;
— КИП и СУЗ в помещении щита управления, включая системы аварийной сигнализации;
— компьютерные системы управления технологическими процессами, осуществляющие сбор и подготовку информации для помещения щита управления;
— КИП и СУЗ для обращения с топливом и его хранения;
— противопожарные системы;
— системы контроля доступа;
— инфраструктура голосовой связи и передачи данных.

— Системы, не важные для безопасности

- Системы управления для функций, не важных для безопасности (например, обессоливания)

Следует учитывать также компьютерные системы, которые не обязательно входят в состав оборудования станции, но, тем не менее, могут воздействовать на безопасность.

Оборудование, не относящееся к технологическому оборудованию станции

— Средства автоматизации делопроизводства

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

- Системы допусков к работе и рабочих заданий: Системы, обеспечивающие координацию производственной деятельности с целью создания благоприятной рабочей обстановки.
- Инженерно-технические системы и системы обслуживания: системы, обеспечивающие выполнение детальных операций по эксплуатации станции, операций обслуживания и технической поддержки.
- Системы управления конфигурацией: системы, отслеживающие конфигурацию станции, включая модели, версии и части оборудования, установленные на ядерной установке.
- Системы управления документацией: системы, используемые для хранения и поиска информации о станции, например, чертежей, протоколов совещаний.
- Интранет: система, обеспечивающая доступ ко всей документации станции – как технической, так и административной – согласно принципу служебной необходимости. Доступ обычно предоставляется только в режиме считывания информации.

— Внешние каналы связи

- Электронная почта: система, используемая для обмена информацией с внешними партнерами.
- Открытый веб-сайт: Система, используемая для предоставления пользователям Интернета информации об установке.
- Дистанционный доступ/доступ третьих лиц: системы, разрешающие строго контролируемый доступ извне к определенным функциям на площадке.

5.4.2. Системы физической безопасности или системы, связанные с физической безопасностью

Устоявшейся классификации физической безопасности для систем физической безопасности, сопоставимой с классификацией безопасности, пока еще не существует. Тем не менее, введение такой классификации для систем установки должно быть важной частью анализа активов. Приведенный ниже список может оказать помощь в разработке такой классификации:

— Системы физического контроля доступа: системы, используемые для обеспечения того, чтобы только уполномоченные лица имели доступ в зоны площадки, соответствующие выполняемой ими функции;
— инфраструктура голосовой связи и передачи данных;

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— база данных о допуске к конфиденциальной информации: используется для обеспечения того, чтобы лица, имеющие соответствующий допуск к конфиденциальной информации, получали доступ к части площадки или к имеющейся на площадке информации;
— системы мониторинга и контроля охранной сигнализации: используются для контроля всей охранной сигнализации на площадке и в помощь при оценке тревожных сигналов;
— компоненты обеспечения безопасности компьютеров и сетей;
— системы учета и контроля ядерных материалов.

5.5. ДИФФЕРЕНЦИРОВАННЫЙ ПОДХОД К КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Безопасность компьютерных систем должна основываться на дифференцированном подходе, при котором меры безопасности применяются пропорционально потенциальным последствиям атаки. Одна из практических реализаций дифференцированного подхода заключается в разбиении компьютерных систем на *зоны*, причем дифференцированные принципы защиты применяются для каждой зоны на основе *уровня* требований физической безопасности, присвоенного этой зоне. Разбиение компьютерных систем на различные уровни и зоны должно основываться на их значимости для безопасности и физической безопасности (см. раздел 5.4). Тем не менее, **следует обеспечивать, чтобы в дифференцированном подходе учитывались и оказывали на него влияние результаты процесса оценки риска**.

5.5.1. Уровни физической безопасности

Уровни физической безопасности – это абстракция, определяющая степени защиты физической безопасности, требуемые для различных компьютерных систем на установке. Для каждого уровня при дифференцированном подходе потребуются различные наборы защитных мер, удовлетворяющие требования физической безопасности этого уровня. Некоторые защитные меры применяются ко всем компьютерным системам на всех уровнях, в то время как другие являются специфическими для определенного(ых) уровня(ей).

Модель уровня физической безопасности допускает более простое распределение защитных мер для различных компьютерных систем на основе категоризации системы (отнесения ее к определенному уровню) и определения набора защитных мер, соответствующих этому уровню.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Уровни и связанные с ними защитные меры должны быть надлежащим образом документированы в ПОКБ.

5.5.2. Зоны

Зоны – это логическое и физическое понятие, позволяющее группировать компьютерные системы для административного управления, коммуникации и применения защитных мер. Зональная модель позволяет объединять в группы для целей администрирования и применения защитных мер компьютеры, имеющие одинаковую или аналогичную важность для безопасной и надежной эксплуатации станции.

При применении зональной модели следует соблюдать следующие рекомендации:

— каждая зона включает системы, имеющие одинаковую или сопоставимую важность для физической безопасности и безопасности установки;
— системы, относящиеся к одной зоне, имеют аналогичные потребности в отношении защитных мер;
— различные компьютерные системы, принадлежащие одной зоне, образуют область надежной связи для внутренней коммуникации в пределах этой зоны;
— зональные границы требуют механизмов развязки для потоков данных на основе политики, зависящей от конкретной зоны;
— с целью улучшения конфигурации зоны могут быть разделены на субзоны.

Поскольку зоны состоят из систем с одинаковой или сопоставимой важностью для безопасности и физической безопасности установки, каждой зоне может быть присвоен уровень, указывающий защитные меры, подлежащие применению в отношении всех компьютерных систем в этой зоне. Однако связь между зонами и уровнями не взаимно однозначна; в тех случаях, когда для нескольких зон требуется одинаковая степень защиты, одинаковый уровень может быть присвоен нескольким зонам. Зоны отражают логическое и физическое группирование компьютерных систем, в то время как уровни представляют степень требуемой защиты.

Зональная модель должна быть надлежащим образом документирована в ПОКБ, включая краткий обзор всех компьютерных систем, всех соответствующих линий связи, всех зональных пересечений и всех внешних подключений.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

5.5.3. Пример применения модели уровней физической безопасности

Пример применения на различных уровнях мер физической безопасности представлен ниже. Он отражает только одну из возможных практических реализаций дифференцированного подхода; точный выбор уровней и связанных с ними важнейших мер физической безопасности следует варьировать в соответствии с рассматриваемой средой, спецификой установки и результатами специализированного анализа риска физической безопасности.

В данном примере практического осуществления:

— меры базового уровня следует применять в отношении всех компьютерных систем;
— как показано на рис. 5, уровни физической безопасности различны: от уровня 5 (необходима наименьшая защита) и до уровня 1 (необходима максимальная защита);
— меры, соответствующие каждому уровню, не являются совокупными (поэтому возможны повторения).

Базовый уровень

Для надлежащих систем и уровней следует применять указанные ниже меры базового уровня:

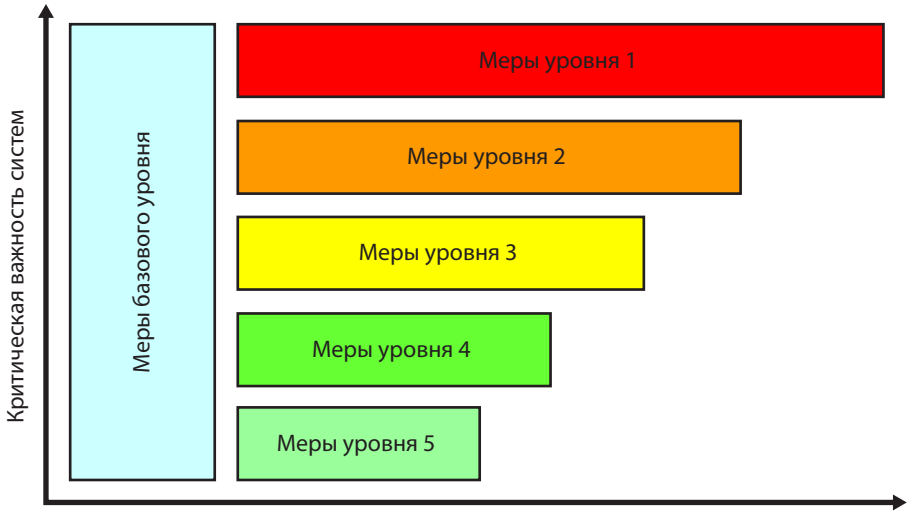


РИС. 5. Уровень физической безопасности/строгость мер.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

— для каждого уровня определяются политика и виды практической деятельности;
— эксплуатационные процедуры физической безопасности излагаются в письменном виде с целью ознакомления с ними всех пользователей;
— персонал, которому разрешен доступ к системе, должен иметь соответствующую квалификацию и опыт и в необходимых случаях должен иметь допуск к конфиденциальной информации;
— пользователям предоставляется доступ только к тем функциям и тем системам, которые им необходимы для выполнения рабочих заданий;
— осуществляются надлежащий контроль доступа и аутентификация пользователей;
— действуют системы или процедуры обнаружения аномалий;
— осуществляется мониторинг уязвимостей прикладных программ и систем, и принимаются соответствующие меры;
— периодически проводятся оценки уязвимости систем;
— сменные носители должны контролироваться в соответствии с эксплуатационными процедурами физической безопасности;
— следует строго соблюдать регламенты технического обслуживания компонентов, обеспечивающих безопасность компьютеров и сетей;
— строгая регистрация и мониторинг компонентов, обеспечивающих безопасность компьютеров и сетей (например, шлюзов безопасности, систем обнаружения проникновения, систем предотвращения проникновения, серверов виртуальных частных сетей (VPN)[1]);
— действуют надлежащие процедуры резервного копирования/восстановления;
— физический доступ к компонентам и системам ограничен в соответствии с их функциями.

Уровень 1

В дополнение к мерам базового уровня, защитные меры уровня 1 следует использовать для систем, например, систем защиты, которые являются жизненно важными для установки и требуют самого высокого уровня физической безопасности. Эти меры могут включать следующее:

[1] Частная виртуальная сеть (VPN) – это сеть, созданная с использованием средств связи с открытым доступом для соединения узлов, с применением шифрования и других механизмов физической безопасности для обеспечения того, чтобы доступ к сети имели только зарегистрированные пользователи и чтобы был невозможен перехват данных.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— не должно быть разрешено поступление в системы уровня 1 никаких сетевых потоков данных любого вида (например, подтверждений, сигнализации) от систем с более низкими уровнями физической безопасности. Должна быть возможной только строго исходящая коммуникация. Следует иметь в виду, что строго односторонняя коммуникация такого рода сама по себе не гарантирует надежности и целостности данных (можно рассмотреть возможность резервирования/исправления ошибок). Следует также учитывать, что это исключает любой вид протоколов «взаимной идентификации» (включая TCP/IP[2]), даже в случае контролируемых направлений подключения. Исключения крайне нежелательны и могут рассматриваться только строго в индивидуальном порядке и в том случае, если они подкреплены полным обоснованием и анализом риска физической безопасности[3];
— меры по обеспечению целостности и эксплуатационной готовности систем, как правило, разъясняются в обоснованиях безопасности;
— дистанционный доступ с целью обслуживания не допускается;
— физический доступ к системам строго контролируется;
— число сотрудников, которым предоставлен доступ к системам, ограничено до абсолютного минимума;
— в отношении любых утвержденных модификаций, производимых в компьютерных системах, применяется правило двух лиц;
— следует проводить регистрацию и мониторинг всех действий;
— каждый ввод данных в системы утверждается и проверяется на индивидуальной основе;
— в отношении любых модификаций, включая обслуживание аппаратных средств, обновления и модификации программного обеспечения, применяются строгие организационные и административные процедуры.

Уровень 2

В дополнение к мерам базового уровня, защитные меры уровня 2 следует использовать для систем, например, систем оперативного управления, которые требуют высокого уровня физической безопасности. Эти меры могут включать следующее:

[2] Протокол управления передачей/Межсетевой протокол — протоколы передачи данных.

[3] Некоторые государства-члены убеждены в том, что исключения недопустимы ни в коем случае.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— разрешается только исходящий, односторонний сетевой поток данных от систем уровня 2 к системам уровня 3. В противоположном (входящем) направлении могут приниматься только необходимые сообщения-подтверждения или сообщения о контролируемых сигналах (например, для TCP/IP);
— дистанционный доступ с целью обслуживания может разрешаться только на индивидуальной основе и в течение определенного рабочего периода. В случае использования он должен быть защищен с помощью эффективных мер, и пользователи должны соблюдать определенную (договорную) политику обеспечения физической безопасности;
— число сотрудников, которым предоставлен доступ к системам, сведено к минимуму, причем проводится четкое различие между пользователями и административным персоналом;
— физические соединения с системами следует строго контролировать;
— приняты все разумные меры по обеспечению целостности и готовности систем;
— оценка уязвимости, включающая воздействие на системы, может приводить к неустойчивости станции или технологического процесса и поэтому возможность ее проведения следует рассматривать только в случае использования испытательных стендов, запасных систем, во время заводских приемочных испытаний или длительных запланированных периодов простоя.

Уровень 3

В дополнение к мерам базового уровня, защитные меры уровня 3 следует использовать для систем диспетчерского управления в реальном времени, не требуемых для эксплуатации, например, систем диспетчерского управления технологическим процессом в реальном времени в помещении щита управления, характеризуемых средним уровнем серьезности различных киберугроз. Эти защитные меры могут включать следующее:

— доступ к Интернету из систем уровня 3 не разрешен;
— для ключевых ресурсов осуществляется мониторинг регистрации и контрольных следов;
— для защиты этого уровня от неконтролируемых информационных потоков из систем уровня 4 и обеспечения только определенной и ограниченной деятельности предусматриваются шлюзы безопасности;
— следует контролировать физические соединения с системами;
— дистанционный доступ с целью обслуживания разрешается на индивидуальной основе при условии, что он надежно контролируется;

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

удаленный компьютер и пользователь должны соблюдать определенную политику обеспечения физической безопасности, оговариваемую в контракте;
— доступные пользователям системные функции контролируются с помощью механизмов управления доступом и на основе принципа служебной необходимости. Любое исключение из этого принципа должно быть тщательно изучено и должна быть обеспечена защита с помощью других средств (например, физического доступа).

Уровень 4

В дополнение к мерам базового уровня, меры уровня 4 следует использовать для систем управления техническими данными, используемых для управления деятельностью по обслуживанию или эксплуатации, связанной с компонентами или системами, требуемыми технической спецификацией для эксплуатации (например, допуск к работе, рабочие заказы, контролируемый вывод из эксплуатации, управление документацией), характеризуемых умеренным уровнем серьезности различных киберугроз. Меры уровня 4 включают следующее:

— внесение модификаций в системы разрешается только утвержденным и квалифицированным пользователям;
— доступ к Интернету из систем уровня 4 может предоставляться пользователям при условии применения надлежащих защитных мер;
— для защиты этого уровня от неконтролируемых информационных потоков от внешних сетей компании или площадки и обеспечения определенной деятельности предусматриваются шлюзы безопасности, которые контролируются;
— следует контролировать физические соединения с системами;
— дистанционный доступ с целью обслуживания разрешается и контролируется; удаленный компьютер и пользователь должны соблюдать определенную политику обеспечения физической безопасности, оговариваемую в контракте и контролируемую;
— доступные пользователям системные функции контролируются с помощью механизмов контроля доступа. Любое исключение из этого принципа должно быть тщательно изучено и должна быть обеспечена защита с помощью других средств;
— дистанционный внешний доступ разрешен для утвержденных пользователей при условии функционирования надлежащих механизмов контроля доступа.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Уровень 5

Меры уровня 5 следует использовать для систем, не являющихся непосредственно важными для целей технического контроля или эксплуатации, например, систем автоматизации делопроизводства, характеризуемых низким уровнем серьезности различных киберугроз. Меры уровня 5 включают следующее:

— внесение модификаций в системы разрешается только утвержденным и квалифицированным пользователям;
— доступ к Интернету из систем уровня 5 разрешается при условии применения надлежащих защитных мер;
— дистанционный внешний доступ разрешается утвержденным пользователям при условии функционирования надлежащих мер контроля.

5.5.4. Зоны разделения

С целью предотвращения несанкционированного доступа, а также распространения ошибок из зоны с более низкими требованиями защиты в зону с более высокими требованиями, на границах зоны требуются механизмы разделения потоков данных.

Технические и административные меры, обеспечивающие разделение зон, должны быть адаптированы к индивидуальным требованиям защитных уровней. Не должен допускаться прямой канал соединения, проходящий через несколько зон.

6. УГРОЗЫ, УЯЗВИМОСТИ И УПРАВЛЕНИЕ РИСКОМ

В следующем ниже разделе ниже представлены фундаментальные понятия, используемые при управлении риском для компьютерных систем. Управление риском актуально на всех стадиях жизненного цикла систем установок, включая проектирование, разработку, эксплуатацию и обслуживание. В разделе 6.2 представлен краткий обзор необходимых этапов всесторонней методологии управления риском. В разделах 6.3 и 6.4 основное внимание уделяется тем этапам, на которых проявляются специфические для ядерной промышленности особенности.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

6.1. ОСНОВНЫЕ ПОНЯТИЯ И ВЗАИМОСВЯЗИ

Риск в контексте компьютерной безопасности – это потенциальная возможность того, что заданная угроза использует уязвимости актива или группы активов и тем самым нанесет ущерб организации. Он измеряется как сочетание вероятности события и серьезности его последствий.

На рис. 6 представлена диаграмма, показывая взаимосвязи между понятиями угрозы, уязвимости и риска [16].

6.2. ОЦЕНКА РИСКА И УПРАВЛЕНИЕ РИСКОМ

Оценка риска является важным инструментальным средством для определения наилучшего места размещения ресурсов и усилий при анализе уязвимостей и вероятности их использования.

Это процесс, посредством которого выявляются и документируются конкретные сочетания угроз, уязвимостей и последствий и разрабатываются соответствующие защитные меры контроля. Оценка угроз и уязвимостей создает основу для подготовки контрмер, необходимых для предотвращения или смягчения последствий атак на компьютерные системы.

Основными этапами методологии оценки риска и управления риском являются:

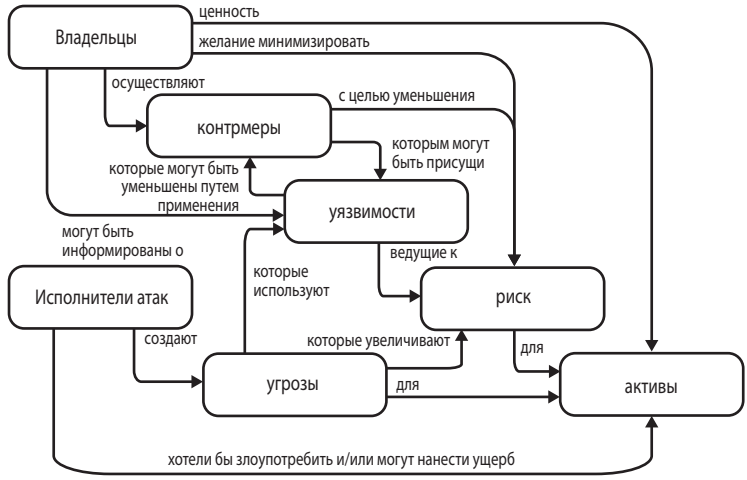


РИС. 6. Понятия и взаимосвязи в сфере безопасности (адаптировано из ИСО 13335-1 2004 [16]).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— определение периметра и общих условий;
— идентификация и определение характера угрозы;
— оценка уязвимости;
— уточнение сценария атаки;
— вероятность успешного использования;
— оценка уровня риска;
— определение контрмер.

Для осуществления систематического и согласованного анализа и оценки риска должен использоваться четко определенный процесс, в рамках которого могут соблюдаться существующие стандарты. Многочисленные методологии и инструментальные средства оценки риска или управления им достигли зрелости и способны эффективно структурировать такой процесс, и поэтому они приняты широкими кругами специалистов. Большинство из них основано на общих понятиях и логике. Современным международным стандартом является документ ИСО/МЭК 27005 – «Information Security Risk Management» (Управление рисками информационной безопасности) [4]. Еще один конкретный пример методологии приведен в приложении II. Национальным компетентным органам может потребоваться для использования конкретная методология или политика оценки риска, а на установках могут, помимо этого, иметься свои собственные методология или политика.

Интересный обзор методов и инструментальных средств оценки риска подготовлен ENISA (Европейское агентство сетевой и информационной безопасности), которое посвятило этому обзору специальную веб-страницу [17].

Необходимость оценки систем, глубина оценки и частота обновления анализов риска зависят от важности систем с точки зрения их функции безопасности и физической безопасности. Когда происходят модификации системы, необходимо рассмотреть вопрос о проведении нового анализа или, по крайней мере, рассмотрения. Другими причинами могут быть внедрение нового оборудования, программного обеспечения, процедур или существенное изменение комплексов навыков операторов. Число потенциальных угроз и уязвимостей обычно увеличивается при переходе от автономных систем к взаимосвязанным.

Если проведение анализа риска, связанного с конкретными угрозами, практически нецелесообразно, рекомендуется использовать образцовую практику и хорошие инженерно-технические принципы.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

6.3. ИДЕНТИФИКАЦИЯ И ОПРЕДЕЛЕНИЕ ХАРАКТЕРА УГРОЗ

Рис. 7 иллюстрирует постоянную тенденцию к росту изощренности атак и уменьшению объема знаний, необходимого для организации такой атаки. В программах по компьютерной безопасности следует стремиться к поддержанию такого уровня оценки, при котором охватывается весьма широкий диапазон возможных сценариев атаки.

Публикации об уязвимости промышленных систем управления регулярно появляются на основных мероприятиях, организуемых хакерами. Учитывая то обстоятельство, что они в целом дают запоздалую картину состояния навыков и интересов реальных хакеров, это должно являться еще одним фактором, побуждающим к улучшению информированности. Кроме того, недавно национальными ГКАР (группами компьютерного аварийного реагирования) была начата публикация сведений об уязвимостях программного обеспечения ПСУ, что способствует укреплению открытости перед общественным мнением и сообществом по вопросам компьютерной безопасности и концентрации интереса на таких решениях и слабостях продуктов.

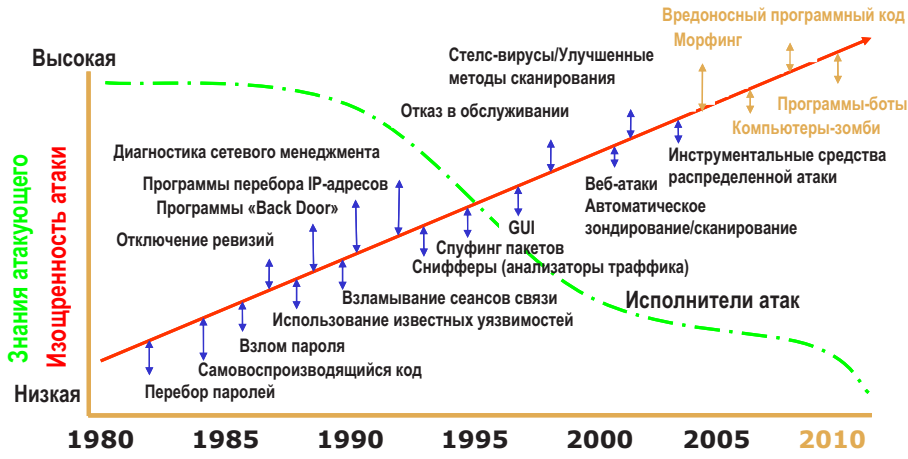


РИС. 7. Рост сложности угроз по мере распространения исполнителей атак[4]

[4] LIPSON, H.F., Tracking and Tracing Cyber-Attacks: Technical Challanges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009 (2000) 10.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Поэтому после того, как организованы надлежащая поддержка и ресурсы, при определении начальных мер по разработке программы компьютерной безопасности следует сконцентрироваться на понимании потенциальных угроз, исходя из профилей данных вероятных исполнителей атаки и сценариев атаки. Возможным первым шагом может стать создание матрицы профилей данных исполнителей атаки с перечислением вероятных исполнителей атаки, их мотиваций и потенциальных целей. Матрица профилей данных исполнителей атаки может затем быть использована для разработки вероятных сценариев атаки; в следующих ниже подразделах этот процесс исследуется более подробно.

6.3.1. Проектная угроза

Важным инструментальным средством, используемым для определения уровней угрозы и в качестве основы для разработки средств обеспечения безопасности, является проектная угроза (ПУ). ПУ представляет собой заявление о свойствах и характеристиках потенциальных нарушителей (внутренних и/или внешних). ПУ разрабатывается на основе надежной информации, полученной с применением специальных средств, но она не предназначена для того, чтобы стать заявлением о фактических преобладающих угрозах. Исходя из современных представлений о характере угроз, ПУ представляет собой наиболее серьезную угрозу, на защиту от которой должна быть рассчитана защита установки. Государства используют ПУ в своих системах регулирования для определения надлежащего распределения ресурсов с целью защиты ядерного материала и ядерных установок от враждебных действий. (Более подробная информация о ПУ содержится в [18].)

Следует рассмотреть возможность включения в такие сценарии угроз либо автономных атак с использованием компьютерных систем/атак, направленных против таких систем, либо координированных атак, включающих использование компьютерных систем.

6.3.2. Профили данных исполнителей атак

В таблицах 1 и 2 представлен возможный набор профилей данных исполнителей атак. В таблице 1 основное внимание уделяется внутренним угрозам/угрозам, исходящим от внутренних нарушителей (обсуждение угроз, исходящих от внутренних нарушителей, содержится также в [19]), в то время как в таблице 2 рассматриваются определенные возможные внешние угрозы. В таблицах общие типы исполнителей атак связываются с имеющимися у них ресурсами, продолжительностью атаки, инструментальными средствами, которые, вероятно, будут использоваться, и мотивацией исполнителей атак.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Профили данных необходимо адаптировать с учетом конкретных типов установок. Поэтому необходимо организовать надлежащий процесс сбора данных с использованием специальных средств для обеспечения полноты и актуальности матрицы данных об исполнителях атак на каждой установке.

6.3.3. Сценарии атак

При разработке сценариев атак можно учитывать различные воз-можные варианты. Ядерная установка может подвергнуться атаке с целью:

— подготовки к последующей координированной атаке, направленной на организацию саботажа на станции и/или изъятие ядерного материала;
— создание угрозы здоровью людей или экологической безопасности;
— организации атаки, направленной против другой площадки;
— создания атмосферы хаоса и страха;
— получения финансовой выгоды для преступной группировки;
— создания неустойчивостей на основных рынках и достижения прибылей для конкретных рыночных игроков.

В зависимости от задач или целей атаки исполнитель атаки будет стремиться воспользоваться различными системными уязвимостями. Такие атаки могут приводить к:

— несанкционированному доступу к информации (утрате конфиденциальности);
— перехвату и изменению информации, программного обеспечения, аппаратных средств, и т.д. (утрате целостности);
— блокировке линий передачи данных и/или отключению систем (утрате работоспособности);
— несанкционированному проникновению в системы передачи данных или компьютеры (утрате надежности).

Все эти аспекты могут иметь серьезные последствия для функциональных возможностей компьютерных систем и оказывать на них серьезное воздействие, что может создавать прямую или косвенную угрозу безопасности и физической безопасности установки. При разработке сценариев атак следует учитывать технологические тенденции и легкость доступа при совершении атак на технологии. Некоторые сценарии, иллюстрирующие вымышленные, но реалистические атаки на ядерную установку, рассматриваются в приложении I.

ТАБЛИЦА 1. ВНУТРЕННИЕ УГРОЗЫ

Исполнитель атаки	Ресурсы	Продолжительность	Инструментальные средства	Мотивация
Тайный агент	Содействие «социальной инженерии». Доступ к системе на определенном уровне. Имеется доступ к системной документации и экспертным знаниям.	Может быть различной, но, как правило, не может составлять многие часы.	Наличие доступа, знание программирования и системной архитектуры: — возможное знание действующих паролей; — возможность внедрения специально разработанных программ «backdoor» и/или программ-троянов; — возможная внешняя экспертная поддержка.	Хищение деловой информации, технологических секретов, личных данных. Экономическая выгода (продажа информации конкурентам). Шантаж.
Рассерженный служащий/ пользователь	Средние/мощные ресурсы. Доступ к системе на определенном уровне. Наличие системной документации и экспертных знаний относительно конкретных видов деятельности и эксплуатации систем.	Может быть различной, но, как правило, не может составлять многие часы.	Наличие доступа, знание программирования и системной архитектуры. Возможное знание действующих паролей. Способность вводить «дилетантские» инструментальные средства или скрипты (потенциально более сложные в случае наличия определенных компьютерных навыков)	Месть, разрушение, создание хаоса. Хищение деловой информации. Удивить работодателя/ других служащих. Нанести ущерб репутации или привести к утрате доверия.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

ТАБЛИЦА 2. ВНУТРЕННИЕ УГРОЗЫ

Исполнитель атаки	Ресурсы	Продолжительность	Инструментальные средства	Мотивация
Хакер-любитель	Квалификация может быть различной, но, как правило, она невысока. Слабое знание систем, помимо связанного с открытой информацией.	Значительная, но с невысокой настойчивостью.	Широкодоступные скрипты и инструментальные средства. Возможна определенная доработка инструментальных средств.	Развлечение, подтверждение статуса. Случайный выбор цели. Возможность воспользоваться «легкой добычей».
Воинственный противник ядерной энергетики	Ограниченные ресурсы, но может иметься финансовая поддержка по тайным каналам. Доступ к инструментальным средствам киберсообщества. Слабое знание систем, помимо связанного с открытой информацией.	Целью атак могут быть определенные заранее известные события (например, празднования, выборы). Значительная, с высокой настойчивостью и мотивацией.	Имеются компьютерные навыки. Возможна поддержка со стороны сообщества хакеров. «Социальная инженерия».	Убежденность в миссии спасения мира. Расшатывание общественного мнения по определенным вопросам. Воспрепятствование деловым операциям.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

ТАБЛИЦА 2. ВНУТРЕННИЕ УГРОЗЫ (продолж.)

Исполнитель атаки	Ресурсы	Продолжительность	Инструментальные средства	Мотивация
Рассерженный служащий/ пользователь, которому отказано в предоставлении услуг)	Ограниченные ресурсы, если не действует в составе большей группы. Может все еще обладать системной документацией. Возможно использование неконтролируемого прежнего доступа. Возможны связи с персоналом установки.	Различно, в зависимости от состава задействованной группы людей.	Возможное знание действующих паролей. Возможно использование неконтролируемого прежнего доступа. Возможно создание системных программ «backdoor» в период работы. «Социальная инженерия».	Месть, разрушение, создание хаоса. Хищение деловой информации. Удивить работодателя/ других служащих. Нанести ущерб репутации или привести к утрате доверия.
Организованная преступность	Обширные ресурсы. Использование экспертных знаний в области кибернетики.	Различная, но в основном небольшой длительности.	Скрипты, инструментальные средства собственной разработки. Могут быть использованы «наемные хакеры». Могут использоваться бывшие/работающие служащие. «Социальная инженерия».	Шантаж. Хищение ядерного материала. Вымогательство (финансовая выгода). Игра на финансовых и связанных с репутацией опасениях бизнеса. Информация для продажи (техническая, деловая или личная).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

ТАБЛИЦА 2. ВНУТРЕННИЕ УГРОЗЫ (продолж.)

Исполнитель атаки	Ресурсы	Продолжительность	Инструментальные средства	Мотивация
Государство	Обширные ресурсы и экспертные знания. Деятельность по сбору информации с использованием спецсредств. Возможный опыт обучения/ эксплуатации в связи с системой.	Различная.	Группы подготовленных киберэкспертов. Сложные инструментальные средства. Могут использоваться бывшие/ работающие служащие. «Социальная инженерия».	Сбор информации с использованием спецсредств. Создание точек доступа для последующих действий. Хищение технологии.
Террорист	Разнообразные навыки. Возможный опыт обучения/ эксплуатации в связи с системой.	Значительная, с весьма высокой настойчивостью.	Скрипты, инструментальные средства собственной разработки. Могут быть использованы «наемные хакеры». Могут использоваться бывшие/ работающие служащие. «Социальная инженерия».	Сбор информации с использованием спецсредств. Создание точек доступа для последующих действий. Создание хаоса. Месть. Воздействие на общественное мнение (создание обстановки страха).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

6.4. УПРОЩЕННЫЕ РЕЗУЛЬТАТЫ ОЦЕНКИ РИСКА

В таблице 3 приведены, исключительно для целей иллюстрации, примеры систем, которые могут иметься на ядерной установке. В ней указаны потенциальные последствия успешных атак на рассматриваемые системы, соответствующие последствия для установки и общие примеры соответствующих контрмер.

Фундаментальное для анализа риска понятие вероятности в этой таблице не учитывается. Вероятность успешных атак, а также потенциальные последствия зависят от контекста и рассматриваемой установки. Кроме того, для каждой системы, рассматриваемой при оценке риска, следует проводить более полную оценку требований в отношении конфиденциальности, целостности и готовности.

7. ОСОБЫЕ СООБРАЖЕНИЯ, КАСАЮЩИЕСЯ ЯДЕРНЫХ УСТАНОВОК

Ввиду уникального характера ядерной промышленности, в сфере компьютерной безопасности ядерных установок должны рассматриваться дополнительные проблемы, помимо тех, которые связаны с компьютерной безопасностью сетей ИТ в сфере бизнеса или даже сопоставимых систем управления технологическими процессами вне ядерной промышленности. В следующих ниже разделах изложены некоторые из этих связанных с ядерной промышленностью проблем.

7.1. ЭТАПЫ ЖИЗНЕННЕГО ЦИКЛА И РЕЖИМЫ РАБОТЫ УСТАНОВОК

Конструкции и эксплуатационные характеристики ядерных установок могут быть самыми разнообразными. Существует ряд этапов жизненного цикла и режимов работы установок, в том числе:

— Проектирование, строительство и ввод в эксплуатацию.
— Эксплуатация:
  • работа на мощности:
  • пуск станции;
  • горячий останов;
  • холодный останов;
  • перегрузка топлива и техническое обслуживание.
— Снятие с эксплуатации.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

ТАБЛИЦА 3. ТИПИЧНЫЕ СИСТЕМЫ НА ЯДЕРНЫХ УСТАНОВКАХ

Система	Последствия для компьютерной безопасности	Потенциальные воздействия на установку	Предлагаемые контрмеры
Система защиты реактора	Утрата целостности критических для безопасности программного обеспечения/данных. Утрата функциональной готовности.	КРИТИЧЕСКИЕ Ухудшение безопасности станции, радиоактивный выброс.	Меры уровня безопасности 1
Система управления технологическим процессом	Утрата целостности связанных с управлением программного обеспечения/данных. Утрата функциональной готовности.	ЗНАЧИТЕЛЬНЫЕ Ухудшение эксплуатации станции.	Меры уровня безопасности 2
Система допусков к работе и рабочих заданий	Утрата целостности данных и эксплуатационной готовности системы.	СРЕДНИЕ Неправильные действия в отношении компонентов. Нарушение нормального режима эксплуатации и обслуживания.	Меры уровня безопасности 4
Система физического контроля доступа	Утрата эксплуатационной готовности и целостности систем доступа на площадке. Утрата конфиденциальности данных о доступе на площадке.	ЗНАЧИТЕЛЬНЫЕ Предоставление доступа лицам, не имеющим соответствующего разрешения. Лица, которым разрешен доступ, не имеют возможности получить доступ к требуемым им зонам.	Меры уровня безопасности 2

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

ТАБЛИЦА 3. ТИПИЧНЫЕ СИСТЕМЫ НА ЯДЕРНЫХ УСТАНОВКАХ (продолж.)

Система	Последствия для компьютерной безопасности	Потенциальные воздействия на установку	Предлагаемые контрмеры
Система управления документо-оборотом	Утрата конфиденциальности, доступности и целостности данных.	СРЕДНИЕ Информация используется для планирования более серьезных атак.	Меры уровня безопасности 4
Электронная почта	Утрата конфиденциальности, целостности и готовности.	НЕЗНАЧИТЕЛЬНЫЕ Возрастание административной нагрузки. Затруднение повседневной работы.	Меры уровня безопасности 5

На этих этапах жизненного цикла и режимах работы могут быть задействованы различные системы и может существовать различная рабочая обстановка. Например, в периоды интенсивного обслуживания часто производятся замены, модификации и испытания оборудования или может требоваться доступ дополнительного персонала и третьих сторон/подрядчиков. Эти разнообразные условия следует учитывать в ПОКБ. В частности, на различных этапах жизненного цикла может потребоваться серьезный пересмотр ПОКБ.

7.2. РАЗЛИЧИЯ МЕЖДУ СИСТЕМАМИ ИТ И ПРОМЫШЛЕННЫМИ СИСТЕМАМИ УПРАВЛЕНИЯ

Компьютерные системы и сетевые архитектуры, поддерживающие эксплуатацию атомной станции, не являются стандартными компьютерными системами с точки зрения архитектуры, конфигурации или требований к функционированию. Эти системы могут быть классифицированы как специализированные промышленные системы управления (ПСУ). Хотя в процессе эволюции ПСУ прошли путь от строго специализированных устройств до решений, основанных на более широком использовании общепринятых архитектур вычислительных систем, между ПСУ и стандартными системами на базе ИТ все же имеются существенные различия, которые необходимо учитывать в любом ПОФБ.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

В таблице 4 представлены на основе материалов НИСТ (Национального института стандартов и технологий США) [20] данные об основных различиях между ПСУ и классическими системами на базе ИТ.

7.3. ТРЕБОВАНИЯ В ОТНОШЕНИИ ДОПОЛНИТЕЛЬНЫХ ВОЗМОЖНОСТЕЙ ПОДКЛЮЧЕНИЯ И СВЯЗАННЫЕ С ЭТИМ ПОСЛЕДСТВИЯ

Все более проблемной областью для ПСУ становится растущая желательность обеспечения возможности подключения и взаимодействия между бизнес-системами и техническими системами с одной стороны и эксплуатационными системами – с другой. Ввиду желания руководства корпораций, планировщиков и инженеров получить доступ к данным станции в реальном времени, между жестко ограниченными сетями управления, обеспечивающими работу станции, и неограниченными сетями передачи данных, используемыми для корпоративного доступа, создаются межсетевые мосты. Такой межсетевой мост может представлять собой шлюз для проникновения в сеть.

Еще одной уникальной архитектурной характеристикой является существование удаленных аварийных центров. Эти аварийные операционные центры являются удаленными пунктами для мониторинга и аварийной эксплуатации станции в случае, если в результате инцидента перестает работать основной пункт управления. Требования в отношении мониторинга/поддержания некоторых элементов управления станцией приводят к необходимости передачи потоков данных через некоторую среду передачи данных. Эта среда является потенциальным путем для ухудшения характеристик и входа в основную систему. Кроме того, требования в отношении дублирования функций приводят к необходимости соблюдения согласованных требований физической безопасности в двух системах. Невыполнение обслуживания одной системы может создать путь для проникновения и ввода кодов-эксплойтов.

Необходимость дистанционного анализа, обслуживания или обновления может также приводить к появлению подобных уязвимостей. Прежде, чем давать согласие на введение такой дополнительной возможности подключения и взаимодействия, необходимо провести тщательный анализ риска.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

ТАБЛИЦА 4. РАЗЛИЧИЯ МЕЖДУ СИСТЕМАМИ НА БАЗЕ ИТ И ПСУ [23]

Категория	Система на базе информационных технологий	Промышленная система управления
Требования к рабочим характеристикам	Не является системой реального времени Срабатывание должно быть стабильным Требуется высокая производительность Могут быть приемлемыми большие задержки и флуктуации	Является системой реального времени Критически важным является время срабатывания Приемлема умеренная производительность Большие задержки и/или флуктуации являются серьезной проблемой
Требования к эксплу-атационной готовности	Такие виды реакции, как перезагрузка, приемлемы Недостатки в плане эксплуатационной готовности зачастую могут быть допустимы, в зависимости от эксплуатационных требований системы	Такие виды реакции, как перезагрузка, могут оказаться неприемлемыми ввиду требований процесса к эксплуатационной готовности Отключения должны планироваться заблаговременно, за несколько дней/недель Высокая эксплуатационная готовность требует обширных испытаний перед вводом в эксплуатацию
Требования в отношении управления риском	Конфиденциальность и целостность данных являются главными требованиями Отказоустойчивость менее важна — кратковременное отключение не создает значительного риска Главным последствием в плане риска является задержка выполнения бизнес-операций	Главным требованием является безопасность персонала, а затем защита технологического процесса Отказоустойчивость весьма важна, даже кратковременное отключение неприемлемо Основными последствиями в плане риска являются несоблюдение регулирующих положений, потеря жизней людей, оборудования или продукции
Вопросы физической безопасности, которым уделяется основное внимание в архитектуре	Первоочередное внимание уделяется защите активов ИТ и информации, хранящейся в этих активах или передаваемой между ними Для центрального сервера может требоваться высокая степень защиты	Главной целью является защита периферийных клиентов (например, таких периферийных устройств, как контроллеры технологического процесса) Защита центрального сервера также является важной
Неумышленные последствия	Решения по обеспечению физической безопасности проектируются на основе типичных систем ИТ	Инструментальные средства обеспечения физической безопасности должны проходить тестирование, с тем чтобы гарантировать, что они не создают угрозы нормальной работе ПСУ
Взаимодействие с критическими временными параметрами	Менее критическое взаимодействие в аварийных ситуациях Может быть осуществлен в необходимой степени контроль доступа с жесткими ограничениями	Критически важной является реакция на взаимодействие людей и другие виды взаимодействия в аварийных ситуациях. Доступ к ПСУ следует строго контролировать, но при этом не должны создаваться препятствия взаимодействию «человек-машина»
Эксплуатация системы	Системы проектируются для использования с типичными операционными системами Обновления являются несложными при наличии автоматизированных средств развертывания	Различные и разрабатываемые по заказу операционные системы, зачастую без возможностей обеспечения физической безопасности Изменения программного обеспечения должны производиться осторожно, обычно поставщиками программного обеспечения, ввиду наличия специализированных алгоритмов управления и возможности наличия измененных аппаратных средств и программного обеспечения

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

ТАБЛИЦА 4. РАЗЛИЧИЯ МЕЖДУ СИСТЕМАМИ НА БАЗЕ ИТ И ПСУ [23]

Категория	Система на базе информационных технологий	Промышленная система управления
Ресурсные ограничения	Системы задаются с достаточными ресурсами для поддержки добавления сторонних прикладных программ, таких как решения по обеспечению физической безопасности	Системы проектируются с целью поддержки планируемого производственного процесса, с минимальной памятью и вычислительными ресурсами в поддержку добавления технологии физической безопасности
Системы связи	Стандартные коммуникационные протоколы Главным образом проводные сети с определенными локализованными возможностями беспроводной связи Типичная практика работы с сетями ИТ	Многочисленные специальные и стандартные коммуникационные протоколы Используется несколько типов средств связи, включая специализированную проводную и беспроводную (радио- и спутниковую связь) Сети являются сложными и иногда требуют экспертных знаний инженеров по системам управления
Управление изменениями	Изменения программного обеспечения осуществляются своевременно при наличии хорошей политики и процедур физической безопасности. Процедуры зачастую автоматизированы.	Изменения программного обеспечения должны полностью подвергаться тестированию и проводиться в системе постепенно с целью сохранения целостности системы управления. Отключения ПСУ зачастую должны планироваться и распределяться по графику заблаговременно, за несколько дней/недель
Комплексная поддержка	Допускаются разнообразные стили поддержки	Сервисная поддержка обычно осуществляется единственным поставщиком
Срок службы компонентов	Срок службы составляет порядка 3-5 лет	Срок службы составляет порядка 15-20 лет
Доступ к компонентам	Компоненты обычно локальны и легкодоступны	Компоненты могут быть изолированными, удаленными и требовать значительных физических усилий для получения доступа к ним

7.4. СООБРАЖЕНИЯ, КАСАЮЩИЕСЯ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Многие современные регулирующие положения, касающиеся валидации или сертификации оборудования атомных станций, были разработаны в расчете на аналоговое оборудование. Темпы его устаревания невысоки. С другой стороны, планы обеспечения безопасности ИТ и образцовая практика подразумевают регулярные обновления и исправления программных и цифровых компонентов, поскольку эти компоненты устаревают намного быстрее.

Поэтому важно рассмотреть проблемы, создаваемые исправлениями и обновлениями программного обеспечения цифровых ядерных систем управления или мониторинга. В наихудшем сценарии каждую модификацию

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

или пересмотр программного обеспечения можно рассматривать как системное изменение, способное привести к необходимости валидации определенной системы или даже повторной сертификации некоторых критических систем. Поскольку реализация такого подхода оказывается затруднительной, результатом может стать отставание в установке исправлений или сознательное решение об отсрочке обновления программного обеспечения. С целью ограничения этих эффектов следует проводить различие между нормальным обслуживанием, при котором избегают выполнения таких процессов, и системными модификациями, требующими повторного тестирования или даже повторной сертификации критических систем. Во всех случаях любые модификации систем безопасности или связанных с безопасностью систем и систем физической безопасности должны выполняться в соответствии с согласованными процедурами.

7.5. УЧЕТ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ПРИ ПРОЕКТИРОВАНИИ И В СПЕЦИФИКАЦИЯХ КОМПЬЮТЕРНЫХ СИСТЕМ

При первоначальном проектировании и разработке многих существующих систем и контрольно-измерительной аппаратуры для управления технологическими процессами и промышленных систем управления компьютерная безопасность не была основным соображением. Недавняя тенденция к обеспечению возможностей подключения и взаимодействия между системами и технологическими процессами, интеграции коммерческих готовых компьютерных систем и активизации злоумышленной деятельности в отношении компьютеров (то есть, взлома защиты компьютерных систем) привела к необходимости рассматривать компьютерную безопасность в качестве основного требования при приобретении нового оборудования.

В связи с этим следует осуществлять формализацию требований физической безопасности в качестве части переговоров по контрактам с поставщиками. В качестве инструментального средства для формализации таких требования физической безопасности может использоваться документ ИСО «Common Criteria» («Общие критерии») (ISO 15408) [21]. Еще одним примером является попытка определить «Procurement Language for Control Systems» («Язык закупок для систем управления») [22] Департаментом национальной безопасности США, опубликовавшим руководящие материалы и рекомендации по определению требований кибербезопасности и специфическому языку закупок при приобретении систем управления.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

7.6. ПРОЦЕДУРА КОНТРОЛЯ ДОСТУПА ТРЕТЬИХ СТОРОН/ПОСТАВЩИКОВ

Весьма важно учитывать уровень безопасности любой третьей стороны и поставщиков. Крайне важно, чтобы департамент физической безопасности работал в тесном сотрудничестве с департаментом контрактов для обеспечения того, чтобы положения по физической безопасности включались в каждый контракт.

Организации в ядерной промышленности часто предоставляют контракты внешним подрядчикам; в некоторых из этих контрактов участвуют субподрядчики, хранящие информацию или активы, отмеченные грифами конфиденциальности, в собственных помещениях. Если при предоставлении такого контракта и его последующем исполнении не соблюдаются строгие правила, то несущие грифы конфиденциальности информация и активы, связанные с контрактом, могут подвергнуться риску вредного воздействия или неправомочного раскрытия.

Ввиду вышеизложенных факторов важно, чтобы ответственное руководство каждой площадки/организации в ядерной промышленности поддерживало тесные рабочие отношения с подрядчиком с целью обеспечения учета важнейших аспектов безопасности во время разработки и выполнения контракта и в ходе окончательной передачи объекта.

В тех случаях, когда это считается необходимым, следует проводить проверки и аудиты для обеспечения того, чтобы в системе менеджмента подрядной организации были надлежащим образом учтены вопросы физической безопасности и чтобы в практической деятельности и мерах организации соблюдались требования системы.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

СПРАВОЧНЫЕ МАТЕРИАЛЫ

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

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

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

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

[5] 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).

[6] COUNCIL OF EUROPE, Convention on Cybercrime, ETS No. 185, COE, Strasbourg (2001).

[7] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Система управления для установок и деятельности, Серия норм безопасности МАГАТЭ, № GS-R-3, МАГАТЭ, Вена (2008).

[8] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Применение системы управления для установок и деятельности, Серия норм безопасности МАГАТЭ, № GS-G-3.1, МАГАТЭ, Вена (2009).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[10] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Ядерная проверка и сохранность материала. Физическая защита: цели и основополагающие принципы, документ GOV/2001/41, МАГАТЭ, Вена (2001).

[11] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Физическая защита ядерного материала и ядерных установок, документ INFCIRC/225/Rev.4, МАГАТЭ, Вена (1999).

[12] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Руководящие материалы и соображения по осуществлению документа INFCIRC/225/Rev.4 «Физическая защита ядерного материала и ядерных установок», IAEA-TECDOC-967 (Rev.1), МАГАТЭ, Вена (2002).

[13] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Системы контрольно-измерительных приборов и управления, важные для безопасности атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.3, МАГАТЭ, Вена (2008).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

[15] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Глоссарий МАГАТЭ по вопросам безопасности. Терминология, используемая в области ядерной безопасности и радиационной защиты. Издание 2007 года, МАГАТЭ, Вена (2008).

[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology - Security Techniques - Management of Information and Communications Technology Security - Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Geneva (2004).

[17] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, Inventory of Risk Management/Risk Assessment Methods and Tools, http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-tools.

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

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

[20] STOUFFER, K.A., FALCO, J.A., SCARFONE, K., Guide to Industrial Control Systems (ICS) Security — Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Rep. NIST SP-800-82, National Institute of Standards and Technology, Chicago (2011).

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology - Security Techniques - Evaluation Criteria for IT Security, ISO/IEC 15408:2008, ISO, Geneva (2008).

[22] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Cyber Security Procurement Language for Control Systems, September (2009), http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_ 100809.pdf

[23] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Risk Management - Vocabulary, ISO/IEC Guide 73:2009, ISO/IEC, Geneva (2009).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

БИБЛИОГРАФИЯ

AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Security Technologies for Industrial Automation and Control System, ANSI/ISA-TR99.00.01-2007, ANSI, Washington DC, (2007).

FEDERAL MINISTRY OF THE INTERIOR, National Plan for Information Infrastructure Protection, BMI, Berlin (2005).

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Ядерная проверка и сохранность материала. Физическая защита: цели и основополагающие принципы, документ GOV/2001/41, МАГАТЭ, Вена (2001).

INTERNATIONAL SOCIETY FOR AUTOMATION, Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems and Automation Society, ISA-TR99.00.02-2004, ISA, Research Triangle Park, NC (2004).

KOREA INSTITUTE OF NUCLEAR SAFETY, Cyber Security of Digital Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N09-DR, KINS, Seoul (2007).

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE, Good Practice Guide: Process Control and SCADA Security, Version 2.0, NISCC, November (2006).

NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 08-09 (Rev. 5), NEI, Washington DC (2010).

NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC, Rockville, MD (2010).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, Paris (2002).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks-Towards a Culture of Security, DSTI/ICCP/REG(2003)5/REV1, OECD, Paris (2003).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, DSTI/ICCP/REG(2005)1/FINAL, OECD, Paris (2005).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Приложение I

СЦЕНАРИИ АТАК НА СИСТЕМЫ ЯДЕРНЫХ УСТАНОВОК

Как указано в разделе 6.3, характер и форма атак с использованием компьютеров, защиту от которых необходимо обеспечивать, могут быть самыми различными. Хотя типы атак могут различаться, к их последствиям на высоком уровне относятся:

— несанкционированный доступ к информации или ее перехват (потеря конфиденциальности);
— несанкционированная модификация информации, программного обеспечения, аппаратных средств, и т.д. (потеря целостности);
— блокирование линий передачи данных и/или отключение систем (утрата готовности).

При разработке профилактических мер, направленных против компьютерных атак, весьма важно понимать характер атак и потенциальных мест, которые могут использоваться при атаке или исполнителями атак для получения соответствующей информации и доступа к компьютерным системам, являющимся целью атак. **Приведенные ниже сведения – это всего лишь примеры, цель которых – побудить читателей после того, как они смогут лучше понять угрозы, осмыслить ситуацию в своей собственной организации/системе и, если это необходимо, соответствующим образом скорректировать меры по обеспечению безопасности.** Хотя приведенные примеры атак являются вымышленными, они связаны с возможными сценариями, разработанными на основе аналогичных атак, зафиксированных в других отраслях промышленности. Продумывание таких сценариев – это хороший способ обеспечения того, чтобы в плане обеспечения безопасности учитывалась динамика изменяющейся обстановки в отношении угроз.

Хорошо спланированная компьютерная атака состоит из ряда этапов. Эти этапы включают:

— определение цели;
— изучение обстановки;
— доступ к системе /нарушение ее нормальной работы;
— выполнение атаки;
— сокрытие следов в поддержку отрицания виновности.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

В следующих ниже подразделах перечислены три предполагаемых сценария компьютерных атак. Первый сценарий, одной из целей которого является сбор информации, может рассматриваться в качестве подготовительного по отношению к следующим двум сценариям.

Сценарий I – Сбор информации в поддержку злоумышленного действия

Цель атаки — получить физический доступ к контролируемым (с ограниченным доступом) зонам установки для того, чтобы поддержать последующую атаку.

При этом интерес представляет лицо, контролирующее карты доступа и определяющее порядок доступа. Для получения физического доступа к зонам ограниченного доступа необходимо нарушить нормальную работу компьютера, управляющего картами доступа, и нарушить нормальную работу системы управления кодами доступа. Исполнитель атаки намерен действовать в качестве субподрядчика, поставляющего части оборудования.

Возможными целями при сборе информации в поддержку атаки являются:

— личная информация для последующего вымогательства или «социальной инженерии»;
— проектная документация системы контроля доступа;
— стратегические и инженерно-технические планы систем безопасности или других соответствующих зон станции;
— графики работы — график работы станции, распорядок дня, кто работает, когда они работают, кто в отпуске, когда происходят определенные изменения;
— список поставщиков и когда они работают на оборудовании;
— инвентарные списки оборудования и деталей;
— пароли и меры контроля доступа;
— административно-технические меры контроля доступа;
— информация о разработчиках программного обеспечения и о текущих проектах;
— сетевая архитектура;
— архитектура систем дистанционной передачи данных.

К потенциальным методам сбора этой информации относятся:

— «социальная инженерия»;
— поиск открытой информации в Интернете;
— поиск полезной информации в информационных отходах;

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

— war dialling (компьютерный перебор телефонных номеров с целью поиска модема), war driving (поиск беспроводных сетей путем передвижения на автомобиле);
— атаки электронной почты – «фишинг»[1] с целью получения доступа к сетям, использование программ перехвата вводимой с клавиатуры информации;
— установка программного обеспечения или устройств на хост-машины – через жесткий диск, карту памяти или компакт-диск;
— подслушивание ввода паролей или ввода кодов доступа (вручную, с использованием средств аудио- или видеонаблюдения).

Элементы атаки могут включать:

— получение карты доступа (контактной карты) и кода доступа;
— хищение/дублирование имеющейся карты доступа;
— доступ к программатору карт доступа с целью создания новой карты;
— создание входных данных о новом служащем;
— отождествление с личными данными недавно уволенного служащего;
— получение желательного уровня доступа.

Как только карта и коды получены, исполнитель атаки использует полученную информацию для организационной деятельности с целью скрытного проникновения на установку в качестве лица, доставляющего части оборудования.

Сценарий II – Атака с отключением или нарушением нормальной работы одной или нескольких компьютерных систем

Цель атаки – организовать саботаж на атомной электростанции и воспрепятствовать незамедлительному возврату станции в эксплуатацию.

В данном примере в период останова субподрядчик проводит тесты на системе управления подачей питательной воды. Подрядчик создает пункт удаленного доступа для мониторинга и тестирования системы из своего офиса. После того, как подрядчик завершает работу, пункт доступа по недосмотру продолжает действовать.

[1] «Фишингом» называют попытки получить мошенническим образом чувствительную информацию, такую как имена пользователей, пароли и подробные сведения о кредитной карточке, путем маскировки под заслуживающий доверия объект при электронной коммуникации.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Исполнитель атаки собрал на станции информацию, которая указывает, что субподрядчик ранее работал на станции и является основной целью для получения информации относительно станции. Исполнитель атаки проводит фишинг-атаку на электронную почту в офисе субподрядчика и внедряет в систему руткит, получая административный контроль. В результате исполнитель атаки получает доступ к компьютерной сети подрядчиков и узнает планы тестирования на станции, а также определяет порт удаленного доступа, который не был заблокирован станцией.

Используя эту информацию, злоумышленник имеет возможность организовать атаку с отказом в обслуживании(DoS)[2] на систему управления подачей питательной воды путем заглушения сети трафиком, что вызывает сбой системы. Система была рассчитана на работу только при минимальной нагрузке по трафику.

После того, как исполнитель атаки получил доступ, проанализировал сеть и определил протокол связи, он проводит атаку. В результате атаки система управления подачей питательной воды перестает реагировать на команды, что приводит к ручному аварийному останову станции. Причина сбоя системы управления подачей питательной воды не может быть определена сразу же, и станция остается в режиме останова для проведения расследования.

Сценарий III – Нарушение нормальной работы компьютерной системы как инструментальное средство координированной атаки

Цель атаки – хищение ядерного материала во время его перемещения между хранилищами. Компьютерная атака используется для внесения изменений в систему контроля и отслеживания инвентарного количества с целью сокрытия потери похищенного материала.

В результате разведки и сбора сведений с применением спецсредств был определен процесс маркировки и прослеживания перемещений радиоактивного материала между хранилищами. Он включает установку на каждый предмет МРЧИ[3] (метки радиочастотной идентификации) с описанием компонента и перечислением содержимого.

План атаки включает помощь внутреннего нарушителя с целью изъятия материала во время его перемещения. Этапы атаки таковы:

---

[2] Отказ в обслуживании (DoS) – это предотвращение санкционированного доступа к ресурсам системы или внесение задержек в работу системы и выполнение ее функций.

[3] Радиочастотная идентификация: технология, используемая для идентификации и отслеживания с применением радиочастотных сигналов.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

— перехват груза во время его перемещения;
— изъятие небольшого количества транспортируемого радиоактивного материала;
— перепрограммирование чипа РЧИД с целью введения информации об оставшемся количестве;
— модификация данных системы отслеживания инвентарного количества таким образом, чтобы отразить новое количество, как отправляемое, а похищенное количество - как все еще находящееся на хранении в отправляющей установке.

Компьютерная атака нацелена на получение через сеть доступа к базе данных по инвентарным количествам и модификацию файла регистрации инвентарных количеств и передач.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Приложение II

МЕТОДОЛОГИЯ ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Процесс идентификации, контроля, устранения или уменьшения потенциальных угроз компьютерной безопасности на ядерной установке следует осуществлять систематически и согласованно, в соответствии с действующими стандартами. В настоящем приложении более углубленно рассматривается конкретная методология. Выбор именно этой методологии из многих имеющихся не подразумевает, что МАГАТЭ рекомендует ее, и она приведена лишь в качестве детального примера. Общее введение в оценку риска содержится в разделе 6.1.

Вообще говоря, для того, чтобы понять угрозы и уязвимости для конкретной компьютеризированной системы, необходимо вначале проанализировать эту систему с функциональной и технической точек зрения и выявить соответствующие факторы обеспечения надежности, которую необходимо поддерживать. Затем необходимо определить и проанализировать риски, связанные с этими факторами.

Ниже приводится краткий обзор метода EBIOS. «EBIOS» – это французское сокращение принципа, означающего *формулирование потребностей и определение целей безопасности* (**expression des besoins et identification des objectifs de securite**). Он был разработан Центральным бюро информационной безопасности Франции (DCSSI — Direction Centrale de la Securite des Systemes d'Information)[1].

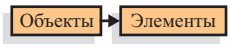
EBIOS предусматривает формализованный подход к оценке и рассмотрению рисков в области безопасности информационных систем, включая инструментальные средства поддержки для заключения контрактов с компетентными органами, подготовки документов и улучшения информированности.

В настоящем документе изложены только основные принципы подхода, адаптированные из документации, доступной на вебсайте поддержки DCSSI.

[1] Методы обеспечения безопасности информационных систем: http://www.ssi.gouv.fr/site_rubrique113.html.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Изучение общих условий и определение периметра



Первым шагом является определение общих технических и связанных с бизнес-процессами и регулированием условий исследования. В частности, информационная система основана на **основных элементах**, функциях и информации, определяющих совокупную выгоду этой информационной системы для организации.

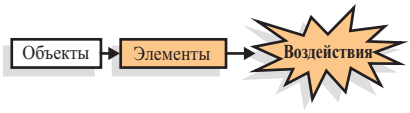
Например, система, контролирующая систему теплоносителя электростанции, использует различного рода информацию, такую как результаты измерений, параметры и результаты вычислений, а также различные функции, позволяющие выполнять эти вычисления.

Основные элементы связаны с рядом **объектов** различных типов: аппаратными средствами, программным обеспечением, сетями, организациями, человеческими ресурсами и площадками.

Рассмотрим, например, параметр, используемый для запуска определенного насоса системы теплоносителя. Он связан с контролирующими компьютерами, программным обеспечением обработки данных, операторами, состоянием источников охлаждения, состоянием станции, соответствующими регулирующими положениями и т.п.

Результат: Цель исследования (Общие условия + элементы + объекты).

Определение чувствительных элементов



Для обеспечения правильного функционирования бизнес-процесса необходимо определить **чувствительность** каждого существенного элемента.

Это определение основано на различных **критериях безопасности**, таких как готовность, целостность и конфиденциальность. Если эта чувствительность не учтена, возникнет **воздействие** на организацию, которое может принимать различные формы, например, нарушение физической ядерной безопасности, ухудшение безопасности, ухудшение выполнения деятельности, потеря доверия клиентов или финансовые потери.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Возвращаясь к примеру параметра запуска насоса системы теплоносителя электростанции, требование наличия и целостности для этой информации должно быть высоким, с тем чтобы избежать любого вредного воздействия на материал, окружающую среду или персонал, а также на эксплуатационную готовность станции.

Результат: Чувствительность элементов.

Исследование угроз

Для каждой организации характерны специфические факторы угрозы, зависящие от ее естественного окружения, культуры, репутации, области деятельности и т.д. Фактор угрозы может характеризоваться типом (природный, связанный с человеком или экологический) и причиной (случайный или преднамеренный).

Фактор угрозы может использовать различные **методы атаки**, которые поэтому необходимо определить. Метод атаки характеризуется атрибутами физической безопасности (например, эксплуатационной готовностью, целостностью, конфиденциальностью), которые он может нарушить, и вероятными факторами угрозы.

Возвращаясь к данному примеру, на атомной электростанции необходимо принимать во внимание большое количество факторов угрозы, детально рассмотренных в разделе 6.3:

— шпионаж/кражу технологии;
— рассерженных служащих/пользователей (внутренних или внешних;)
— хакеров-любителей;
— кибератакистов;
— представителей организованной преступности;
— государства;
— террористов.

А также методы атак:

— подслушивание;
— лавинная адресация/отказ в обслуживании;

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

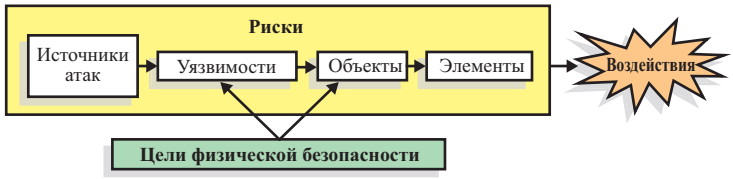
— создание программных ловушек/проникновение в систему обходным путем;
— атаки с целью взлома имен пользователей/паролей (атаки методом прямого перебора, с использованием словарей и т.п.).

Каждому объекту присущи **уязвимости**, которыми могут воспользоваться факторы угрозы, применяя соответствующие методы атаки. Поэтому можно указать ряд уязвимостей, связанных с системой теплоносителя АЭС:

— возможность существования скрытых функций, введенных на этапах проектирования и разработки (программное обеспечение);
— использование оборудования, не подвергшегося оценке (аппаратные средства);
— возможность создания или изменения системных команд в онлайновом режиме (сети);
— сеть, которая может использоваться для вмешательства в программное обеспечение, относящееся к системным ресурсам (сети);
— легкость проникновения на площадку с использованием косвенных путей доступа (помещения);
— несоблюдение операторами инструкций (персонал);
— отсутствие мер безопасности на этапах проектирования, монтажа и эксплуатации (организация).

Результат: Формализация угроз (включая сценарии).

Определение целей физической безопасности



Теперь определим, какое влияние на существенные элементы могут оказывать факторы угрозы и их методы атак: это – **риск**.

Риск представляет возможный ущерб. Это является следствием того факта, что фактор угрозы может повлиять на существенные элементы, используя определенный метод атаки для того, чтобы воспользоваться уязвимостью объектов, от которых зависят данные элементы.

В приведенном примере существует риск того, что чувствительная информация будет использована путем создания программных ловушек

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

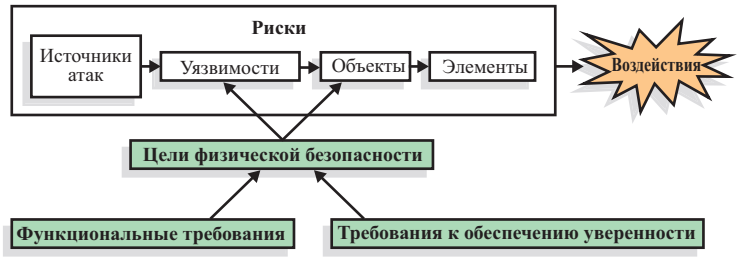
благодаря возможности создания или изменения системных команд, связанных с сетью, что может провести к последствиям в отношении материала, окружающей среды, безопасности персонала, эксплуатационной готовности станции и общественного доверия.

Цели физической безопасности состоят главным образом в снижении уязвимости объектов, представляющих все сохраняющиеся риски. Очевидно, что нет смысла в защите того, что не подвергается опасности. Однако по мере роста потенциального риска должна также возрастать строгость целей физической безопасности. Поэтому такие цели представляют собой полностью адаптированный набор технических требований.

Одна из целей физической безопасности атомной электростанции в данном примере состоит в том, чтобы обеспечить защиту при создании и модификации связанных с сетью **системных команд** для системы теплоносителя.

Результат: Цели физической безопасности.

Определение требований физической безопасности



Группа, отвечающая за осуществление подхода, должна затем выработать точные спецификации для необходимых функций физической безопасности. После этого она должна продемонстрировать, что эти **функциональные требования** полностью соответствуют целям физической безопасности.

В данном примере функциональные требования по защите создания и модификации системных команд, связанных с сетью, могут включать:

— ряд самопроверок, регулярно выполняемых системой в нормальном режиме эксплуатации с целью подтверждения того, что она работает правильно;
— физический и логический контроль доступа.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

И наконец, ответственная группа должна определить **требования к обеспечению уверенности**, позволяющие достигнуть и затем продемонстрировать необходимый уровень уверенности.

Одно из требований к обеспечению уверенности может заключаться в том, что разработчик должен выполнить анализ устойчивости системных функций физической безопасности при требуемом уровне устойчивости.

Результат: Функциональные требования и требования к обеспечению уверенности.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Приложение III

РОЛЬ ОШИБКИ ЧЕЛОВЕКА В КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

В данном приложении рассматриваются вопросы действий человека в связи с компьютерной безопасностью; в частности, анализируется, как действия человека могут повлиять на способность организации сопротивляться атаке, распознавать атаку, восстанавливать важные данные/услуги и адаптироваться к появляющимся угрозам. Исследования продолжают стимулировать разработку технических решений, таких как программное обеспечение для мониторинга безопасности, программы обнаружения/предотвращения проникновения, усовершенствованные системы аутентификации и более надежные методы шифрования, но при этом человеческий фактор в качестве причины и профилактической меры в сфере компьютерной безопасности зачастую игнорируется.

Во многих докладах ошибка человека указывается в качестве основной причины нарушений компьютерной безопасности. Согласно недавним оценкам, доля нарушений, связанных с ошибкой человека, составляет 60-80%. Большинство этих ошибок, возможно, удалось бы предотвратить путем увеличения инвестиций в информирование и более четкой организации эксплуатации и надзора.

Одной из целей программы по компьютерной безопасности является обеспечение живучести системы/живучести при эксплуатации. Элементами живучести системы являются:

— устойчивость системы к атакам;
— распознавание атак и оценка ущерба;
— восстановление важнейших сервисов и полное восстановление обслуживания;
— адаптация и эволюция системы в качестве защиты от будущих атак.

В таблице III–1 перечислены эти области, требующие особого внимания, и делается попытка категоризировать общие типы ошибок человека в процессах и применениях. В ней указаны ошибки человека, связанные как с системными администраторами, так и с пользователями систем. Данный перечень не является исчерпывающим; его цель - проиллюстрировать уровень взаимодействия с человеком, связанного с осуществлением этих систем и процессов.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

ТАБЛИЦА III–1. РАСПРОСТРАНЕННЫЕ ОШИБКИ ЧЕЛОВЕКА

Процесс/применение	Распространенные ошибки человека
Устойчивость к атакам	
Ограничение доступа (Системное администрирование)	—Неправильно распределены полномочия доступа к файлам. —Продолжают действовать ненужные серверные процессы. —Оставлены открытыми уязвимые порты. —Предоставлен физический доступ. —Не используются скринсейверы с паролем. —Не устанавливаются системные исправления. —Нет понимания значения установки исправлений. —Загрузка/установка вредоносного/поврежденного программного обеспечения.
Создание/использование паролей	—Пароли записываются. —Слабые пароли. —Использование заданных по умолчанию паролей. —Раскрытие пароля. —Неиспользование пароля. —Использование одного и того же пароля в защищенных и незащищенных системах.
Распознавание атак и определение ущерба	
Системы обнаружения проникновения	—Неправильная конфигурация (набор правил). —Не устанавливаются системные обновления. —Невнимательный просмотр регистрационного файла.
Аудит регистрационных файлов	—Недостаточно внимательный просмотр регистрационных файлов. —Неуделение внимания тенденциям на протяжении ряда регистрационных периодов.
Восстановление системы	
Создание резервных копий и восстановление	—Невыполнение операций по созданию резервных копий. —Несвоевременное выполнение операций по созданию резервных копий. —Неправильная конфигурация. —Физическое повреждение носителей резервных копий. —Случайное удаление данных. —Хранение носителей резервных копий в не имеющем физической защиты/незащищенном месте. —Использование неисправных носителей. —Неправильная маркировка носителей. —Физическое разрушение носителей. —Невыполнение тестирования процедур восстановления. —Невыполнение операций по созданию нескольких копий критической системной информации. —Непринятие мер по хранению носителей резервных копий в месте, расположенном вне площадки.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

ТАБЛИЦА III–1. РАСПРОСТРАНЕННЫЕ ОШИБКИ ЧЕЛОВЕКА

Процесс/применение	Распространенные ошибки человека
Адаптация к новым угрозам	
Процедуры компании	—Незнание политики компании. —Нарушение политики компании. —Отсутствие в компании политики восстановления данных. —Использование устарелой политики. —Невыполнение проверки политики/рабочих процедур. —Неприменение мер по обеспечению соблюдения политики.

Хотя основное внимание в таблице уделено отрицательным аспектам действий человека, необходимо также отметить и положительное влияние этих действий. Будучи иногда самым слабым звеном в цепочке, человек-оператор или служащий может сыграть роль блокирующего фактора, предотвращающего отказ или ухудшение работы системы. Технология никогда не обеспечит полного решения проблем. Служащие являются одним из уровней стратегии глубокоэшелонированной защиты для обеспечения физической безопасности/жизнеспособности систем. Результаты обследований регулярно показывают, что главной проблемой физической безопасности являются недостаточная информированность и подготовка в сфере компьютерной безопасности.

Для того чтобы служащих можно было в полной мере использовать в качестве актива для обеспечения компьютерной безопасности и жизнеспособности систем, необходимо, чтобы они обладали:

— глубоким пониманием важности их роли в общем плане обеспечения компьютерной безопасности;
— знаниями и навыками в сфере компьютерной безопасности, необходимыми для выполнения своих служебных обязанностей;
— пониманием того, что эффективная культура физической безопасности начинается с них.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

ОПРЕДЕЛЕНИЯ

Для целей данной публикации следующие ниже термины используются в указанных здесь значениях. Эти определения могут отличаться от тех, которые используются в других дисциплинах. В тех случаях, когда это было возможно, определения были взяты из выпущенных публикаций МАГАТЭ, хотя значения нескольких терминов соответствуют специфическому контексту компьютерной безопасности. Другие определения заимствованы из международных стандартов (например, [1, 15, 23] в настоящей публикации).

Атака (attack). Попытка разрушить, лишить защиты, изменить, отключить, похитить актив или получить несанкционированный доступ к нему или неправомочно использовать его (ИСО).

Аутентификация (authentication). Обеспечение уверенности в том, что заявленная характеристика объекта является правильной (ИСО).

Глубокоэшелонированная защита (defence in depth). Сочетание последовательных уровней систем и мер по защите целей от угроз физической ядерной безопасности.

Готовность (availability). Свойство, обеспечивающее доступность и возможность использования по требованию объектом, имеющим разрешение (ИСО).

Информационная безопасность (information security). Сохранение конфиденциальности, целостности и доступности информации.
Примечание: Кроме того, могут также быть затронуты другие свойства, такие как аутентичность, подотчетность, безотказность и надежность (ИСО).

Инцидент, связанный с компьютерной безопасностью (computer security incident). Событие, при котором фактически или потенциально подвергается опасности конфиденциальность, целостность или готовность компьютерных, сетевых или цифровых информационных систем или доступность информации, которую система обрабатывает, хранит или передает, или которое представляет собой нарушение или неизбежный риск нарушения политики безопасности, процедур безопасности или приемлемых правил пользования.

Настоящая публикация была заменена публикацией № 17-Т (Rev. 1).

Компьютерная безопасность (computer security). Специфический аспект информационной безопасности, относящийся к компьютерным системам, сетям и цифровым системам.

Контрмера (countermeasure). Действие, предпринимаемое с целью противодействия угрозе или устранения или уменьшения уязвимостей.

Контроль доступа (access control). Способ обеспечения санкционированного и ограниченного доступа к активам на основе требований бизнес-процессов и безопасности (ИСО).

Конфиденциальность (confidentiality). Свойство, в силу которого информация не предоставляется и не раскрывается по запросам не имеющих разрешения лиц, объектов или процессов (ИСО).

Оценка риска (risk assessment). Общий процесс систематического определения, рассмотрения, анализа и оценки риска.

Периметр компьютерной безопасности (computer security perimeter). Логическая граница вокруг сети, к которой подключены критические активы и доступ к которой контролируется.

Политика обеспечения компьютерной безопасности (computer security policy). Совокупность директив, регулирующих положений, правил и практики, предписывающая порядок того, как организация управляет компьютерами и компьютерными системами и обеспечивает их защиту.

Риск (risk). Потенциальная возможность того, что заданная угроза использует уязвимости актива или группы активов и тем самым нанесет ущерб организации. Он измеряется как сочетание вероятности события и серьезности его последствий.

Служебная необходимость (need to know). Принцип, в соответствии с которым пользователям, процессам и системам предоставляется доступ только к той информации, возможностям и активам, которые необходимы для выполнения возложенных на них функций.

Социальная инженерия (social engineering). Нетехническая форма сбора информации или атаки, при которой взаимодействие с людьми используется для принуждения людей, путем манипулирования их сознания, к неосознанному нарушению процедур безопасности,

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

например, раскрытию информации или выполнению других действий, воздействующих на безопасность.

Угроза (threat). Потенциальная причина нежелательного инцидента, который может приводить к нанесению ущерба системе или организации (ИСО).

Примечание: В других публикациях серии изданий МАГАТЭ по физической безопасности «угроза», как правило, определяется как «лицо или группа лиц, имеющих мотивацию, намерение и потенциал совершить злоумышленное действие». Однако в настоящей публикации данный термин используется в контексте компьютерной безопасности, где угроза не обязательно связана с одним или несколькими лицами.

Уязвимость (vulnerability). Слабость актива или мер контроля, которая может быть использована для осуществления угрозы (ИСО).

Целостность (integrity). Способность защиты точности и полноты активов (ИСО).

Ядерная установка (nuclear facility). Установка (включая связанные с ней здания и оборудование), на которой осуществляется производство, переработка, использование, обработка, хранение или захоронение (утилизация) ядерного материала и для которой требуется разрешение или лицензия.

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

IAEA
Международное агентство по атомной энергии

Где заказать публикации МАГАТЭ

В указанных странах публикации МАГАТЭ могут быть приобретены у перечисленных ниже поставщиков или в крупных книжных магазинах. Оплата может производиться в местной валюте или купонами ЮНЕСКО.

АВСТРАЛИЯ
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Телефон: +61 3 9210 7777 • Факс: +61 3 9210 7788
Эл. почта: service@dadirect.com.au • Веб-сайт: http://www.dadirect.com.au

БЕЛЬГИЯ
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Телефон: +32 2 538 43 08 • Факс: +32 2 538 08 41
Эл. почта: jean.de.lannoy@infoboard.be • Веб-сайт: http://www.jean-de-lannoy.be

ВЕНГРИЯ
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Телефон: +36 1 257 7777 • Факс: +36 1 257 7472 • Эл. почта: books@librotrade.hu

ГЕРМАНИЯ
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Телефон: + 49 228 94 90 20 • Факс: +49 228 94 90 20 или +49 228 94 90 222
Эл. почта: bestellung@uno-verlag.de • Веб-сайт: http://www.uno-verlag.de

ИНДИЯ
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Телефон: +91 22 22617926/27 • Факс: +91 22 22617928
Эл. почта: alliedpl@vsnl.com • Веб-сайт: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Телефон: +91 11 23268786, +91 11 23257264 • Факс: +91 11 23281315
Эл. почта: bookwell@vsnl.net

ИСПАНИЯ
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Телефон: +34 91 781 94 80 • Факс: +34 91 575 55 63
Эл. почта: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Веб-сайт: http://www.diazdesantos.es

ИТАЛИЯ
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Телефон: +39 02 48 95 45 52 или 48 95 45 62 • Факс: +39 02 48 95 45 48
Эл. почта: info@libreriaaeiou.eu • Веб-сайт: www.libreriaaeiou.eu

КАНАДА
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Телефон 1-800-865-3457 • Факс: 1-800-865-3450
Эл. почта: customercare@bernan.com • Веб-сайт: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Телефон: +613 745 2665 • Факс: +613 745 7660
Эл. почта: order.dept@renoufbooks.com • Веб-сайт: http://www.renoufbooks.com

КИТАЙ
Публикации МАГАТЭ на китайском языке:
China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

НИДЕРЛАНДЫ
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Телефон: +31 (0) 53 5740004 • Факс: +31 (0) 53 5729296
Эл. почта: books@delindeboom.com • Веб-сайт: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Телефон: +31 793 684 400 • Факс: +31 793 615 698
Эл. почта: info@nijhoff.nl • Веб-сайт: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Телефон: +31 252 435 111 • Факс: +31 252 415 888
Эл. почта: infoho@swets.nl • Веб-сайт: http://www.swets.nl

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

НОВАЯ ЗЕЛАНДИЯ
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Телефон: +61 3 9210 7777 • Факс: +61 3 9210 7788
Эл. почта: service@dadirect.com.au • Веб-сайт: http://www.dadirect.com.au

ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Телефон: +800 253-9646 или +212 963-8302 • Факс: +212 963-3489
Эл. почта: publications@un.org • Веб-сайт: http://www.un.org

РЕСПУБЛИКА КОРЕЯ
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137 130
Телефон: +02 589 1740 • Факс: +02 589 1746 • Веб-сайт: http://www.kins.re.kr

СЛОВЕНИЯ
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Телефон: +386 1 432 31 44 • Факс: +386 1 230 14 35
Эл. почта: import.books@cankarjeva-z.si • Веб-сайт: http://www.cankarjeva-z.si/uvoz

СОЕДИНЕННОЕ КОРОЛЕВСТВО
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Телефон (заказы): +44 870 600 5552 • (справки): +44 207 873 8372 • Факс: +44 207 873 8203
Эл. почта (заказы): book.orders@tso.co.uk • (справки): book.enquiries@tso.co.uk • Веб-сайт: http://www.tso.co.uk

Онлайн-заказы
DELTA Int Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Эл. почта: info@profbooks.com • Веб-сайт: http://www.profbooks.com

Книги по экологии
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Телефон: +44 1438748111 • Факс: +44 1438748844
Эл. почта: orders@earthprint.com • Веб-сайт: http://www.earthprint.com

СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346
Телефон: 1-800-865-3457 • Факс: 1-800-865-3450
Эл. почта: customercare@bernan.com • Веб-сайт: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Телефон: +888 551 7470 (бесплатный) • Факс: +888 568 8546 (бесплатный)
Эл. почта: order.dept@renoufbooks.com • Веб-сайт: http://www.renoufbooks.com

ФИНЛЯНДИЯ
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Телефон: +358 9 121 41 • Факс: +358 9 121 4450
Эл. почта: akatilaus@akateeminen.com • Веб-сайт: http://www.akateeminen.com

ФРАНЦИЯ
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Телефон: +33 1 42 01 49 49 • Факс: +33 1 42 01 90 90
Эл. почта: formedit@formedit.fr • Веб-сайт: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Телефон: + 33 1 47 40 67 02 • Факс +33 1 47 40 67 02
Эл. почта: romuald.verrier@lavoisier.fr • Веб-сайт: http://www.lavoisier.fr

ЧЕШСКАЯ РЕСПУБЛИКА
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Телефон: +420 26603 5364 • Факс: +420 28482 1646
Эл. почта: nakup@suweco.cz • Веб-сайт: http://www.suweco.cz

ЯПОНИЯ
Maruzen Company Ltd, 1-9-18, Kaigan, Minato-ku, Tokyo, 105-0022
Телефон: +81 3 6367 6079 • Факс: +81 3 6367 6207
Эл. почта: journal@maruzen.co.jp • Веб-сайт: http://www.maruzen.co.jp

Заказы и запросы в отношении информации можно также направлять непосредственно по адресу:

Группа сбыта и маркетинга, Международное агентство по атомной энергии -
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
Эл. почта: sales.publications@iaea.org • Веб-сайт: http://www.iaea.org/books

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

12-12794

Настоящая публикация была заменена публикацией № 17-T (Rev. 1).

Цель настоящей публикации – обеспечить понимание важности вопросов компьютерной безопасности как фундаментальной составной части общего плана обеспечения физической безопасности ядерных установок. Еще одной целью является предоставление для ядерных установок руководящих материалов по осуществлению программы компьютерной безопасности, а также рекомендаций по оценке существующих программ, анализу критических цифровых активов и определению соответствующих мер по снижению риска.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА
ISBN 978–92–0–435510–9
ISSN 1816–9317