Разработки и управление системой менеджмента информационной безопасности

Холодков А.С. – заместитель генерального директора АНО «ЦНКЭС», заместитель руководителя Органа по сертификации систем менеджмента АНО «ЦНКЭС»

Раздел 4.3 ГОСТ РВ 0015–002–2012 «Система разработки и постановки на производство военной техники. Системы менеджмента качества. Общие требования» определяет, что в организации должен быть определен и документально оформлен порядок организации и выполнения работ по защите информации об образцах военной продукции, учитывающий характер и условия выполнения оборонного заказа при несанкционированном воздействии на информацию.

Большинство организаций, сертифицировавших СМК на соответствие требованиям вышеуказанного стандарта, ограничивают выполнение требований раздела 4.3 созданием документированной процедуры, описывающей свою деятельность по защите информации.

При выполнении госзаказа, на стадии разработки контрактов (договоров), как показывает практика, организации необходимо иметь документально оформленный порядок выполнения работ по обеспечению информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001–2006 и сертифицированную систему менеджмента информационной безопасности (СМИБ) на соответствие требованиям данного стандарта, что должны поддержать и ВП (так как СМИБ, а не СМК обеспечивает в полном объеме защиту данных и информации на всех стадиях работ по разработке и производству оборонной продукции).

Управление СМИБ осуществляется на уровне организации совершенно другими должностными лицами и подразделениями чем в СМК. В организации разрабатывается и принимается Политика информационной безопасности, разрабатываются цели и планы СМИБ, определяются функции и ответ-

ственность в области СМИБ и другие действия в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001–2006.

Ниже, приведена таблица с примерами проводимых мероприятий и необходимых документов при создании и функционировании СМИБ, которая учитывает также требования государственных нормативных документов в данной области (см. Библиографию).

Перечень мероприятий по обеспечению информационной безопасности при проектировании (разработке), производстве образцов военной продукции в организации

Политика информационной безопасности организации

1. Политика информационной безопасности		
Цель: Обеспечить управление и поддержку высшим руководством Организации информационной безопасности в соответствии с требованиями бизнеса и соответствующими правовыми нормами.		
1.1.	Документ политики информационной безопасности	Документ политики информационной безопасности должен быть утвержден руководством Организации, издан и надлежащим образом доведен до сведения всех сотрудников организации и соответствующих сторонних организаций
1.2.	Пересмотр политики информационной безопасности	Политика информационной безопасности в Организации, должна пересматриваться либо через запланированные интервалы времени, либо в случае значительных изменений для обеспечения ее сохраняющейся пригодности, адекватности и эффективности
2. Организация информационной безопасности в организации		
2.1. Внутренняя организация		
Цель: Менеджмент информационной безопасности в Организации		
2.1.1.	Обязательства руководства в отношении информационной безопасности	Руководство Организации, должно активно поддерживать информационную безопасность в организации посредством четкого управления, видимой поддержки, четкого распределения обязанностей и признания ответственности в отношении информационной безопасности
2.1.2.	Координация вопросов информационной безопасности	Деятельность по информационной безопасности должна координироваться представителями различных подразделений Организации, имеющими соответствующие задачи и должностные функции

2.1.3.	Распределение ответственности по информационной безопасности	Все меры ответственности по информационной безопасности должны быть четко определены
2.1.4.	Процесс авторизации на использование средств обработки информации	Руководство Организации должно определить и реализовать процесс авторизации на использование новых средств обработки информации
2.1.5.	Соглашения о конфиденциальности	Требования по конфиденциальности или соглашения о неразглашении, отражающие потребности Организации в защите информации, должны быть определены и регулярно пересматриваться
2.1.6	Контакт с различными инстанциями	Должны поддерживаться нужные контакты с соответствующими инстанциями
2.1.7	Контакт со специальными группами по интересам	Должны поддерживаться нужные контакты со специальными группами по интересам или другими советами по безопасности и профессиональными ассоциациями
2.1.8	Независимый пересмотр информационной безопасности	Подход организации к менеджменту информационной безопасности и ее реализации (т.е. цели контроля, меры контроля, политики, процессы и процедуры информационной безопасности) должен пересматриваться независимым образом через запланированные интервалы времени или после значительных изменений в реализации безопасности
3. Внешние стороны		
Цель: Поддерживать безопасность информации и средств обработки информации в Организации, при наличии доступа к ним внешних сторон в процессах обработки, передачи или управления		
3.2.1	Идентификация рисков, связанных с внешними сторонами	Риски для информации и средств обработки информации, являющиеся следствием бизнес-процессов, в которых участвуют внешние стороны, должны быть идентифицированы, и соответствующие меры контроля должны быть реализованы прежде, чем будет предоставлен доступ
3.2.2	Рассмотрение требований безопасности при работе с клиентами	Все определенные требования безопасности должны быть рассмотрены прежде, чем клиентам будут даны права доступа к информации или активам организации

3.2.3	Рассмотрение требований безопасности в договорах с третьей стороной	Договоры с третьей стороной, включающие доступ, обработку, передачу или менеджмент информации, или средств обработки информации организации, или дополнение продуктами или сервисами средств обработки информации, должны охватывать все соответствующие требования безопасности

4. Классификация информации

Цель: Обеспечить уверенность в том, что информационные активы защищены на надлежащем уровне

4.1	Основные принципы классификации	Информация должна быть классифицирована в терминах по ее значимости, правовым требованиям, важности и критичности для организации
4.2	Маркировка и обработка информации	В соответствии с системой классификации, принятой в организации, должна быть разработана и реализована совокупность процедур для маркировки и обработки информации

5. Вопросы безопасности, связанные с персоналом

Цель: Обеспечить уверенность в том, что сотрудники Организации, подрядчики и пользователи третьей стороны осознают свою ответственность и способны выполнять предусмотренные для них роли и снижать риск от воровства, мошенничества и нецелевого использования оборудования

5.1	Роли и ответственности	Роли и ответственность в области безопасности сотрудников Организации, подрядчиков и пользователей третьей стороны должны быть определены и документированы в соответствии с политикой информационной безопасности организации
5.2	Проверка персонала при найме	Основная проверка всех кандидатов на постоянную занятость, подрядчиков и пользователей третьей стороны должна проводиться в соответствии с законами, инструкциями и правилами этики, соответственно требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и предполагаемым рискам
5.3	Условия приема на работу	Как часть своего договорного обязательства, сотрудники Организации, подрядчики и пользователи третьей стороны должны соглашаться и подписывать условия своего трудового договора, в котором должна устанавливаться их ответственность и ответственность организации относительно информационной безопасности

6. В течение занятости		
Цель: Обеспечить уверенность в том, что сотрудники Организации, подрядчики и пользователи третьей стороны осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, и оснащены для поддержки политики безопасности организации при выполнении своих служебных обязанностей и для снижения риска человеческих ошибок		
6.1	Обязанности руководства	Руководство Организации должно требовать, чтобы сотрудники, подрядчики и пользователи третьей стороны обеспечивали безопасность в соответствии с установленными политиками и процедурами организации
6.2	Осведомленность, образование и обучение в области информационной безопасности	Все сотрудники Организации, при необходимости, подрядчики и пользователи третьей стороны должны пройти соответствующее обучение и получать регулярно обновленные варианты политик и процедур организации, нужные для выполнения их должностных функций
6.3	Дисциплинарный процесс	Должен существовать действующий дисциплинарный процесс, применяемый к сотрудникам Организации, совершившим нарушение безопасности
7. Прекращение занятости или смена работы персонала		
Цель: Обеспечить уверенность в том, что сотрудники Организации, подрядчики и пользователи третьей стороны покидают организацию или меняют место работы должным образом		
7.1	Ответственности при прекращении занятости	Ответственность при прекращении занятости или смене места работы должна быть четко определена и установлена
7.2	Возврат активов	Все сотрудники Организации, подрядчики и пользователи третьей стороны обязаны вернуть все активы организации, находящиеся в их пользовании, по истечении срока действия их занятости, договора или соглашения
7.3	Аннулирование прав доступа	Права доступа всех служащих, подрядчиков и пользователей третьей стороны к информации и средствам обработки информации должны быть аннулированы по истечении срока действия занятости, договора или соглашения, или скорректированы после смены места работы в организации
8. Физическая безопасность и безопасность от воздействия окружающей среды		
8.1 Зоны безопасности		
Цель: Предотвращать неавторизованный физический доступ, повреждение и воздействие на помещения и информацию Организации		

8.1.1	Физический периметр безопасности	Для защиты зон, где имеется информация и средства обработки информации, должны использоваться периметры безопасности (барьеры, такие как стены, проходные, оборудованные средствами контроля входа по идентификационным карточкам, или сотрудник на стойке регистрации)
8.1.2	Физические средства контроля входа	Зоны безопасности должны быть защищены соответствующими средствами контроля входа, чтобы обеспечить уверенность в том, что только авторизованный персонал может получить доступ в зону
8.1.3	Безопасность зданий, производственных помещений и оборудования	Физическая безопасность зданий, производственных помещений и оборудования должна быть разработана и применена
8.1.4	Защита от внешних угроз и угроз окружающей среды	Физическая защита от нанесения ущерба в результате пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных и антропогенных бедствий должна быть разработана и применена
8.1.5	Работа в зонах безопасности	Физическая защита и инструкции по работе в зонах безопасности должны быть разработаны и применены
8.1.6	Зоны общественного доступа, приемки и отгрузки	Места доступа, такие как зоны приема, отгрузки и другие места, где неавторизованные лица могут проникнуть в помещения, должны контролироваться и, по возможности, должны быть изолированы от средств обработки информации во избежание неавторизованного доступа
9. Безопасность оборудования		
Цель: Предотвращать потерю, повреждение или компрометацию активов и прерывание деятельности организации		
9.1	Размещение и защита оборудования	Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности неавторизованного доступа
9.2	Поддерживающие услуги	Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с отказами поддерживающих услуг
9.3	Безопасность кабельной сети	Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживаются информационные услуги, необходимо защищать от перехвата информации или повреждения

9.4	Техническое обслуживание оборудования	Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности
9.5	Безопасность оборудования, используемого вне помещений организации	При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны учитываться различные риски, связанные с работой вне помещений организации
9.6	Безопасная утилизация или повторное использование оборудования	Все компоненты оборудования, содержащие носители данных, должны быть проверены с целью обеспечения уверенности в том, что любые чувствительные данные и лицензионное ПО были удалены или переписаны безопасным образом до их утилизации (списания)
9.7	Вынос имущества	Оборудование, информацию или ПО можно выносить из помещения организации только на основании соответствующего разрешения

10. Менеджмент коммуникаций и функционирования

10.1 Операционные процедуры и ответственность

Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации

10.1.1	Документальное оформление операционных процедур	Операционные процедуры должны быть документально оформлены, поддерживаться и быть доступными для всех авторизованных пользователей
10.1.2	Менеджмент изменений	Изменения в средствах обработки информации и системах должны контролироваться
10.1.3	Разграничение обязанностей	Обязанности и области ответственности должны быть разграничены в целях снижения возможностей неавторизованной или непреднамеренной модификации, или нецелевого использования активов Организации
10.1.4	Разграничение средств разработки, тестирования и эксплуатации	Средства разработки, тестирования и эксплуатации должны быть разделены с целью снижения рисков неавторизованного доступа или изменения операционной системы

10.2 Менеджмент оказания услуг третьими сторонами

Цель: Реализовать и поддерживать соответствующий уровень информационной безопасности и оказания услуг в соответствии с договорами оказания услуг третьими сторонами (внешними лицами и/или организациями)

10.2.1	Оказание услуг	Должна быть обеспечена уверенность в том, что средства контроля безопасности, определения и уровни оказания услуг, включенные в договор оказания услуг третьей стороной, реализованы, функционируют и поддерживаются третьей стороной
10.2.2	Мониторинг и анализ услуг, оказываемых третьими сторонами	Услуги, отчеты и контрольные записи, обеспечиваемые третьей стороной, должны подвергаться мониторингу и анализироваться, а также должны регулярно проводиться аудиты
10.2.3	Менеджмент изменений в услугах, оказываемых третьими сторонами	Изменения при оказании услуг, включая поддержку и совершенствование существующих политик, процедур и средств контроля информационной безопасности, должны управляться с учетом критичности систем и процессов бизнеса, а также результатов переоценки рисков
10.3 Планирование нагрузки и приемки систем		
Цель: Свести к минимуму риск сбоев в работе систем		
10.3.1	Менеджмент производительности	Использование ресурсов должно подвергаться мониторингу, корректироваться и прогнозироваться на будущие потребности мощности, чтобы обеспечить требуемую производительность системы
10.3.2	Приемка систем	Должны быть определены критерии принятия новых информационных систем, новых версий и обновлений, а также проводиться необходимое тестирование систем в процессе разработки и перед их приемкой
10.4 Защита от вредоносного и мобильного кода		
Цель: Защищать целостность программного обеспечения и информации		
10.4.1	Средства контроля против вредоносного кода	Должны быть реализованы средства контроля с целью обнаружения, предотвращения или восстановления после проникновения вредоносного кода, а также процедуры, обеспечивающие соответствующую осведомленность пользователей
10.4.2	Средства контроля против мобильного кода	Там, где разрешено использование мобильного кода, конфигурация должна обеспечивать, что авторизованный мобильный код исполняется соответственно четко определенной политике безопасности, а неавторизованный мобильный код не будет исполняться
10.5 Резервирование		
Цель: Поддерживать целостность и доступность информации и средств обработки информации		

10.5.1	Резервирование информации	Резервные копии информации и программного обеспечения должны извлекаться и тестироваться на регулярной основе в соответствии с принятой политикой резервирования

10.6 Менеджмент безопасности сети

Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры Организации

10.6.1	Средства контроля сетевых ресурсов	Сети должны адекватно управляться и контролироваться, чтобы обеспечить их защиту от угроз и поддерживать безопасность систем и приложений, использующих сеть, включая информацию, передаваемую по сетям
10.6.2	Безопасность сетевых услуг	Средства безопасности, уровни обслуживания и требования менеджмента всех сетевых услуг должны быть определены и включены в любой договор о сетевых услугах, независимо от того, будут ли они обеспечиваться силами организации или третьей стороной

10.7 Обращение с носителями информации

Цель: Предотвратить неавторизованное раскрытие, модификацию, удаление или разрушение активов и прерывание деятельности бизнеса

10.7.1	Менеджмент использования сменных носителей информации	Должны существовать процедуры менеджмента использования сменных носителей информации
10.7.2	Утилизация носителей информации	Носители информации, когда в них больше нет необходимости, должны надежно и безопасно утилизироваться, используя формальные процедуры
10.7.3	Процедуры обработки информации	С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования, необходимо установить процедуры обработки и хранения информации
10.7.4	Безопасность системной документации	Должна быть обеспечена защита системной документации от неавторизованного доступа

10.8 Обмен информацией

Цель: Поддерживать безопасность информации и ПО при обмене внутри Организации и с любой внешней сущностью

10.8.1	Политики и процедуры обмена информацией	Должны существовать формальные процедуры, политики и меры контроля для защиты обмена информацией при использовании всех типов коммуникации

10.8.2	Соглашения по обмену информацией	Должны быть установлены соглашения для обмена информацией и ПО между Организации и внешними сторонами
A.10.8.3	Физические носители информации при пересылке	Носители информации должны быть защищены от неавторизованного доступа, неправильного использования или повреждения во время их транспортировки за пределами физических границ Организации
A.10.8.4	Электронный обмен сообщениями	Информация в электронном обмене сообщениями должна быть защищена надлежащим образом

10.9 Услуги электронной торговли

Цель: Обеспечить безопасность услуг электронной торговли и их безопасное использование

10.9.1	Электронная торговля	Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошеннической деятельности, оспаривания контрактов, а также от неавторизованного раскрытия и модификации
10.9.2	Транзакции в режиме online	Информация, используемая в online транзакциях, должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, неавторизованного изменения сообщений, неавторизованного раскрытия, неавторизованного копирования или возвращения сообщений
10.9.3	Общедоступная информация	Целостность информации, которая сделана доступной в общедоступной системе, должна быть защищена для предотвращения неавторизованной модификации

10.10 Мониторинг

Цель: Обнаруживать неавторизованные действия, связанные с обработкой информации

10.10.1	Ведение журналов аудита	Должны вестись и храниться в течение согласованного периода времени журналы аудита, регистрирующие действия пользователей, нештатные ситуации и события, имеющие отношение к информационной безопасности, чтобы помочь в будущих расследованиях и проведении мониторинга контроля доступа
10.10.2	Мониторинг использования систем	Должны быть установлены процедуры для мониторинга использования средств обработки информации, а результаты мониторинга должны регулярно анализироваться

10.10.3	Защита информации журналов регистрации	Средства регистрации и информация журналов регистрации должны быть защищены от вмешательства и неавторизованного доступа
10.10.4	Журналы регистрации администратора и оператора	Действия системного администратора и системного оператора должны регистрироваться
10.10.5	Регистрация неисправностей	Неисправности должны регистрироваться, анализироваться, и в их отношении должны приниматься соответствующие действия
10.10.6	Синхронизация часов	Часы всех соответствующих систем обработки информации в пределах организации или зоны безопасности должны быть синхронизированы с согласованным точным источником времени

11. Контроль доступа

11.1 Требование бизнеса к контролю доступа

Цель: Контролировать доступ к информации

11.1.1	Политика контроля доступа	Должна быть установлена политика контроля доступа, которая документируется и пересматривается с учетом требований бизнеса и безопасности к доступу

11.2 Менеджмент доступа пользователей

Цель: Предотвратить неавторизованный доступ пользователей к информационным системам и обеспечить авторизованный доступ пользователей к этим системам

11.2.1	Регистрация пользователей	Должна существовать формализованная процедура регистрации и снятия с регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и услугам
11.2.2	Менеджмент привилегий	Предоставление и использование привилегий должно быть ограниченным и контролируемым
11.2.3	Менеджмент паролей пользователей	Предоставление паролей должно контролироваться посредством формализованного процесса менеджмента
11.2.4	Пересмотр прав доступа пользователей	Руководство Организации должно осуществлять периодически пересмотр прав доступа пользователей, используя формальный процесс

11.3 Ответственность пользователей

Цель: Предотвращать неавторизованный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации

11.3.1	Использование паролей	Пользователи должны следовать общепринятой практике в области безопасности при выборе и использовании паролей

11.3.2	Оборудование, оставленное пользователями без присмотра	Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра
11.3.3	Политика «чистого стола» и «чистого экрана»	Должна быть принята политика «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политика «чистого экрана» в отношении средств обработки информации
11.4 Контроль сетевого доступа		
Цель: Защита сетевых сервисов		
11.4.1	Политика использования сетевых услуг	Пользователям следует предоставлять доступ только к тем услугам, к которым они специально были авторизованы
11.4.2	Аутентификация пользователя для внешних соединений	Для контроля доступа удаленных пользователей должны применяться соответствующие методы аутентификации
11.4.3	Идентификация оборудования в сетях	Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием
11.4.4	Защита диагностических и конфигурационных портов при удаленном доступе	Доступ к портам конфигурации и диагностики должен быть контролируемым физически и логически
11.4.5	Принцип разделения в сетях	В сетях должны применяться принципы разделения групп информационных услуг, пользователей и информационных систем
11.4.6	Контроль сетевых соединений	Подключение пользователей к совместно используемым сетям, особенно, к тем, которые выходят за границы Организации (организации), необходимо ограничивать в соответствии с политикой контроля доступа и требованиями бизнес-приложений
11.4.7	Контроль маршрутизации в сети	Должны быть внедрены средства контроля маршрутизации в сети для обеспечения того, что компьютерные соединения и потоки информации не нарушают политики контроля доступа для бизнес-приложений
11.5 Контроль доступа к операционной системе		
Цель: Предотвратить неавторизованный доступ к операционным системам		
11.5.1	Безопасные процедуры регистрации	Доступ к операционным системам должен контролироваться безопасным процессом регистрации

11.5.2	Идентификация и аутентификация пользователя	Все пользователи должны иметь уникальные идентификаторы только для персонального использования, а для подтверждения заявленной личности пользователя должны быть выбраны подходящие методы аутентификации
11.5.3	Система менеджмента паролей	Системы менеджмента паролей должны быть интерактивными и обеспечивать качественные пароли
11.5.4	Использование системных утилит	Необходимо ограничивать и строго контролировать использование системных утилит, которые могут обойти средства контроля операционных систем и приложений
11.5.5	Периоды бездействия в сеансах	Бездействующие сеансы должны отключаться после определенного периода бездействия
11.5.6	Ограничение времени соединения	Ограничение времени соединения должно использоваться для обеспечения дополнительной безопасности для приложений высокого риска

11.6 Контроль доступа к приложениям и информации

Цель: Предотвращение неавторизованного доступа к информации в системах приложений

11.6.1	Ограничения доступа к информации	Доступ к информации и функциям систем приложений должен предоставляться пользователям и персоналу поддержки только в соответствии с определенной политикой контроля доступа
11.6.2	Изоляция систем, обрабатывающих важную информацию	Системы, обрабатывающие важную информацию, должны иметь выделенную (изолированную) вычислительную среду

12. Приобретение, разработка и обслуживание информационных систем

12.1 Требования к безопасности информационных систем

Цель: Обеспечить уверенность в том, что безопасность является неотъемлемой частью информационных систем

12.1.1	Анализ и спецификация требований безопасности	В формулировках требований бизнеса для новых информационных систем или усовершенствования существующих информационных систем должны быть специфицированы требования к средствам контроля безопасности

12.2 Корректность обработки данных в приложениях

Цель: Предотвратить ошибки, потерю, неавторизованную модификацию или неправильное использование информации в приложениях

12.2.1	Подтверждение корректности ввода данных	Входные данные для приложений должны проходить процедуру подтверждения с целью обеспечения уверенности в их корректности и соответствии
12.2.2	Контроль обработки данных в приложении	С целью обнаружения искажений (ошибок или преднамеренных действий) при обработке информации, в приложения следует включить возможность выполнения контрольных проверок
12.2.3	Целостность сообщений	Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, а также определены и реализованы соответствующие средства контроля
12.2.4	Подтверждение корректности данных вывода	Данные, выводимые из приложения, должны проходить проверку с целью подтверждения корректности обработки хранимой информации и соответствия обстоятельствам
12.3 Криптографические меры контроля		
Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами		
12.3.1	Политика использования криптографических мер контроля	Должна быть разработана и внедрена политика использования криптографических средств контроля для защиты информации
12.3.2	Управление ключами	Для поддержки организацией криптографических методов должна использоваться система управления ключами
12.4 Безопасность системных файлов		
Цель: Обеспечить безопасность системных файлов		
12.4.1	Контроль программного обеспечения	Должны быть процедуры для контроля инсталляции программного обеспечения в операционные системы
12.4.2	Защита данных тестирования системы	Данные тестирования следует тщательно отбирать, защищать и контролировать
12.4.3	Контроль доступа к исходным текстам программ	Доступ к исходным текстам программ должен быть ограничен
12.5 Безопасность в процессах разработки и поддержки		
Цель: Поддерживать безопасность программ и информации в прикладных системах		
12.5.1	Процедуры контроля изменений	Внесение изменений должно контролироваться использованием соответствующих формализованных процедур контроля изменений

12.5.2	Технический анализ приложений после изменений в операционных системах	При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений для обеспечения отсутствия негативного влияния на работу и безопасность Организации
12.5.3	Ограничения на внесение изменений в пакеты программ	Необходимо избегать модификаций программных пакетов, а все необходимые изменения должны подлежать строгому контролю
12.5.4	Утечка информации	Возможности для утечки информации должны быть предотвращены
12.5.5	Разработка программного обеспечения с привлечением сторонних организаций	Разработка программного обеспечения с привлечением сторонних организаций должна вестись под надзором и мониторингом организации

12.6 Менеджмент технических уязвимостей

Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей

12.6.1	Контроль технических уязвимостей	Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры для рассмотрения, связанного с ними риска

13. Менеджмент инцидентов информационной безопасности

13.1 Сообщения о событиях и недостатках информационной безопасности

Цель: Обеспечение того, что события информационной безопасности и недостатки, связанные с информационными системами, сообщаются способом, позволяющим своевременно предпринять корректирующее действие

13.1.1	Сообщение о событиях информационной безопасности	О событиях информационной безопасности должно сообщаться по соответствующим каналам менеджмента незамедлительно, насколько это возможно
13.1.2	Сообщения о недостатках безопасности	Все сотрудники, подрядчики и пользователи третьей стороны, пользующиеся информационными системами и услугами, должны замечать и сообщать о любых наблюдаемых или подозреваемых недостатках безопасности в системах или услугах

13.2 Менеджмент инцидентов информационной безопасности и усовершенствований

Цель: Обеспечить последовательный и эффективный подход в применении к менеджменту инцидентов информационной безопасности

13.2.1	Ответственность и процедуры	Должны быть установлены ответственность и процедуры, чтобы обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности
13.2.2	Изучение инцидентов информационной безопасности	Должны быть механизмы, позволяющие вести мониторинг и классифицировать инциденты информационной безопасности по типам, объемам и стоимостям
13.2.3	Сбор свидетельств	Если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, тогда должна собираться, храниться и представляться информация согласно правилам оформления свидетельств, изложенным в соответствующих инструкциях

14. Соответствие требованиям

14.1 Соответствие требованиям законодательства

Цель: Избегать любых нарушений норм уголовного и гражданского права, требований законодательства и регулирующих органов или договорных обязательств, а также требований безопасности

14.1.1	Определение применимого законодательства	Все применимые требования законодательства и регулирующих органов, а также договорные обязательства и подход Организации к выполнению этих требований, следует четко определить, документально оформить и поддерживать на актуальном уровне для каждой информационной системы и организации
14.1.2	Права интеллектуальной собственности	Должны быть внедрены соответствующие процедуры для обеспечения соответствия законодательным, регулирующим и контрактным требованиям, накладываемым на использование материалов с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом частной собственности
14.1.3	Защита учетных записей Организации	Важные учетные записи организации должны быть защищены от потери, разрушения и фальсификации в соответствии с требованиями законодательства, регулирующих органов, контрактов и бизнеса
14.1.4	Защита данных и приватность персональной информации	Защита данных и приватность персональной информации должны обеспечиваться согласно требованиям соответствующего законодательства, регулирующих органов и, возможно, условиям договора

14.1.5	Предотвращение нецелевого использования средств обработки информации	Должны применяться меры контроля для предотвращения нецелевого использования средств обработки информации пользователями
14.2 Вопросы аудита информационных систем		
Цель: Максимизация эффективности процесса аудита информационных систем и минимизация негативного влияние, связанного с данным процессом		
14.2.1	Меры контроля аудита информационных систем	Требования и деятельности аудита, включающие проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов
14.2.2	Защита инструментальных средств аудита информационных систем	Доступ к инструментальным средствам аудита информационных систем необходимо защищать с целью предотвращения любой возможности их неправильного использования или компрометации

Определение, документирование и внедрение в организации вышеуказанных требований и мероприятий, позволяют ей провести подготовку и выйти на этап сертификации системы менеджмента информационной безопасности. Но это, только одна из ступеней систем менеджмента.

По моему мнению, организациям, выполняющим оборонный заказ необходимо иметь комплексную систему менеджмента, состоящую из: системы менеджмента качества, системы менеджмента информационной безопасности и системы экологического менеджмента, которые должны быть документированы, внедрены и сертифицированы установленным порядком, что позволит им минимизировать уровень проблем, возникающих при разработке (проектировании), производстве, утилизации продукции, управлении другими процедурами, которые заложены в стандарты, определяющие требования к вышеуказанным системам.

Библиография

1. Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» № СМ-№ 912–51, утвержденное постановлением Правительства РФ от 15.09.1993 № 912-51.

2. «Модель иностранных технических разведок на период до 2020 г.», утвержденная приказом ФСТЭК России от 25.12.2009 № 038 (введена в действие с 01.09.2010).

3. «Список норм и методик по противодействию акустической речевой разведке», утвержден решением ФСТЭК от 28.05.2007 № 015.

4. «Список норм и методик по противодействию визуальной оптико-электронной разведке», утвержден решением ФСТЭК от 28.05.2007 № 015.

5. «Список норм и методик по противодействию радио и радио-техническим разведкам», утвержден решением ФСТЭК от 28.05.2007 № 015.

6. «Методики оценки возможностей иностранных технических разведок (МВТР–2010)» ФСТЭК. Издание второе, доработанное, 2005.

7. «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам». Решение Гостехкомиссии России от 23.05.1997 № 55. Стр. 97.