УДК 629.039.58 DOI:10.18324/2077-5415-2020-4-80-87

Методика создания и внедрение системы менеджмента информационной безопасности на промышленном предприятии

П.А. Лонцих[a], О.М. Сафонова[b]

Иркутский национальный исследовательский технический университет, ул. Лермонтова, 83, Иркутск, Россия
[a] palon@list.ru, [b] olyastefanovskaya@mail.ru
[a] https://orcid.org/0000-0001-8326-2935, [b] https://orcid.org/0000-0001-6121-7690
Статья поступила 11.11.2020, принята 20.11.2020

В статье рассматриваются аспекты создания системы менеджмента информационной безопасности, деловых процессов с использованием различных инструментов и механизмов. Проблемы обеспечения информационной безопасности являются жизненно необходимыми для успешного функционирования современной компании или предприятия. Система менеджмента информационной безопасности (далее СМИБ) представляет собой некую часть всеобщей системы менеджмента качества, основанную на подходе к оценке деловых рисков при создании, внедрении, функционировании, а также улучшении информационной безопасности в целом. Повышение количества атак, связанных с информационной безопасностью, неправильное управление большими объемами данных наносят удар по функционированию предприятия, понижая его производительность и функциональность. В таких обстоятельствах предприятия должны сопоставлять принципы риск-менеджмента, создавая надежную СМИБ. Незаменимым элементом на пути к созданию целостной СМИБ является стандарт ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»). Авторами предложена разработка требований к системе СМИБ, включая общую методику создания, внедрения и оценку эффективности механизмов. Рассмотрены два наиболее известных стандарта по внедрению СМИБ, а именно ISO/IEC 27001:2013 и ISO/IEC 27005:2018. В настоящее время наблюдается повышенный интерес к этим стандартам со стороны организаций, работающих в различных отраслях. Соответствие ему становится важным фактором коммерческого успеха компании благодаря целому ряду преимуществ, которые она получает. Применен процессный подход к построению СМИБ и управлению рисками на основе этих стандартов.

Ключевые слова: информационная безопасность; система менеджмента информационной безопасности; риски, процессный подход, сертификация.

Methodology for the creation and implementation of an information management security system at an industrial enterprise

P.A. Lontsikh[a], O.M. Safonova[b]

Irkutsk National Research Technical University; 83, Lermontov St., Irkutsk, Russia
[a] palon@list.ru, [b] olyastefanovskaya@mail.ru
[a] https://orcid.org/0000-0001-8326-2935, [b] https://orcid.org/0000-0001-6121-7690
Received 11.11.2020, accepted 20.11.2020

The article discusses aspects of creating an information security management system, business processes using various tools and mechanisms. Information security issues are vital to the successful functioning of a modern company or enterprise. The information security management system (ISMS) is a certain part of the overall quality management system, based on the approach to assessing business risks for the creation, implementation, operation, and information security in general. Improving the quality of information security, improper management of large amounts of data affects the functioning of the enterprise, its productivity and functionality. Thus, enterprises must compare risk management principles to create a robust ISMS. An indispensable element on the path to creating an integrated ISMS is the ISO / IEC 27001 standard (GOST R ISO / IEC 27001 "Information technology." (GOST R ISO / IEC 27001 "Information technology. Methods and means of ensuring security. Information security management systems. Requirements"). The authors propose requirements for an information security management system (ISMS), including a general methodology for creating, implementing and evaluating the effectiveness of ISMS mechanisms. The two most well-known ISMS implementation standards, ISO / IEC 27001: 2013 and ISO / IEC 27005: 2018, have been reviewed and there is now an increased interest in these standards from organizations in various industries. Compliance is becoming an important factor in the commercial success of the company due to a number of benefits that it receives. A process approach was applied to building ISMS and risk management based on these standards.

Keywords: information security; information security system; risks; process approach; certification.

Введение. Незаменимым элементом на пути к созданию целостной системы менеджмента информационной безопасности выступает стандарт ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Требования»), который применим к любому предприятию или компании [1; 5; 6]. Данный стандарт отвечает всем требованиям СМИБ.

Для формирования основных требований к СМИБ стандарт определяет три ключевых показателя, это:

– оценка существующих рисков, с которыми может столкнуться компания;

– компания должна соблюдать все законодательные и нормативные требования;

– создание комплекса требований к обработке, хранению информации.

Рассматриваемый стандарт также обеспечивает:

– цели и принципы применяемые к информационной безопасности;

– подходы к управлению рисками;

– управление информационной безопасностью с соблюдением законодательства;

– процессы СМИБ;

– определение статуса мероприятиий по обеспечению информационной безопасности;

– использование внешних и внутренних аудитов для определения соответствия СМИБ;

– политика информационной безопасности.

Внедрение данного стандарта позволит обеспечить защиту от современных информационных рисков, а именно хищения информации и всевозможных виртуальных угроз.

Требования к созданию СМИБ. СМИБ содержит:

– разработку политики безопасности на стратегическом уровне;

– оценку рисков, связанных с возникновением угрозы;

– определение и внедрение мер безопасности, направленных на устранение угроз;

– мониторинг системы с помощью внутреннего аудита и анализа со стороны руководства.

При разработке стандартов для систем менеджмента качества Международная организация по стандартизации соблюдает принципы их совместимости и взаимодополняемости.

Совместимость проявляется в применении аналогичных методов и инструментов управления, например, принципов надзора за документами, разработки организационной политики, проведения обзоров системы управления, внутренних аудитов, выявления несоответствий (или инцидентов), корректирующих действий. Такой подход облегчает одновременное внедрение систем. Также стоит отметить, что в случае разрозненного внедрения стандартов лучше всего работает решение, при котором организация сначала внедряет систему менеджмента качества, охватывая всю компанию и тем самым знакомя сотрудников с новыми методами работы. Системы менеджмента, разработанные ISO, хорошо дополняют друг друга, позволяя развить организацию в направлении концепции всеобщего управления качеством (TQM).

Становление системы менеджмента информационной безопасности согласно требованиям ISO/IEC 27001 опирается на PDCA модель (рис. 1) [5; 8]:

- Plan (т. е. планирование) — на данной фазе происходит создание СМИБ, анализ всевозможных рисков, а также построение задач по их устранению.
- Do (т. е. действие) — этап внедрения соответствующих действий.
- Check (т. е. проверка) — оценка аудиторами уровня эффективности внедрения системы менеджмента информационной безопасности.
- Act (т. е. улучшения) — на этом этапе происходит создание и непосредственное выполнение корректирующих мер.

Рис. 1. Процессный подход в рамках СМИБ [8]

В создании СМИБ выделяют следующие основные шаги:

- принятие решения директором компании о создании СМИБ, информирование персонала;
- подготовка к созданию СМИБ;
- анализ всевозможных рисков;
- разработка политики СМИБ;
- внедрение СМИБ в эксплуатацию;
- подготовка к процессу сертификации.

Далее рассмотрим шаги подробнее.

1. Принятие решения директором компании о создании СМИБ [1], информирование персонала. Решение о создании СМИБ должно приниматься высшим руководством организации (директор, совет директоров и т. д.). Так руководство компании выражает свою поддержку началу создания СМИБ. Также руководитель компании обязан оповестить персонал компании о внедрении данного процесса.

2. Подготовка к созданию СМИБ [1]. Первое, что нужно предпринять на данном этапе, — это создать рабочую команду, которая будет нести ответственность за внедрение системы менеджмента информационной безопасности. В команду должны входить:

- управленческое звено организации;
- руководители подразделений, которые охватывает внедрение СМИБ;
- работники подразделений, способные обеспечить информационную безопасность предприятия, имеющие образование по направлениям ИТ-технологий.

Входящие в состав рабочей группы сотрудники должны понимать универсальные составляющие систем менеджмента качества, знать требования применяемого стандарта, а также должны пройти обучение, по вопросам внедрения и функционирования СМИБ [10].

Помимо прочего, в состав рабочей группы также могут входить привлеченные консультанты.

Второй шаг на данном этапе — это нормативно-методическое обеспечение. На этом этапе рабочая группа нуждается во всей нормативно-методической базе документов, что успешно позволит создать сильную систему менеджмента информационной безопасности компании.

Ниже приведены стандарты, которыми следует руководствоваться при создании СМИБ [1]:

- ISO/IEC 27000. Словарь и определения.
- ISO/IEC 27001.
- ISO/IEC 27003. Руководство по внедрению СМИБ.
- ISO/IEC 27004. Метрики ИБ.
- ISO/IEC 27005:2018. Информационные технологии. Методы безопасности. Управление рисками информационной безопасности [1; 5; 6].

Следующий шаг — выбор области деятельности компании, которая будет охвачена СМИБ. Для этого нужно учесть следующие факторы:

- вид деятельности компании;
- целевая информация, безопасность которой должна быть обеспечена;
- деловые процессы, обеспечивающие обработку информации. Под деловыми процессами мы понимаем внедрение какой-либо программы, которая способна автоматизировать работу организации. В качестве примера приведем внедрение системы электронного документооборота, которая является многофункциональным программно-техническим комплексом для автоматизации управления организацией в условиях распределенного использования информации разными специалистами [11]. Данный деловой процесс охватывает обработку самой различной документации — приказы, распоряжения, протоколы и выписки из протоколов, договоры, дополнительные соглашения и акты, приказы об обучении и командировании; техническая и нормативная документация; кадровые, тендерные, учетные документы, аудио- и видеоконтент, графические файлы и т. д.
- работники и отделы предприятия, вовлеченные в данные процессы;
- программно-технические методы, ИТ-технологии предприятия.

Результатом данного шага является согласованная с руководителем компании область деятельности, в рамках которой планируется создание СМИБ [1].

Четвертый шаг — выявление всех несоответствий для уточнения плана работ и необходимых затрат на создание СМИБ. Здесь анализируются организационные действия, которые затрагивают планирование, внедрение, аудит и модернизацию шагов по обеспечению информационной безопасности компании. Отличным решением на четвертом этапе выступает заказ у организации по сертификации предварительного аудита с целью нахождения всевозможных несоответствий. Результатом таких работ должен стать список несоответствий требованиям стандарта, а также план работ по внедрению СМИБ.

2. Анализ всевозможных рисков. Главной целью, решаемой в процессе создания и внедрения СМИБ, ставится изучение и анализ рисков информационной безопасности.

В процессе изучения и анализа имеют место быть [2]:

- идентификация активов в границах выбранной части деятельности. Активы — это все то, что имеет ценность для организации, ее успешного развития и функционирования. Некоторые активы классифицируются очевидным образом. Но некоторые активы (например, люди, использующие информационные системы) требуют особой идентификации, при которой шансы нарушения режима информационной безопасности равны нулю. Может быть использована следующая идентификация активов:
  - Аппаратура.
  - Программное обеспечение.
  - Данные.
  - Люди.
  - Документация.
- определение ценности идентифицированных активов;
- идентификация угроз и уязвимостей для идентифицированных активов;
- оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;
- выбор критериев принятия рисков;
- подготовка плана обработки рисков.

Выполнение вышеперечисленных условий осуществляется в соответствии с разрабатываемой процедурой анализа рисков, где отражена методология и определены организационные аспекты по каждому из этих условий.

Анализ рисков — основа СМИБ. Необходимо выбрать такой метод анализа рисков, который можно использовать с минимальными изменениями, причем на постоянной основе. В решении данной проблемы есть два пути. Первый путь — использовать уже существующие инструменты для оценки рисков [15]. Второй путь, наоборот, — разработка своего собственного решения, которое наилучшим образом будет подходить к специфике деятельности организации. Последний путь немного выгоднее в связи с тем, что большая часть организаций, осуществляющих ту или иную методику анализа рисков, не отвечают требованиям стандарта. Авторы статьи выде-

лили типичные недостатки существующих методик анализа рисков, это:

- типичный набор ИТ-угроз, который в основном невозможно изменить;
- принятие в качестве активов (под активами понимаются информационные входные/выходные данные; информационные записи; ресурсы: люди, инфраструктура, оборудование, программное обеспечение компании) только программно-технических и информационных ресурсов — без рассмотрения человеческих ресурсов, сервисов или других ресурсов [12];
- общая сложность методики в понимании ее устойчивого и повторяющегося использования.

В процедуре анализа рисков проводится идентификация всевозможных угроз, анализируется допустимость появления каждой из таких угроз и, учитывая ущерб для актива, задается граница риска, который, в свою очередь, отражает степень критичности угрозы [3]. Весомо и то, что согласно требованиям стандарта в ходе анализа рисков должны быть идентифицированы меры принятия рисков и возможные степени риска. Такие степени должны базироваться на преимуществах стратегических, организационных и управленческих целей предприятия. Управленческое звено предприятия обращается к данным степеням, принимая решения касаемо принятия контрмер для противодействия обнаруженным рискам. Если выявленный риск превысил допустимый уровень критичности, руководство компании должно принять одно из следующих безотлагательных решений:

- принятие риска;
- избежание риска;
- перевод риска в другую область (его страхование).

3. Разработка политики СМИБ. Разработка нормативной базы, которая так важна для функционирования СМИБ, может проводиться одновременно с реализацией мероприятий плана обработки рисков. На данном этапе разрабатываются документы, которые указаны в стандарте. Обычно на этом этапе входят следующие процедуры [1]:

- область деятельности СМИБ;
- политика СМИБ;
- механизмы обеспечения информационной безопасности (политика антивирусной защиты; политика предоставления доступа к информационным ресурсам; политика использования средств криптографической защиты)
- процедуры СУИБ, а именно [4]:

– управление документацией;
– внутренние аудиты;
– корректирующие действия;
– предупреждающие действия;
– управление инцидентами. Инцидент — единичное событие непредсказуемого характера, способное повлиять на бизнес-процессы организации, скомпрометировать и нарушить степень защиты информационной безопасности. Управление данным процессом основано на определении угрозы, оповещении всех сотрудников компании об инциденте, регистрация инцидента (для анализа инцидента как процесса с целью получить определенный опыт для предотвращения последующих угроз), устранение причин и последствий, расследование инцидента, при котором всю имеющуюся информацию отправляют в ИТ-службы, службы безопасности и поддержки [9].

– оценка эффективности механизмов управления СМИБ. Примером мгновенного управления инцидентом может стать программа «СёрчИнформ КИБ», *которая экстренно реагирует на нарушения политик безопасности и снабжает ИТ-специалиста большой доказательной базой [14]*.

Нами разработаны процедуры, которые охватывают следующие ключевые процессы СМИБ:

- управление рисками;
- управление эффективностью системы;
- управление персоналом;
- управление документацией и записями системы управления информационной безопасности;
- пересмотр и модернизация системы.

Опираясь на вышеперечисленное, следует отметить, что, в результате данного процесса не только создается документальная база СМИБ, но и происходит реальное распределение обязанностей по обеспечению безопасности информации среди персонала организации.

4. Внедрение СМИБ в эксплуатацию. Датой ввода СМИБ в эксплуатацию является дата утверждения руководством организации положения о применимости СМИБ. Такое положение публично и отражает цели и средства, которые выбрала компания в целях устранения рисков [5]:

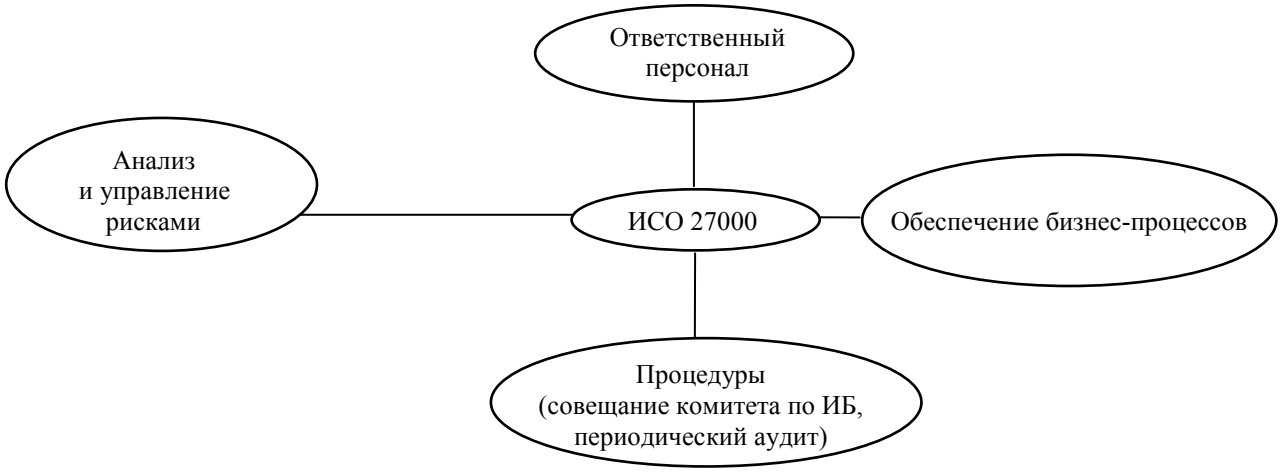

Рис. 2. Основные механизмы СМИБ

Разработанное нами Положение включает:

- средства управления и контроля, выбранные на этапе обработки рисков;
- существующие в компании средства управления и контроля;
- инструменты, обеспечивающие выполнение требований законодательства;
- инструменты, обеспечивающие выполнение корпоративных обязательств.

При внедрении СМИБ в работу компании задействуются все разработанные методы и методики, способные реализовать выбранные цели (см. рис. 2).

5. Внутренний аудит систем менеджмента информационной безопасности.

Планирование внутренних аудитов СМИБ. Проведение регулярных внутренних аудитов СМИБ на основе стандарта ISO/IEC 27005:2018 [1] осуществляется в соответствии с Программой. Приложением к программе внутренних аудитов СМИБ является график планирования выборочного проведения внутренних аудитов подразделений и площадок предприятия.

При составлении программы внутренних аудитов СМИБ учитываются место и важность процессов, предполагаемых к проверке, результаты всестороннего анализа деятельности подразделений и площадок предприятия за прошедший год со стороны руководства (в том числе финансовые показатели), данные систематического мониторинга функционирования процессов СМ, практики работы внешних аудиторов/экспертов или внутренних аудиторов, а также любая значимая для целей проверки информация от потребителей и других заинтересованных сторон. Программа аудитов должна планироваться с учетом важности процессов, областей деятельности и результатов предыдущих аудитов. В программе в графе «Примечания» могут указываться причины, по которым данное подразделение или процесс были включены в программу. При этом каждое подразделение или площадка предприятия, осуществляющие управление отдельными программами сертификации, должно проверяться посредством внутренних аудитов через запланированные интервалы времени. Периодичность и объем внутренних аудитов СМИБ на основе стандарта ISO/IEC 27005:2018 [1] определяются с учетом результатов предыдущих внешних и внутренних аудитов, поступления жалоб и апелляций. При планировании внутреннего аудита департаментов (отделов) предприятий с несколькими структурными подразделениями или направлениями деятельности эти подразделения или направления деятельности могут быть проверены отдельно (самостоятельно), что должно быть отражено в годовой Программе внутренних проверок предприятия.

Все подразделения включаются в программу внутренних аудитов согласно приложению к программе внутренних аудитов на три года. Каждое подразделение попадает в выборку не реже 1 раза в три года в очном или дистанционном формате. При отсутствии замечаний к деятельности подразделения по решению представителя руководства по качеству период может быть увеличен, но не более чем до 5 лет. В программу аудитов должны быть включены все органы, предоставляющие услуги на основе аутсорсинга. Подразделения-исполнители, осуществляющие деятельность по программе сертификации СМИБ, проверяются ежегодно посредством дистанционных методов (веб-конференция, выборочная проверка дел, анализ деятельности в рамках ежегодной оценки и т. д.) и не реже, чем 1 раз в три года посредством визита в офис.

В ходе внутреннего аудита СМИБ на основе стандарта ISO/IEC 27005:2018 [1] такого органа обязательно оцениваются результаты оценки рисков, внутренние запросы, количество клиентов, наличие жалоб, требования заключенного договора подряда.

Ответственность за общее руководство разработкой и согласованием программы внутренних аудитов СМИБ на основе стандарта ISO/IEC 27005:2018 лежит на представителе руководства по качеству. Планирование внутренних аудитов СМИБ на основе стандарта ISO/IEC 27005:2018 может осуществляться в рамках общего планирования деятельности на предстоящий год. Программа внутренних аудитов утверждается представителем руководства по качеству. После утверждения программы ее электронный экземпляр размещается на сайте предприятия [1; 5; 6].

В особых случаях возможно проведение внеплановых аудитов, предпосылками к чему могут быть:

– существенное изменение нормативной документации по предоставляемым услугам;

– поступление жалоб, апелляций на действия или результаты деятельности предпритятия;

– завершение работ по реализации мер корректирующего и предупреждающего действия;

– проработка договора (контракта) с определенными требованиями Заявителя;

– приказ генерального директора предприятия;

– результаты оценки подразделений-исполнителей;

– результаты оценки рисков;

– существенное изменение объема работ по конкретному направлению (в подразделении РР);

– расширение СМИБ на основе стандарта ISO/IEC 27005:2018 (например, разработка или аккредитация новых программ (областей) деятельности).

Внеплановый аудит может быть назначен по устному или письменному распоряжению представителя руководства по качеству или высшего руководства предприятия.

Требования к компетентности внутренних аудиторов СМИБ на основе стандарта ISO/IEC 27005:2018 [1]. Члены группы аудита должны пройти соответствующую подготовку и удовлетворять следующим критериям компетентности для проведения внутренних аудитов.

Принципы, процедуры и методы аудита:

- применять принципы, процедуры и методы аудита [1; 16];
- результативно планировать и организовывать работу;
- проводить аудит в течение согласованного времени;
- устанавливать приоритеты и концентрироваться на важных вопросах;

• собирать информацию посредством результативного опроса, наблюдений и анализа документов, записей и данных;

• понимать и принимать во внимание мнения технических экспертов;

• понимать применимость и последствия использования метода выборки в ходе аудита;

• проверять соответствие и точность собранной информации;

• подтверждать достаточность и пригодность свидетельств аудита для обоснования наблюдений аудита и заключений по результатам аудита;

• оценивать те факторы, которые влияют на достоверность наблюдений аудита и заключений по результатам аудита;

• использовать рабочие документы для записей в ходе мероприятий аудита;

• документировать наблюдения аудита и подготавливать соответствующие отчеты по аудиту;

• обеспечивать конфиденциальность и защиту информации, данных, документов и записей;

• результативно обмениваться информацией, устной или письменной;

• понимать типы рисков, связанных с процессом проведения аудита;

• применять риск-ориентированное мышление, включая определение рисков и возможностей;

• обладать навыками проведения аудита;

• обладать языковыми навыками, достаточными для проведения внутреннего аудита;

• обладать навыками взаимодействия в случае возникновения аварийных ситуаций.

6. Подготовка к процессу сертификации. На этом этапе компании рекомендуется пройти предварительный аудит. Предварительный аудит проводится тем же органом по сертификации, в котором предполагается прохождение сертификации в целом. Уже по результатам предварительного аудита орган по сертификации составляет отчет, в нем отмечаются все плюсы созданной СМИБ, а также все несоответствия и рекомендации по их устранению (при этом СМИБ компании должна профункционировать не менее 6 мес.). Результатом последенего этапа выступает СМИБ компании, которая готова к прохождению процесса сертификации.

Рассмотрев все основные этапы (а также требования к ним) создания СМИБ, можно сказать, что данный процесс весьма сложен. Но усилия, которые будут задействованы на создание СМИБ, позволят этой компании выйти на новый уровень функционирования, а также повысить свои конкурентные преимущества [5; 16].

Подходы к управлению рисками. Так как риски ИБ являются основными не для всех предприятий, наиболее часто используются несколько основных подходов к управлению рисками, различающиеся глубиной и уровнем формализма.

Рациональный подход основывается на проведении высокоуровневой оценки рисков с целью определения того, какие системы наиболее подвержены рискам [10]. Для некритичных систем можно ограничиться применением базового подхода, принимая решения по управлению рисками на основании уже сложившегося опыта, опираясь на примеры успешной практики.

Процессная модель управления рисками на основе ISO/IEC 27005:2018 [1]**.** Стандарт ISO/IEC 27005:2018 «Информационные технологии. Методы безопасности. Управление рисками информационной безопасности» отличается тем, что организациям предоставляется возможность разработать свой собственный подход к управлению рисками на основе стандарта ISO 27005 [1].

Главная цель ISO/IEC 27005 [1] основывается на реализации процесса, который состоит из циклических мероприятий по отношению к управлению рисками в сфере информационной безопасности. Для этого и используется процессный подход [8].

Рассматриваемый стандарт использует ту же процессную модель, что и описанный выше стандарт, включая в себя планирование, реализацию, проверку, действия (табл.). В то время как ISO 27001 [1] описывает общий непрерывный цикл управления безопасностью, ISO/IEC 27005 [1] содержит его проекцию на процессы управления рисками информационной безопасности [5; 6].

Процессная модель на основе стандарта ISO/IEC 27005

PLAN Планирование и организация 1. Определение политики 2. Определение методологии 3. Оценка рисков	ACT Поддержка и совершенствование 1. Переоценка рисков 2. Совершенствование методологии 3. Пересмотр политик 4. Повышение осведомленности
DO Внедрение и эксплуатация 1. Обработка рисков 2. Разработка и реализация плана обработки рисков 3. Внедрение механизмов контроля	CHEK Мониторинг и аудит 1. Процедуры мониторинга 2. Контроль факторов риска 3. Аудит

В системе управления рисками на фазе планирования определяются политика и методология управления рисками, выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей. На фазе реализации происходят анализ рисков и внедрение инструментов контроля, которые предназначены для минимизации рисков. Высшим руководством компании осуществляется одно из четырех решений по каждому риску: проигнорировать, избежать, передать внешней стороне или же минимизировать [5; 18].

На фазе так называемой проверки внимание уделяется функционированию инструментов контроля. На этапе «действия» по результатам анализа проводимых проверок, выполняются корректирующие меры, включающие переоценку уровня критичности рисков, корректировку методологии управления рисками, а также плана обработки рисков.

Заключение. Таким образом, создание системы менеджмента информационной безопасности являет-

ся весьма сложным и длительным процессом. Создавая такого рода систему, не стоит забывать о наличии рисков, которыми нужно уметь управлять, применяя наиболее подходящий поход к устранению этих рисков. Сумев создать и сертифицировать СУИБ, компания получает ряд преимуществ, а именно [1; 5; 6]:

- повышение конкурентных преимуществ;
- рост компании в рейтингах, переход на международный уровень;
- повышение стоимости акций;
- демонстрация партнерам и клиентам компании высокого уровня своей надежности за счет высокой защиты информации;
- снижение рисков для активов компании, связанных с возможными затратами;
- повышение прозрачности процесса управления информационной безопасностью в компании.

Перечисленные преимущества приобретаются в результате получения сертификата соответствия СМИБ компании требованиям рассмотренных в статье стандартов. Самым трудоемким этапом на пути к сертификации является само создание СМИБ.

Литература

1. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management.
2. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization.
3. Сячина Т.Ю. О современных методах менеджмента информационной безопасности // Научно-технические ведомости СПГПУ. 2015. № 2. С. 284.
4. Дорофеев А.А., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2016. № 1 (2). С. 32.
5. Livshitz I.I., Lontsikh P.A., Kunakov E.P., Lontsikh N.P., Tatarnikova L.I. Improving the Activities of Machine-Building Enterprises Through the Use of Digital Technologies // Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Quality Management, Transport. Sep. 2019. International Conference. P. 145–148.
6. Livshitz I.I., Lontsikh P.A., Kunakov E.P., Semenov V.V., Kibirev Y.V. Statistic. Method for Life-Cycle Processes of Digital Enterprises within Integrated Management Systems // Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Quality Management, Transport. Sep. 2019. International Conference. P. 37–41.
7. Eliseev S.V., Livshitz I.I., Lontsikh P.A., Karasev S. Specific Modes of Formation of Dynamic States for Robotic Systems and their Control Systems, Taking into Account the Connectivity of Movements in Two Coordinates // Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Quality Management, Transport. Sep. 2019. International Conference. P. 333–338.
8. Lontsikh P.A., Nagornaya A.V. Justification of implementation of methods of evaluation of efficiency and efficiency of qms at enterprises // Problems of economic development and entrepreneurship 2016. P. 278–291.
9. Livshits I.I., Lontsikh P.A. Analysis of current trends in the certification of information security management systems for the requirements of iso 27001 // Bulletin of Irkutsk State Technical University. 2015. № 3 (98). P. 268–273.
10. Bondaruk A.M. Automated quality management systems in technological processes. Ufa: monogr., 2017. 144 p.
11. Efimov V.V. Means and methods of quality management. Study Guide. M .: KnoRus, 2018. 670 p.
12. Marquardt M. The right questions - an effective method of management. How leaders find optimal solutions by asking questions. M.: Omega-L, SmartBook, 2017. 240 p.
13. Serenkov P.S. Quality management methods. Methodology of risk management standardization. M.: INFRA-M, 2018. 221 p.
14. Shishkin I.F. Metrology, standardization and quality management. M.: Standards, 2018. 342 p.
15. Лонцих П.А.и др. Управление процессами: обеспечение качества технологических систем: монография. Иркутск: Изд-во ИрГТУ, 2014. 344 с.
16. Архипкин О.В., Лескова Т.М. Обеспечение качества и конкурентоспособности предприятий: Иркутск: Изд-во ИрГТУ, 2014. 163 с.
17. Лонцих П.А., Шулешко А.Н., Марцынковский Д.А. Управление качеством. Прогнозирование, риск-менеджмент, оптимизация: монография. Саарбрюккен: Lambert Academic Publishing, 2011. 301 с.
18. Лонцих П.А., Вейц В.Л., Шулешко А.Н. Системы управления качеством и оптимизация инструментов качества. Иркутск: ИрГТУ, 2007. 248 с.
19. Teilans A.A., Romanovs A.V., Merkuryev Yu.A., Dorogovs P.P., Kleins A.Ya., Potryasaev S.A. / Assessment of Cyber Physical System Risks with Domain Specific Modelling and Simulation. SPIIRAS Proceedings. 2018. Issue 4 (59). P. 115 –139 / DOI 10.15622/sp.59.5
20. Hu F. Cyber-Physical Systems: Integrated Computing and Engineering Design // New York: CRC Press. 2018. 398 p.

References

1. ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management.
2. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements, International Organization for Standardization.
3. Syachina T.YU. About modern methods of information security management // St. Petersburg State Polytechnical University Journal. 2015. № 2. P. 284.
4. Dorofeev A.A., Markov A.S. Information security management: basic concepts // Voprosy kiberbezopasnosti.(Cybersecurity issues). 2016. № 1 (2). P. 32.
5. Livshitz I.I., Lontsikh P.A., Kunakov E.P., Lontsikh N.P., Tatarnikova L.I. Improving the Activities of Machine-Building Enterprises Through the Use of Digital Technologies // Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Quality Management, Transport. Sep. 2019. International Conference. P. 145–148.
6. Livshitz I.I., Lontsikh P.A., Kunakov E.P., Semenov V.V., Kibirev Y.V. Statistic. Method for Life-Cycle Processes of Digital Enterprises within Integrated Management Systems // Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Quality Management, Transport. Sep. 2019. International Conference. P. 37–41.
7. Eliseev S.V., Livshitz I.I., Lontsikh P.A., Karasev S. Specific Modes of Formation of Dynamic States for Robotic Systems and their Control Systems, Taking into Account the Connectivity of Movements in Two Coordinates // Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Quality Management, Transport. Sep. 2019. International Conference. P. 333–338.

8. Lontsikh P.A., Nagornaya A.V. Justification of implementation of methods of evaluation of efficiency and efficiency of qms at enterprises // Problems of economic development and entrepreneurship 2016. P. 278–291.
9. Livshits I.I., Lontsikh P.A. Analysis of current trends in the certification of information security management systems for the requirements of iso 27001 // Bulletin of Irkutsk State Technical University. 2015. № 3 (98). P. 268–273.
10. Bondaruk A.M. Automated quality management systems in technological processes. Ufa: monogr., 2017. 144 p.
11. Efimov V.V. Means and methods of quality management. Study Guide. M .: KnoRus, 2018. 670 p.
12. Marquardt M. The right questions - an effective method of management. How leaders find optimal solutions by asking questions. M.: Omega-L, SmartBook, 2017. 240 p.
13. Serenkov P.S. Quality management methods. Methodology of risk management standardization. M.: INFRA-M, 2018. 221 p.
14. Shishkin I.F. Metrology, standardization and quality management. M.: Standards, 2018. 342 p.
15. Loncih P.A. i dr. Process management: ensuring the quality of technological systems: monografiya. Irkutsk: Izd-vo IrGTU, 2014. 344 p.
16. Arhipkin O.V., Leskova T.M. Ensuring the quality and competitiveness of enterprises: Irkutsk: Izd-vo IrGTU, 2014. 163 p.
17. Loncih P.A., SHuleshko A.N., Marcynkovskij D.A. Quality management. Forecasting risk management, optimization: monografiya. Saarbryukken: Lambert Academic Publishing, 2011. 301 p.
18. Loncih P.A., Vejc V.L., SHuleshko A.N. Quality management systems and optimization of quality tools. Irkutsk: IrGTU, 2007. 248 p.
19. Teilans A.A., Romanovs A.V., Merkuryev Yu.A., Dorogovs P.P., Kleins A.Ya., Potryasaev S.A. / Assessment of Cyber Physical System Risks with Domain Specific Modelling and Simulation. SPIIRAS Proceedings. 2018. Issue 4 (59). P. 115 –139 / DOI 10.15622/sp.59.5.
20. Hu F. Cyber-Physical Systems: Integrated Computing and Engineering Design // New York: CRC Press. 2018. 398 p.