УДК 004.05

Никоноров Д.В.,
студент магистратуры
2 курс, кафедра «Информатика и вычислительная техника»
ФГБОУ ВО «МГТУ «СТАНКИН»
Россия, г. Москва

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Аннотация: *Обеспечение качества производимой продукции на современном этапе развития предприятия требует оценки рисков по широкому спектру предполагаемых воздействий, в частности, требуется оценивать вопросы информационной безопасности исполняемых проектов как с точки зрения наличия внешних угроз, так и с точки зрения существования внутренних угроз. В статье предложены методы разработки документации системы менеджмента качества организации, которая включает в себя в качестве основного документа политику информационной безопасности предприятия.*

Ключевые слова: *управление информационной безопасностью, политика информационной безопасности, системы менеджмента качества.*

Annotation: *Ensuring product quality at the present stage of company development requires a risk assessment for a wide range of expected impacts, in particular, it is required to assess the information security issues of executed projects both from the point of view of the presence of external threats and from the point of view of internal threats existence. The paper suggests methods for developing documentation of the organization quality management system, which includes the company information security policy as the main document.*

Keywords: *information security management, information security policy,*

quality management system.

Управление информационной безопасностью как часть системы управления современным предприятием в настоящее время активно исследуется с точки зрения внедрения новых технологий [1], использования и классификации мер по предотвращению угроз, которые могут привести к нарушению конфиденциальности, разрушению целостности или ограничению доступности имеющейся или накопленной информации [2], применение различных моделей описания предприятия, как, например, выявление уровня зрелости [3] с целью выявления имеющихся внутренних угроз и обеспечения наиболее эффективного противостояния этим угрозам, совершенствование нормативно-правового регулирования с целью обеспечения информационной безопасности, обеспечение планирования производственных процессов [4]. Разработка вопросов управления, которые решаются на современном уровне при помощи систем менеджмента качества, позволяет дать рекомендации для создания систем управления информационной безопасностью как части интегрированной системы менеджмента современного предприятия радиоэлектронной отрасли.

Программа обеспечения информационной безопасности предприятия должна в первую очередь опираться на изучение контекста организации, подробный анализ бизнес–процессов и соответствующей бизнес–среды с учетом перспектив развития современной радиоэлектроники. К наиболее важным процессам и объектам, которые требуют управления и отражения в политике информационной безопасности, следует отнести следующие:

- доступ к информации и функции ограничения этого доступа, то есть те, которые предусматривают предоставление доступа только тем лицам, которые были соответствующим образом распознаны или выявлены;
- подотчетность любого объекта, то есть возможность однозначно проследить соответствующие действия, а также (в соответствии со

стандартами менеджмента качества) управлять документами, которые описывают, регламентируют и отражают указанные действия;

- оповещение о нарушениях системы безопасности, которые должны иметь ранжирование или шкалирование, позволяющее использовать мощный аппарат предупреждающих и корректирующих действий, которые подробно разработаны в системах менеджмента качества и активно используются в интегрированных системах менеджмента;
- ценности организации, к которым следует относить не только материальные ценности и технологии, но и ценности, которые могут быть выражены в организационной культуре или микроклимате, созданном в отдельном подразделении или даже на отдельном рабочем месте, что особенно важно для осуществления поверхностного монтажа и обеспечения качества электронных средств на всех стадиях производства;
- процесс осуществления проверок или внутреннего аудита, а также выделенный отдельно процесс документирования порядка проведения и результатов указанных проверок с обязательным прямым указанием на основной документ (или комплекс документов), который отражает основные полученные сведения и соответствующую хронологию;
- процесс признания идентичности, который должен быть распространен не только на признание аутентичности электронной компонентной базы и работающего персонала, но и на признание аутентичности информационных потоков, включающих в себя указания и распоряжения руководства или смежных служб;
- доступность информационно ценных объектов— это свойство сходно с активно используемым в системах менеджмента качества свойством доступности компонентов на каждом входе, выходе или при осуществлении процесса производства электронных средств, когда весь процесс производства распределен по нескольким предприятиям отрасли;
- процесс создания и хранения резервных копий информации, который

также сходен с аналогичным процессом при обеспечении качества электронных средств;

- процесс распознавания личности по биометрическим данным, а также плотно связанные с ним процессы создания, хранения и преобразования соответствующих баз данных, что также имеет аналоги в системах менеджмента качества в радиоэлектронной отрасли;
- процесс ранжирования или классификации информации, включающий в себя имеющуюся или (что является наиболее актуальной частью этого процесса) хронологически изменяющуюся схему, на основании и в соответствии с которой созданная или используемая система должна обеспечить адекватное реагирование на возникшую угрозу или возможность;
- процесс обеспечение конфиденциальности, то есть описание реакций системы, связанных с отказом в доступе для нераспознанных (или неавторизованных) пользователей, а также дополнительные действия, которые могут быть применены в случае распознания применения активных схем построения запросов с целью получения сведений об имеющихся или предполагаемых путей обхода системы информационной защиты.

Политика информационной безопасности организации включает в себя, кроме перечисленных выше процессов и объектов, набор руководящих принципов, практических методов и процедур, а также совокупность правил информационной безопасности, которые предназначены для использования при обеспечении соответствующей деятельности предприятия.

В заключение следует отметить, что разработка политики информационной безопасности и внедрение на её основе программы информационной безопасности в интегрированную систему менеджмента или (при отсутствии таковой) в систему менеджмента качества предприятия в качестве одного из основных документов при обеспечении управления соответствующими действиями по достижению поставленных целей в этой области позволит снизить или предусмотреть своевременное реагирование на

риски, связанные с деятельностью в как на уровне государства, так и при выходе на международный рынок.

Использованные источники:

1. Сизов В.А. Проблемы внедрения siem-систем в практику управления информационной безопасностью субъектов экономической деятельности / В.А. Сизов, А.Д. Киров // Открытое образование. – 2020. – Т. 24. – № 1. – С. 69–79.

2. Исаева М.Ф. О внутренних угрозах информационной безопасности / М.Ф. Исаева // Международный научно-исследовательский журнал. – 2019. – № 5-1 (83). – С. 26–28.

3. Поляничко М.А. Применение модели зрелости для противодействия инсайдерским угрозам информационной безопасности / М.А. Поляничко // Международный научно-исследовательский журнал. – 2019. – № 4-1 (82). – С. 57–59.

4. Малюк А.А. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности / А.А. Малюк, А.В. Морозов // Безопасность информационных технологий. – 2019. – Т. 26.– № 4. – С. 21–36.