УДК 65.011.8

Д. В. Варламова
Университет ИТМО, Санкт-Петербург, e-mail: varlamova@limtu.ru

В. Б. Филатова
Университет ИТМО, Санкт-Петербург, e-mail: fif13@mail.ru

Н. О. Абдураимова
Университет ИТМО, Санкт-Петербург, e-mail: Naziko_97@list.ru

ВОПРОСЫ ИНТЕГРАЦИИ СИСТЕМ МЕНЕДЖМЕНТА КАЧЕСТВА И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: обеспечение качества, информационная безопасность, риск, уязвимость, данные, качество.

Следуя тенденции участившихся случаев несанкционированного доступа к данным, а также динамичного роста объема информации, необходима надежная система информационной безопасности. Несмотря на то, что система менеджмента качества и информационные технологии в наши дни не являются тесно связанными областями, принципы качества могут быть применены к защите данных. В данной статье раскрыта тема специфики информационной безопасности, описана теория менеджмента качества, приведены примеры влияния совместной работы отделов качества и кибербезопасности. Также, перечислены принципы качества и раскрыто понятия обеспечения качество, его эффект применительно к информационным технологиям. Данная работа содержит список тестов, производимых отделом защиты данных, такие как тест на проникновение, аудит безопасности и другие, и какую роль эти тесты играют в системе менеджмента качества. Приведены в пример различные инструменты качества, такие как статистические методы и матрица рисков, а также способ измерить риск. Кроме того, в данной статье выполнен анализ перспектив интеграции систем менеджмента качества и информационной безопасности и даны базовые рекомендации по организации работы двух данных областей.

D. V. Varlamova
ITMO University, Saint Petersburg, e-mail: varlamova@limtu.ru

V. B. Filatova
ITMO University, Saint Petersburg, e-mail: fif13@mail.ru

N. O. Abduraimova
ITMO University, Saint Petersburg, e-mail: Naziko_97@list.ru

QUALITY AND INFORMATION SECURITY MANAGEMENT SYSTEMS INTEGRATION ISSUES

Keywords: quality assurance, cyber security, risk, vulnerability, data, quality.

Following the trend of more frequent cases of unauthorized access to data, as well as the dynamic growth of the volume of information, a reliable information security system is needed. Although quality management system and information technology are not closely related areas these days, quality principles can be applied to data protection. This article reveals the topic of the specifics of information security, describes the theory of quality management, provides examples of the impact of joint work of quality and cybersecurity departments. Also, the principles of quality are listed and the concept of quality assurance is disclosed, its effect in relation to information technology. This work contains a list of tests performed by the data protection department, such as penetration tests, security audits and others, and what role these tests play in the quality management system. Various quality tools, such as statistical methods and a risk matrix, and a way to measure risk are illustrated. In addition, this article analyzes the prospects for integrating quality management systems and information security and provides basic recommendations for organizing the work of these two areas.

Введение

Информационная безопасность и управление качеством часто рассматриваются как отдельные дисциплины. Однако методы ведения бизнеса, конечно, постоянно меняются, а это означает, что организациям необходимо знать, как вопросы информационной безопасности напрямую влияют на вопросы управления качеством. Область информационной безопасности является чрезвычайно важной, так как с каждым годом все большее число сфер деятельности переходит в информационный формат, и, как следствие, растет количество данных, которые необходимо защищать. Регулирование безопасности, выявление потенциальных проблем, устранение уязвимостей и причин их возникновения – все это является процессами, а значит ими можно управлять и измерить их качество. Таким образом, возможно рассмотрение информационной безопасности с точки зрения управления качеством.

Информационная безопасность в широком смысле – это предотвращение взлома программного обеспечения. Взломы, как правило, нацелены на получение доступа к учетным записям и веб-сайтам с целью уничтожения, изменения или удаления фундаментальных данных и информации. Однако, поскольку сегодня существует множество устройств, перед кибербезопасностью стоит сложная задача по обеспечению безопасности этих устройств. Что делает область информационной безопасности в наши дни еще более сложной, так это то, что хакеры или злоумышленники с течением времени адаптируются к новым способам защиты и находят новые пути избежать их.

Целью данной работы является определение того, как принципы управления качеством способны повысить уровень информационной безопасности, а также каким образом это может быть применимо на практике. В статье поставлены такие задачи, как описание теории об управлении качеством и информационной безопасности, раскрытие основных процессов, связанных с защитой информации, и применение к ним принципов системы менеджмента качества.

Материалы и методы исследования

При написании данной работы использовались такие методы как сопоставление, сравнение и анализ. Также, были использована научная литература, стандарты в исследуемой области и цифровые источники информации.

Результаты исследования и их обсуждение

Для того, чтобы процесс внедрения методов защиты информации принес положительные результаты, необходимо обеспечить строгое соблюдение требований по обеспечению качества. Информационная безопасность требует нескольких уровней защиты. Кроме того, важно соблюдать совокупность и слаженность работ людей, технологий и процессов, чтобы принятые меры были эффективными.

Другими словами, организация единой системы управления угрозами нужна для автоматизации всех составляющих процесса, а также для роста и совершенствования базовых функций безопасности, таких как обнаружение, расследование и устранение уязвимостей.

Информационная безопасность включает в себя три фактора:

a) люди,

b) технологии,

c) процессы.

Под людьми подразумеваются пользователи, в обязанности которых входит понимание и выполнение базовых правил безопасности информации. Например, создание надежных паролей, наблюдение и осторожность с данными в электронной почте и социальных сетях и резервное копирование данных.

Технологии чрезвычайно важны для обеспечения компаний и физических лиц средствами кибербезопасности, которые способствуют защите от атак. В усиленной защите нуждаются три из составляющих информационных технологий – это конечные устройства, облако и сети. Наиболее широко используемые инструменты, применяемые для сведения к минимуму числа уязвимостей в этих объектах, включают:

a) межсетевые экраны нового поколения,

b) DNS-фильтрация,

c) защита от вредоносных программ,

d) антивирусное программное обеспечение,

e) решения для защиты электронной почты.

Понятие обеспечение качества применимо ко всякому систематическому процессу, выполняемому для постановления факта того, соответствует ли услуга или продукт

требованиям, установленным для такого продукта или услуги. Также, это относится и к процессам разработки, проектировки и производства, которые также должны соответствовать определенным требованиям. Этот правило реализуется для роста доверия потребителей и, как следствие, улучшение престижа организации. Кроме того, это воздействует на рабочие процессы и эффективность и позволяет компании быть более конкурентоспособной.

Обеспечение качества – это комплекс мероприятий, проводимый для предупреждения ошибок и несоответствий в производимой продукции и устранения проблем при транспортировке продукции или оказания услуг клиентам; определение, данное в стандарте ГОСТ Р ИСО 9000-2015 «Системы менеджмента качества. Основные положения и словарь» – часть менеджмента качества, направленная на обеспечение уверенности в том, что требования к качеству будут выполнены [2].

Продукты и услуги производятся под «руководством» обеспечения качества. Это дает ответственность за обеспечение соответствия требованиям, потребностям и ожиданиям конечных пользователей. При следовании этим принципам, в организации возрастет рентабельность инвестиций и, следовательно, лояльность потребителей. Гарантия качества означает то, что продукт не имеет несоответствий на всех стадиях своего жизненного цикла.

Инструменты обеспечения качества в области защиты информации:

a) Матрица рисков;
b) Контрольные диаграммы;
c) Сравнительный анализ;
d) Статистическая выборка;
e) Блок-схема;
f) Методологии управления качеством;
g) Диаграммы причин и следствий;
h) Гистограмма;
i) Диаграмма Парето;
j) Диаграмма запуска;
k) Корреляционная диаграмма;
l) Осмотр [1].

Эти инструменты могут быть применены и при контроле процессов защиты информации. В международном стандарте ISO/IEC 27001 некоторые принципы системы менеджмента качества, раскрываются следующим образом:

1) Постоянное улучшение – предприятие должно непрерывно улучшать пригодность, соответствие и результативность системы менеджмента информационной безопасности.

2) Лидерство руководителя – Высшее руководство должно демонстрировать лидерство и обязательства в отношении системы менеджмента информационной безопасности посредством гарантии того, что информационная политика безопасности и цели в сфере информационной безопасности установлены и согласуются со стратегией организации; что требования системы менеджмента информационной безопасности встроены в процессы организации; что ресурсы, необходимые для системы менеджмента информационной безопасности, доступны; что система менеджмента информационной безопасности достигает ожидаемых результатов; что оказывается поддержка усилий сотрудников, направленных на обеспечение результативности системы менеджмента информационной безопасности; стимулируется непрерывное совершенствование и поощряется демонстрация лидерства на различных уровнях управления в границах установленной ответственности [3].

В целом, в стандартах серии ISO 9000 нет такого понятия, как KPI показатели, но в стандарте ГОСТ Р ИСО 9001-2015 «Системы менеджмента качества. Требования» в пункте 4.4.1.c говорится следующее: «Организация должна определять процессы, необходимые для системы менеджмента качества, и их применение в рамках организации, а также: определять и применять критерии и методы (включая мониторинг, измерения и соответствующие показатели результатов деятельности), необходимые для обеспечения результативного функционирования этих процессов и управления ими.»[4] Следуя данному высказыванию, можно выделяют следующий показатель, получивший от Центра Интернет-безопасности название «классическое уравнение риска»:

$$\text{Риск} = f\left\{\frac{\text{уязвимости} + \text{угрозы} + \text{последствия}}{\text{меры противодействия}}\right\}$$

Если упростить суть данного показателя, то уравнение показывает, что чем больше и эффективнее будут приняты меры противодействия, тем меньше будет риск. Также, значимую роль играет текущее состояние защищенности системы, в том числе и не устранённые последствия от прошлых атак.

Принцип постоянного улучшения начинает работать сразу после внедрения технических средств защиты, так как злоумышленники могут действовать в динамике организации [5]. В данном случае уместно и полезно использовать такой инструмент качества, как матрица рисков – это матрица, которая используется во время оценки риска для определения уровня риска путем рассмотрения категории вероятности или вероятности в зависимости от категории серьезности последствий. Это простой механизм для повышения видимости рисков и содействия принятию управленческих решений [6]. При составлении такой матрицы для повышения системы кибербезопасности, в нее можно включить поля с указанием названия атаки или уязвимости, ответственных лиц и предложения по предупреждению или исправлению опасности.

Чтобы сделать системы безопасными, очень важно внедрить и соблюдать международные стандарты безопасности, а также сосредоточиться на факторах риска приложений и программного обеспечения, поэтому группы обеспечения качества и безопасности должны работать вместе, контролируя реализацию этих требований. Особого внимания требуют нижеперечисленные области применения:

a) Контроль доступа. Это одна из базовых опций приложения, которая должна быть защищена. Контроль доступа используется для предупреждения доступа нежелательных пользователей к веб-сайту или приложению, а также для создания ролей, дающих пользователям возможность получать доступ только к определенной информации или определенным функциям.

b) Безопасность приложения. Должна проводиться постоянная работа от начала проекта до его производственного выпуска. Все уровни организации должны действовать вместе, чтобы избежать утечек или уязвимостей безопасности программного обеспечения. Рекомендуется не задерживать проверки и аудиты безопасности до конца проекта, чтобы избежать нарушения сроков выпуска или трудностей из-за проблем с безопасностью.

c) Управление информацией. Данный раздел отвечает за обеспечение безопасности информации организации. Посредством управления информацией осуществляется проверка, нет ли каких-либо уязвимостей безопасности, которые ставят под угрозу или утечку информацию предприятия. В настоящее время информация является одним из самых ценных активов для предприятий.

d) Единый вход. Эта область контролирует, кто имеет доступ к программному обеспечению или приложению, а также способствует лучшему контролю доступа пользователей и управление ими. Однако, это требует усиленного планирования по конфигурации различных ролей, необходимых для потребителей, а также тесного взаимодействия между командами по обеспечению качества и безопасности.

Недостаточно знать, на каких областях нужно сделать акцент, еще важно понимать, как кибербезопасность может быть реализована в проекте и как спланировать его так, чтобы безопасность стала целью. Для этого правильным подходом будет являться гибкая методология, которая должна включать следующие аспекты:

e) Планирование и определение. На данном этапе проводится анализ имеющихся рисков и уязвимостей, которые необходимо устранить, а также по мере возможности произвести сортировку этих уязвимостей, чтобы знать, на чем сделать фокус в первую очередь.

f) Обзор и дизайн: здесь рассматриваются реальные варианты рисков, их последствий и проектные решения для каждого из них. Важно не только решить эти сценарии, но и усилить защиту программного продукта против всех возможных угроз.

g) Проверка разработки и безопасности. На этом этапе группы проектирования и безопасности работают в тесном взаимодействии, по мере написания кода для программного продукта или веб-сайта группа безопасности периодически проверяет его, чтобы убедиться, что в приложении нет уязвимых мест, а также для отдела качества и безопасности, чтобы вникнуть в характеристики этого приложения, его логику и функциональность.

h) Тесты качества и безопасности. Этот этап предназначен для совместной работы отделов качества и безопасности. На данном этапе выполняются тесты функциональности, логики и безопасности.

В основном существует семь типов тестов безопасности:

1) Сканирование уязвимостей. Эти тесты, как следует из их названия, представляют собой высокоуровневую проверку разных видов уязвимостей, существующих в приложении или программе.

2) Сканирование безопасности. Данные тесты являются более тщательным анализом программ и всей системы. При них проверяется не только безопасность системы, а также всей сети, чтобы выяснить, есть ли в ней какие-либо опасные или уязвимые места, которые необходимо устранить.

3) Тесты на проникновение. Эти тесты имитируют хакерскую атаку. Они производятся для моделирования ситуации того, как система отреагирует на внешнюю атаку.

4) Управление рисками. Это тесты, которые не относятся только к программе или продукту, они также устанавливают, как возможные риски безопасности обрабатываются внутри предприятия. Здесь рассматривается управленческий аспект организации. Эти тесты производятся, чтобы сформировать меры безопасности и действия, которые помогут избежать или минимизировать риски безопасности.

5) Аудит безопасности. При данном тесте проводятся испытания программ и операционных систем на наличие утечек безопасности. Такие тесты не ограничиваются только определенными приложениями, они производятся для полных систем.

6) Этический взлом. Данный вид испытаний безопасности выполняется для систем предприятия, имитирующих способ атаки хакера на организацию. В отличие от реального взлома, эта атака не имеет цели достать недоступные данные предприятия, а ищет доказательства недостатков или утечек безопасности, которые необходимо исправить.

7) Управление положением. Это испытания анализа безопасности, этического взлома и управления рисками в сочетании, которые в целом представляют картину общего уровня безопасности предприятия.

Выполнение каждого из этих тестов в каждом проекте не является обязательным, но важно рассчитывать на все эти испытания во время разработки проекта, чтобы выяснить необходимую стратегию и объем. Также, очень важно вовлекать в работу отдел по обеспечению качества на ранних этапах каждого проекта. Это эффективнее, когда отдел качества работает с самого начала, потому что исправить проблемы безопасности и требований намного сложнее, когда проектирование проекта почти закончена или когда проект близок к завершению.

Заключение

Очень важно обеспечить безопасность веб-сайтов, программного обеспечения, баз и хранилищ данных, а также других программных приложений, то есть контролировать уязвимости, составлять статистику, показывающую наиболее опасные и незащищенные места и стремиться к нулю несоответствий, предупреждая и отражая кибератаки. Для этого необходимо принять такие меры, как измерение рисков. Для успешной реализации системы защиты информации требуется совместная работа специалистов отдела информационных технологий и отдела менеджмента качества. Даже если нет возможности организовать какой-либо уровень интеграции между системой безопасности и системой менеджмента качества, следует оценить различия между риском информационной безопасности и риском для целей качества. После того, как это будет сделано каждой организацией, можно будет понять и реализовать области взаимосвязи между рисками качества и информационной безопасности в каждой области.

Библиографический список

1. QA Platforms team, «Cybersecurity Quality Assurance». – 2019. [Электронный ресурс]. URL: https://qa-platforms.com/cybersecurity-quality-assurance/ (дата обращения: 25.10.2020).

2. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь (Издание с Поправкой). М.: Стандартинформ, 2019. 79 с.

3. ISO/IEC 27001 Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования. © ISO/IEC 2013. 32 с.

4. ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования (Переиздание). М.: Стандартинформ, 2020. 50 с.

5. Applying Total Quality Management Principles to Cybersecurity and IT Management. – 2018. [Электронный ресурс]. URL: https://thrivenextgen.com/applying-total-quality-management-principles-to-cybersecurity-and-it-management/ (дата обращения 26.10.2020).

6. Talbot J. What's right with risk matrices? – 2018. [Электронный ресурс]. URL: https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices (дата обращения 27.10.2020).

7. QA and Cybersecurity. – 2019. [Электронный ресурс]. URL: https://medium.com/@qantum_en/qa-and-cybersecurity-fa1968cd728c.