УДК: 004.056.5

ОБСЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ РЕСТОРАНА

Ашымова Айзада Жаасынбековна, *старший преподаватель кафедры «Программное обеспечение коммпьютерных систем» КГТУ им. Раззакова, Кырыгзстан,72044, г.Бишкек, e-mail: a_aizada_kg@mail.ru*
Беккулова Кыял Абдыкапаровна, *старший преподаватель кафедры «Программное обеспечение коммпьютерных систем» КГТУ им .Раззакова, Кырыгзстан,72044, г.Бишкек, e-mail: nimatta@mail.ru.*

Аннотация. Цель статьи – выявление потенциальных угроз и уязвимостей, предотвращение инцидентов, исключение либо минимизация выявленных угроз, а также провести аудит соответствия внутреннему аудиту информационной системы ресторана.

Ключевые слова: информационная система ресторана, активы, подлежащие защите, информационные активы, уязвимости активов, источник угроз информационной безопасности, модель угроз информационной безопасности, модель нарушителя информационной безопасности, политика информационной безопасности.

SURVEY OF PROTECTION OF THE INFORMATION SYSTEM OF THE RESTAURANT

Ashymova Ayzada Zhaasynbekovna, *senior lecturer of the Department "Software of computer systems" KGTU named after Razzakov, Kyrgyzstan, 72044, Bishkek, e-mail: a_aizada_kg@mail.ru*
Bekkulova Kyial Abdykaparovna, *senior lecturer of the Department "Software of computer systems" KGTU named after Razzakov, Kyrgyzstan, 72044, Bishkek, e-mail: nimatta@mail.ru.*

The purpose of the article is to identify potential threats and vulnerabilities, prevent incidents, exclude or minimize identified threats, and audit compliance with the internal audit of the restaurant's information system

Key words: information system of the restaurant, assets subject to protection, information assets, vulnerability of assets, source of information security threats, information security threats model, infringing information security model, information security politics.

В информационной системе ресторана (ИСР) хранится и передаются информации относящаяся к профессиональной тайне, коммерческой тайне, служебной тайне и персональные данные, а также формируется отчет по основным бизнес процессам ресторана. Основными бизнес-процессами информационной системы ресторана Обслуживание клиентов и обработка заказов своевременно. ИСР является системой подключенным к интернету общего пользования. Технические средства ИСР, в частности оборудования сервера, расположены в помещении, находящемся в пределах контролируемой зоны ресторана. Информационные активы хранятся на серверах-баз данных ресторана, данные которых вводятся с рабочих станций сотрудников (АРМ), в том числе информация ограниченного доступа. А также имеются АРМ администраторов: АРМ-администратора ИБ и АРМ-администратора ИСР.

Модель нарушителя информационной безопасности

По признаку принадлежности к ИС все нарушители делятся на две группы:

– внешние нарушители Н-1 – физические лица, осуществляющие целенаправленное деструктивное воздействие, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

– внутренние нарушители Н-2 – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

Н-1 Внешний нарушитель:

В качестве внешнего нарушителя информационной безопасности рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИС, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки. Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только вовремя ее передачи по каналам связи.

Н-2 Внутренний нарушитель:

К такому виду нарушителя могут относиться (список лиц должен быть уточнен в соответствии с группами пользователей, описанных в Политике информационной безопасности):

– пользователи ИС т.е. сотрудники, имеющие право доступа к ИС (категория I);

– сотрудники, не имеющие права доступа к ИС (категория II);

– администраторы ИС (категория III);
– разработчики и поставщики программно-технических средств, расходных материалов, услуг (категория IV).

Полномочия нарушителей значительным образом зависят с функционирующих границах контролируемой зоны ограничительных условий, с которых главным представляется осуществление комплекса организационно-технических мер, в том числе по выбору, расстановке и обеспечению высокой профессиональной подготовки сотрудников, допуску физических лиц внутрь контролируемой зоны и контролированию за порядком проведения работ, нацеленных на устранение и пресечение несанкционированного допуска. Лица категорий I и III хорошо знакомы с основными алгоритмами, протоколами, исполняемыми и используемыми в определенных подсистемах и ИС в полном, а кроме того с использующимися принципами и концепциями безопасности. Подразумевается, что они могли бы использовать типовое оборудование или для идентификации уязвимостей, либо для осуществления угроз ИБ. Это оборудование может быть, равно как составляющей настоящих денег, таким образом и способен иметь отношение к свободно получаемому (к примеру, программное обеспечение, полученное из доступных внешних источников). Помимо этого, предполагается, то что эти лица могли бы пользоваться специальным оборудованием. К лицам данных категорий ввиду их исключительной роли в ИС должен использоваться совокупность специальных организационно-режимных мер по их подбору, принятию в работу, предназначению на должность и контролю выполнения функциональных обязанностей.

Этапы управления инцидентами ИБ

В соответствии со структурой и спецификой информационной системы ресторана было определено, что к инцидентам информационной безопасности относится любое негативное событие или активность (наблюдаемое в действии), которое подвергает опасности:

– Конфиденциальность, целостность или доступность защищаемой информации;
– Сеть, к которой подключена ИСР (включая оборудование, приложения и данные);
– Непрерывность функционирования ИСР;
– Целостность или доступность программного обеспечения.
– Исходя из разработанной модель угроз и нарушителя ИБ и политики ИБ информационной системы ресторана будем рассматривать следующие инциденты:
– Утечка конфиденциальной информации (нарушение конфиденциальности);
– Нарушение целостности конфиденциальной информации;
– Несанкционированное копирование или изменение конфиденциальной информации;
– Атаки типа «отказ в обслуживании» (DoS/Ddos);
– Внедрение вредоносного кода
– В соответствии с [4] в разработанной политике управления инцидентами присутствуют 5 подпроцессов управления:
– Планирование и подготовка;
– Обнаружение и оповещение;
– Оценка и принятие решения;
– Реагирование;
– Извлеченные уроки.

Аудит информационной безопасности.

Административный состав должен спустя запланированные интервалы (никак не реже один раз в год) проанализировать СУИБ организации, для того чтобы гарантировать её непрерывную применимость, соответствие и результативность. Данный анализ необходимо охватывать в себе установление возможностей улучшения и потребности изменение СУИБ, в

том числе политики информативной безопасности и целей информационной безопасности.

Организация соответственна осуществлять внутренние аудиты (контроля) посредством запланированные интервалы периода в целях определения того, что система менеджмента качества: отвечает запланированным мероприятиям, требованиям к системе менеджмента качества, разработанным организацией; внедрена эффективно и поддерживается в рабочем состоянии.

Программа аудитов (ревизий) обязана намечаться с учетом статуса и значимости действий и площадей, подлежащих аудиту, а также итогов предыдущих аудитов. Критерии, область использования, частота и методы аудитов должны быть определены. Выбор аудиторов и проведение аудитов обязаны гарантировать объективность и непредвзятость процесса аудита. Аудиторы не обязаны проверять собственную свою работу. [5] Должна быть определена документированная процесс с целью определения ответственности и условий, связанных с планированием и проведением аудитов, ведением записей и составлением отчетов о итогах. Журнал о аудитах и их итогах обязаны поддерживаться в рабочем состоянии. Руководитель, отвечающее за контролируемые сфере работы, обязано предоставить, для того чтобы все без исключения требуемые корректировки и корректирующие действия предпринимались в отсутствии избыточной откладывания с целью ликвидации найденных несоответствий и вызвавших их факторов. Дальнейшие действия обязаны содержать в себе верификацию установленных граней и доклад о итогах верификации.

Организации, каковой необходимо проводить аудиты, необходимо организовать план аудита, позволяющую устанавливать эффективность системы менеджмента данной организации. План аудита может быть заключать в себе аудиты, включающие один или ряд стандартов согласно системам менеджмента, проводимые согласно отдельности либо в котором-или комбинации [1]. Высочайшее управление обязано гарантировать, для того чтобы миссии плана аудита существовали определены, и установить один либо ряд компетентных лиц, отвечающих за руководство планом аудита. Масштаб и содержимое плана аудита должны находиться в зависимости с масштаба и характера деятельности контролируемой организации, а кроме того с специфичности, сложности и уровня зрелости системы менеджмента, подлежащей аудиту. Основополагающее интерес нужно выделить адекватному распределению ресурсов плана аудита с целью выполнения аудита наиболее необходимых элементов системы менеджмента. Они могут содержать в себе основные свойства продукта, угрозы, сопряженные с охраной здоровья и техникой безопасности, или важные экологические аспекты и руководство ими.

Разработка целей программы внутреннего аудита

Высшему управлению следует предоставить разработку целей плана аудита, с целью этого для того чтобы управлять планированием и проведением аудитов, ему кроме того необходимо гарантировать продуктивное введение проекты аудита. Цели проекты аудита соответственны должны согласовываться и способствовать осуществле нии политики и целей системы менеджмента. Цели могут быть основаны на рассмотрении следующих требований:

- приоритетов руководства;
- коммерческих и/или деловых намерений;
- характеристик процессов, продуктов и проектов, а также любых изменений к ним;
- требований системы (систем) менеджмента;
- правовых и других требований, которые организация принимает на себя;
- необходимости в оценке поставщиков;
- потребностей и ожиданий заинтересованных сторон (включая потребителей);
- показателей и характеристик деятельности проверяемой организации, что отражается в случаях возникновения нарушений, дефектов, инцидентов или жалоб потребителей;

– рисков для проверяемой организации;
– результатов предыдущих аудитов;
– уровня достигнутого развития системы менеджмента.
– Примеры целей программы аудита могут включать в себя следующее:
– содействие улучшению системы менеджмента и ее характеристик;
– выполнение внешних требований, например, сертификации, на соответствие требованиям стандарта системы менеджмента;
– проверку соответствия контрактным требованиям;
– получение или поддержание уверенности в возможностях поставщика;
– оценку совместимости и согласованности целей системы менеджмента с политикой системы менеджмента и общими бизнес-целями организации.

Выводы: в результате обследование информационной системы ресторана были выявлены модели угроз и нарушителя ИБ, а также был описан объект, его структурно-функциональные характеристики и основные процессы, выявлены уязвимости данных объектов, угрозы к этим уязвимостям. Определены источники угроз ИБ, нарушители ИБ. В результате, на основе перечней угроз, нарушителей и уязвимостей были определены инциденты, а также проведена оценка частных и групповых показателей ИБ на инциденты ИБ. Была составлена программа внутреннего аудита ИБ ИСР. Были определены цели и задачи проведения внутреннего аудита, субъекты внутреннего аудита. Определены активы, которые необходимо проверять в соответствии с программой. В организации внутреннего аудита были определены необходимы действия для подготовки и проведения аудита ИБ.

Список литературы

1. ГОСТ Р ИСО/МЭК ТО 18044-2007 — Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
2. ISO/IEC 27035:2011- Информационная технология. Методы обеспечения безопасности.
3. Управление инцидентами информационной безопасности.
4. СТО БР ИББС 1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.
5. СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».
6. ГОСТ Р ИСО 19011–2012 «Руководящие указания по аудиту систем менеджмента».
7. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). «Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
8. РФ ФСТЭК России от 15 февраля 2008 года «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
9. ФСТЭК России 2015г «Методика определения угроз безопасности информации в информационных системах», проект документа.
10. ГОСТ Р ИСО/МЭК 27001-2006. "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования".
11. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. Учебник. Управление рисками ИБ Книга 2. 2-ое издание.

12. РС БР ИББС 2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».