

Отчёт по проектной деятельности:

«Анализ подходов к оценке зрелости процессов информационной безопасности на основе зарубежных фреймворков».

Студент 2 курса

факультета Информационных технологий

группы 191-331

Горшков А.Г.

Научный руководитель:

Агеева Елена Александровна

ОГЛАВЛЕНИЕ

Введение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

Описание . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .4

Краткая выписка . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .6

Заключение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

ВВЕДЕНИЕ

Моим проектом было рассмотрение ГОСТ Р ИСО/МЭК 27001-2006(далее ГОСТ). Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.

Было довольно сложно правильно подойти к этому заданию, т.к. анализ ГОСТа с целью выявления рисков Информационной Безопасности(далее ИБ) в иностранных компаниях подразумевает выявления основных частей ГОСТА, и анализ уязвимостей в компании. В самом ГОСТе все части являются основными, ведь ГОСТ сам является выпиской с основополагающими понятиями.

Моя работа представляет собой кратко сформированный анализ самого ГОСТа и компаний, которые могут быть подвержены рискам ИБ связанных с ним.

Также в мою работу включён анализ подхода к рискам ИБ непосредственно в самом ГОСТе.

ОПИСАНИЕ

Как сказано в предисловии:

“ПОДГОТОВЛЕН Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России") и Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл") на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте -

Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2005\* "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems - Requirements", IDT)”.

В данном стандарте достаточно точно и чётко указаны все, на мой взгляд, требования в данной области, которые необходимо рассмотреть.

Настоящий стандарт состоит из нескольких частей:

-Введение

-Текст ГОСТа

-Приложение A

-Приложение B

-Приложение C

Основная информация из введения – это то, что в данном стандарте будет рассматриваться система менеджмента информационной безопасности на основе модели PDCA:

“В настоящем стандарте представлена модель "Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)" (PDCA), которая может быть применена при структурировании всех процессов СМИБ”.

Сам текст ГОСТа состоит из 8 частей, здесь выделить что-то основное довольно трудно, т.к. все части настоящего стандарта являются основополагающими.

В приложении A рассмотрены меры управления (рекомендации), которые тоже необходимы в рассмотрении, т.к. они непосредственно говорят о том, какими действиями какие риски можно избежать или снизить.

В приложении B рассмотрены принципы Организации экономического сотрудничества и развития, их тоже необходимо учесть при формировании системы менеджмента информационной безопасности.

В приложении C рассмотрены сравнения структуры настоящего стандарта со структурой международных компаний. То есть представлена разница между непосредственным стандартом ISO 27001:2005 и этим ГОСТом. В начале указано, что принципиальной разницы между настоящим стандартом ГОСТ и соответствующим ему стандартом ISO нет, но тем не менее небольшие различия имеются. Именно они и рассмотрены в этом приложении.

Данный ГОСТ является весьма “объёмным” и для его введения компания должна обладать весьма неплохими информационными активами и хорошей осведомлённостью в этой сфере, также большими финансовыми ресурсами, т.к. введение, рассмотренной в ГОСТЕ системы требует больших вложений.

В настоящем стандарте реализован профессиональный подход к рискам в области ИБ. Полностью изучены возможные риски в той мере, в какой это возможно на данный момент, и изложена вся суть реализации СМИБ (системы менеджмента информационной безопасности). Но тем не менее, проблема, как и в любой сфере, не сформирована на 100% и развивается каждый день. Поэтому как и любой стандарт ISO 27001 требует «непрерывного улучшения»: систематического исправления и предотвращения несоответствий в системе управления информационной безопасностью. С помощью корректирующих и превентивных действий можно исправить несоответствие и предотвратить его повторное появление в будущем.

Если говорить о сертификации, то на самом деле пройти её намного сложнее, чем это описано в различных источниках. Подтверждением является тот факт, что в России на сегодняшний день всего 78 компаний прошли сертификацию на соответствие. При этом за рубежом это один из наиболее популярных стандартов, отвечающих растущим запросам бизнеса в области ИБ. Такая востребованность внедрения обусловлена не только ростом и усложнением типов угроз, но и требованиями законодательства, а также клиентов, которым необходимо сохранение полной конфиденциальности их данных.  
  
Несмотря на то, что сертификация СМИБ является непростой задачей, сам факт выполнения требований международного стандарта ISO/IEC 27001 может дать серьезное конкурентное преимущество на глобальном рынке.

КРАТКАЯ ВЫПИСКА

Здесь я собрал, на мой взгляд, основные выписки из каждой из глав в содержание настоящего ГОСТа.

Настоящий стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Настоящий стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ) среди общих бизнес-рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности (ИБ).  
  
Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается. С учетом целей настоящего стандарта используемый процесс основан на применении модели PDCA.

Разработка СМИБ. Организация должна осуществить следующее:

a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия;

b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;

c) определить подход к оценке риска в организации;

d) идентифицировать риски;

e) проанализировать и оценить риски;

f) определить и оценить различные варианты обработки рисков;

g) выбрать цели и меры управления для обработки рисков;

h) получить утверждение руководством предполагаемых остаточных рисков;

i) получить разрешение руководства на внедрение и эксплуатацию СМИБ;

j) подготовить Положение о применимости;

Внедрение СМИБ. Организация должна осуществить следующее:

a) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ;

b) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

c) внедрить меры управления, для достижения целей управления;

d) определить способ измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получить сравнимые и воспроизводимые данные.

e) реализовать программы по обучению и повышению квалификации сотрудников;

f) управлять работой СМИБ;

g) управлять ресурсами СМИБ;

h) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Документация должна включать в себя записи решений руководства, позволяющие обеспечивать контроль выполнения решений руководства и политик организации, а также обеспечивать воспроизводимость документированных результатов.  
  
Важно иметь обратную связь выбранных мер управления с результатами процессов оценки и обработки риска, а также последних с политикой СМИБ и целями СМИБ.

Для предоставления свидетельств соответствия требованиям и результативности функционирования СМИБ необходимо вести и поддерживать в рабочем состоянии учетные записи. Учетные записи необходимо контролировать и защищать. СМИБ должна принимать во внимание все нормативно-правовые требования и договорные обязательства, имеющие отношение к ИБ. Записи должны быть четкими, легкоидентифицируемыми и восстанавливаемыми. Меры управления, требуемые для идентификации, хранения, защиты, поиска, определения сроков хранения и уничтожения записей должны быть документированы и реализованы.

Руководство организации должно предоставлять доказательства выполнения своих обязательств в отношении разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ путем осуществления следующих мер:

a) разработки политики СМИБ;

b) обеспечения разработки целей и планов СМИБ;

c) определения функций и ответственности в области ИБ;

d) доведения до всех сотрудников организации информации о важности достижения целей информационной безопасности и соответствия ее требованиям политики организации, об их ответственности перед законом, а также о необходимости непрерывного совершенствования в реализации мер ИБ;

e) выделения необходимых и достаточных ресурсов для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ;

f) установления критериев принятия рисков и уровней их приемлемости;

g) обеспечения проведения внутренних аудитов СМИБ;

h) проведения анализа СМИБ со стороны руководства.

Организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие установить, что цели управления, меры управления, процессы и процедуры СМИБ:

a) соответствуют требованиям настоящего стандарта и соответствующим законам или нормативным документам;

b) соответствуют установленным требованиям ИБ;

c) результативно внедряются и поддерживаются;

d) функционируют должным образом.

Руководство должно в соответствии с утвержденным графиком периодически (не менее одного раза в год) проводить анализ СМИБ организации в целях обеспечения ее постоянной пригодности, адекватности и результативности. Результаты анализа должны содержать предложения по изменению СМИБ и оценку их реализации в интересах обеспечения выполнения требований политики и целей информационной безопасности. Результаты таких проверок должны быть зафиксированы документально, а учетные записи должны быть сохранены.

Входные данные для анализа СМИБ со стороны руководства должны включать в себя следующую информацию:

a) результаты предыдущих аудитов и анализа СМИБ;

b) результаты взаимодействия с заинтересованными сторонами;

c) методы, средства или процедуры, которые могут быть использованы в организации для совершенствования функционирования и повышения результативности СМИБ;

d) правовое обоснование предупреждающих и корректирующих действий;

e) уязвимости или угрозы, которые не были адекватно учтены в процессе предыдущей оценки рисков;

f) результаты количественной оценки результативности СМИБ;

g) последующие действия, вытекающие из предыдущего анализа со стороны руководства;

h) любые изменения, которые могли бы повлиять на СМИБ;

i) рекомендации по улучшению.

Организация должна постоянно повышать результативность СМИБ посредством уточнения политики ИБ, целей ИБ, использования результатов аудитов, анализа контролируемых событий, корректирующих и предупреждающих действий, а также использования руководством результатов анализа СМИБ.

Организация должна проводить мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупредить их повторное возникновение. Организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям СМИБ, с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать последствиям потенциальных проблем.

Организация должна определить изменения в оценках рисков и установить требования к предупреждающим действиям, при этом обращая особое внимание на существенно измененные количественные показатели рисков.  
  
Приоритеты в отношении реализации предупреждающих действий должны быть определены на основе результатов оценки риска.

ЗАКЛЮЧЕНИЕ

Данный стандарт прежде всего адресован крупным или особо важным организациям, обеспечение информационной безопасности которых критично для безопасности.

Также большое внимание уделяется возможным действиям по устранению рисков и контролю. Видно, что документ был написан на широкие массы с должным подходом и профессионализмом. На высоком уровне абстракции такие активности ИБ вполне реализуемы.

Судя по всему в дальнейшем Фреймворк будет активно расширяться и включит в себя ещё много других высокоуровневых функций ИБ.

В целом получается ещё одна важная часть в процессе управления рисками ИБ, грамотное применение которой будет зависеть также и от того, в каком виде он будет окончательно закреплён в определённой компании.