

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная
безопасность систем и технологий»

Специальность 100503 –

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные
автоматизированные системы
управления

ДИПЛОМНАЯ РАБОТА

на тему

ОЦЕНКА ЗРЕЛОСТИ ПРОЦЕССОВ УПРАВЛЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Студент

Палагина Елена Алексеевна

Руководитель

Зефиоров С.Л.

Нормоконтролёр

Фатеев А.Г.

Рецензент инженер 2 кат. ФГУП «Атлас» ПФ

Клейменов В.А.

Работа допущена к защите (протокол заседания кафедры от 20.06.16 № 14)

Заведующий кафедрой

С.Л. Зефиоров

Работа защищена с отметкой

(протокол заседания ГЭК

от 23.06.16 № 8)

Секретарь ГЭК

А.П. Иванов

Пенза 2016

РЕФЕРАТ

Отчет о ВКР содержит 60 с., 1 рис., 6 табл., 4 источника, 2 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УПРАВЛЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СИСТЕМА УПРАВЛЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, ПРОЦЕССЫ УПРАВЛЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, ОЦЕНКА ЗРЕЛОСТИ ПРОЦЕССОВ
УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Объектом исследований в данной дипломной работе является оценка зрелости процессов управления информационной безопасностью организации.

Цель ВКР – разработка методики оценки зрелости процессов управления информационной безопасностью (далее - ИБ) организации.

В процессе работы были описаны процессы управления ИБ организации, произведено описание уровней зрелости процессов управления ИБ, разработаны основные и комплексные показатели оценки зрелости процессов управления ИБ и способ их оценивания, разработаны правила формирования общей оценки зрелости процессов управления ИБ и правила проведения оценки зрелости процессов управления ИБ.

В результате выполнения ВКР разработана методика оценки зрелости процессов управления ИБ, включающая в себя описание уровней зрелости процессов управления ИБ, показателей оценки зрелости процессов управления ИБ, способ оценивания показателей, правила формирования общей оценки зрелости процессов управления ИБ и проведения оценки зрелости процессов управления ИБ.

СОДЕРЖАНИЕ

Введение.....	6
1 Система управления информационной безопасностью организации ...	8
2 Процессы управления информационной безопасности	11
2.1 Процессы планирования СУИБ.....	11
2.2 Процессы реализации и эксплуатации системы управления ИБ.....	19
2.3 Процессы проверки СУИБ	23
2.4 Процессы совершенствования СУИБ	25
3 Способы оценки информационной безопасности	27
4 Структура уровней зрелости управления ИБ	30
5 Модель оценки зрелости СУИБ.....	38
5.1 Исходные данные для проведения оценки зрелости СУИБ	38
5.2 Этапы оценки зрелости СУИБ.....	39
Заключение	41
Список используемых источников	42
Приложение А. Модель зрелости процесса «Установление контекста управления рисками»	43
Приложение Б. Модель зрелости процесса «Управление изменениями АС»	52

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Система управления информационной безопасностью (далее – СУИБ) – часть системы управления организацией, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования информационной безопасности [1].

Уровень зрелости СУИБ – степень способности системы управления информационной безопасностью достижения целей ИБ [1].

Оценка зрелости СУИБ – деятельность, связанная с определением способности системы управления информационной безопасностью достижения целей ИБ [1].

Показатель оценки информационной безопасности – мера или характеристика для оценки информационной безопасности [1].

Свидетельства оценки ИБ – записи, изложение фактов или другая информация, которые имеют отношение к требованиям ИБ и могут быть проверены [1].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система;

ЗМ – защитные меры;

ИБ – информационная безопасность;

СУИБ – система управления информационной безопасностью.

ВВЕДЕНИЕ

Для достижения бесперебойного функционирования организации, необходимо поддерживать систему управления ИБ на должном уровне, что позволит избежать нежелательных последствий кибератак и повысит уровень доверия к организации. СУИБ, представляет собой совокупность связанных между собой и функционирующих процессов управления ИБ. Для контроля и оценки зрелости системы управления информационной безопасности существуют различные стандарты и лучшие практики, которым стремятся соответствовать и которые предписывают применение отработанных методологий и процессов в области ИБ. Оценка зрелости процессов управления ИБ организации основывается на рассмотрении совокупности параметров для каждого из процессов управления ИБ, отражающих достижение того или иного уровня зрелости данного процесса.

Целью выпускной квалификационной работы является разработка методики оценки зрелости процессов управления ИБ организации.

Зрелость процессов управления ИБ является мерой полноты, адекватности и эффективности процессов управления ИБ. Методика оценки зрелости процессов управления ИБ, в отличие от оценки достаточности применяемых защитных мер на объекте, дает возможность оценить полноту, адекватность процессов управления ИБ организации и способность СУИБ постоянно улучшаться.

Для разработки методики зрелости процессов управления ИБ необходимо выполнить следующие задачи:

- описать процессы управления ИБ;
- разработать уровни оценки процессов управления ИБ;
- разработать структуру показателей оценки и описать их содержание;

- разработать способ оценивания показателей;
- разработать правила формирования общей оценки зрелости процессов управления ИБ;
- разработать правила проведения оценки зрелости процессов управления ИБ;
- определить свидетельства оценки для показателей оценки зрелости процессов управления ИБ.

1 Система управления информационной безопасностью организации

В современных условиях информационная сфера организации, представляющая собой совокупность информационных активов, информационной инфраструктуры, сотрудников, осуществляющих сбор, формирование, распространение, хранение и использование информационных активов, играет все большую роль в достижении стратегических целей организации. Это влечет за собой новые требования к информационной сфере и функциям её элементов. Что приводит к увеличению сложности и росту информационной сферы. Изменчивость деятельности организации проявляется в отклонениях от общей тенденции развития организации, что также приводит к усложнению и изменению функций систем и компонентов информационной сферы организации. В связи с появлением все большего количества угроз возрастает неопределенность источников угроз, характеризующаяся отсутствием достаточного количества информации для выявления источников угроз. Из-за постоянного появления более сложных угроз информационной безопасности защитные меры (далее - ЗМ) устаревают (деградируют), что является причиной появления новых уязвимостей информационной безопасности организации.

В связи с этим появляется необходимость управления информационной безопасностью (далее - ИБ) организации. Функцию управления выполняет СУИБ. СУИБ представляет собой совокупность взаимосвязанных и взаимодействующих процессов управления ИБ.

СУИБ – часть общей системы управления, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

СУИБ любого объекта выполняют следующие функции:

- выявление и анализ рисков информационной безопасности;
- планирование и практическая реализация процессов, направленных на минимизацию рисков ИБ;
- контролирование этих процессов;
- внесение в процессы минимизации информационных рисков необходимых корректировок.

Для структурирования всех процессов СУИБ применяется модель PDCA ("Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)") [2]. Модель PDCA представлена на рисунке 1.

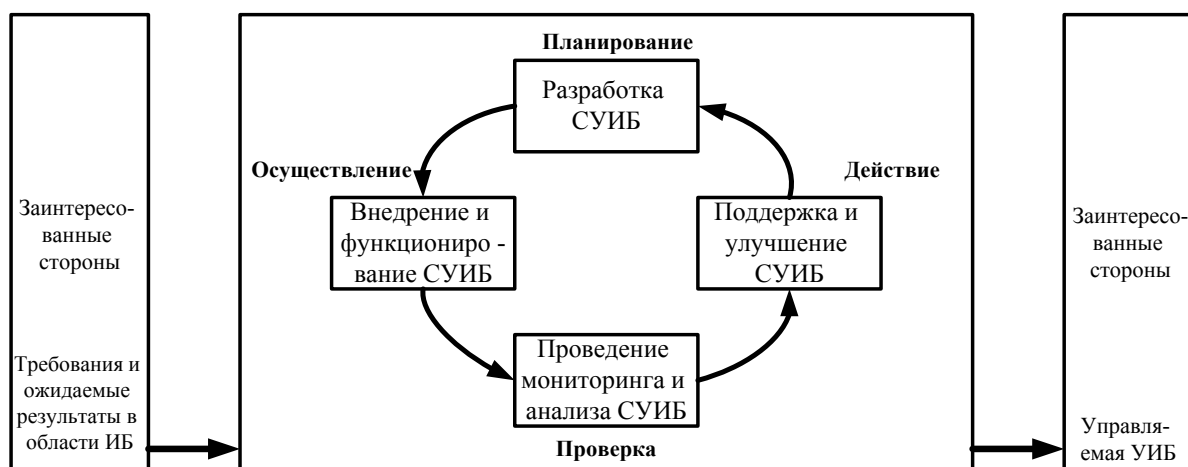


Рисунок 1 – модель PDCA.

Процессы управления, представленные в СУИБ, делятся на: процессы планирования, реализации и поддержки, проверки и совершенствования СУИБ.

На стадии планирования устанавливают политики ИБ, цели, задачи, процессы и процедуры, адекватные потребностям в управлении риска ИБ и совершенствованию СУИБ, для достижения результатов в соответствии с политиками и целями организации.

На стадии реализации осуществляются внедрение и поддержка политики ИБ организации, средств управления (защитных мер), регламентов, процессов и процедур СУИБ организации.

На стадии проверки осуществляются оценка и, если необходимо, измерение эффективности процессов управления ИБ организации на соответствие требованиям политики ИБ, целям и установленным практикам, обеспечивается отчетность высшему руководству о результатах для проведения соответствующего анализа.

На стадии совершенствования осуществляются выработка и принятие корректирующих и превентивных действий, основанных на результатах анализа, для достижения непрерывного усовершенствования СУИБ организации.

2 Процессы управления информационной безопасностью

2.1 Процессы планирования СУИБ

2.1.1 Формирование корпоративной политики ИБ.

Цель: задокументировать правила работы в организации в области ИБ.

Корпоративная политика ИБ – правила, процедуры, практические приемы и руководящие принципы в области ИБ, которыми руководствуется организация в процессе своей деятельности.

Корпоративная политика ИБ описывает:

- цели деятельности организации;
- приоритет направления обеспечения ИБ – может быть определен в корпоративной политике ИБ в зависимости от направления бизнеса организации;
- структуру корпоративного управления ИБ;
- построение системы ИБ – определяется, каким образом создается система ИБ, для достижения необходимого уровня ИБ, соответствующего целям ИБ;
- цели по обеспечению, обучению и осведомлению ИБ;
- обеспечение поддержки и проверки ИБ – основывается на управлении рисками ИБ. Оценка ИБ производится при проведении внешних и внутренних аудитов и мониторинга. Корпоративная политика ИБ указывает на необходимость проверок, их видов и периодичность;
- обстоятельства, при которых корпоративная политика ИБ должна быть пересмотрена или скорректирована: изменение бизнеса или деятельности организации [3].

В зависимости от размера и структуры организации, структура корпоративного управления ИБ включает роли:

- совет по ИБ (комитет) – ответственность за формирование и утверждение корпоративной политики, проведение мониторинга эффективной политики ИБ, принятие решений по ресурсам (люди, финансы), необходимые для обеспечения ИБ;
- ответственный за корпоративную политику ИБ - контроль реализации политики, аудит, мониторинг процессов и защитных мер по обеспечению ИБ;
- служба безопасности или администратор – применение и выполнение процессов и процедур по обеспечению ИБ, администрирование средств, реализующих защитные меры, обработка инцидентов ИБ.

Результат: разработанная корпоративная политика ИБ [3].

2.1.2 Установление контекста управления рисками.

Цель: установление внешнего и внутреннего контекста управления рисками, который включает установление критериев, необходимых для управления ИБ, и области применения управления рисками ИБ.

При установлении критериев принятия риска организация учитывает:

- соблюдение договорных обязательств организации;
- финансовые и материальные последствия;
- соблюдение законодательства;
- репутация и доверие к организации со стороны заинтересованных лиц;
- безопасность, здоровье работников организации;
- эффективность и непрерывность бизнес – деятельности.

Организация должна определять область применения управления рисками ИБ для выбранного объекта, при этом область применения должна охватывать все значимые активы выбранной области.

Для определения области применения управления рисками ИБ учитывается:

- корпоративная политика ИБ;
- особенности организации;
- ограничения, влияющие на область применения.

Результат: установленная область применения управления рисками ИБ и критерии оценивания рисков, критерии влияния риска и критерии принятия риска [3].

2.1.3 Оценка рисков ИБ.

2.1.3.1 Идентификация и определение ценности активов.

Ценность актива включает стоимость актива или затраты по замене поврежденного актива и расходы из-за потери свойств ИБ (конфиденциальности, целостности, доступности).

Ценность актива, в зависимости от характеристик, делится на степени:

- минимальная – устанавливается для активов, утрата которых или потеря свойств безопасности может привести к незначительному снижению качества и снижению доступности;
- средняя – устанавливается для актива, утрата которых или потеря свойств безопасности, может привести: нарушению отдельных договоров обязательств организации и нарушению конфиденциальности информации, связанной с предоставлением услуг;
- высокая – устанавливается для актива, утрата которого или набор свойств безопасности, может привести к нарушению законодательных требований, снижению репутации и доверия со стороны других организаций и лиц, невыполнению договорных обязательств, нарушению конфиденциальности персональных данных, нарушению непрерывности бизнес – процессов;
- критическая - устанавливается для актива, утрата которого или набор свойств безопасности, может привести к нарушению

законодательных требований, невыполнению договорных обязательств организации, потеря репутации и утрата доверия со стороны других организаций и лиц, нарушению конфиденциальности персональных данных и сведений составляющих конфиденциальную тайну, невозможность осуществления бизнес – процессов.

В определении ценности активов участвуют владельцы активов, служба ИБ, представители руководства организации.

Результат: список активов и их ценностей.

2.1.3.2 Идентификация угроз.

Цель: идентификация угроз и возможность их реализации.

Информация об угрозах может быть получена от владельцев активов (процессов), собственников систем, в результате анализа инцидентов, из любых нормативных документов, представляющих список возможных угроз.

Оценка угроз зависит от степени детализации модели угроз, учитывающей основные признаки угроз. Оценка признаков и их обобщение позволяет получить оценку опасности любых идентифицированных угроз [3].

При оценке угроз следует учитывать и оценивать следующие атрибуты угроз:

- продолжительность и непрерывность реализации угрозы ИБ;
- степень локализации угрозы;
- возможность обнаружения угрозы;
- возможность нейтрализации угрозы;
- частота реализации угрозы;
- источник угрозы.

Результат: перечень идентифицированных актуальных угроз для активов и оценка возможности их реализации.

2.1.3.3 Идентификация уязвимостей.

Цель: определение уязвимостей активов и оценка их уровня.

Данные для идентификации и оценки уязвимостей могут быть получены от владельцев активов, специалистов информатизации и ИБ, поставщиков компонентов системы. Уязвимости необходимо идентифицировать для каждого типа активов и зафиксировать в перечне.

Уровень уязвимостей определяется степенью существования уязвимости в активе и возможностью использования этой уязвимости угрозой.

Для каждого актива должны быть определены уровни всех присущих данному активу уязвимостей и зафиксированных в перечне уязвимостей.

Результат: перечень уязвимостей активов и оценка их уровней [3].

2.1.3.4 Идентификация существующих защитных мер.

Цель: определить существующие защитные меры (далее – ЗМ) и их эффективность.

Идентификация существующих ЗМ необходима для того, чтобы избежать дублирования ЗМ и лишних расходов. Необходимо провести проверки для того, чтобы убедиться в правильности функционирования и использования ЗМ там, где это необходимо [3].

Результат: перечень всех существующих ЗМ, их места нахождения и состояния использования.

2.1.3.5 Идентификация последствий.

Цель: идентификация последствий для активов, в результате потери конфиденциальности, целостности, доступности.

Существует два вида последствий:

- операционные последствия. Потеря времени на ремонт или замену актива; снижение безопасности сотрудников, вследствие нарушения ИБ; финансовые затраты, связанные со стоимостью восстановления или приобретения актива;

- последствия, связанные с потерей бизнеса (деятельности). Потеря репутации, вследствие нарушения законодательных (нормативных) обязательств, или вследствие использования внешней стороной информации, полученной из-за нарушения ИБ.

Последствия определяются с помощью идентификации инцидентов и их сценариев.

Сценарий инцидента – описание угрозы, использующий определенную уязвимость или набор уязвимостей во время инцидента.

Результат: перечень сценариев инцидента с их последствиями.

2.1.3.6 Оценка последствий.

Цель: оценка влияния инцидентов на бизнес (деятельность) объекта, с учетом последствий нарушения ИБ (конфиденциальности, целостности, доступности).

Для оценки последствий необходимо знать перечень идентифицированных сценариев инцидентов с их последствиями.

Оценка последствий связана с анализом влияния на бизнес (деятельность) на основе определения ценности активов. В каждой последующей интеграции оценки она будет отличаться (снижаться) из-за наличия и степени эффективности реализации ЗМ.

Результат: перечень последствий сценариев инцидентов и их оценка.

2.1.3.7 Оценка вероятностей инцидентов.

Цель: оценка вероятности (возможности) сценариев инцидентов.

Для оценивания вероятности инцидентов необходим перечень идентификационных сценариев инцидентов с их последствиями, перечень существующих ЗМ.

Необходимо учитывать уровни угроз и уровни уязвимостей, а также перечень существующих ЗМ и их эффективность.

Результат: оценка вероятности (возможности) сценариев инцидентов.

2.1.3.8 Определение уровня риска.

Цель: определение уровня риска для сценариев инцидентов.

Под уровнем риска понимается величина риска, выраженная комбинацией последствий и их вероятностей.

Для определения уровня риска необходим перечень сценариев инцидентов с их последствиями, перечень активов и их оценка, вероятность сценариев инцидентов.

Результат: перечень рисков и значения их уровней [3].

2.1.3.9 Оценивание риска.

Цель: сравнение уровней рисков с критериями оценивания риска и критериями принятия риска.

Оценивание риска – это процесс сравнения результатов анализа риска с критериями риска с целью определения, является ли риск и его величина приемлемыми (допустимыми).

Для того чтобы осуществить оценивание риска необходимы: перечень рисков с их значениями; критерии оценивания риска; критерии принятия риска.

При оценивании риска подготавливается информация для принятия риска и дальнейших действий с ним.

Результат: перечень рисков с назначенными приоритетами их обработки, в соответствии с критериями оценивания риска; перечень приемлемых рисков, в соответствии с критерием принятия риска.

2.1.3.10 Обработка рисков.

Цель: снижение риска до приемлемого уровня и определение плана обработки рисков.

Под обработкой риска понимается процесс модификации риска.

Для обработки риска возможны следующие действия:

- сохранение риска – если уровень риска приемлемый и соответствует критериям принятия риска;

- предотвращение риска - осуществляется путем отказа от действий или условий, вызывающих конкретный риск;
- разделение риска – риск разделяется с другой стороной, которая может эффективно снизить риск;
- снижение риска – осуществляется путем введения ЗМ для того, чтобы остаточный риск соответствовал приемлемому уровню.

При выборе ЗМ должны быть учтены функциональные характеристики ЗМ, а именно: простота, прозрачность для пользователя, стойкость ЗМ, типы выполнения функций (предотвращение, сдерживание, обнаружение, восстановление, мониторинг).

Результат: решение о выборе ЗМ (план обработки риска) и остаточные риски.

2.1.3.11 Принятие рисков.

Цель: формирование решений о принятии риска.

Формирование решений принимается руководством организации.

Для принятия рисков необходим план обработки рисков, остаточный риск и их оценка.

Уровень остаточного риска может не соответствовать критериям принятия риска.

Результат: перечень принятых рисков с обоснованием сохранения тех рисков, которые не соответствуют критериям принятия риска [3].

2.1.4 Формирование политик ИБ автоматизированных систем (АС).

Цель: формирование политик автоматизированных систем (далее - АС) с учетом корпоративной политики ИБ и результатов управления рисками.

Политика ИБ АС должна содержать:

- описание системы, ее компонентов и определение ее границ, а также описание целей с точки зрения бизнеса;
- описание целей ИБ системы;
- описание (перечень) активов системы;

- описание угроз, снижение защищенной актуальности для системы;
- описание уязвимостей системы и ее компонентов;
- описание рисков ИБ системы;
- перечень ЗМ.

Результат: разработанные политики ИБ АС.

2.2 Процессы реализации и эксплуатации системы управления ИБ

2.2.1 Реализация ЗМ.

Цель: реализация ЗМ.

Перед реализацией ЗМ должны быть протестированы. По результатам тестирования составляется отчет.

Для дальнейшего использования и эксплуатации защитных мер разрабатываются должностные инструкции по эксплуатации ЗМ и регламенты использования защитных мер.

Результат: реализованные ЗМ.

2.2.2 Управление изменениями автоматизированных систем.

Цель: контроль соответствия изменений АС требованиям ИБ.

Управление изменениями АС заключается в следующем:

- идентификация и регистрация изменений АС. При этом должно быть точно установлено, что все действия по предъявлению и рассмотрению этих изменений, а также внесение изменений производится уполномоченными лицами;
- анализ и оценка влияния последствий на ИБ;
- учет количества изменений и хронология;
- обновление и корректирующие документации по АС после завершения каждого изменения. Старая документация архивируется, либо уничтожается;

- реализация изменений должна производиться таким образом, чтобы не нарушать реализацию процессов;
- сообщение уполномоченным лицам об изменениях [3].

Для реализации процесса управления изменениями АС необходимы процедуры:

- внесения изменения АС;
- оценки последствий (внесенных) изменений на ИБ;
- доведение информации о внесенных изменениях до заинтересованных лиц.

Результат: учет всех принятых изменений АС.

2.2.3 Реализация программы осведомления об ИБ.

Цель: увеличить уровень осведомления об ИБ таким образом, чтобы ИБ стала неотъемлемой частью деловой деятельности сотрудников.

В программе осведомленности об ИБ должны быть описаны:

- значение ИБ для организации;
- последствия инцидентов ИБ для организации и сотрудников;
- риски ИБ и необходимость ЗМ;
- ограничение доступа в различных областях контролируемой зоны;
- необходимость оповещения о нарушениях и о попытках нарушения ИБ;
- ответственность за нарушение процессов ИБ и нарушение ЗМ.

По результатам осведомления составляются отчеты, в которых фиксируется прохождение сотрудниками программы осведомления.

Корректировка программы осведомления должна производиться при изменении политики ИБ, при вводе новых технологий, значимых активов.

Результат: достижение требуемого уровня осведомления сотрудников об ИБ.

2.2.4 Реализация программы обучения ИБ.

Цель: увеличение компетенции персонала, связанного с обеспечением ИБ.

Программы обучения ИБ направлены на обучение следующих специалистов:

- персонал, связанный и ответственный за функционирование АС;
- персонал, ответственный за обеспечение ИБ по различным направлениям (администраторы управления доступностью, криптографической защиты и т.д.).

Глубина обучения и его длительность зависят от ролей персонала.

Общие темы обсуждения:

- угрозы ИБ;
- уязвимости идентифицированных активов;
- риски ИБ;
- ЗМ и процедуры, необходимые для их правильного использования;
- ответственность за обеспечение ИБ.

Дополнительные темы обсуждения:

- управление инцидентами ИБ;
- физическая безопасность;
- безопасность сотрудников;
- безопасность аппаратных и программных средств.

Результат: достижение требуемого уровня компетенции персонала, связанного с управлением ЗМ [3].

2.2.5 Управление инцидентами ИБ.

Цель: реагирование на инцидент рациональным и эффективным способом; получение знания и опыта из инцидента для использования его в будущем.

Для управления инцидента ИБ должны быть регламентированы следующие процедуры:

- обнаружение и оповещение об инциденте ИБ. Осуществляется сотрудниками и (или) техническими средствами на основе признаков инцидента. Сотрудник, путем наблюдения или с помощью АС, должен сформировать отчет об инциденте ИБ;
- анализ инцидентов ИБ. Заключается в сборе информации об инциденте и принятии решения о реализации инцидента или личности инцидента;
- сдерживание инцидентов ИБ. Заключается в выборе стратегии сдерживания. В организации должна быть определена стратегия для каждого типа инцидента;
- устранение инцидентов ИБ и восстановление после них. Заключается в устранении элементов инцидента после сдерживания;
- сбор и обработка данных об инцидентах ИБ и подготовка отчета об инциденте ИБ. Заключается в сборе данных, которые могут быть использованы при обработке инцидента, статистических данных об инциденте и создании хронологии событий.

Результат: управление инцидентами рациональным и эффективным способом.

2.3 Процессы проверки СУИБ

2.3.1 Мониторинг ИБ.

Целями мониторинга ИБ являются:

- контроль за реализацией в организации положений внутренних и внешних документов по ИБ для обнаружения отклонений от требований ИБ;
- контроль качества используемых ЗМ;
- выявление нештатных, в том числе злоумышленных действий с информационными активами и бизнес-процессами организации;
- выявление событий ИБ, часть из которых в дальнейшем классифицируется как инциденты ИБ;
- выявление уязвимостей активов, которыми могут воспользоваться злоумышленники для реализации атак на системы, сети и сервисы организации;
- обеспечение доказательной базы для расследования инцидентов.

Процессы мониторинга ИБ включают в себя следующую деятельность:

- поиск, отслеживание, наблюдение, накопление, систематизация, оценивание сведений, относящихся к области ИБ;
- прогнозирование состояния и качества всех объектов и процессов в информационной среде организации [3].

Для реализации мониторинга ИБ необходимо создавать журналы для записей событий, связанных с ИБ. Записи мониторинга ИБ следует хранить в течение установленного времени, с целью использования при расследовании инцидентов ИБ, а также с целью корректирующих ЗМ.

При реализации мониторинга фиксируют, как правило, следующие параметры событий: дата/время входа в систему; идентификатор терминала; успешные (не успешные) попытки доступа в систему. Мониторинг реализуется для таких событий, как авторизованные действия, привилегированные действия и другие.

Результат: данные журналов регистрации событий.

2.3.2 Проверка соответствия ИБ.

Цели проверки соответствия ИБ:

- поиск и контроль несоответствия установленных требований ИБ;
- поддержка информативности руководства об ИБ.

Способы проверки соответствия ИБ:

- самооценка ИБ;
- внешний и внутренний аудит ИБ.

Самооценка ИБ – самостоятельный, документированный процесс оценки свидетельств самооценки с целью установленной степени выполнения требований по обеспечению ИБ.

Свидетельства самооценки ИБ – записи, изложения фактов или другая информация, которые имеют отношение к требованиям ИБ и могут быть проверены.

Самооценка ИБ проводится по инициативе руководства организации и, как правило, собственными силами. Цели самооценки зависят от руководства организации.

Результат: отчет по самооценке ИБ.

Аудит ИБ – периодически независимый и документированный процесс, получение свидетельства аудита ИБ и объективов их оценивания, с целью установленной степени выполнения согласованных критериев аудита ИБ.

Свидетельства аудита ИБ – записи, изложения фактов или другая информация, которые имеют отношение к требованиям ИБ и могут быть проверены.

Внутренний аудит ИБ проводит для своих целей сама организация.

Внешний аудит проводят стороны, заинтересованные в деятельности организации.

Результат: отчет и заключение по результатам аудита ИБ.

2.3.3 Анализ ИБ со стороны руководства.

Цель: обеспечить уверенность в том, что система управления ИБ является адекватной ее назначению; определение возможности улучшений процессов управления ИБ.

Анализ ИБ позволяет оценить, нужны ли улучшения и изменения в отношении ИБ. Для процесса анализа необходимо определить необходимый набор данных, которые должны содержать следующую информацию:

- результаты аудитов и самооценки ИБ;
- результаты мониторинга ИБ;
- способы, методы и процессы, которые могут использоваться в организации для улучшения функционирования ЗМ и эффективности системы управления ИБ;
- уязвимости и угрозы, которые не были рассмотрены при оценивании риска;
- действия, предпринятые по итогам предыдущего анализа ИБ со стороны руководства [3].

Результат: документы, в которых представляются рекомендации и предложения по улучшению ИБ.

2.4 Процессы совершенствования СУИБ

Цель: реализация принятых решений по улучшению системы управления ИБ.

К процессу совершенствования ИБ относятся: реализация улучшений в ИБ; информирование об изменениях и их согласования с заинтересованной стороной.

Совершенствование СУИБ осуществляется путем использования корпоративной политики ИБ, целей организации, результатов аудитов внутренних и внешних, анализа отслеживаемых событий, корректирующих и превентивных мер и анализа со стороны руководства.

Реализация корректирующих действий в отношении ЗМ осуществляется для установки причины несогласования ЗМ или других нежелательных ситуаций, приводивших к снижению уровня ИБ, чтобы предотвратить их повторения. Процедура действий в отношении ЗМ АС должны предпринимать для устранения причин возможной несогласованной ЗМ или других возможностей нежелательной ситуации.

На основании реализации корректирующих действий в отношении ЗМ осуществляется информирование и согласование с заинтересованными сторонами об внесенных улучшениях.

Результат: корректирующие действия в отношении системы управления ИБ и плана обработки рисков.

3 Способы оценки информационной безопасности

Оценка ИБ заключается в выработке оценочного суждения относительно зрелости процессов управления ИБ, адекватности используемых защитных мер или целесообразности (достаточности) затрат для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических факторов объекта оценки.

Наряду с важнейшим назначением оценки ИБ – создание информационной потребности для совершенствования ИБ, возможны и другие цели проведения оценки ИБ такие, как:

- определение степени соответствия установленным критериям отдельных областей обеспечения ИБ, процессов управления ИБ, защитных мер;
- выявление влияния критических факторов и их сочетания на ИБ организации;
- сравнение зрелости различных процессов управления ИБ и сравнение степени соответствия различных защитных мер установленным требованиям.

В зависимости от выбранного для оценки ИБ критерия способы оценки ИБ организации на оценку по эталону и рискориентированную оценку.

Способ оценки ИБ по эталону сводится к сравнению деятельности и мер по обеспечению ИБ организации с требованиями, закрепленными в эталоне. По сути дела проводится оценка соответствия ИБ организации установленному эталону. Под оценкой соответствия ИБ организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации. С помощью оценки соответствия ИБ измеряется правильность реализации процессов системы управления ИБ организации и идентифицируются недостатки такой реализации.

В результате проведения оценки ИБ должна быть сформирована оценка степени соответствия ИБ эталону, в качестве которого могут быть приняты процессы управления ИБ, процедуры обеспечения ИБ, защитные меры, соответствующие:

- требованиям законодательства Российской Федерации в области ИБ;
- отраслевым требованиям по обеспечению ИБ;
- требованиям нормативных, методических и организационно-распорядительных документов по ИБ;
- требованиям национальных и международных стандартов в области ИБ.

Основные этапы оценки информационной безопасности по эталону включают выбор эталона и формирование на его основе критериев оценки ИБ, сбор свидетельств оценки и измерение критических элементов (факторов) объекта оценки, формирование оценки ИБ.

Рискориентированная оценка ИБ организации представляет собой способ оценки, при котором рассматриваются риски ИБ, возникающие в информационной сфере организации, и сопоставляются существующие риски ИБ и принимаемые меры по их обработке. В результате должна быть сформирована оценка способности организации эффективно управлять рисками ИБ для достижения своих целей.

В работе для оценки ИБ применяется способ оценки информационной безопасности по эталону. Целью оценки ИБ является оценка процессов управления ИБ организации или объекта (ов) организации. Для достижения такой цели оценки в качестве эталона должна использоваться эталонная модель процессов управления ИБ, которая описывает в зависимости от объекта оценки совокупность из одного или более процессов в терминах назначения, цели и ожидаемых результатов.

Модель оценки процесса основывается на совокупности показателей, которые используются в качестве основы для сбора объективных данных для

определения степени достижения процессов назначения и результатов процессов на основе параметров процесса. Показатели, отображая назначения, результаты и параметры процессов, формируют таким образом эталонные профили процессов.

Международный стандарт ИСО/МЭК 15504 [4] определяет, что для оценки процесса (процессов) может использоваться модель, оценивающая зрелость процесса (процессов). Измерение зрелости процесса (процессов) состоит из структуры измерений, включающей несколько уровней зрелости (возможностей) процесса.

4 Структура уровней зрелости управления ИБ

Оценка процессов управления информационной безопасностью основывается на следующих принципах:

- процессы управления ИБ оцениваются по 5 уровням: от первого (минимального) до пятого (максимального), причём, каждый следующий уровень включает полностью реализацию предыдущих уровней;
- каждый уровень описывается определенным набором показателей и их значениями;
- оценка процессов управления ИБ осуществляется на основе свидетельств оценки зрелости ИБ.

Каждому уровню зрелости сопоставляются соответствующие общие характеристики процессов управления ИБ. Эти характеристики приведены в таблице 1.

Таблица 1 – Общие характеристики (модель) уровней зрелости процессов обеспечения и управления ИБ

Уровень зрелости процессов управления ИБ	Общие характеристики уровней зрелости процессов управления ИБ
Первый уровень	<p>В организации осознается существование проблем ИБ и необходимость их решения.</p> <p>Деятельность в области ИБ реализована в виде некоторых процессов управления ИБ, однако они не всегда достигают ожидаемых результатов.</p> <p>Организованный подход к управлению ИБ отсутствует.</p> <p>В организации могут быть разработаны отдельные локальные нормативные документы по обеспечению ИБ.</p>

Продолжение таблицы 1

Уровень зрелости процессов управления ИБ	Общие характеристики уровней зрелости процессов управления ИБ
Второй уровень	<p>В организации заинтересованы в качественном и своевременном решении существующих проблем ИБ.</p> <p>Деятельность в области ИБ реализована в виде некоторых процессов управления ИБ. Процессы, в основном, достигают своего назначения. Однако многие реализованы бессистемно, реализуются от случая к случаю на индивидуальной основе.</p> <p>В организации разработаны внутренние нормативные документы по некоторым направлениям обеспечения ИБ (например, обеспечение антивирусной защиты, криптографической защиты и т.п.) и некоторым процессам управления ИБ (например, оценка угроз ИБ, уязвимостей, обработка рисков и т.п.).</p> <p>Реализация процессов управления ИБ во многом зависит от компетенции отдельных лиц; в организации не создана система обучения и информирования работников о принятых процессах управления ИБ</p>
Третий уровень	<p>В организации уделяется должное внимание проблемам в области ИБ и их решению, ответственности в области ИБ.</p> <p>Процессы управления ИБ зафиксированы документально (определены цели осуществления процессов, определены ответственность и полномочия, ресурсы, необходимые для осуществления процессов и т. п.). Также определены ожидаемые результаты реализации процессов. Процессы управления ИБ включают в свой состав процедуры, некоторые из которых являются общепринятыми для организации.</p> <p>В организации реализован формализованный подход к обучению и информированию о процессах управления ИБ.</p> <p>В организации может осуществляться планирование, контроль и оценка некоторых процессов обеспечения и управления ИБ, частичный контроль за соблюдением установленных требований, однако процедуры контроля не формализованы</p>

Продолжение таблицы 1

Уровень зрелости процессов управления ИБ	Общие характеристики уровней зрелости процессов управления ИБ
Четвёртый уровень	<p>В организации установлена ответственность за управление ИБ (распределены роли по обеспечению и управлению ИБ, назначены исполнители ролей и т.п.).</p> <p>Регламентированные процессы выполняются управляемым образом: планируются, реализуются, контролируются, измеряются.</p> <p>Осуществляется контроль выполнения требований нормативных документов организации в области ИБ.</p> <p>Процессы управления ИБ соответствуют общепринятой в организации практике.</p> <p>Процессы подвержены измерению (оценке) и постоянному контролю. В случае, если процессы неэффективны, могут быть приняты соответствующие меры по совершенствованию.</p>
Пятый уровень	<p>Определены цели улучшения процессов и процедур управления ИБ, которые обеспечивают достижение стратегических целей организации.</p> <p>Процессы управления ИБ полностью интегрированы в деятельность организации.</p>

Для оценки зрелости организации в области ИБ используются основные и комплексные показатели. Комплексные показатели K_i (i – номер комплексного показателя) зрелости ИБ отражают характеристики уровней зрелости ИБ. Основные показатели K_{ij} (i – номер комплексного показателя, j – номер основного показателя в комплексном показателе) входят в состав комплексных показателей.

Таблица 2 – Комплексные показатели оценки процессов управления ИБ

Обозначение комплексного показателя	Наименование комплексного показателя
K_1	Первый уровень
K_2	Второй уровень
K_3	Третий уровень
K_4	Четвёртый уровень
K_5	Пятый уровень

Соответствующие комплексным показателям основные показатели оценки зрелости процессов управления ИБ представлены в таблице 3.

Таблица 3 – Основные показатели оценки зрелости процессов управления ИБ

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель
К ₁	К _{1.1}	Существуют ли меры и (или) средства, используемые для управления ИБ?
	К _{1.2}	Достигают ли существующие меры и средства, используемые для управления ИБ, ожидаемого результата?
	К _{1.3}	Реализована ли деятельность по управлению ИБ в виде процессов?
К ₂	К _{2.1}	Организовано ли обучение принятым в Организации процессам управления ИБ и информируются ли сотрудники об этих процессах?
	К _{2.2}	Достигает ли процесс управления ИБ ожидаемых результатов?
	К _{2.3}	Определен ли перечень нормативных документов организации, регулирующих процесс управления ИБ?
К ₃	К _{3.1}	Зафиксирован ли документально процесс управления ИБ?
	К _{3.2}	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе управления ИБ?
	К _{3.3}	Определены ли цели осуществления процесса управления ИБ?
	К _{3.4}	Определены ли ответственность и полномочия по осуществлению процесса управления ИБ?
	К _{3.5}	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса управления ИБ?
	К _{3.6}	Определен ли перечень результатов (выходов) процесса управления ИБ?
	К _{3.7}	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса управления ИБ?
	К _{3.8}	Установлены ли в организации требования по осуществлению контроля за реализацией процесса управления ИБ?

Продолжение таблицы 3

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель
	K _{3.9}	Осуществляется ли в организации оценка процесса управления ИБ?
	K _{3.10}	Существует ли в организации контроль за исполнением требований нормативных документов организации в области ИБ?
K ₄	K _{4.1}	Установлена ли (документально зафиксирована) в организации ответственность за процесс управления ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?
	K _{4.2}	Доведены ли ответственность и полномочия по осуществлению процесса управления ИБ до сведения ответственных лиц в организации?
	K _{4.3}	Компетентен ли персонал, осуществляющий процесс управления ИБ?
	K _{4.4}	Регламентирован ли в организации процесс управления ИБ?
	K _{4.5}	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?
	K _{4.6}	Соответствует ли процесс управления ИБ общепринятой практике?
	K _{4.7}	Доступны ли ресурсы и активы, необходимые для осуществления процесса управления ИБ?
	K _{4.8}	Определены ли соответствующие методы для проведения измерения (оценки) процесса управления ИБ?
	K _{4.9}	Реализован ли постоянный контроль за реализацией процесса управления ИБ?
	K _{4.10}	Существует ли возможность принятия мер в случае, если процесс управления ИБ неэффективен?
K ₅	K _{5.1}	Осуществляется ли совершенствование процесса управления ИБ регламентированным образом?
	K _{5.2}	Определяются ли цели улучшения процесса управления ИБ, которые обеспечивают достижение целей деятельности?
	K _{5.3}	Определяются ли возможности улучшений процесса, связанные с новыми технологиями?
	K _{5.4}	Оценивается ли направленность совершенствования процесса управления ИБ на непрерывное улучшение ИБ?

Оценка зрелости процессов управления ИБ организации осуществляется путем анализа следующих процессов:

- формирование корпоративной политики информационной безопасности;
- установление контекста управления рисками;
- идентификация и определение ценности активов;
- идентификация угроз;
- идентификация уязвимостей;
- идентификация существующих защитных мер;
- идентификация последствий;
- оценка последствий;
- оценка вероятностей инцидентов;
- определение уровня риска;
- оценивание риска;
- обработка рисков;
- принятие рисков;
- формирование политик ИБ;
- реализация ЗМ;
- управление изменениями;
- реализация программы осведомления об ИБ;
- реализация программы обучения ИБ;
- управление инцидентами ИБ;
- мониторинг ИБ;
- проверка соответствия ИБ;
- анализ ИБ со стороны руководства;
- совершенствование СУИБ.

Оценка основных показателей процессов управления ИБ производится с помощью шкалы, отражающей уровень реализации оцениваемого процесса (уровень выполнения основного показателя).

Используются следующие обозначения значений оценки:

- Н – не выполнен. Свидетельств выполнения основного показателя мало или они отсутствуют;
- Ч – частично выполнен. Имеются свидетельства частичного, некоторого выполнения основного показателя;
- П – полностью выполнен. Имеются свидетельства полного и систематического подхода и полного выполнения основного показателя. В оцениваемом процессе или процедуре нет существенных слабых мест, связанных с этим основным показателем.

Уровень выполнения основного показателя в представленной шкале следует выражать в процентах выполнения:

- Н – не выполнен (от 0% - до 30% выполнения);
- Ч – частично выполнен (от 30% - до 80% выполнения);
- П – полностью выполнен (от 80% - до 100% выполнения).

Каждый уровень зрелости процесса управления ИБ имеет комплексный показатель, соответствующий основному содержанию характеристики уровня зрелости: первый уровень – K_1 ; второй уровень – K_2 ; третий уровень – K_3 ; четвёртый уровень – K_4 ; пятый уровень – K_5 .

Для каждого процесса можно построить модель уровней зрелости от 1 до 5. В приложениях А и Б представлены разработанные модели зрелости процессов «Установление контекста управления рисками» и «Управление изменениями АС».

Достигнутый процессом управления ИБ уровень зрелости ИБ должен быть получен из оценок комплексных показателей, соответствие которых уровням зрелости ИБ представлено в таблице 4

Таблица 4 – Соответствие комплексных показателей оценки зрелости процессов управления ИБ и их оценок уровням зрелости ИБ

Уровень зрелости	Групповой показатель	Оценка группового показателя
1	2	3
Первый	K ₁ K ₂	Полностью выполнен Частично выполнен
Второй	K ₁ K ₂ K ₃	Полностью выполнен Полностью выполнен Частично выполнен
Третий	K ₁ K ₂ K ₃ K ₄	Полностью выполнен Полностью выполнен Полностью выполнен Частично выполнен
Четвёртый	K ₁ K ₂ K ₃ K ₄ K ₅	Полностью выполнен Полностью выполнен Полностью выполнен Полностью выполнен Частично выполнен
Пятый	K ₁ K ₂ K ₃ K ₄ K ₅	Полностью выполнен Полностью выполнен Полностью выполнен Полностью выполнен Полностью выполнен

Общая оценка зрелости СУИБ формируется из оценок зрелости процессов управления ИБ и определяется как соотношение суммы значений уровней зрелости, достигнутых процессами управления ИБ, к максимальному числу уровней зрелости процессов управления СУИБ.

Так как объектами оценки зрелости СУИБ максимально могут быть описанные выше 23 процесса управления ИБ, то максимальное число уровней зрелости для 23 процессов управления ИБ равно 115.

5 Модель оценки зрелости СУИБ

5.1 Исходные данные для проведения оценки зрелости СУИБ

5.1.1 Свидетельства оценки зрелости должны удовлетворять следующим условиям:

- быть проверяемыми;
- быть актуальными на момент проведения оценки.

5.1.2 Свидетельствами оценки зрелости процессов управления ИБ могут быть:

- локальные документы организации, относящиеся к управлению ИБ;
- письменные ответы работников организации, получаемые в процессе опросов;
- другая информация, которая имеет отношение к показателям оценки, например, результаты наблюдений.

5.1.3 В ходе анализа документов должны осуществляться:

- проверка наличия документально оформленных и утвержденных политик ИБ, руководств, инструкций, регламентов по обеспечению ИБ; оценка их полноты и непротиворечивости;
- проверка наличия свидетельств выполнения мероприятий по управлению информационной безопасностью за истекший период (планы, регистрационные журналы, акты, договоры, отчёты, протоколы и т.д.), оценка их соответствия политикам ИБ организации;
- проверка наличия отчётных документов по результатам предыдущих внутренних и внешних оценок зрелости и полноты реализации указанных в них рекомендаций.

5.1.4 Опрос персонала, участвующего в процессах обеспечения и управления ИБ, должен проводиться в письменной форме.

5.1.5 Наблюдение за деятельностью организации в области ИБ должно проводиться с целью подтверждения функционирования организационно-технических мер защиты, соответствия параметров настроек защитных мер принятым в организации политикам ИБ, регламентам.

5.2 Этапы оценки зрелости СУИБ

Оценка зрелости включает в себя следующие этапы:

- подготовка к оценке;
- проведение оценки;
- подготовка и утверждение заключения и отчета по результатам оценки.

В рамках подготовки к проведению оценки зрелости должны быть выполнены следующие процедуры:

- разработка и согласование плана проведения оценки зрелости СУИБ;
- формирование рабочих документов для регистрации результатов оценки.

Содержание плана проведения оценки зрелости СУИБ:

- цели оценки;
- перечень оцениваемых процессов управления ИБ,
- период проведения оценки;
- роли и обязанности членов участников оценки.

Основными участниками оценки зрелости СУИБ являются:

- руководитель группы оценки;
- оценщик.

Оценщики должны подготовить рабочие документы для регистрации результатов оценки:

- типовые формы для отображения свидетельств оценки;
- формы для регистрации выводов оценки.

Проведение оценки зрелости СУИБ включает следующие действия:

- сбор свидетельств и обеспечение доверия к полученным свидетельствам;
- оценка свидетельств по установленным показателям;
- формирование выводов оценки (определение уровня зрелости СУИБ).

Все полученные свидетельства оценки зрелости и источники их получения должны быть отражены документально.

В документах по результатам оценки указываются ссылки на соответствующие локальные нормативные документы организации, результаты опроса работников организации, а также результаты наблюдений членов группы оценщиков.

Результаты опроса и наблюдений должны быть подтверждены подписями опрашиваемого работника организации и оценщика.

Оценщиком должно быть проведено сопоставление выявленных свидетельств оценки с установленными показателями оценки и сформированы оценки основных показателей, а затем оценки комплексных показателей в соответствии с правилами, указанными в разделе 4.

На основании полученных оценок комплексных показателей оценщиком формируются выводы оценки, которые указывают на уровень зрелости элементов объектов оценки или СУИБ в целом.

ЗАКЛЮЧЕНИЕ

В результате выполнения дипломной работы была разработана модель оценки зрелости процессов управления ИБ.

В первом разделе ВКР было произведено описание системы управления ИБ.

Во втором разделе ВКР описаны процессы управления ИБ.

В третьем разделе описана система оценки ИБ, приведены и описаны методы системы оценки ИБ.

В четвертом разделе описаны уровни зрелости процессов управления ИБ, разработаны основные комплексные показатели оценки зрелости процессов управления ИБ.

В пятом разделе представлены способы получения исходных данных для проведения оценки зрелости СУИБ и действия, осуществляемые в ходе анализа документов, разработаны этапы оценки зрелости СУИБ.

В приложениях А и Б представленные разработанные модели зрелости процессов «Установление контекста управления рисками» и «Управление изменениями АС».

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены полностью.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

- 1 Международный стандарт ИСО/МЭК 15504 – 1:2004 «Информационная технология. Оценка процесса. Понятия и терминология».
- 2 ГОСТ Р ИСО/МЭК 27001 - 2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;
- 3 ГОСТ Р ИСО/МЭК 27002 -2012 «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»;
- 4 Международный стандарт ИСО/МЭК 15504 – 3:2004 «Информационная технология. Оценка процесса. Руководство по проведению оценки»;

ПРИЛОЖЕНИЕ А

(справочное)

Модель зрелости процесса «Установление контекста управления рисками»

Уровень 1

Деятельность по управлению рисками определена в нормативных документах организации. В организации установлены критерии риска, необходимые для управления ИБ.

Определена область применения управления рисками ИБ в организации.

Процесс «Установление контекста управления рисками» не всегда достигает ожидаемых результатов. Не предусмотрены корректировки критериев риска, области применения управления рисками.

Уровень 2.

Осуществляется полная реализация процесса «Установление контекста управления рисками», достигаются результаты процесса, а именно: установлена область применения управления рисками ИБ и критерии оценивания рисков, критерии влияния риска и критерии принятия риска.

Составлен и определен перечень нормативных документов организации, регулирующих процесс.

Процесс «Установление контекста управления рисками» документирован и стандартизирован, суть процесса доводится до заинтересованного персонала.

Определены цели процесса «Установление контекста управления рисками», также идентифицированы ресурсы и информация. Документально зафиксирован персонал, отвечающий за осуществление процесса. Не определены полномочия лиц, несущих ответственность за осуществление процесса «Установление контекста управления рисками».

Требования по осуществлению контроля над реализацией процесса «Установление контекста управления рисками» установлены не в полном объеме. Нет документальной фиксации процесса.

Уровень 3.

Осуществляется полная реализация процесса «Установление контекста управления рисками», в организации определены цели и результаты процесса. Процесс «Установление контекста управления рисками» документирован и стандартизирован, определен перечень нормативных документов организации, осуществляется контроль за выполнением требований нормативных документов организации и внешних регулирующих и надзорных органов в области управления рисками таких, как соблюдение договорных обязательств организации и законодательства.

Процесс «Установление контекста управления рисками» регламентирован. Документально зафиксированы результаты выполнения процесса «Установление контекста управления рисками», формализована практика в области управления ИБ в виде процедур процесса «Установление контекста управления рисками». Установлены требования по осуществлению контроля над реализацией процесса «Установление контекста управления рисками». Контроль за реализацией процесса «Установление контекста управления рисками» осуществляется не постоянно, нет разработанного плана постоянного контроля.

Не периодически осуществляется оценка процесса. Методы для поведения оценки процесса «Установление контекста управления рисками» определены, но документально не зафиксированы.

В организации распределены и документально зафиксированы роли по управлению рисками. Документально зафиксирован ответственный персонал, определены полномочия лиц, несущих ответственность за осуществление процесса. Персонал, осуществляющий процесс «Установление контекста управления рисками» компетентен.

Процесс «Установление контекста управления рисками» соответствует общепринятой практике, ресурсы и активы, необходимые для осуществления

процесса «Установление контекста управления рисками», доступны не в полном объеме.

Уровень 4.

В организации осуществляется полная реализация процесса, определены цели и результаты процесса. Процесс «Установление контекста управления рисками» документирован и стандартизирован, определен перечень нормативных документов организации, осуществляется контроль за выполнением требований нормативных документов организации и внешних регулирующих и надзорных органов в области управления рисками.

Процесс «Установление контекста управления рисками» регламентирован и документально зафиксированы результаты выполнения процесса, формализована практика в области управления ИБ в виде процедур процесса «Установление контекста управления рисками». Установлены требования по осуществлению контроля над реализацией процесса «Установление контекста управления рисками». Разработан и документально зафиксирован план постоянного контроля за реализацией процесса «Установление контекста управления рисками».

Осуществляется оценка процесса «Установление контекста управления рисками» в организации. Методы для проведения оценки процесса «Установление контекста управления рисками» определены и документированы.

В организации распределены и документированы роли по управлению рисками. Документально зафиксирован ответственный персонал, определены полномочия лиц, несущих ответственность за осуществление процесса «Установление контекста управления рисками». Ответственность и полномочия по осуществлению процесса «Установление контекста управления рисками» доведены до ответственных лиц. Персонал, осуществляющий процесс «Установление контекста управления рисками» компетентен.

Процесс соответствует общепринятой практике, ресурсы и активы, необходимые для осуществления процесса «Установление контекста управления рисками» определены и доступны в полном объеме.

Разработаны меры, применяемые в случае, если процесс «Установление контекста управления рисками» не эффективен.

Процесс «Установление контекста управления рисками» совершенствуется, ориентируясь на цели управления рисками, которые обеспечивают достижение целей организации. Процесс совершенствования не регламентирован. Улучшение процесса, связанное с новыми технологиями является возможным. Оценка направленности совершенствования процесса на непрерывное улучшение функционирования процесса на данном этапе реализовывается не в полном объеме.

Уровень 5.

Установление контекста управления в организации доведено до уровня лучших практик по управлению рисками. Выработанная стратегия управления рисками постоянно совершенствуется, ориентируясь на определенные цели управления рисками, которые обеспечивают достижение целей организации, и последние достижения в области технологий. Производится оценка направленности совершенствования процесса на непрерывное улучшение функционирования процесса «Установление контекста управления рисками».

Процесс «Установление контекста управления рисками» документирован и стандартизирован, определен перечень нормативных документов организации, осуществляется контроль за выполнением требований нормативных документов организации и внешних регулирующих и надзорных органов в области управления рисками.

Определены роли по управлению рисками, документирована ответственность и полномочия персонала, несущего ответственность за

осуществление процесса управления рисками. Персонал, осуществляющий процесс «Установление контекста управления рисками» компетентен.

Процесс «Установление контекста управления рисками» регламентирован и документально зафиксированы результаты выполнения процесса, формализована практика в области управления ИБ в виде процедур процесса «Установление контекста управления рисками». Установлены требования по осуществлению контроля над реализацией процесса «Установление контекста управления рисками». Разработан и документально зафиксирован план постоянного контроля за реализацией процесса «Установление контекста управления рисками».

Осуществляется оценка процесса «Установление контекста управления рисками» в организации. Методы для проведения оценки процесса «Установление контекста управления рисками» определены и документированы.

Процесс соответствует общепринятой практике, ресурсы и активы, необходимые для осуществления процесса «Установление контекста управления рисками» определены и доступны в полном объеме.

Разработаны меры, применяемые в случае, если процесс «Установление контекста управления рисками» не эффективен.

Оценка уровня зрелости рассмотренного процесса «Установление контекста управления рисками» СУИБ организации должна осуществляться на основе свидетельств выполненной деятельности по направлениям, соответствующим заявленному или ожидаемому уровню зрелости. В таблице А.1 приведен пример для оценки уровней зрелости по основным показателям оценки зрелости процессов управления ИБ для процесса «Установление контекста управления рисками».

Таблица А.1 – Оценка зрелости процесса «Установление контекста управления рисками».

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель	Уровни зрелости				
			1	2	3	4	5
К1	К _{1.1}	Существуют ли меры и (или) средства, используемые для управления ИБ?	100 %	100 %	100 %	100 %	100 %
	К _{1.2}	Достигают ли существующие меры и средства, используемые для управления ИБ, ожидаемого результата?	100 %	100 %	100 %	100 %	100 %
	К _{1.3}	Реализована ли деятельность по управлению ИБ в виде процессов?	100 %	100 %	100 %	100 %	100 %
К2	К _{2.1}	Организовано ли обучение принятым в Организации процессам управления ИБ и информируются ли сотрудники об этих процессах?	30%	100 %	100 %	100 %	100 %
	К _{2.2}	Достигает ли процесс управления ИБ ожидаемых результатов?	50%	100 %	100 %	100 %	100 %
	К _{2.3}	Определен ли перечень нормативных документов организации, регулирующих процесс управления ИБ?	40%	100 %	100 %	100 %	100 %
К3	К _{3.1}	Зафиксирован ли документально процесс управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.2}	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе управления ИБ?	-	30%	100 %	100 %	100 %
	К _{3.3}	Определены ли цели осуществления процесса управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.4}	Определены ли ответственность и полномочия по осуществлению процесса управления ИБ?	-	50%	100 %	100 %	100 %

Продолжение таблицы А.1

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель	Уровни зрелости				
			1	2	3	4	5
	К _{3.5}	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса управления ИБ?	-	50%	100 %	100 %	100 %
	К _{3.6}	Определен ли перечень результатов (выходов) процесса управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.7}	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса управления ИБ?	-	30%	100 %	100 %	100 %
	К _{3.8}	Установлены ли в организации требования по осуществлению контроля за реализацией процесса управления ИБ?	-	50%	100 %	100 %	100 %
	К _{3.9}	Осуществляется ли в организации оценка процесса управления ИБ?	-	50%	100 %	100 %	100 %
	К _{3.10}	Существует ли в организации контроль за исполнением требований нормативных документов организации в области ИБ?	-	70%	100 %	100 %	100 %
К4	К _{4.1}	Установлена ли (документально зафиксирована) в организации ответственность за процесс управления ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?	-	-	70%	100 %	100 %
	К _{4.2}	Доведены ли ответственность и полномочия по осуществлению процесса управления ИБ до сведения ответственных лиц в организации?	-	-	30%	100 %	100 %
	К _{4.3}	Компетентен ли персонал, осуществляющий процесс управления ИБ?	-	-	70%	100 %	100 %

Продолжение таблицы А.1

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель	Уровни зрелости				
			1	2	3	4	5
	К _{4.4}	Регламентирован ли в организации процесс управления ИБ?	-	-	70%	100 %	100 %
	К _{4.5}	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?	-	-	60%	100 %	100 %
	К _{4.6}	Соответствует ли процесс управления ИБ общепринятой практике?	-	-	70%	100 %	100 %
	К _{4.7}	Доступны ли ресурсы и активы, необходимые для осуществления процесса управления ИБ?	-	-	40%	100 %	100 %
	К _{4.8}	Определены ли соответствующие методы для проведения измерения (оценки) процесса управления ИБ?	-	-	40%	100 %	100 %
	К _{4.9}	Реализован ли постоянный контроль за реализацией процесса управления ИБ?	-	-	50%	100 %	100 %
	К _{4.10}	Существует ли возможность принятия мер в случае, если процесс управления ИБ неэффективен?	-	-	30%	100 %	100 %
К5	К _{5.1}	Осуществляется ли совершенствование процесса управления ИБ регламентированным образом?	-	-	-	50%	100 %
	К _{5.2}	Определяются ли цели улучшения процесса управления ИБ, которые обеспечивают достижение целей деятельности?	-	-	-	70%	100 %
	К _{5.3}	Определяются ли возможности улучшений процесса, связанные с новыми технологиями?	-	-	-	70%	100 %
	К _{5.4}	Оценивается ли направленность совершенствования процесса управления ИБ на непрерывное улучшение ИБ?	-	-	-	30%	100 %

ПРИЛОЖЕНИЕ Б

(справочное)

Модель зрелости процесса «Управление изменениями АС»

Уровень 1.

Деятельность по управлению изменениями АС определена в нормативных документах организации. В организации осуществляется идентификация и регистрация изменений АС, используемая для управления изменениями АС.

Установлены действия по предъявлению и изменению АС. Процесс «Управления изменениями АС» не всегда достигает ожидаемых результатов.

В организации определен перечень нормативных документов, регулирующих процесс «Управления изменениями АС».

Уровень 2.

В организации осуществляется реализация процесса «Управления изменениями АС», достигаются результаты процесса, а именно: учет всех принятых изменений АС. Установлены действия по предъявлению и изменению АС. Реализована деятельность в рамках процесса управления изменениями АС, осуществляется анализ и оценка последствий на ИБ, производится учет количества изменений.

Процесс «Управления изменениями АС» документирован и стандартизирован, суть процесса доводится до заинтересованных лиц. Не создана система регулярного информирования сотрудников об изменениях в процессе «Управления изменениями АС».

В организации определен и документально зафиксирован перечень нормативных документов, регулирующих процесс «Управления изменениями АС».

Определены цели осуществления процесса «Управления изменениями АС», также идентифицированы ресурсы и информация, необходимая для осуществления процесса. Определены ответственные лица, отвечающие за осуществление процесса. Не определены полномочия лиц, несущих ответственность за осуществление процесса «Управления изменениями АС».

Требования по осуществлению контроля соответствия изменения АС установлены не в полном объеме. Нет документальной фиксации процесса.

Уровень 3.

В организации определены и документально зафиксированы цель и перечень результатов осуществления процесса «Управления изменениями АС». Осуществляется идентификация и регистрация изменений АС, анализ и оценка последствий на ИБ, производится учет количества изменений и их хронология. Процесс «Управления изменениями АС» регламентирован.

В организации документирован перечень нормативных документов, регулирующих процесс управления изменениями АС. Осуществляется и документально фиксируется контроль за исполнением требований нормативных документов организации, нормативных требований внешних регулирующих и надзорных организаций в области ИБ.

Сотрудники систематически информируются об изменениях в процессе «Управления изменениями АС». В организации распределены и документально зафиксированы роли по обеспечению ИБ процесса управления изменениями АС, назначены исполнители указанных ролей. Определены ответственность и полномочия лиц, осуществляющих процесс «Управления изменениями АС». Персонал, осуществляющий процесс управления изменениями АС, компетентный.

Осуществляется формализация практики в области управления АС в виде процедур процесса «Управления изменениями АС». Установлены и документально зафиксированы требования по осуществлению контроля соответствия изменения АС требованиям ИБ. Контроль за реализацией процесса «Управления изменениями АС» осуществляется не регулярно, нет разработанного плана постоянного контроля.

Процесс «Управления изменениями АС» соответствует общепринятой практике, ресурсы и активы, необходимые для осуществления процесса управления доступны частично.

В организации неперiodически осуществляется оценка процесса «Управления изменениями АС», но не определены методы для проведения оценки процесса «Управления изменениями АС».

Уровень 4.

В организации осуществляется полная реализация процесса, определена цель и перечень результатов осуществления процесса. Процесс «Управления изменениями АС» документирован и стандартизирован, определен перечень нормативных документов, осуществляется контроль за исполнением требований нормативных документов организации, нормативных требований внешних регулирующих и надзорных организаций в области ИБ.

Процесс «Управления изменениями АС» регламентирован и соответствует общепринятой практике. Ресурсы и активы, необходимые для осуществления процесса управления доступны в полном объеме. Документально зафиксированы результаты выполнения процесса «Управления изменениями АС» Формализована практика в области управления ИБ в виде процедур процесса «Управления изменениями АС».

Установлены и документированы требования по осуществлению контроля соответствия изменения АС. Разработан план постоянного контроля за реализацией процесса «Управления изменениями АС».

В организации определены и документированы методы для проведения оценки процесса «Управления изменениями АС». Осуществляется оценка процесса.

Назначены и документально зафиксированы роли по управлению изменениями АС. Документирован ответственный персонал, определены полномочия лиц, несущих ответственность за осуществление процесса «Управления изменениями АС». Сведения относительно ответственности и полномочий по осуществлению процесса «Управления изменениями АС»

доведены до ответственных лиц. Персонал, осуществляющий процесс управления изменениями АС, компетентный.

Разработаны меры, применяемые в случае, если процесс управления рисками не эффективен.

Разрабатывается план совершенствования процесса «Управления изменениями АС». Процесс совершенствования не регламентирован. В организации определены цели совершенствования процесса, которые обеспечивают достижение целей деятельности организации. Улучшения процесса, связанное с новыми технологиями является возможным. Оценка направленности совершенствования процесса на непрерывное улучшение функционирования процесса на данном этапе реализуется не в полном объеме.

Уровень 5.

Управление изменениями АС в организации доведено до уровня лучших практик по контролю соответствия изменений АС требованиям ИБ. Выработанная стратегия управления изменениями АС постоянно совершенствуется, ориентируясь на определенные цели и новые технологии. Производится оценка направленности совершенствования процесса «Управления изменениями АС» на непрерывное улучшение функционирования процесса.

Процесс «Управления изменениями АС» документирован и стандартизирован, определен перечень нормативных документов, осуществляется контроль за исполнением требований нормативных документов организации, нормативных требований внешних регулирующих и надзорных организаций в области ИБ.

Определены роли по управлению изменениями АС. Документирована ответственность и полномочия персонала, несущего ответственность за осуществление процесса «Управления изменениями АС». Персонал, осуществляющий процесс управления изменениями АС, компетентный.

Осуществляется систематическое информирование уполномоченных лиц об изменениях процесса «Управления изменениями АС».

Процесс «Управления изменениями АС» регламентирован и соответствует общепринятой практике. Ресурсы и активы, необходимые для осуществления процесса управления доступны в полном объеме. Документально зафиксированы результаты выполнения процесса «Управления изменениями АС» Формализована практика в области управления ИБ в виде процедур процесса «Управления изменениями АС».

Установлены требования по осуществлению контроля соответствия изменения АС. Разработан и документально зафиксирован план постоянного контроля за реализацией процесса «Управления изменениями АС».

Разработаны меры, применяемые в случае, если процесс управления рисками не эффективен.

В организации определены и документированы методы для проведения оценки процесса «Управления изменениями АС». Осуществляется оценка процесса.

Оценка уровня зрелости рассмотренного процесса «Управления изменениями АС» СУИБ организации должна осуществляться на основе свидетельств выполненной деятельности по направлениям, соответствующим заявленному или ожидаемому уровню зрелости. В таблице Б.1 приведен пример для оценки уровней зрелости по основным показателям оценки зрелости процессов управления ИБ для процесса «Управления изменениями АС».

Таблица Б.1 – Оценка зрелости процесса «Управление изменениями АС».

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель	Уровни зрелости				
			1	2	3	4	5
К1	К _{1.1}	Существуют ли меры и (или) средства, используемые для управления ИБ?	100 %	100 %	100 %	100 %	100 %
	К _{1.2}	Достигают ли существующие меры и средства, используемые для управления ИБ, ожидаемого результата?	100 %	100 %	100 %	100 %	100 %
	К _{1.3}	Реализована ли деятельность по управлению ИБ в виде процессов?	100 %	100 %	100 %	100 %	100 %
К2	К _{2.1}	Организовано ли обучение принятым в Организации процессам управления ИБ и информируются ли сотрудники об этих процессах?	30%	100 %	100 %	100 %	100 %
	К _{2.2}	Достигает ли процесс управления ИБ ожидаемых результатов?	70%	100 %	100 %	100 %	100 %
	К _{2.3}	Определен ли перечень нормативных документов организации, регулирующих процесс управления ИБ?	70%	100 %	100 %	100 %	100 %
К3	К _{3.1}	Зафиксирован ли документально процесс управления ИБ?	-	30%	100 %	100 %	100 %
	К _{3.2}	Регламентирован ли в организации подход к обучению и информированию о реализованном процессе управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.3}	Определены ли цели осуществления процесса управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.4}	Определены ли ответственность и полномочия по осуществлению процесса управления ИБ?	-	50%	100 %	100 %	100 %
	К _{3.5}	Идентифицированы ли ресурсы и информация, необходимая для осуществления процесса управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.6}	Определен ли перечень результатов (выходов) процесса управления ИБ?	-	70%	100 %	100 %	100 %

Продолжение таблицы Б.1

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель	Уровни зрелости				
			1	2	3	4	5
	К _{3.7}	Формализована ли существующая в организации практика в области управления ИБ в виде процедур процесса управления ИБ?	-	40%	100 %	100 %	100 %
	К _{3.8}	Установлены ли в организации требования по осуществлению контроля за реализацией процесса управления ИБ?	-	70%	100 %	100 %	100 %
	К _{3.9}	Осуществляется ли в организации оценка процесса управления ИБ?	-	50%	100 %	100 %	100 %
	К _{3.10}	Существует ли в организации контроль за исполнением требований нормативных документов организации в области ИБ?	-	70%	100 %	100 %	100 %
К4	К _{4.1}	Установлена ли (документально зафиксирована) в организации ответственность за процесс управления ИБ (распределены роли по обеспечению ИБ, назначены исполнители ролей и т.п.)?	-	-	70%	100 %	100 %
	К _{4.2}	Доведены ли ответственность и полномочия по осуществлению процесса управления ИБ до сведения ответственных лиц в организации?	-	-	30%	100 %	100 %
	К _{4.3}	Компетентен ли персонал, осуществляющий процесс управления ИБ?	-	-	70%	100 %	100 %
	К _{4.4}	Регламентирован ли в организации процесс управления ИБ?	-	-	70%	100 %	100 %
	К _{4.5}	Существует ли в организации контроль за исполнением требований всех нормативных документов организации и нормативных документов внешних регулирующих и надзорных органов в области ИБ?	-	-	70%	100 %	100 %

Продолжение таблицы Б.1

Обозначение комплексного показателя	Обозначение основного показателя	Основной показатель	Уровни зрелости				
			1	2	3	4	5
	K _{4.6}	Соответствует ли процесс управления ИБ общепринятой практике?	-	-	70%	100 %	100 %
	K _{4.7}	Доступны ли ресурсы и активы, необходимые для осуществления процесса управления ИБ?	-	-	40%	100 %	100 %
	K _{4.8}	Определены ли соответствующие методы для проведения измерения (оценки) процесса управления ИБ?	-	-	30%	100 %	100 %
	K _{4.9}	Реализован ли постоянный контроль за реализацией процесса управления ИБ?	-	-	70%	100 %	100 %
	K _{4.10}	Существует ли возможность принятия мер в случае, если процесс управления ИБ неэффективен?	-	-	60%	100 %	100 %
K5	K _{5.1}	Осуществляется ли совершенствование процесса управления ИБ регламентированным образом?	-	-	-	30%	100 %
	K _{5.2}	Определяются ли цели улучшения процесса управления ИБ, которые обеспечивают достижение целей деятельности?	-	-	-	70%	100 %
	K _{5.3}	Определяются ли возможности улучшений процесса, связанные с новыми технологиями?	-	-	-	30%	100 %
	K _{5.4}	Оценивается ли направленность совершенствования процесса управления ИБ на непрерывное улучшение ИБ?	-	-	-	50%	100 %

МИНОБРАЗОВАНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«ПЕТЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056.5

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники
Выпускающая кафедра:
Информационная безопасность систем
и технологий
Учебная группа ППИ

УТВЕРЖДАЮ
Зав. кафедрой ИИСТ
к.т.н., доцент  С.Л. Зефирова
«27» 04 2016 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ
РАБОТУ

студента группы ППИ Палагиной Елены Алексеевны

Специальность 100503 – Информационная безопасность
автоматизированных систем

Тема дипломного проекта: Оценка зрелости процессов управления
информационной безопасностью.

Руководитель ВКР

к.т.н., доцент, зав. кафедрой ИИСТ

 Зефирова Сергей Львович

Нормоконтролер

к.т.н., доцент

 Фатеев А.Г.

1 Цели и задачи ВКР

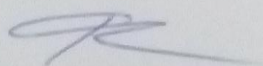
Цели работы: разработка методики оценки зрелости процессов управления информационной безопасностью (ИБ) организации.

Методика предназначена для оценки ИБ организации.

2 Тактико-технические требования к выполнению ВКР

Технические требования:

- объектом оценки должны быть процессы управления ИБ организации, представляющие в совокупности систему управления ИБ (СУИБ) организации;
- должны быть описаны процессы планирования, реализации и поддержки, проверки, совершенствования СУИБ в контексте их целей, реализации и результатов;
- должна быть определены и описаны уровни зрелости процессов управления ИБ;
- должна быть разработана структура показателей оценки зрелости процессов управления ИБ;
- должны быть разработаны показатели оценки зрелости процессов управления ИБ;
- должен быть разработан способ оценивания показателей оценки зрелости процессов управления ИБ;
- должны быть разработаны правила формирования общей оценки зрелости процессов управления ИБ организации;
- должны быть разработаны правила проведения оценки зрелости процессов управления ИБ и определены виды свидетельств оценки для показателей оценки зрелости процессов управления ИБ.



В ВКР должны быть рассмотрены следующие вопросы:

- описание процессов управления ИБ;
- описание уровней зрелости процессов управления ИБ;
- разработка структуры показателей оценки и описания их содержания;
- способ оценивания показателей;
- правила формирования общей оценки зрелости процессов управления ИБ.

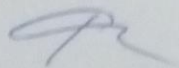
3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- процессы управления ИБ организации - 1 л., ф. А1 (плакат);
- уровни зрелости процессов управления ИБ организации - 2 л., ф. А1 (плакат);
- структура показателей оценки зрелости процессов управления ИБ – 1 л., ф. А1 (плакат);
- способ оценивания показателей оценки зрелости управления ИБ – 1 л., ф. А1 (плакат);
- формирование общей оценки зрелости процессов управления ИБ – 1 л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.



4 Сроки выполнения ВКР

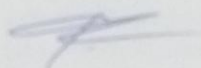
Тема утверждена приказом ректора ИГУ № 491 от «25» 04 2016 г.

Дата выдачи задания «13» марта 2016 г.

Время дипломного проектирования с «18» апреля 2016 г.
по «10» июля 2016 г.

Задание к исполнению принял «13» марта 2016 г.

Исполнитель ВКР Палагина Е.А. Палагина Е.А.



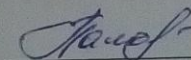
Ректору Пензенского
государственного университета
А. Д. Гулякову
студентки 5 курса ФПИТЭ
очной формы обучения
Палагиной Елены Алексеевны

заявление.

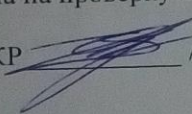
Я, Палагина Елена Алексеевна, студентка 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломного проекта на тему «Оценка зрелости процессов управления информационной безопасности», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлена с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 /Е.А. Палагина/
20.06.2016

ВКР представлена на проверку 20.06.2016.

Руководитель ВКР  /С.Л. Зефирова/

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Оценка зрелости процессов управления информационной безопасностью» студентки 5 курса Е.А. Палагиной специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР к.т.н, доцент, зав. кафедрой ИБСТ Зефилов Сергей Львович.

Отчет о проверке № 1

ФИО: Иванов Алексей Петрович
дата отправки: 20.06.2016 19:15:21
пользователь: [user@antiplagiat.ru](#) / ID: 1267388
отчет предоставлен сервисом «Антиплагиат»
на сайте [http://www.antiplagiat.ru](#)

Информация о документе

№ документа: 47
Имя исходного файла: ВКР_Палагина_ЕА_11014.doc
Размер текста: 454 кБ
Тип документа: Не указано
Символов и знаков: 73278
Слов и текстов: 6312
Число предложений: 433

Информация об отчете

Дата: Отчет от 20.06.2016 19:15:22 • Последний готовый отчет
Комментарий: не указан
Оценка оригинальности: 90,86%
Занимательность: 9,14%
Цитирование: 0%



Оригинальность: 90,86%
Занимательность: 9,14%
Цитирование: 0%

21.06.2016 г.

Секретарь ГЭК

С.Л. Зефилов

А.П.Иванов

ОТЗЫВ
на выпускную квалификационную работу
Палагиной Елены Алексеевны

Тема выпускной квалификационной работы: «Оценка зрелости процессов управления информационной безопасностью».

Для улучшения информационной безопасности (ИБ), для достижения целей защищённости информационной сферы организации необходимо проверять и оценивать информационную безопасность. Известно несколько способов оценки ИБ: оценка ИБ по эталону, оценка по экономическим показателям и рискориентированная оценка ИБ.

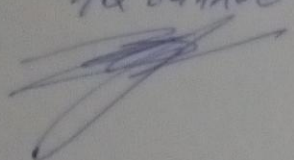
Оценка ИБ по эталону предполагает формирование идеальных, правильных компонентов, обеспечивающих ИБ, с которыми сравниваются реальные компоненты (защитные меры или процессы управления ИБ). При оценке ИБ по наличию определённого (эталонного) набора защитных мер можно оценить только текущее состояние защищённости. Оценка процессов управления ИБ позволяет определить возможности процессов, их способность поддерживать достижение целей ИБ, т.е. зрелость процессов. Оценка зрелости процессов управления ИБ является универсальной оценкой и может использоваться для любой организации, любого объекта или системы.

Таким образом, тема ВКР Палагиной Е.А., посвящённая оценке зрелости процессов управления ИБ, является актуальной.

В работе определены и описаны процессы управления ИБ организации, разработаны уровни зрелости процессов управления ИБ, структура показателей оценки и их содержание, способ оценивания показателей и формирование оценки системы управления ИБ. Кроме того разработаны модели зрелости для двух процессов управления ИБ: «установление контекста управления рисками» и «управление изменениями автоматизированных систем».

Требования технического задания ВКР полностью выполнены.

ВКР Палагиной Е.А. выполнена в соответствии с требованиями, предъявляемым к ВКР по специальности 100503, и может быть представлена к защите в ГЭК.

12.09.10


Руководитель ВКР



С.Л.Зефиров

Рецензия
на дипломный проект студента 5 курса
Пензенского государственного университета
Палагиной Елены Алексеевны на тему:
Методика анализа уязвимостей программного обеспечения
Специальность 100503

Дипломный проект Палагиной Е.А. посвящен разработке методики оценки зрелости процессов управления информационной безопасностью.

ВКР выполнена в полном соответствии перечню пунктов технического задания, пояснительная записка обладает должной структурой и содержанием.

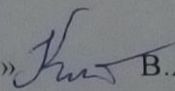
В результате выполнения ВКР Палагиной Е.А. был предложен подход к оценке зрелости процесса управления информационной безопасностью. Используемые в подходе методы оценки применяются в соответствии с международным стандартом ИСО/МЭК 15504-3:2004, что подтверждает практическую значимость ВКР.

К недостаткам ВКР следует отнести то, что предложенная методика не была апробирована на практике.

Несмотря на указанный недостаток считаю, что рецензируемая ВКР может быть допущена к защите в ГАК, а Палагина Е.А. заслуживает оценки «хорошо».

С учетом актуальности темы, трудоемкости и сложности выполнения данную ВКР оцениваю в 7 баллов.

Рецензент,

инженер второй категории ПФ ФГУП «НТЦ «Атлас»  В.А.Клейменов

