(точное число). Производить оценку запросов на изменение могут зарегистрированные участники команды, прикрепленные к данному проекту. Параметры критериев для оценки должны быть приведены к единой шкале оценки, чтобы сформировать матрицу ответов, по мнению каждого участника «эксперта». На основе экспертной оценки будут выбраны итоговые бальные значения каждого критерия (измеряемые по пятибалльной шкале). Каждый критерий следует помножить на вес критерия, после чего сложить их произведения друг с другом. Полученное число будет являться рейтингом критерия. Запрос, имеющий наибольший рейтинг критерия, будет являться предпочтительным для работы [4].

Утверждение изменений, формирование планов обновлений, координация реализации изменения и завершение изменения. К работе принимаются те изменения, которые имеют наибольший рейтинг в результате экспертной оценки. Используя сортировку по количеству необходимых для реализации дней, а также по затрачиваемым ресурсам и пользуясь фильтром «истекает срок давности» менеджер проекта может строить планы по текущим изменениям. На этапе координации реализации изменения реализуются программистами с одной стороны, и тестируются, с другой стороны. При успешной реализации RFC возле задания следует нажать кнопку «Завершено», после чего заранее подготовленный текст будет направлен заказчику данного пожелания по email.

Заключение. Основным результатом работы становится проект систему управления изменениями программного продукта. В проекте были учтены основные аспекты управления изменениями в соответствии с библиотекой ITIL. При соблюдении всех обозначенных тезисов разработанный ПП устранит большинство имеющихся подходов по управлению изменению: исключится дублирование информации за счет обязательного этапа проверки RFC; будут реализованы напоминания о «поджимающих» сроках реализации RFC; за счет отправки сообщения заказчику о завершении реализации его RFC будет налажена обратная связь; благодаря разработанной методики оценки RFC будет сформирован рейтинг всех запросов на изменения. Основными преимуществами разработанного ПП станет: удобство в использовании, отсутствие избыточности функционала, возможность выбирать приоритетные задачи для изменения ПП.

Литература.

1. Бараксанов, Д.Н. Математическое и программное обеспечение поддержки принятия решений при продвижении программного продукта на корпоративный рынок: дис. на соискание ученой степени канд. тех. наук: 05.13.10 / Бараксанов Дмитрий Николаевич. – Томск, 2016. – 186 с.
2. ITIL [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/ITIL, свободный (дата обращения: 16.10.2016).
3. Свободный ITIL [Электронный ресурс]. – Режим доступа: http://wikiitil.ru/itilrus.html, свободный (дата обращения: 16.10.2016).
4. Силич, М.П. Основы теории систем и системного анализа: учеб. пособие / М.П. Силич, В.А. Силич. – Томск: Изд-во Томск. гос. ун-та систем управления и радиоэлектроники, 2013. – 340 с.

СИСТЕМА КРИТЕРИЕВ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.К. Курманбай, студенка гр. 17В41
Научный руководитель: Разумников С.В.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E–mail:aigera_0796@mail.ru

Проблема обеспечения информационной безопасности (ИБ) современных автоматизированных и информационных систем является одной из самых важных. Сложность этих систем, разветвленность составляющих их основу компьютерных сетей еще больше усугубляют ситуацию. Под информационной безопасностью в ИС и ИТ понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Учитывая жесткие универсальные шкалы классов безопасности и обеспечении гибкости в подходе к оценке безопасности различных систем ИТ, была разработана система критериев информационной безопасности на основе изучения открытых источников информации так же изучения существующих других систем критериев. Таких как:

- "Гармонизированные критерий европейских стран"
- "Канадские критерии оценки безопасности компьютерных продуктов"
- Федеральных критериях безопасности информационных технологий" США

Данные критерии обобщили содержание и опыт использования различных книг и ее интерпретаций, развили оценочные уровни доверия Европейских критериев, воплотили в реальные структуры концепцию типовых профилей защиты Федеральных критериев США [1].

Предлагается система критериев и показателей для оценки ИБ ИС, которая представлена в таблице 1. В данной системе проведена классификация широкого набора функциональных требований и требований доверия к безопасности, определены способы их группирования и принципы использования [2]. Так же в оценке информационной безопасности информационных систем и технологии были учтены и количественные показатели: временные затраты на установление средств защиты и стоимость реализации обеспечения безопасности.

Таблица 1

Система критериев оценки ИБ

Название показателя ИБ	Роль показателя в оценке
1. Конфиденциальность (К)	
Анонимность пользователей (анонимность сеансов работы с системой) (Ап)	Процесс защиты идентификатора и данных
Защита от мониторинга сеансов работы с системой (Змср)	Процесс защиты системы
Использование псевдонимов (Ип)	Вымышленное имя, используемое для деятельности вместо настоящего (данного при рождении, зафиксированного в официальных документах);
2. Аудит (А)	
Анализ протокола аудита (Апа)	Систематический, независимый и документированный процесс получения свидетельств в форме наблюдений и их объективной оценки с целью определения степени выполнения требований ISO 9001:2008, государственных регламентов, внутренних стандартов предприятия, а также с целью оценки эффективности работы подразделения.
Доступ к протоколу аудита (Дпа)	Доступность протокола
Регистрация и учет событий (Рус)	Подтверждение факта передачи информации по требованию; автоматическое подтверждение факта передачи информации; подразумевает использование как стандартных средств операционных систем, так и специальных средств учета событий безопасности
3. **Управление безопасностью (Уб)**	
Управление средствами защиты (Усз)	Контроль и управление
Управление параметрами и конфигурацией средств защиты (Упксз)	Настройки средств защиты информации
Административные роли (Ар)	Роль администратора
Ограничение времени действия атрибутов безопасности (Овдаб)	Временные ограничения в использовании некоторых свойств системы
Управление атрибутами безопасности (Уаб)	Управление свойствами системы
4. **Защита(З)**	
Политика управления доступом (Пуд)	Определяет правила и методы защиты информационной системы
Импорт информации (Ии)	Перенос информации с одной среды в другую
Целостность внутрисистемной передачи информации при использовании внешних каналов (Цвпи)	Целостность информации состояние информации, при котором отсутствует любое ее изменение: либо изменение осуществляется; только преднамеренно субъектами, имеющими на него право
Средства управления доступом (Суд)	Совокупность программных и технических средств

Название показателя ИБ	Роль показателя в оценке
5. Идентификация и аутентификация	
Реакция на неудачные попытки аутентификации (Рнпа)	Действия при неудачных попытках
Атрибуты безопасности пользователей (Абп)	Свойства безопасности для пользователей
Аутентификация пользователей (Ауп)	Процедура проверки подлинности, например, проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей
6. Реализуемость (Р)	
Стоимость реализации обеспечения безопасности (Ср)	Денежные средства необходимые для обеспечения безопасности
Временные затраты на установление средств защиты (Вз)	Время необходимое для установки средств защиты

Основным отличием данной системы критериев в оценке информационной безопасности является непосредственно: систематизация и классификация требований по иерархии "критерий" – "показатель" с уникальными идентификаторами требований, что обеспечивает удобство использования. Так же открытость для последующего наращивания совокупности требований. Данная система является наиболее полной совокупностью требований безопасности информационных систем и технологий [3].

Положения системы критериев имеют достаточно общий характер и не ограничиваются только собственно областью проблем безопасности ИТ, к которым применимы системы критериев.

В данной работе будет использоваться «5–ти» бальная шкала для оценки информационной безопасности. При определении данной шкалы было выделено пять уровней ИБ (таблица 2).

Таблица 2

Шкала оценки критериев

Баллы	Описание назначение балла
1	Полное невыполнение требований безопасности согласно стандарту
2	Частичное выполнение требований безопасности согласно стандарту
3	Частичное невыполнение требований безопасности согласно стандарту
4	Соответствие требованиям ИБ по стандарту ISO
5	Превосходит необходимые стандарты

Экспертами будет оценены предложные информационные системы с использованием данной 5–ти бальной шкалы.

Если информационная система соответствует определенному выбранному критерию, то экспертом назначается оценка «4», если не соответствует, то он рассматривает на сколько идет несоответствие и выставляет оценку «2» или «1» ссылаясь на свою знания и опыт. Система признается приемлемой и допустимой, если экспертом будет присвоен балл «4» или «5». В случае, когда экспертом присевается оценка «3» то учитывается совокупность баллов по всем показателям и критериям [4, 5].

Литература.

1. Официальный сайт www.riskwatch.com Электронный ресурс: Режим доступа http://www.riskwatch.com/ Дата обращения: 10.05.2016г.
2. Разумников С.В. Интегральная модель оценки эффективности и рисков облачных ИТ-сервисов для внедрения на предприятии // Фундаментальные исследования. - 2015 - №. 2-24. - С. 5362-5366.
3. Разумников С.В. Анализ возможности применения методов Octave, RiskWatch, Cramm для оценки рисков ИТ для облачных сервисов //Современные проблемы науки и образования. -2014 -№ 1. -С. 1. -Режим доступа: http://www.science-education.ru/115-12197.
4. Разумников С.В. Использование метода линейного программирования для оценки эффективности применения облачных ИТ-сервисов // Приволжский научный вестник. - 2013 - №. 7(23). - С. 43-45.