УДК 004

ПРОГРАММНЫЙ ПРОДУКТ ОЦЕНКИ РИСКА И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ РАЗРАБОТАННОЙ ИНТЕГРАЛЬНОЙ МОДЕЛИ РИСКА И ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ ПРИ ВНЕДРЕНИИ ИС

Курманбай А.К., студенка гр. 17В41
Научный руководитель: Разумников С.В.
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
г Юрга

Цель разработки данной информационной системы – оценка информационной безопасности ИС при внедрении ИТ.

Система призвана упростить и усовершенствовать процесс оценки ИБ при внедрении ИТ, также призвана помочь в снижении возможных рисков, связанных с ИБ, и полностью автоматизировать процесс оценки ИТ. В ходе этого была разработана интегральная модель оценки риска и информационной безопасности ИС и ИТ, на основе разработанной системы критериев (табл. 1).

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 эф-

Название показателя ИБ	Роль показателя в оценке
	фективности 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
5. Идентификация и аутентификация	
Реакция на неудачные попытки аутентификации (Рнпа)	Действия при неудачных попытках
Атрибуты безопасности пользователей (Абп)	Свойства безопасности для пользователей

Название показателя ИБ	**Роль показателя в оценке**
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

Где интегральный показатель вычисляется по формуле 1.

$$П_{ИБ} = \sum_{i=1}^{n} Kr_i \cdot v_1 \quad , \qquad (1)$$

где, $И_{ИБ}$ – интегральный показатель;

Kr – критерии;

v_1 – коэффициенты весомости.

Распишем формулу подробнее (1а)

$$И_{ИБ} = v_1 \cdot К + v_2 \cdot А + v_3 \cdot Уб + v_4 \cdot З + v_5 \cdot И + v_6 \cdot Р \quad , \qquad (1а)$$

где, $И_{ИБ}$ – интегральный показатель;

К – Критерий «Конфиденциальность»;

А – Критерий «Аудит»;

Уб – Критерий «Управление безопасностью»;

З – Критерий «Защита»;

И – Критерий «Идентификация и аутентификация»;

Р – Критерий «Реализуемость».

v_1, v_2, v_3, v_4, v_5, v_6 – коэффициенты весомости критерия интегрального показателя информационной безопасности.

Критерий «Конфиденциальность» вычисляется по формуле 2.

$$К = v_{11} \cdot Ап + v_{12} \cdot Змср + v_{13} \cdot Ип \quad , \qquad (2)$$

где Ап – Анонимность пользователей (анонимность сеансов работы с системой);

Змср – Защита от мониторинга сеансов работы с системой;

Ип – Использование псевдонимов;

$v_{11}; v_{12}; v_{13};$ – коэффициенты весомости критерия «Конфиденциальность».

Критерий «Аудит» вычисляется по формуле 3.

$$А = v_{21} \cdot Апа + v_{22} \cdot Дпа + v_{23} \cdot Рус \quad , \qquad (3)$$

где Апа – анонимность протокола аудита;

Дпа – доступ к протоколу аудита;

Рус – регистрация и учет;

v_{21}; v_{22}; v_{23}; – коэффициенты весомости критерия «Аудит».

Критерий «Управление безопасности» вычисляется по формуле 4.

$$Уб = Усз \cdot v_{31} + Упксз \cdot v_{32} + Ар \cdot v_{33} + Овдаб \cdot v_{34} + Уаб \cdot v_{35} \quad (4)$$

где Усз – управление средствами защиты;

Упксз – управление параметрами и конфигурацией средств защиты;

Ар – административные роли;

Овдаб – ограничение времени действия атрибутов безопасности;

Уаб – управление атрибутами безопасности;

$v_{31}; v_{32}; v_{33}; v_{34}; v_{35}$; – коэффициенты весомости критерия «Управление безопасности».

Критерий «Защита» вычисляется по формуле 5.

$$З = Пуд \cdot v_{41} + Ии \cdot v_{42} + Цвпи \cdot v_{43} + Суд \cdot v_{44} \quad (5)$$

где Пуд – политика управления доступом;

Ии – импорт информации;

Цвпи – целостность внутрисистемной передачи информации при использовании внешних каналов;

Суд – средства управления доступом;

$v_{41}; v_{42}; v_{43}; v_{44}$ – коэффициенты весомости критерия «Защита».

Критерий «Идентификация и аутентификация» вычисляется по фор. 6.

$$И = Рнпа \cdot v_{51} + Абп \cdot v_{52} + Ауп \cdot v_{53} \quad (6)$$

где Рнпа – Реакция на неудачные попытки аутентификации;

Абп – Атрибуты безопасности пользователей;

Ауп – Аутентификация пользователей;

$v_{51}; v_{52}; v_{53}$ – коэффициенты весомости критерия «Идентификация и аутентификация».

Критерий «Реализуемость» вычисляется по формуле 6.

$$Р = Ср \cdot v_{61} + Вз \cdot v_{62} \quad (7)$$

где, Ср – стоимость реализации обеспечения безопасности;

Вз – временные затраты на установление средств защиты;

$v_{61}; v_{62}$; – коэффициенты весомости критерия «Ресурсный критерий».

Разработанная интегральная модель будет использована в основе программного обеспечения по автоматизации оценка риска и информационной безопасности.

Список литературы:

1. ГОСТ Р 55368 – 2012/ ISO/IEC Guide 28:2004 Оценка соответствия. Методические указания по системе сертификации продукции третьей стороной.

2. Разумников С.В., Фисоченко О.Н., Лунегов В.Ю. Информационная система оценки возможности корпоративных ИТ-приложений для миграции в облачную среду [Электронный ресурс] // Современные проблемы науки и образования. - 2014 - №. 4. - С. 1. - Режим доступа: http://www.science-education.ru/118-13924.

3. Разумников С.В. Использование метода линейного программирования для оценки эффективности применения облачных ИТ-сервисов // Приволжский научный вестник. - 2013- №. 7(23). - С. 43-45.

4. Малюк А.А. Теория защиты информации. – М.:Горячая линия – Телеком, 2012. – 184 с. – ISBN 978–5–9912–0246–6.

5. Османов А. А., Юдин Д. Е., Тринкин М. Г., Науменко В. В. Анализ проблем обеспечения информационной безопасности электронной коммерции [Текст] // Технические науки: проблемы и перспективы: материалы III междунар. науч. конф. (г. Санкт–Петербург, июль 2015 г.). – СПб.: Свое издательство, 2015. – С. 99–101.