V.S. Oladko[1], A.A Belozerova[2]
[1]Federal state educational budget institution of higher professional education "Financial University under the Government of the Russian Federation", 125499, Moscow, Kronstadt Blvd., 37B,
e-mail: oladko.vs@yandex.ru, ORCID iD is 0000-0003-0500-8928
[2] Volgograd State University, 400062, Volgograd, PR-t Universitetsky, 100,
e-mail: angel_cute_14@mail.ru, ORCID iD is 0000-0003-0387-4152

The model for risk assessment ERP-systems information security

Keywords: risk, threat, protection mechanisms
The article deals with the problem assessment of information security risks in the ERP-system. ERP-system functions and architecture are studied. The model malicious impacts on levels of ERP-system architecture are composed. Model-based risk assessment, which is the quantitative and qualitative approach to risk assessment, built on the partial unification 3 methods for studying the risks of information security - security models with full overlapping technique CRAMM and FRAP techniques developed.

В.С. Оладько[1], А.А. Белозерова[2]
[1]Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации» Колледж информатики и программирования,125499, Москва, Кронштадтский б-р, 37б,
e-mail: oladko.vs@yandex.ru, ORCID iD is 0000-0003-0500-8928
[2]Федеральное государственное автономное образовательное учреждение высшего образования «Волгоградский государственный университет», Россия, 400062, Волгоград , Университетский проспект, 100,
e-mail: angel_cute_14@mail.ru, ORCID iD is 0000-0003-0387-4152

МОДЕЛЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ERP–СИСТЕМ

Ключевые слова: риск, угроза, механизмы защиты
Статья посвящена проблеме оценки рисков информационной безопасности ERP –системы. Исследованы функции и архитектура ERP-системы. Составлена модель злоумышленных воздействий на уровни архитектуры ERP-системы. Разработана модель оценки рисков в основе, которой лежит количественно-качественный подход к оценке рисков, построенный на частичном объединении 3 методик исследования рисков ИБ - модели безопасности с полным перекрытием, методики CRAMM и методики FRAP.

Введение

На сегодняшний день одним из основных условий стабильного функционирования предприятия на рынке становится совершенствование процедур организационно-экономического управления. В частности, использование и разработка эффективных систем управления данными, информационными потоками и бизнес-процессами. Часто в качестве подобных средств управления и планирования ресурсов используют ERP - системы (Enterprise Resource Planning), данные системы предоставляют возможность работать на интегрированном информационном поле множеству удаленных пользователей, что обеспечивает максимальный эффект при управлении крупными производствами и корпорациями. При этом в ERP-системе, как в центральной информационной системе предприятия, сосредоточено большое количество конфиденциальной информации и данных ограниченного доступа. Например, персональные данные сотрудников и клиентов предприятия, финансовая информация, коммерческая тайна, оперативная и служебная

информация. Раскрытие такой информации или нарушение доступности и целостности в результате различного рода инцидентов информационной безопасности (ИБ) может принести предприятию значительный ущерб, выраженный как в материальной так и не материальной форме. Поэтому проблемы обеспечения ИБ и контроля рисков актуальны для ERP-систем.

Проблемы информационной безопасности ERP-системы

Анализ источников [1,2] показывает, что возможности ERP- системы можно разделить на функциональные и технологические. Основными функциями ERP-системы являются: планирование ресурсов; ведение конструкторских и технологических спецификаций; оперативное управление финансами, включая составление финансового плана, финансовый и управленческий учёт; управление запасами и закупками и др. Таким образом, в ERP-системе, сосредоточено большое количество информации, необходимой для повседневной деятельности сотрудников: данные о клиентах, кадровые данные, финансовая информация, платежные данные и реквизиты, коммерческая тайна, и т. д. Именно поэтому ERP-системы представляют интерес для злоумышленников с точки зрения злонамеренного воздействия.

Анализ [1,3] показывает, что технологически ERP-системы обладают сложной архитектурой, объединяющей в себе различные технологии, такие как серверы приложений, базы данных, межплатформенное программное обеспечение, веб-сервер, операционные системы, системы управления идентификаторами и пр. В обобщённом виде типовая ERP-система состоит из трех уровней компонентов, связанных через клиент-серверную архитектуру: уровень базы данных (БД); уровень приложений; уровень представления (пользовательский). Подобная трехуровневая клиент-серверная архитектура может расширяться в многоуровневую систему. При этом добавляются компоненты для работы с глобальными сетями. С учетом уровней архитектуры ERP-системы можно составить следующую модель злоумышленных воздействий на ее структурные компоненты и данные (см. таблицу 1).

Таблица 1 - Модель воздействий злоумышленника на уровни архитектуры ERP-системы

Уровень архитектуры	Угрозы	Последствия
Сетевой уровень	− возможность перехвата и модификации трафика; − эксплуатация уязвимостей сетевых протоколов, шифрования или аутентификации; − сканирование сети; − DDos и Dos-атаки; − подмена трафика;	− нарушение конфиденциальности информации и ее утечка; − нарушение доступности данных, сервисов и служб; − прерывание бизнес-процесса − нарушение целостности.
Уровень ОС	− программные уязвимости ОС; − слабые пароли ОС; − небезопасные настройки и ошибки в конфигурации ОС; − вредоносное ПО; − недокументированные возможности; − повышение привилегий и получение административного доступа	− нарушение конфиденциальности информации и ее утечка; − нарушение целостности; − нарушение доступности данных

Уровень СУБД, БД	− переполнение буфера; − format string; − атака на пароли; − повышение привилегий внутри СУБД; − PL/SQL инъекции; − несанкционированный доступ к данным и журналам транзакций; − уничтожение и нарушение целостности данных и журналов транзакций;	− нарушение конфиденциальности информации и ее утечка; − нарушение доступности данных, сервисов и служб; − прерывание бизнес-процесса − нарушение целостности.
Уровень представлений и приложений	− эксплуатация уязвимостей веб-приложений − переполнения буфера и format string в веб-серверах и application-серверах − небезопасные привилегии на доступ	− нарушение конфиденциальности информации и ее утечка; − нарушение целостности

Обеспечение той или иной степени защищенности информации от угроз необходимо на каждом из выделенных уровней. При этом выбор механизмов защиты информации на вышеуказанных уровнях ERP-системы зависит от специфики конкретного проекта и от уровня риска каждой угрозы.

Формализованная модель оценки рисков

Для решения задачи оценки рисков ИБ при использовании ERP-системы процедуру оценки рисков можно представить следующей последовательностью шагов:

- определение видов и стоимости объектов (данных, ресурсов и т.п.) ERP- системы;
- составление модели актуальных для ERP-системы угроз, задание параметров, позволяющих оценить такие характеристики угрозы как ущерб, вероятность реализации и разрушительность;
- расчет рисков от реализации каждой угрозы из модели актуальных угроз, расчет общего риска, классификация рисков по уровню допустимости;
- формирование отчета и выдача рекомендаций по обработке рисков.

Формализовано оценка риска ERP-систем описывается множеством концептов.

$$OR=\{A, TR, MP, DR\} \quad (1)$$

где A – множество используемых активов, TR-множество угроз, MP-множество механизмов используемых для защиты в ERP-системе, DR – множество, характеризующее допустимость риска от угрозы.

Активы (объекты) ERP-системы $A=\{A_i\}_{i=\overline{1,m}}$, m-число активов, участвующих в оценки рисков ИБ ERP-системы, являются частью общей информационной инфраструктуры предприятия, в которую предприятие напрямую вкладывает средства и которые, соответственно, представляют ценность и требует защиты со стороны предприятия. Как правило, ценность актива определяется его стоимостью. А в связи с тем, что зачастую невозможно определить точную стоимость актива и предприятия в целом, то предлагается ценность актива $C(A_i^j)$ оценивать нормированной величиной в диапазоне от 0 до 1, которая будет показывать отношение цены актива $Cost(A_i^j)$ к величине капитала всего предприятия $Cost$.

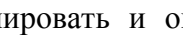
Каждая угроза ИБ  , где *n* – количество рассматриваемых при оценке риска угроз, из множества угроз безопасности ERP-систем *TR*, описывается следующим вектором параметров  , где *v* – частота возникновения данной угрозы за фиксированный промежуток времени, *p* – вероятность успешной реализации угрозы, *d* – коэффициент разрушительности угрозы. Каждый из перечисленных выше параметров предлагается нормировать и оценивать в диапазоне значений  . Значение частоты возникновения угрозы *v*, с учетом подхода изложенного в [21], будет определяться экспертным путем в соответствии со шкалой, представленной в таблице 2.

Таблица 2 – Шкала значений частоты возникновения угрозы

Описание	Значение в качественной шкале	Значение в количественной шкале
угроза происходит в среднем, не чаще, чем каждые 10 лет	очень низкая	[0, 0.05)
угроза происходит в среднем один раз в 3 года	Низкая	[0.05, 0.1]
угроза происходит в среднем раз в год	Средняя	(0.1, 0.4]
угроза происходит в среднем один раз в четыре месяца	Высокая	(0.4, 0.66]
угроза происходит в среднем раз в месяц	очень высокая	(0.66, 1]

Значение вероятности успешной реализации угрозы в ERP-системе тесно связано с наличием в ERP-системе различных механизмов и функций безопасности  , которые в соответствии с моделью безопасности с полным перекрытием должны в идеальном случае перекрывать все возможные угрозы активом объектам исследуемой системы. В этом случае связь между угрозами и механизмами защиты ERP-системы будет описываться матрицей отношений *RM:TR×MP*, см. формулу 2. перекрывает

 (2)

А так как для противодействия одной угрозе может быть использовано несколько механизмов защиты, имеющих различную вероятность отражения одного и того же типа угроз, то с учетом формулы 2, предлагается вероятность успешной реализации угрозы - *p* в ERP-системе рассчитывать по формуле 3.

 (3)

где P_{MPl} - вероятность перекрытия угрозы MP_l средством защиты.

Коэффициент разрушительности угрозы *d* определяется экспертным путем, выражает степень негативного воздействия угрозы на активы ERP-системы и определяет тяжесть последствий для предприятия в целом. В таблице 3 представлена шкала возможных значений коэффициента разрушительности угрозы.

Таблица 3 - Шкала возможных значений коэффициента разрушительности угрозы

Описание	Значение в качественной форме	Значение в количественной форме
Вследствие воздействия угрозы происходит нарушение конфиденциальности и целостности информации, уничтожение данных, длительная потеря доступности сервисов, фиксируется остановка критически важных бизнес-процессов, что приводит к существенному ущербу для предприятия, потере репутации или неполучению существенной прибыли	Высокий	(0.66, 1]
Вследствие воздействия угрозы наблюдается частичное нарушение доступности и целостности данных, происходит кратковременное прерывание бизнес-процессов и работы критических процессов или систем, которое приводит к ограниченным финансовым потерям	Средний	(0.3, 0.66]
Вследствие воздействия угрозы наблюдается частичное нарушение доступности и целостности данных, не имеющих существенную ценность, возможен кратковременный сбой или перерыв в работе сервисов и подсистем, не вызывающий ощутимых финансовых потерь.	Низкий	[0, 0.3]

В свою очередь каждая угроза может воздействовать не на всю ERP-систему, а на один или несколько определенных активов, следовательно, при оценке рисков от каждой конкретной угрозы, необходимо составить бинарных отношений матрицу отношений между угрозами и активами ERP-системы $RMA:TR \times A$ (см. формулу 4).

(4)

В этом случае, ущерб $u(TR_k)$ от каждой угрозы $T_i \in \{T_1, \ldots, T_n\}$ будет рассчитываться по формуле 5.

(5)

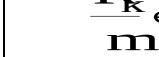
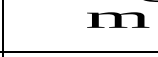
Таким образом, риск $R_k(TRA)$ от каждой угрозы $T_i \in \{T_1, \ldots, T_n\}$ будет зависеть от характеристик самой угрозы и ценности активов, на которые данная угроза направлена, и с

учетом формул 1,3, 4 и 5 будет рассчитываться как (см. формулу 6).

 (6)

Каждый рассчитанный риск от реализации угрозы классифицируется в соответствии с качественной шкалой DR={уровень A, уровень B, уровень C, уровень D} по следующему правилу (см. таблицу 4).

Таблица 4 – Правила классификации рисков ИБ по уровням

Уровень	Описание	Правило присвоения
уровень A	недопустимый риск, поэтому действия связанные с риском должны быть выполнены немедленно и в обязательном порядке;	
уровень B	недопустимый риск, действия связанные с риском должны быть предприняты	
уровень C	частично допустимый риск, требуется мониторинг ситуации, может быть застрахован и передан на аутсорсинг	
уровень D	допустимый риск, никаких действий в данный момент предпринимать не требуется	

Общий риск рассчитывается по формуле 6 и классифицируется по аналогии с частным риском по каждой угрозе, в соответствии с правилами таблицы 4.

$$R=\sum_{k=1}^{|TR|} R_k \qquad (7)$$

Таким образом, онтологическую модель процесса оценки риска ИБ в ERP-системе можно представить в виде следующей схемы, см. рисунок 1.

Данная модель отражает взаимосвязь основных концептов процесса оценки рисков ИБ в ERP-системе. Может быть использована: лицом, принимающим решения в качестве методики при проведении оценки рисков ИБ; при разработке алгоритма оценки риска ИБ в ERP-системе; для определения набора входных и выходных данных, а также основных функций при автоматизации процесса оценки риска в виде программы.

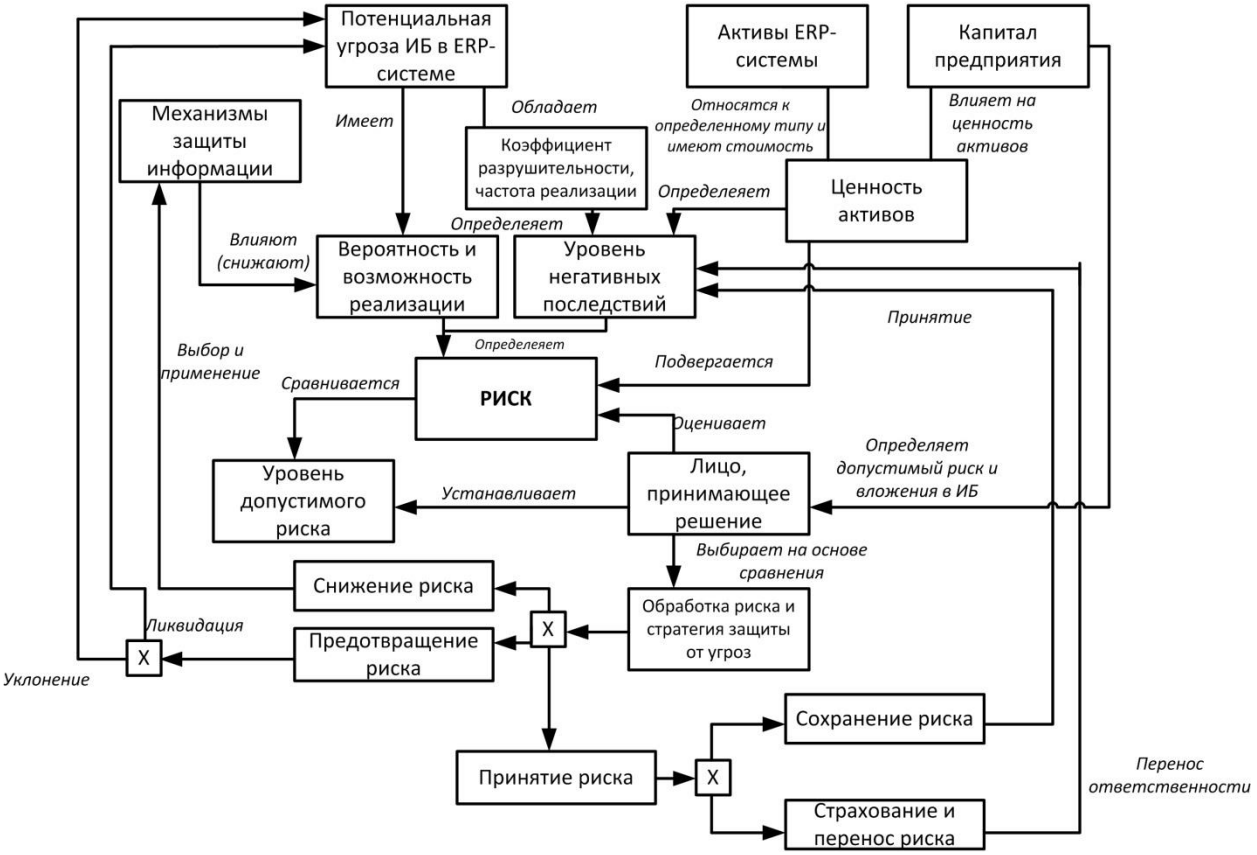


Рисунок 1. Онтологическая модель оценки риска ИБ в ERP-системе.

ЗАКЛЮЧЕНИЕ

В основе разработанной модели лежит количественно-качественный подход к оценке рисков, построенный на частичном объединении 3 методик исследования рисков ИБ - модели безопасности с полным перекрытием, методики CRAMM и методики FRAP. Подобный комплексный подход позволяет учитывать существующие в системе угрозы, активы и механизмы защиты и взаимосвязи и взаимовлияния между ними между ними, классифицировать риски, от актуальных угроз, по степени допустимости с использованием качественной шкалы с 4 уровнями опасности и выработать рекомендации по обработки каждого риска в зависимости от принадлежности его к тому или иному уровню. Предложенная модель была автоматизирована и представлена в виде программы с графическим пользовательским интерфейсом.

СПИСОК ЛИТЕРАТУРЫ:

1. Зырянов Ю. Информационная безопасность ERP-систем.URL: http://citforum.ru/gazeta/49/ (дата обращения 15.06.2016)
2. Дмитринко А.И., Долгова Т.Г. Информационная безопасность ERP-систем//Актуальные проблемы авиации и космонавтики. 2011.№7.Т1.С. 443.
3. Бычков С.А. Сущность и влияние ERP-системы на эффективность деятельности предприятия// Актуальные проблемы гуманитарных и естественных наук.2012. №9.
4. Юсупов Р., Волков С. Методики и программные продукты для оценки рисков//ИНТУИТ [электронный ресурс].: URL: http://www.intuit.ru/studies/courses/531/387/lecture/8996 (дата обращения 13.05.2016).

5. CRAMM [Электронный ресурс]. – Режим доступа: http://www.cramm. com/overview/expert.htm/

REFERENCES:

1. Zyryanov YU. Informatsionnaya bezopasnost' ERP-sistem.URL: http://citforum.ru/gazeta/49/ (data obrashcheniya 15.06.2016)
2. Dmitrinko A.I., Dolgova T.G. Informatsionnaya bezopasnost' ERP-sistem//Aktual'nyye problemy aviatsii i kosmonavtiki. 2011.№7.T1.S. 443.
3. Bychkov S.A. Sushchnost' i vliyaniye ERP-sistemy na effektivnost' deyatel'nosti predpriyatiya// Aktual'nyye problemy gumanitarnykh i yestestvennykh nauk.2012. №9.
4. Yusupov R., Volkov S. Metodiki i programmnyye produkty dlya otsenki riskov//INTUIT [elektronnyy resurs].: URL: http://www.intuit.ru/studies/courses/531/387/lecture/8996 (data obrashcheniya 13.05.2016).
5. CRAMM [Elektronnyy resurs]. – Rezhim dostupa: http://www.cramm. com/overview/expert.htm/