УДК 004.056
DOI: 10.12737/20289

К.Е. Шинаков, М.Ю. Рытов, О.М. Голембиовская, К.В. Чиркова

ОЦЕНКА РИСКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ, ОБРАБАТЫВАЮЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

Рассмотрена проблема определения ценности информационных ресурсов, оценка уязвимостей и угроз, а также оценка риска информационной безопасности с учетом обозначенных параметров.

Ключевые слова: информационные системы, конфиденциальная информация, оценка риска безопасности, метод Черчмена - Акоффа.

K.E. Shinakov, M.Yu. Rytov, O.M. Golembiovskaya, K.V. Chirkova

SAFETY RISK ASSESSMENT OF INFORMATION SYSTEMS PROCESSING CONFIDENTIAL INFORMATION

Confidential information processing in information systems under conditions of the universal informatization in both state-owned and private companies is an urgent problem.

Many operators processing a trade secret or personal data underestimate possible damage caused by the disclosure, deletion or change of confidential information and afterwards become victims either of deliberate criminals or suits of workers whose rights were violated. In such a way, the safety risk assessment of confidential information processed in information systems is a priority trend both for an operator and for a subject of confidential information. As a result of the investigation carried out there was developed a procedure for risk assessment of information systems processing confidential information in which it is possible to define and process a critical group of threats, and also a system for the definition of sufficient and the best set of counter-measures among possible ones. At the intermediate and final stage there is defined a significance of an information safety risk witnessing of measures carried out for the assurance of confidential information safety.

Key words: information systems, confidential information, estimate of safety risk, Churchman-Ackoff method.

Обработка конфиденциальной информации в информационных системах в условиях повсеместной информатизации как государственных, так и частных организаций является актуальным вопросом.

Для обеспечения защищенной обработки такой информации используются организационные, программные и технические средства защиты. Однако конечным элементом в последовательности «актив – уязвимость – угроза» является риск. Данный параметр является исчерпывающим и достаточным для качественного определения мер по его устранению или минимизации.

Ввиду этого предлагаемая методика включает в себя следующие этапы:

1. Оценка ценности элементов конфиденциальной информации.
2. Оценка уязвимостей и угроз безопасности конфиденциальной информации.
3. Оценка риска информационной безопасности.

В рамках этапа оценки ценности элементов конфиденциальной информации прогнозируется возможный ущерб от угроз, относящихся к ресурсам, который определяется суммой возможных убытков от недополучения прибыли, штрафов в части нарушения законодательства и стоимости восстановления информационного ресурса.

Таким образом, оценка ценности элементов конфиденциальной информации имеет вид

$$P=p_1+p_2+p_3,$$

где P – итоговый ущерб от угрозы ресурсу; p_1 – ожидаемые потери (убытки, недополучение прибыли); p_2 – максимальный штраф за нарушение законодательства РФ; p_3 – стоимость восстановления ресурса.

Ожидаемые потери p_1 вводятся обладателем информационного ресурса на основе его экспертного мнения.

Для определения p_2 используется табл. 1, содержащая статьи Кодекса Российской Федерации об административных правонарушениях [1], нарушение которых влечёт административное наказание юридического лица.

Таблица 1

Оценка стоимости конфиденциальной информации относительно наложения штрафов в соответствии с законодательством РФ

№	Наименование статьи	Наказание административное (количественное)	Наказание административное (качественное)
1	Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	От пяти до десяти тысяч рублей	Отсутствует
…	…	…	…

Для определения p_3:

- данные по обслуживанию продуктов фирмы «1С» были получены из прайслиста компании «BRG» – официального партнера фирмы «1С» [2];
- данные о стоимости обслуживания прикладного и системного ПО были получены из среднестатистических значений стоимости подобных работ;
- данные о фактической стоимости физического оборудования были получены из среднестатистических значений стоимости конкретных моделей оборудования.

Таким образом, можем сформировать таблицу для определения ущерба (ценности) конфиденциальной информации, фрагмент которой представлен в табл. 2.

Таблица 2

Определение ущерба

Ресурсы	Угрозы	Ожидаемые потери p_1	Максимальный штраф за нарушение законодательства РФ p_2	Стоимость восстановления p_3	Итоговый ущерб от угрозы ресурсу P
База данных сотрудников («1С: Бухгалтерия»)	Угроза утечки информации по каналам ПЭМИН	Заполняется экспертом	25000,00	0,00	25000,00
	Кража, модификация, уничтожение информации	Заполняется экспертом	30000,00	7500,00	37500,00
	Непреднамеренная модификация (уничтожение) информации работниками	Заполняется экспертом	30000,00	7500,00	37500,00
…	…	…	…	…	…

На втором этапе определяется вероятность реализации угроз. Для данного этапа целесообразно определить наличие уязвимостей на объекте.

Вероятность реализации угрозы вычисляется по формуле $V_{ry} = \sum_{i=1}^{n} k_i \, a_i$, где a_i – коэффициент важности. $V_{ry} \leq 1$.

Следовательно, коэффициент важности a_i должен удовлетворять условию $\sum_{i=1}^{n} a_i = 1$.

Для наглядности применения метода за основу было взято предприятие с некими актуальными для него угрозами и соответствующими уязвимостями.

Значение параметра k_i (табл. 3) показывает, актуальна ли данная уязвимость для предприятия: если $k_i = 1$, то уязвимость актуальна; если $k_i = 0$, то уязвимость не актуальна.

Таблица 3

Определение вероятности реализации угроз

№	Угроза	Определение вероятности			Вероятность реализации угрозы V_{ry}
		Уязвимость	Ответ k_i	Коэффициент важности a_i	
1	Угроза утечки акустической информации	Отсутствуют шумогенераторы	0	0,5	0,3
		Индекс звукоизоляции дверей менее 40 дБ	1	0,3	
		Переговорные не проходили аттестацию (проходили более 5 лет назад)	0	0,2	
2	Угроза утечки видовой информации	Отсутствуют жалюзи на окнах	1	0,15	0,9
		Расположение ПК мониторами к окнам	0	0,1	
		Светопропускаемость окон 100%	1	0,4	
		Отсутствует контроль доступа	1	0,3	
		Не регламентирована политика «чистого стола»	1	0,05	
3	Угроза утечки информации по каналам ПЭМИН	Отсутствует экранирование кабельных коммуникаций	1	0,5	0,8
…	…	…	…	…	…

На третьем этапе определяется риск безопасности элементов конфиденциальной информации. За основу для определения меры риска была взята приведенная в [3] матрица (табл. 4).

Таблица 4

Матрица определения риска информационной безопасности

Степень вероятности возникновения угрозы		Низкая			Средняя			Высокая		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Простота использования соответствует коэффициенту важности уязвимости для определенной угрозы.

Разрушение или сбой в работе любого из имеющихся на предприятии активов влечет за собой различные финансовые потери. Именно ввиду этого было принято

решение обозначить баллы ценности, дав им денежные значения.

В ходе исследования и применения различных комбинаций значений ценности активов, степени вероятности возникновения угрозы и простоты использования были определены значения перечисленных параметров.

Промежуточные денежные значения были определены исходя из значений вероятного ущерба *P* для ресурсов. Ценность активов определяется согласно следующей шкале:

0 – 0…5000 рублей;

1 – 5000…10000 рублей;

2 – 10000…50000 рублей;

3 – 50000…100000 рублей;

4 - свыше 100000 рублей.

Промежуточные значения были определены исходя из значений вероятности реализации угрозы V_{ry} (табл. 3).

Степень вероятности возникновения угрозы и простота использования определяются по следующей шкале:

0 – 0,4 – низкая;

0,5 – 0,7 – средняя;

0,8 – 1 – высокая.

Таблица 5

Определение меры риска угроз согласно ГОСТ Р ИСО/МЭК 27005-2010

Идентификатор угрозы (*a*)	Последствия (ценность актива) (*b*)	Степень вероятности возникновения угрозы (*c*)	Мера риска (*d*)	Ранжирование угроз (*e*)
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

В табл. 5 приведены 3 основных параметра:

b – величина, соответствующая ущербу от повреждения или разрушения актива (оценивается в баллах и соответствующих им денежных единицах);

c – величина, соответствующая вероятности возникновения угрозы;

d – величина, показывающая, насколько опасна угроза для предприятия.

Данные параметры были определены согласно табл. 6 и соответствующим значениям шкал ценности активов, вероятности возникновения угрозы и простоты использования.

Столбец «Ранжирование угроз» было решено не использовать, так как сравнение проводится не между отдельными угрозами, а между группами угроз: «Конфиденциальность», «Целостность (изменение)», «Целостность (удаление)», «Доступность».

Таблица 6

Определение меры риска угроз

Идентификатор угрозы (*a*)	Последствия (ценность актива) (*b*)	Степень вероятности возникновения угрозы (*c*)	Мера риска (*d*)	Возможный ущерб для предприятия, руб.
Угроза утечки акустической информации	0	0,3	0	0,00
Угроза утечки видовой информации	0	0,9	8	0,00
Угроза утечки информации по каналам ПЭМИН	2	0,8	8	25000,00
Кража физических ресурсов	2	0,72	16	43200,00
…	…	…	…	…
Общий показатель	34	19,33	207	1134422,00

Для минимизации риска было принято решение о выделении критичной группы угроз из перечня и применении контрмер для их нейтрализации.

Для сравнения групп угроз между собой выбран метод Черчмена - Акоффа, который предполагает последовательную корректировку оценок, указанных экспертами.

Согласно методу Черчмена - Акоффа, альтернативы ранжируются по предпочтительности [4].

В качестве альтернатив α_i были определены несколько промежуточных параметров, характеризующих группы угроз: ценность актива, степень вероятности возникновения угрозы, мера риска и возможный ущерб (табл. 7).

В качестве оценок альтернатив $\varphi(\alpha_i)$ были определены два параметра, по которым и проводилось сравнение групп угроз: вероятный ущерб и коэффициент риска.

Коэффициент риска – показатель, определяющий критичность группы угроз и объединяющий все показатели данной группы, кроме возможного ущерба.

$$K_r = \frac{b+c+d}{\text{кол-во угроз группы}}.$$

Вероятный ущерб – ущерб, который будет нанесен предприятию в случае осуществления угроз.

$$P_{vr} = \frac{p}{c}.$$

Таблица 7

Сравнение показателей для групп угроз

Группа угроз	Последствия (ценность актива) (*b*)	Степень вероятности возникновения угрозы (*c*)	Мера риска (*d*)	Возможный ущерб (*p*)	Вероятный ущерб P_{vr}	Коэффициент риска K_r
Начальные значения	34	19,33	207	1134422,00	58687,00	9,64
Конфиденциальность	21	15,27	139	478502,00	31336,00	7,96
Целостность (изменение)	13	8,25	75	207577,00	25160,00	8,02
Целостность (удаление)	34	12,63	156	1072778,00	84938,00	11,25
Доступность	24	8,4	99	871523,00	103752,00	10,95

Критичную группу угроз определяем по соотношению коэффициента риска и вероятного ущерба.

Наибольшие значения коэффициента риска имеют группы угроз «Целостность (удаление)» и «Доступность».

Угрозы группы «Доступность» имеют наибольшее значение вероятного ущерба, следовательно, эту группу примем за критичную.

На следующем этапе оценивается эффективность контрмер (путем сравнения их между собой) и осуществляется ранжирование по эффективности:

1-***** (наилучшие);

2-**** (хорошие);

3-*** (средние);

4-** (посредственные);

5-** (недостаточно эффективные).

Пример ранжирования контрмер для уязвимости «Отсутствуют камеры видеонаблюдения» представлен в табл. 8.

Таблица 8

Ранжирование контрмер для уязвимости «Отсутствуют камеры видеонаблюдения»

Отсутствуют камеры видеонаблюдения			
Характеристики	VidStar VSV-2120VR-AHD (вариофокальная купольная видеокамера)*****	VidStar VSD-2360FR-AHD (купольная видеокамера)****	VidStar VSD-1361FR-AHD (купольная видеокамера)***
Тип корпуса	Купольный	Купольный	Купольный
Климатическое исполнение	Уличное	Внутреннее	Внутреннее
Антивандальное исполнение	Нет	Нет	Нет
Разрешение камеры	2 Мрх	2 Мрх	1,2 Мрх
Тип объектива	Вариофокальный	Фиксированный	Фиксированный
Изображение	Цветное	Цветное	Цветное
Ночной режим	Да	Да	Да
Стоимость	4200,00	3690,00	3240,00

В табл. 9 каждой угрозе и соответствующим ей уязвимостям сопоставляются несколько вариантов контрмер с указанием их стоимости.

Таблица 9

Контрмеры для угроз группы «Доступность»

№	Угроза	Определение контрмер			
		Уязвимость	Ответ k_i	Контрмера	Стоимость контрмеры, руб.
4	Кража физических ресурсов	В двери не вмонтированы замки	0	Врезка замков	2000,00 на 1 дверь
		Отсутствуют камеры видеонаблюдения	1	VidStarVSV-2120VR-AHD (вариофокальная купольная видеокамера)	4200,00
				VidStarVSD-2360FR-AHD (купольная видеокамера)	3690,00
				VidStar VSD-1361FR-AHD	3240,00
		Отсутствуют датчики движения	1	SRDT-15 (комбинированный (ИК+ СВЧ) детектор)	2562,00
				MR-CRT (пассивный ИК - детектор)	2013,00
				«Астра-5 А» (ИО-409-10)	551,00
				«Рапид» (ИО-409-28)	390,00
				М-903D	331,00
		Отсутствуют магнитоконтактные детекторы	0	ИО 102-4 (миниатюрный)	80,00
				ИО-102-5 (миниатюрный, врезной)	74,00
				ИО102-2 (СМК-1) (накладной)	40,00
		Отсутствуют датчики разбития окон	1	GBD-2 (детектор разбития стекла)	1000,00
				DG457 Glasstrek (акустический датчик разбития стекла)	2560,00

На заключительном этапе оценивается остаточная мера риска после применения контрмер для угроз группы «Доступность» (табл. 10).

Таблица 10

Определение остаточной меры риска после устранения угроз группы «Доступность»

Идентификатор угрозы (*a*)	Последствия (ценность актива) (*b*)	Степень вероятности возникновения угрозы (*c*)	Мера риска (*d*)	Возможный ущерб (*p*)
Угроза утечки акустической информации	0	0,3	0	0,00
Угроза утечки видовой информации	0	0,6	3	0,00
Угроза утечки информации по каналам ПЭМИН	2	0,8	5	25000,00
Утрата ключей и атрибутов доступа	0	0,5	1	1781,00
Разглашение информации, модификация, уничтожение работниками, допущенными к ее обработке	3	1	16	64669,00
Перехват за пределами контролируемой зоны	0	0,55	3	0,00
Перехват в пределах контролируемой зоны внешними нарушителями	0	0,1	0	0,00
Перехват в пределах контролируемой зоны внутренними нарушителями	0	0,8	6	0,00
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов, открытых портов и служб, соединений и др.	0	0,11	0	0,00
Общий показатель	5	4,76	34	91450,00

В результате проведенного исследования была разработана методика оценки риска безопасности информационных систем, обрабатывающих конфиденциальную информацию, в которой имеется возможность определения и обработки критичной группы угроз, а также методика определения достаточного и наилучшего из возможных наборов контрмер.

СПИСОК ЛИТЕРАТУРЫ

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (ред. от 31.12.2014) (с изм. и доп., вступ. в силу с 11.01.2015).
2. Официальный сайт «Bussines relationship group».-Режим доступа: http://www.brg-consulting.ru/.
3. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
4. Методы качественного оценивания систем. Методы экспертных оценок // Научная энциклопедия Book-Science. - Режим доступа: http://book-science.ru.

1. Code of the Russian Federation of Administrative Delinquency of 30.12.2001 №195-ФЗ (ed. от 31.12.2014) (withchanges and supplements came into force since 11.01.2015).
2. Official website “Business relationship group”.- access mode: http://www.brg-consulting.ru/.
3. SARS RF ISO/IEC 27005-2010. Information technology. Methods and means of information safety support. Management of information safety risk.
4. Methods of system quality assessment. Methods of expert assessments // Scientific Encyclopedia Book-Science. – Access mode: http://book-science.ru.

Статья поступила в редколлегию 18.02.2016.
Рецензент: д.т.н., профессор Брянского государственного технического университета Лозбинев Ф.Ю.

Сведения об авторах:

Шинаков Кирилл Евгеньевич, ассистент кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: nirsamy-bgtu@yandex.ru.
Рытов Михаил Юрьевич, к.т.н., доцент Брянского государственного технического университета, e-mail: rmy@tu-bryansk.ru.
Голембиовская Оксана Михайловна, к.т.н., доцент кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: nirsamy-bgtu@yandex.ru.
Чиркова Ксения Вячеславовна, студент группы 13-БАС кафедры «Системы информационной безопасности» Брянского государственного технического университета, e-mail: nirsamy-bgtu@yandex.ru.

Shinakov Kirill Eugenievich, Assistant of the Dep. “Information Safety Systems” Bryansk State Technical University,
e-mail: nirsamy-bgtu@yandex.ru.
Rytov Mikhail Yurievich, Can.Eng., Assistant Prof., Bryansk State Technical University, e-mail: rmy@tu-bryansk.ru.
Golembiovskaya Oksana Mikhailovna, Can.Eng., Assistant Prof. of the Dep. “Information Safety Systems” Bryansk State Technical University, e-mail: nirsamy-bgtu@yandex.ru.
Chirkova Ksenia Vyacheslavovna, Student of 13-BAS group of the Dep. “Information Safety Systems” Bryansk State Technical University, e-mail: nirsamy-bgtu@yandex.ru.