Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 6, Is. 4, pp. 124-132, 2015

DOI: 10.13187/vesp.2015.6.124
www.ejournal21.com

Theoretical Questions

UDC 004.056.53

The Assessment of Losses Caused By the Offenses in the Information Sphere

[1] Natalia M. Zaitseva
[2] Ruslan A. Nurdinov

[1] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiy prospekt, 49
E-mail: zaytsevanm@yandex.ru
[2] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiy prospekt, 49
E-mail: nurdinov.ra@mail.ru

Abstract

The article describes the importance of assessing the damage in the investigation of offenses. The breached properties of information from a variety of offenses in the information sphere are determined. It is considered the main methods of quantifying losses caused by the implementation of threats offered in methods of risk analysis. The offered method allows assessing losses caused by offences in the information sphere, leading to a breach of confidentiality, integrity and availability of information assets.

Keywords: information, offense, amount of damage, quantitative evaluation of risks, properties of information, losses.

Введение

Информационная сфера, «…являясь системообразующим фактором жизни общества..» [Доктрина ИБ РФ], является также весьма привлекательной сферой деятельности для нечистоплотных людей и просто преступников. Ежегодно совершается множество правонарушений в области поиска, создания, обработки, передачи, получения, хранения, защиты и использования информационных активов [1].

Под информационным активом понимается информация с реквизитами, позволяющими ее идентифицировать, и имеющая ценность для организации [ЦБ РФ СТО БР ИББС-1.0-2010].

Особенностью правонарушений в информационной сфере является то, что существенный вред можно нанести внезапно, минимальными силами и средствами, находясь практически вне зоны реальной досягаемости. Противоправные действия в области информационных технологий, такие как нарушение работы ЭВМ и АСУ, несанкционированное уничтожение, модификация, копирование информационных

активов, могут привести не только к большому имущественному ущербу, но и нанесению физического вреда людям [2].

При расследовании любого преступления, прежде всего, выявляется характер и размер причиненного вреда или ущерба [1]. Определение размера ущерба важно не только для решения вопроса о его возмещении, но и для правильной квалификации правонарушения, определения вида ответственности (гражданско-правовая, административная или уголовная). Так, согласно ст. 272 УК РФ, в зависимости от размера ущерба, за неправомерный доступ к информации возможно наказание от штрафа до ограничения свободы на срок до 5 лет [4].

В случае кражи или повреждения материального объекта ущерб определяется на основании стоимости его замены или восстановления. Оценить ущерб от нарушения свойств нематериального объекта, такого как информационный актив, гораздо сложнее.

Нарушение свойств информационного актива может привести как к материальному (прямому и косвенному), так и нематериальному ущербу. Для следственных органов трудности обычно возникают при оценке косвенного материального ущерба (например, упущенной выгоды), а особенно нематериального ущерба (например, подрыва репутации).

На практике отсутствует однозначная позиция относительно количественной оценки правового ущерба в информационной сфере. Цель работы – разработать комплексную методику количественной оценки ущерба от правонарушений в информационной сфере.

Материалы и методы

При написании публикации были рассмотрены официальные документы, регламентирующие отношения в информационной сфере, и рекомендации по защите информации. Также были использованы новые методики и результаты последних исследований в области количественной оценки рисков.

Методологическую основу исследования составили диалектический, функциональный, системно-структурный подходы. Для формирования понятий используются логические приемы, определения, описания, анализ и синтез.

Обсуждение

Правонарушения, совершаемые в информационной сфере, реально наносят ущерб предприятиям и частным лицам, но, из-за определенной специфики, убытки редко возмещаются в должной мере [1].

Количественная оценка величины ущерба позволяет определить реальные последствия от совершенного правонарушения. Согласно п. 2 ст. 15 ГК РФ, убытки включают в себя расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, реальный ущерб (утрата или повреждение имущества) и упущенную выгоду, заключающуюся в неполучении доходов вследствие нарушения права [8].

Как уже упоминалось выше, правонарушения в информационной сфере можно разделить на уголовные, административные и гражданско-правовые. Ниже приведены основные статьи, устанавливающие ответственность за правонарушения в информационной сфере, приведенные в Уголовном кодексе РФ (таблица 1) и Кодексе РФ об административных правонарушениях (таблица 2). Для каждой статьи указано, какие свойства информационных активов (ИА) при этом нарушаются: конфиденциальность (К), целостность (Ц) и/или доступность (Д).

Таблица 1

Нарушение свойств информации при совершении уголовных преступлений в информационной сфере

Статья Уголовного кодекса РФ (N 63-ФЗ РФ)		Нарушаемые свойства ИА		
Номер	Название	К	Ц	Д
137	Нарушение неприкосновенности частной жизни	+	–	–
138	Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений	+	–	–
138.1	Незаконный оборот специальных технических средств, предназначенных для негласного получения информации	+	–	–
140	Отказ в предоставлении гражданину информации	–	–	+
142	Фальсификация избирательных документов, документов референдума	–	+	–
142.1	Фальсификация итогов голосования	–	+	–
144	Воспрепятствование законной профессиональной деятельности журналистов	–	–	+
146	Нарушение авторских и смежных прав	–	+	–
172.1	Фальсификация финансовых документов учета и отчетности финансовой организации	–	+	–
183	Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну	+	–	–
187	Неправомерный оборот средств платежей	+	+	+
237	Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей	–	+	+
272	Неправомерный доступ к компьютерной информации	+	+	+
273	Создание, использование и распространение вредоносных компьютерных программ	+	+	+
274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей	+	+	+

Таблица 2

Нарушение свойств информации при совершении административных правонарушений в информационной сфере

Статья Кодекса об административных правонарушениях (N 195-ФЗ)		Нарушаемые свойства ИА		
Номер	Название	К	Ц	Д
5.1, 5.4, 5.13, 5.25, 5.46	Статьи о возможных нарушениях при проведении референдума	–	+	+
5.39	Отказ в предоставлении информации	–	–	+

6.1	Сокрытие источника заражения ВИЧ-инфекцией, венерической болезнью и контактов, создающих опасность заражения	–	–	+
6.30	Невыполнение обязанностей об информировании граждан о получении медицинской помощи в рамках программы государственных гарантий бесплатного оказания гражданам медицинской помощи и территориальных программ государственных гарантий бесплатного оказания гражданам медицинской помощи	–	–	+
7.12	– Нарушение авторских и смежных прав, изобретательских и патентных прав	+	–	+
8.5	Сокрытие или искажение экологической информации	–	+	+
10.7	Сокрытие сведений о внезапном падеже или об одновременных массовых заболеваниях животных	–	–	+
Статья Кодекса об административных правонарушениях (N 195-ФЗ)		Нарушаемые свойства ИА		
Номер	Название	К	Ц	Д
11.30	Умышленное сокрытие авиационного происшествия или инцидента	–	+	+
13.11	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	–	+	+
14.48	Представление недостоверных результатов исследований (испытаний)	–	+	–
13.14	Разглашение информации с ограниченным доступом	+	–	–
15.6	Непредставление (несообщение) сведений, необходимых для осуществления налогового контроля	–	–	+
13.19	Нарушение порядка представления статистической информации	–	–	+

Выявление свойств ИА, подверженных воздействию, позволяет облегчить оценку ущерба.

Анализ существующих подходов

Вопрос оценки ущерба информационным активам зачастую рассматривается в методиках анализа рисков [7]. В информационной безопасности (ИБ) анализ рисков возник в связи с необходимостью прогнозирования и сопоставления затрат на систему защиты информации и возможного ущерба от реализации угроз. Наиболее известные методы оценки: качественный и количественный анализ [6].

В качественном анализе посредством экспертных оценок определяется зависимость значения риска от определенных факторов – вероятности наступления события и величины ущерба от наступления данного события. Значения большинства из необходимых параметров принимается на основе мнений экспертов, что ставит результаты в зависимость от их квалификации и профессионализма.

Количественная оценка применяется в ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями, выраженными в деньгах, процентах, времени, человеческих ресурсах и т.д. Такой анализ

часто использует инструментарий теории вероятностей, математической статистики, теории исследования операций.

Сравнив существующие подходы к оценке рисков, можно сделать вывод, что только количественная оценка позволяет конкретно рассчитать возможный ущерб [5,6].

Рассмотрим подходы к оценке ущерба в наиболее распространенных количественных методиках оценки рисков: CRAMM, RiskWatch, ГРИФ. Данный выбор обусловлен популярностью этих методик и наличием достаточно полной информации о них в литературе свободного доступа.

В основе методики CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Ценность физических ресурсов в CRAMM определяется стоимостью их восстановления в случае разрушения. Выделяются следующие виды причинения ущерба ресурсам системы: недоступность, разрушение, нарушение конфиденциальности, модификация, ошибки, связанные с передачей информации. Для оценки возможного ущерба используют следующие параметры [7]: ущерб репутации организации, нарушение действующего законодательства, ущерб для здоровья персонала, ущерб, связанный с разглашением персональных данных, финансовые потери от разглашения информации, финансовые потери, связанные с восстановлением ресурсов, потери, связанные с невозможностью выполнения обязательств, дезорганизация деятельности. Для информационных активов и программного обеспечения осуществляется оценка ущерба по балльной шкале со значениями от 1 до 10, которым соответствуют диапазоны значений потерь, выраженных в деньгах.

В методике RiskWatch показателем ущерба является параметр ожидаемых годовых потерь (Annual Loss Expectancy, ALE), который может быть рассчитан двумя способами. RiskWatch использует определенные американским институтом стандартов NIST оценки, называемые LAFE и SAFE. LAFE (Local Annual Frequency Estimate) – показывает, сколько раз в год в среднем данная угроза реализуется в данном месте. SAFE (Standard Annual Frequency Estimate) – показывает, сколько раз в год в среднем данная угроза реализуется в этой «части мира». Стоит отметить, что для отечественных организаций использование данных оценок проблематично, что обусловлено, прежде всего, сложностью сбора достоверной статистики, характеризующей частоту реализации угроз в разных частях страны.

ГРИФ – программный продукт отечественного производства компании Digital Security. Основной особенностью ГРИФ является то, что оценка ущерба осуществляется отдельно для нарушения конфиденциальности, целостности и доступности информационного актива. Такой подход, прежде всего, позволяет декомпозировать задачу оценки ущерба от нарушения безопасности информационного актива на три отдельные, непересекающиеся подзадачи: оценку потерь от нарушения конфиденциальности, целостности и доступности информации.

Результаты

С точки зрения защиты информации, как упоминалось выше, наиболее важны три свойства информации: конфиденциальность, целостность и доступность. Убытки предлагается оценивать как совокупность ущерба, причиненного вследствие нарушения каждого из этих свойств.

Нарушение доступности информации подразумевает ограниченность доступа к ресурсу или полное его отсутствие, которое может произойти как в случае преднамеренного, так и случайного действия.

Формула для расчета потерь от угроз доступности [10]:

$$L_a = F_{RS} + F_R + F_{LP} + F_D\,, \qquad (1)$$

где F_{RS} – потери от несвоевременного оказания услуг по доступу к информации; F_R – потери, связанные с восстановлением информации; F_{LP} – потери, связанные с упущенной

выгодой, F_D – потери, связанные с простоем деятельности в связи с невозможностью использования информации.

Потери от несвоевременного оказания услуг по доступу могут быть зафиксированы в договоре в виде неустойки.

Потери, связанные с восстановлением работоспособности (F_R) рассчитываются:

$$F_R = \sum_{i=1}^{n} S_i + \sum_{j=1}^{l} Z_j \cdot t_j \cdot (1 + k_p) \cdot (1 + d_s), \quad (2)$$

где S_i – стоимость восстановления i-го поврежденного информационного актива; n – количество поврежденных информационных активов; Z_j – часовая зарплата j-го сотрудника, восстанавливающего информацию; t_j– время в часах, затраченное j-ым сотрудником на восстановление; k_p – коэффициент премирования; d_s – доля отчислений в социальные фонды; l – количество сотрудников, восстанавливающих работоспособность.

Потери, связанные с упущенной выгодой (F_{LP}) определяются по формуле [10]:

$$F_{LP} = D * \frac{t_d + t_r}{T} \quad (3)$$

где D – годовой доход от использования информации; t_d – время простоя в связи с невозможностью использовать информацию; t_v – время восстановления доступа к информации; T - период использования актива в течение года.

Потери, связанные с простоем из-за невозможности использования информации:

$$F_D = \frac{\sum_{i=1}^{n} Zi}{T} * t_d \quad (4)$$

где Zi – доход в месяц человека, использующего информацию; i – количество человек, использующих информацию; t_d – время простоя; T – время работы с информацией в месяц.

К категории наиболее небезопасных угроз следует отнести непреднамеренные ошибки лиц, которые имеют неограниченный доступ к информационному ресурсу.

Информация может быть скомпрометирована, тогда мы говорим о нарушении конфиденциальности. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [9].

Потери в этом случае будут складываться из нескольких составляющих (4): затраты на оповещение пострадавших (F_{NA}), расследование утечки (F_{IL}), оплата юридических услуг в случае судебных разбирательств (F_{LF}). Возможна выплата штрафов (F_F) и затраты на проведение PR-кампании (F_{PR}) для восстановления репутации.

$$L_c = F_{NA} + F_{IL} + F_{LF} + F_F + F_{PR} \quad (5)$$

При нарушении требования конфиденциальности стороны часто лишены необходимой доказательственной базы и поэтому чаще используют неустойку или

компенсацию вместо возмещения убытков, размер которых они заранее определили в договоре, либо отказываются при отсутствии доказательств от взыскания убытков [11, 12].

Нарушение целостности информации подразумевает модификацию данных. Информация может быть подвержена изменениям преднамеренно и непреднамеренно. Непреднамеренное изменение представляет собой сбои, отказы системы и т.д. Преднамеренное – умышленное изменение с целью получения выгоды, и представляет больший для нас интерес.

Для угроз целостности потери могут быть подсчитаны по формуле [10]:

$$L_i = F_{UM} + F_R + F_{LP} \ , \qquad (6)$$

где F_{UM}– потери от несанкционированной модификации информации; F_R – потери, связанные с восстановлением информации; F_{LP} – потери, связанные с утратой возможного дохода.

Размер F_{UM} будет зависеть от значимости информации, целостность которой нарушена.

Потери при восстановлении информации могут быть рассчитаны по формуле (2). Следует учесть, что при одновременном нарушении целостности и доступности ущерб необходимо рассчитать один раз.

Потери, связанные с утратой возможного дохода, определяются по формуле:

$$F_{LP} = D * \frac{t_d + t_r}{T} \qquad (7)$$

где D – годовой доход от использования информации; t_d – время простоя; t_v – время восстановления целостности информации; T – период использования информационного актива в течение года.

Заключение

Ущерб от правонарушений в информационной сфере можно рассчитать с помощью количественной оценки. При оценке необходимо учитывать как финансовые (материальные) потери, так и нематериальные потери. В представленном походе наибольшее внимание уделено определению ущерба в отношении информационных активов. Также были установлены взаимосвязи между наиболее значимыми правонарушениями в информационной сфере и их влиянием на свойства информации.

Дальнейшие исследования направлены на разработку методики оценки рисков ИБ, обусловленных правонарушениями в информационной сфере.

Примечания:

1. Полушкин, А. В. Информационное правонарушение :Понятие и виды: автореферат диссертации на соискание ученой степени кандидата юридических наук. 2009. 26 с.

2. Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий: Учебное пособие. СПб.: СПб юридический институт Ген. прокуратуры РФ. 2007. 69 с.

3. Баркалова Е. В. К вопросу об определении вреда при расследовании преступлений против собственности // Криминалист. 2013. №1 (12)

4. Уголовный кодекс Российской Федерации : [федеральный закон: принят Гос. Думой 24 мая 1996 г.: по состоянию на 1 мая 2012 г.]. Москва : ЭКСМО, 2012. 176 с.

5. Вихров Н.М., Нырков А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С., Нурдинов Р.А.. Анализ информационных рисков // Морской вестник. 2015. №3. С.81.

6. Зайцева Н.М. Обоснование затрат на создание системы безопасности, основанное на анализе информационных рисков // Сборник трудов IV Всероссийского конгресса молодых ученых. 2015. С. 157-160.

7. Астахов, А.М. Искусство управления информационными рисками / А.М. Астахов. М.: ДМК-Пресс, 2010. 312 с.

8. Гражданский кодекс Российской Федерации (часть первая) [Электронный ресурс]: [федеральный закон: от 30.11.1994 г. № 51-ФЗ, в ред. от 13.07.2015 г.] – Режим доступа : www.consultant.ru (дата обращения: 07.12.2015)

9. Федеральный закон РФ № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» (ред. от 28.07.2012)

10. Никуленко Е.Д., Губенко Н.Е. Анализ модели для оценки потерь, связанных с реализацией угроз и уязвимостей для информационных систем // Сборник материалов II всеукраинской научно-технической конференции студентов, аспирантов и молодых ученных «Информационные управляющие системы и компьютерный мониторинг (ИУС та КМ-2010)». Донецк: ДонНТУ, 2011 Т.1, с. 260-263

11. Садиков О.Н. Убытки в гражданском праве Российской Федерации. М.: Статут, 2009. С. 9.

12. Илюшина М. Н., Челышев М. Ю., Ситдикова Р. И. Коммерческие сделки: теория и практика: Учебно-практическое пособие / Под общ. ред. М. Н. Илюшиной. М.: РПА МЮ РФ, 2005. С. 147–154.

13. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: [федеральный закон : от 30.12.2001 N 195-ФЗ, в ред. от от 28.11.2015г.] – Режим доступа : www.consultant.ru (дата обращения: 09.12.2015)

References:

1. Polushkin, A. V. Informatsionnoe pravonarushenie:Ponyatie i vidy: avtoreferat dissertatsii na soiskanie uchenoi stepeni kandidata yuridicheskikh nauk. 2009. 26 s.

2. Kushnirenko S. P. Metodika rassledovaniya prestuplenii v sfere vysokikh tekhnologii: Uchebnoe posobie. – SPb.: SPb yuridicheskii institut Gen. prokuratury RF. 2007. 69 s.

3. Barkalova E. V. K voprosu ob opredelenii vreda pri rassledovanii prestuplenii protiv sobstvennosti – Kriminalist. 2013. №1 (12)

4. Ugolovnyi kodeks Rossiiskoi Federatsii : [federal'nyi zakon: prinyat Gos. Dumoi 24 maya 1996 g.: po sostoyaniyu na 1 maya 2012 g.]. Moskva: EKSMO, 2012. 176 s.

5. Vikhrov N.M., Nyrkov A.P., Katorin Yu.F., Shnurenko A.A., Bashmakov A.V., Sokolov S.S., Nurdinov R.A.. Analiz informatsionnykh riskov // Morskoi vestnik. 2015. №3. S.81.

6. Zaitseva N.M. Obosnovanie zatrat na sozdanie sistemy bezopasnosti, osnovannoe na analize informatsionnykh riskov // Sbornik trudov IV Vserossiiskogo kongressa molodykh uchenykh. 2015. S. 157-160.

7. Astakhov, A.M. Iskusstvo upravleniya informatsionnymi riskami / A.M. Astakhov. M.: DMK-Press, 2010. 312 s.

8. Grazhdanskii kodeks Rossiiskoi Federatsii (chast' pervaya) [Elektronnyi resurs]: [federal'nyi zakon : ot 30.11.1994 g. № 51-FZ, v red. ot 13.07.2015 g.] – Rezhim dostupa : www.consultant.ru (data obrashcheniya: 07.12.2015)

9. Federal'nyi zakon RF № 149-FZ ot 27.07.2006 «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» (red. ot 28.07.2012)

10. Nikulenko E.D., Gubenko N.E. Analiz modeli dlya otsenki poter', svyazannykh s realizatsiei ugroz i uyazvimostei dlya informatsionnykh sistem // Sbornik materialov II vseukrainskoi nauchno-tekhnicheskoi konferentsii studentov, aspirantov i molodykh uchennykh «Informatsionnye upravlyayushchie sistemy i komp'yuternyi monitoring (IUS ta KM-2010)». Donetsk: DonNTU, 2011. T.1, s. 260-263.

11. Sadikov O. N. Ubytki v grazhdanskom prave Rossiiskoi Federatsii. M.: Statut, 2009. c. 9.

12. Ilyushina M. N., Chelyshev M. Yu., Sitdikova R. I. Kommercheskie sdelki: teoriya i praktika: Uchebno-prakticheskoe posobie / Pod obshch. red. M. N. Ilyushinoi. M.: RPA MYu RF, 2005. S. 147–154.

13. Kodeks Rossiiskoi Federatsii ob administrativnykh pravonarusheniyakh [Elektronnyi resurs]: [federal'nyi zakon : ot 30.12.2001 N 195-FZ, v red. ot ot 28.11.2015g.] – Rezhim dostupa : www.consultant.ru (data obrashcheniya: 09.12.2015)

УДК 004.056.53

Оценка ущерба от правонарушений в информационной сфере

[1] Наталья Михайловна Зайцева
[2] Руслан Артурович Нурдинов

[1] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: zaytsevanm@yandex.ru
[2] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: nurdinov.ra@mail.ru

Аннотация. В данной статье показана важность оценки ущерба при расследовании правонарушений. Определены нарушаемые свойства информационных активов от различных правонарушений в информационной сфере. Рассмотрены основные способы количественной оценки ущерба от реализации угроз, предлагаемые в методиках анализа рисков. Предложена методика, которая позволяет осуществлять количественную оценку ущерба от правонарушений в информационной сфере, приводящих к нарушению конфиденциальности, целостности и доступности информационных активов.

Ключевые слова: информация, правонарушение, размер ущерба, количественная оценка рисков, свойства информации, потери.