ОЦЕНКА УЩЕРБА ПОЛЬЗОВАТЕЛЮ ОТ КИБЕРПРЕСТУПНОСТИ В ЗАРУБЕЖНЫХ СТРАНАХ

ESTIMATION OF DAMAGE TO THE USER FROM CYBERCRIME IN FOREIGN COUNTRIES

B. Shvyrev

Summary. The paper provides an overview of foreign literature devoted to the study of the magnitude and structure of damage caused by cybercrime to an individual user of information systems. The literature extensively describes the damage from cyberthreats against firms and enterprises. This dynamic is typical both for Russia and for foreign countries. There are a number of objective difficulties with collecting information on all incidents and incidents caused by cybercrime against the user. The question of processing the information received is also relevant. The main problem of analyzing the damage from cybercrime is caused by a small amount of initial data, which is combined into a single array of various sources.

The paper proposes to treat the array as multidimensional. Measurable values of damage from cybercrime are heterogeneous, hard-to-formalize values.

For data analysis, both the traditional extrapolation method and the probabilistic approach to damage calculation are used.

Comparison of damage statistics to the user in Europe and the US is expressed by comparable numerical values, but not always the same interpretation. The article highlights the importance of developing methods for analyzing disparate data on damage from cybercrime, taking into account the experience of researchers from foreign countries.

Keywords: damage from cybercrime, categories of costs for cybercrime, operational risks, identity theft.

Швырев Борис Анатольевич
К.ф.-м.н., в.н.с., ФКУ Научно-исследовательский институт ФСИН России
bor2275@yandex.ru

Аннотация. В работе приводится обзор зарубежной литературы посвященной исследованию величины и структуры ущерба, наносимого киберпреступностью индивидуальному пользователю информационных систем. В литературе широко представлено описание ущерба от киберугроз относительно фирм и предприятий. Такая динамика характерна как для России, так и для зарубежных стран. Существует ряд объективных трудностей со сбором информации о всех инцидентах и происшествиях, вызванных киберпреступностью по отношению пользователя. Так же актуален вопрос о обработке полученной информации. Основная проблема анализа ущерба от киберпреступности обусловлена малым количеством исходных данных, которые объединяют в единый массив из разнообразных источников.

В работе предлагается рассматривать массив как многомерный. Измеряемые значения ущерба от киберпреступности являются разнородными трудно формализуемыми величинами.

Для анализа данных используются как традиционный метод экстраполяции результатов, так и вероятностный подход к расчету ущерба.

Сравнение статистик величины ущерба пользователю в Европе и США выражается сравнимыми числовыми значениями, но не всегда имеют одинаковую трактовку. В статье отмечается важность развития методов анализа разнородных данных об ущербе от киберпреступности с учетом опыта исследователей из зарубежных стран.

Ключевые слова: ущербе от киберпреступности, категории затрат на киберпреступность, операционные риски, кража личных данных.

Оценка стоимости киберпреступности одинаково сложная задач, как и сбор и анализ статистических данных об ущербе от киберпреступности в отношении индивидуального пользователя или общества в целом. В настоящее время основной подход к расчету ущерба основываются на экстраполяции результатов, полученных на малом объеме выборок или точечных значениях на все общество или социум в целом. Иногда это подход приводит к весьма значимым результатам способным шокировать общественность, так в 2012 году аналитики оборонного ведомства Великобритании озвучили оценку общей стоимости киберпреступности в Великобритании в 27 миллиардов долларов в год [1].

Основная проблема анализа ущерба от киберпреступности обусловлена малым количеством исходных данных, которые объединяют в единый массив из разнообразных источников. Целесообразно рассматривать этот массив как многомерный. Измеряемые значения ущерба от киберпреступности являются разнородными трудно формализуемыми величинами. Формируется сложная задача сведения потока данных и значений, описывающих разнородную информацию относительно ущерба от киберпреступности, в единый массив доступный для математической обработки и определения характеристик и зависимостей. Так же отмечается недостаточное количество данных по ряду критериев,

что уже гарантированно приводит к возникновению аномальных ошибок. Наибольшая сложность возникает с единичными выбросами значений измеряемый параметров, которые сильно искажают и преувеличивают результаты.

Анализ зарубежной литературы показал, что оценка отдельных затрат и их объединение на разных уровнях не всегда обеспечивают точную совокупную стоимость киберпреступности. Даже если объединение разнородных данных выполнено удовлетворительно, это приводит только к общей оценке для конкретного типа киберугроз. Так, опрос среди коммерческих фирм может привести к получению результата ущерба от киберпреступности только на уровне фирм. Он не учитывает оказываемого влияния на потребителей, затраты на правоохранительную деятельность или другие последствия. Достаточно часто исследователи просто экстраполируют потери на уровне фирм, чтобы оценить общую потерю общества. Но многие потери на уровне фирмы не являются убытками для общества.

В статье [2] предлагается подход, обеспечивающий основу для систематизации определения затрат на киберпреступность. Авторы выделяют три основные категории затрат: прямые потери, косвенные потери и затраты на защиту информации. Кроме того, они отделяют киберпреступления от вспомогательной инфраструктуры информационной системы. Они используют свою структуру для упорядочения категорий затрат и предоставляют оценки существующих источников данных.

Вне контекста киберпреступности относительно пользователя, располагается хотя и несколько связанная с ней другая проблема измерения и оценки совокупных потерь, возникающих в финансовых учреждениях в отношении операционных рисков. Эта проблема лежит в основе страховой отрасли, но также касается финансовых учреждений в контексте управления операционными рисками. Операционные риски могут возникать, например, из-за неспособности управлять бизнес-процессами и обеспечения информационной безопасности с учетом знаний, и опыта IT -специалистами. В статье [3] предложен вероятностный подход к анализу ущерба от киберпреступности, в котором используется распределения вероятности потерь — это простой способ измерения операционного риска с использованием частоты и серьезности данных о потерях. Он имеет три основных компонента: частотное распределение потерь, распределение вероятности степени тяжести потерь и совокупное распределение вероятности потерь, которое объединяет два предыдущих. Распределения вероятности для моделирования потерь киберпреступности структурно сопоставимы с распределения вероятности потерь.

В работе [4] описываются методы распределения потерь при обследовании, используемом при управлении операционным риском — это параметрическое распределение вероятности, метод теории экстремальных значений и оценка капитала на основе непараметрической эмпирической выборки. Для моделирования тяжести потерь рассматриваются различные одно- и двухпараметрические распределения вероятности, в том числе такие как: Гамма распределение, усеченное логнормальное распределение и распределение Вейбула.

Известны исследования, проведенные авторами в [5], а также опубликованные отчеты профильных организаций в области информационной безопасности [6,7] и сведения государственных организации [8], в которых сообщается о понесенных предприятиями расходах от киберпреступности, информация ущерба, понесенного обычным потребителем крайне мала.

В США Harrell [9,10] провел опрос большого числа респондентов более чем 60000 человек относительно понесенного ущерба от кражи личных данных. Опрос показал, что в 2014 году 7% пользователей США стали жертвой кражи личных данных. Наиболее распространенные угрозы были связаны с кредитными картами и банковскими счетами. Опрос предусматривал прямые и косвенные издержки для жертв. Разделялась непосредственная потеря денег от дополнительных расходов, с которыми сталкиваются жертвы киберпреступления, таких как судебные издержки, возврат товара или другие расходы. Средняя финансовая потеря пострадавших, которые подверглись кражи личных данных за последние 12 месяцев, составляет 1343 доллара США, при этом отмечается медиана выборки 300 долларов США, что свидетельствует о значительном разбросе потерь денежных средств.

В ЕС специальная организация Eurobarometer является самым важным ресурсом по предоставлению информации о киберпреступности [11]. Организация регулярно представляет отчеты о киберпреступности, типах кибератак и понесенных издержек для всех 28 государств-членов ЕС. Отдельно выделяются некоторые формы кражи личных данных среди других типов, таких как мошенничество в Интернете, мошенничество, вымогательство и заражение вредоносными программами. 7% пользователей Интернета в ЕС в 2014 году стали жертвами кражи идентификационных данных [11]. Можно отметить схожесть числовых значений кражи личной информации в ЕС и США, но отмеченное сходство таковым не является так как определялась по различным критериям.

Так проведенные исследования в [12] рассмотрели широкий спектр вопросов, связанных с киберпреступ-

ностью и кибербезопасностью для потребителей в Великобритании. Основное внимание уделено в ней приблизительной оценке затрат, вызванных вымогательством денег и личной информации после заражения персональных компьютеров.

В 2015 году Германский институт экономических исследований (DIW Berlin) сообщил, что ежегодные затраты на киберпреступность для потребителей в Германии составляют 3,4 млрд. Евро, что составляет 0,1% ВВП или 41,5 евро на одного гражданина [13].

Представленные данные показывают большую сумму потерянных из-за киберпреступлений денежных средств, что в Европе, что в США. Отдельного внимания заслуживает различие в расчетах ущерба от киберпреступлений относительно личных данных в Европе и США. Озвученные суммы 3,4 млрд.евро и 27 млрд.долларов в год кажутся астрономическими и мало сопоставимыми друг с другом и действительностью. Отражение действительности и анализ истинных структурных издержек, вызванных киберпреступлениями является важной задачей не только государственных организаций, но и профессианальных объединений и предприятий в области информационной безопасности. Приведенные подходы, используемые исследователями зарубежных стран, имеют одновременно свои сильные стороны и слабые выражаемые в неполноте описания явлений. Развитие методов анализа разнородных данных об ущербе от киберпреступности является перспективным направлением исследований в котором необходимо учитывать опыт исследователей из зарубежных стран.

ЛИТЕРАТУРА

1. Detica, Office of Cyber Security, and Information Assurance. The cost of cyber crime. Technical report, 2011. URL www.cabinetoffice.gov.uk/ resource-library/cost-of-cyber-crime.
2. Ross Anderson, Chris Barton, Rainer Bohme, Richard Clayton, Michel J. G. Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the cost of cybercrime. In Rainer Boohme, editor, Economics of Information Security and Privacy, pages 265–300. Springer Berlin, Heidelberg, 2013.
3. Antoine Frachot, Olivier Moudoulaud, and Thierry Roncalli. Loss distribution approach in practice. pages 527–554. Risk Books, London, 2004.
4. Kabir Dutta and Jason Perry. A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital. FRB of Boston Working Paper, 2006.
5. PwC. Global State of Information Security survey. Technical report, PricewaterhouseCoopers, 2015. URL www.pwc.com/gx/en/issues/ cyber-security/information-security-survey.
6. Kaspersky Lab. Global IT Security Risks Survey. Technical report, 2015. URL www.media.kaspersky.com/en/business-security/ it-security-risks-survey-2015.pdf.
7. Ponemon Institute, 2015, Cost of Cyber Crime Study: Global. Technical report, 2015. URL www8.hp.com/us/en/software-solutions/ ponemon-cyber-security-report/.
8. Federation of small businesses. Cyber security and fraud: The impact on small businesses, 2013. URL www.fsb.org.uk/policy/assets/fsb_ cyber_security_and_ fraud_paper_final.pdf.
9. Erika Harrell. Victims of identity theft, 2012. Technical report, Bureau of Justice Statistics (BJS) and US Deptarment of Justice and Office of Justice Programs of the United States of America, 2012.
10. Erika Harrell. Victims of identity theft, 2014. Technical report, Bureau of Justice Statistics (BJS) and US Deptarment of Justice and Office of Justice Programs of the United States of America, 2015.
11. European Commission. Special Eurobarometer 404 Cyber security. Wave EB79.4, 2013, 2015.
12. Julio Hernandez-Castro and Eerke Boiten. Cybercrime prevalence and impact in the UK. Computer Fraud & Security, 2014(2):5–8, 2014.
13. Johannes Rieckmann and Martina Kraus. Tatort internet: Kriminalitat verursacht biirgern schaden in milliardenhohe. DIW Wochenbericht, 82: 295–301, 2015.

Журнал «Современная наука: актуальные проблемы теории и практики»