УДК 341.9; 343.9.018.3

Н.И. Глухов[1], С.И. Носков[1], П.Ю. Попов[1]

[1]Иркутский государственный университет путей сообщения, г. Иркутск

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДИНАМИКИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Аннотация. При изучении закономерностей, сложившихся в сфере киберпреступности, использован статистический материал отдела «К» ГУ МВД России по Иркутской области. Проведен тщательный анализ приведенных статистических данных, в ходе которого решен ряд частных задач: путем проведения конкурса моделей подобрана наиболее адекватная форма связи между независимыми переменными из множества ее альтернативных вариантов (их общее число составляет несколько сотен), оценены численные значения параметров, проведена верификация построенной модели на основе использования известных количественных критериев. При проведении этого анализа были задействованы эффективные регрессионные методы и соответствующие программные средства.

Ключевые слова: киберпреступность, математическая модель, информационная безопасность, компьютерная информация, регрессионные методы исследования.

N.I. Gluchov[1], S.I. Noskov[1], P.Y. Popov[1]

[1]Irkutsk State University of Communications, Irkutsk

MATHEMATICAL MODEL OF DYNAMICS COMPUTER CRIMES

Abstract. In the study of the patterns prevailing in the field of cybercrime, used statistical material of the department "K" of the State Ministry of Internal Affairs of Russia for the Irkutsk region. A thorough analysis of the statistical data was carried out, during which a number of particular problems were solved: by holding a model competition, the most adequate form of communication between independent variables from the set of its alternative variants was selected (their total number is several hundred), the numerical values of parameters were evaluated, the constructed model was verified based on the use of well-known quantitative criteria. In conducting this analysis, effective regression methods and appropriate software were used.

***Keywords*:** cybercrime, mathematical model, information security, computer information, regression research methods.

Введение. Исследование проблемы киберпреступности приобрело в наше время особую актуальность. Причиной тому является в том числе увеличение количества и разнообразия компьютерных преступлений, а также то, что они становятся все более сложными и изощрёнными.

Необходимо отметить, что вместе с компьютерными преступлениями также активно развиваются и иные компьютерные инциденты, которые способны причинить существенный вред обладателю информации, однако исследование проблемы именно компьютерных преступлений является особо актуальным и объясняется тем, что по степени своей общественной опасности, по размеру потенциального ущерба, который может быть причинен обладателю информации среди прочих последние представляют наибольшую опасность для информационной безопасности как в целом, так и для каждого человека в отдельности.

Таким образом рассматривать проблемы информационной безопасности в современном мире без изучения темы компьютерных преступлений на наш взгляд было бы не верно.

Еще одной важной особенностью компьютерных преступлений отличающей их от других компьютерных инцидентов является то, что такие события очень подробно регламентированы правовыми актами, а именно регламентированы вопросы выявления, предупреждения, пресечения, раскрытия преступлений и дальнейшего их расследования. Кроме того, относительно компьютерных преступлений регламентировано ведение единой государственной статистики, позволяющей анализировать положение дел в данной области.

Указанные обстоятельства позволяют предположить, что для более глубокого исследования темы компьютерных преступлений и их динамики необходимо рассмотреть этот вопрос помимо общего подхода и с точки зрения изучения закономерностей сложившихся в сфере компьютерных преступлений на основе статистического материала при помощи математической модели.

В силу того, что современные информационные технологии не позволяют создавать системы защиты информации, которые были бы способны гарантировать полную защищенность, то совершено очевидно, что вторжение (компьютерный инцидент) в то или иное информационное пространство — это вопрос времени и/или необходимости для злоумышленника (т.е. насколько важно это для злоумышленника, какие ресурсы он готов для этого задействовать).

По указанной причине динамика компьютерных преступлений зависит в том числе от того насколько грамотно будут реализовываться процедуры раскрытия и расследования компьютерных преступлений, документирования следов преступлений, доказывания виновности причастных к ним лиц и установления обстоятельств, имеющих значение для раскрытия и дальнейшего расследования таких преступлений. Правильное документирование следов таких преступлений в свою очередь является очень важным этапом в обеспечении информационной безопасности поскольку от того на сколько грамотно будут зафиксированы и задокументированы их следы будет зависеть как перспектива установления виновных лиц, их мотивов и целей, так и будут ли иметь такие документы юридическую силу (силу доказательства в суде).

Как показывает практика работы отдела «К» ГУ МВД России по Иркутской области большинство организаций не готовы к такого рода инцидентам. Более чем в 70% организаций-респондентов отсутствуют инструкции о действиях в случае инцидентов. Более 85% организаций-респондентов не имеют инструкций о сохранении и правильном документировании доказательств вторжения для последующего представления в правоохранительные органы.

Одновременно с развитием информационных технологий увеличивается число пользователей различными информационными (компьютерными) системами. На сегодняшний день прослеживается прямая зависимость роста компьютерных преступлений от увеличения общего количества пользователей компьютерными технологиями. Так, число пользователей сети Интернет в России, выходящих в сеть хотя бы раз за сутки, составляет 48% (56,3 млн. человек) населения. Годовой прирост интернет-пользователей, выходящих в сеть хотя бы раз в месяц, составил 7%, а для суточной аудитории данный показатель равен 12% [11, с. 310].

Рост преступлений в указанной сфере во многом связан с появлением новых информационных технологий, средств связи, социальных сетей, в которых компьютерная информация становится объектом преступного посягательства.

Необходимо иметь в виду и тот факт, что с ростом преступлений в сфере компьютерной информации также растет уровень латентности (скрытности) указанных преступлений. Одновременно с развитием информационных технологий в целом, развиваются и технологии, позволяющие обеспечивать преступникам свою анонимность при совершении противоправных действий, в частности скрывать следы своих действий, а в случае их обнаружения – удалять такие следы. Таким образом становится все сложнее выявлять, раскрывать и в дальнейшем расследовать соответствующие преступления.

По данным МВД России, наиболее криминогенной группой населения, выделяемой в статистике, являются лица в возрасте от 30 до 49 лет: их доля в структуре преступности доходит до 47 %. Последние совершают около 36 % особо тяжких и 35 % тяжких преступлений. Преступления в сфере компьютерной информации по этому признаку отличаются от среднестатистических. Так, возраст преступника, совершающего преступления указанной категории, составляет от 18 до 30 лет [11, с. 311].

В науке выделяют и другие причины роста компьютерных преступлений, а именно цифрового неравенства [12, с. 139]. Оно проявляется и в том, что лицензионное программное обеспечение в России является не доступным для большого количества населения по причине дороговизны. Вместе с тем, для большого количества пользователей не является осудительным использование контрафактных компьютерных программ. По указанной причине на «сером» рынке появилось огромное количество способов приобретения нелицензионных программ. Такое программное обеспечение в несколько раз дешевле лицензионного аналога, а в большинстве случаев совершенно бесплатно. Для того, чтобы лицензионная программа стала бесплатной ее нужно «взломать», то есть использовать вредоносную компьютерную программу, заведомо предназначенную для нейтрализации средств защиты компьютерной информации. Такие действия подпадают под признаки состава преступления, предусмотренного ст. 273 УК РФ.

Фактором, влияющим на рост компьютерных преступлений, является и то обстоятельство, что в нелицензионном программном обеспечении очень часто вмонтированы вредоносные компьютерные программы, предназначенные для управления (администрирования) компьютером пользователя без его ведома. Устанавливая, к примеру, нелицензионный «Windows», пользователь может стать частью сети «Ботнет», то есть на компьютер пользователя будет скрыто установлено программное обеспечение, позволяющее злоумышленнику выполнять различные действия, используя инфицированный компьютер, например, для совершения ddos-атак.

Еще одной разновидностью цифрового неравенства являющейся причиной роста компьютерных преступлений является существующий и постоянно увеличивающийся разрыв между преступниками и их жертвами в вопросе информационной грамотности, в области знаний по защите информации. Проявление цифрового неравенства заключается в небрежном неграмотном отношении к цифровой информации, выражающемся в установлении простых паролей для защиты информации и нарушении сроков их использования, либо вообще в отсутствии средств защиты цифровой информации. Очень часто преступникам удается достичь своих противоправных целей по причине полной безграмотности населения в вопросах защиты информации.

Изучение закономерностей, сложившихся в сфере киберпреступности, будем проводить на статистическом материале Иркутской области. В табл. 1 приведены поквартальные данные по возбужденным уголовным делам по статьям, имеющим прямое или опосредованное отношение к рассматриваемой проблеме, за 2016-2018 г.г.

Таблица 1.

Количество возбужденных уголовных дел по компьютерным преступлениям в Иркутской области

Период/ Статья УК РФ	*Ст. 272 X1*	*Ст. 273 X2*	*Ст. 159.6 X3*	*Ст. 183 X4*	*Ст. 137 X5*	*Ст. 138 X6*
1кв. 2016	1	2	20	0	2	4
2 кв. 2016	14	3	17	20	2	2
3 кв. 2016	0	5	18	0	3	1
4 кв. 2016	26	0	30	25	2	1
1 кв. 2017	2	2	14	2	0	3
2 кв. 2017	3	0	17	3	0	0
3 кв. 2017	2	1	15	4	0	0
4 кв. 2017	0	2	13	0	4	0
1 кв. 2018	2	4	1	0	2	0
2 кв. 2018	7	1	2	0	2	11
3 кв. 2018	14	2	1	0	3	7
4 кв. 2018	1	0	0	0	5	0

Приведем формулировки самих статей.

Статья 272. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Статья 273. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Статья 159.6. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Статья 183. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом. Незаконные разглашение или использование таких сведений, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Статья 137. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Статья 138 Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

С точки зрения взаимосвязи приведенных выше преступлений необходимо выделить ст. 272 УК РФ (неправомерный доступ к охраняемой законом компьютерной информации, повлекшие определенные последствия). Указанное преступление на практике очень часто выступает в роли одного из незаконных способов для совершения других преступлений, а именно преступлений, предусмотренных ст.ст. 137, 138, 183, 159.6 УК РФ. На сегодняшний день почти во всех сферах жизнедеятельности человека информация (личная, банковская, коммерческая тайна, тайна связи и др.) хранится, обрабатывается и передается при помощи информационных технологий в виде компьютерной информации, соответственно для того чтобы преступнику «добраться» до такой информации ему необходимо предварительно осуществить неправомерный доступ к охраняемой законом и интересующей его компьютерной информации, с целью реализации своего преступного умысла. Значительно реже совершение преступления, предусмотренного ст. 272 УК РФ является самой целью. Таким образом рост или падение числа преступлений, предусмотренных ст.ст. 137, 138, 183, 159.6 УК РФ в значительной степени влияет на динамику преступлений, предусмотренных ст. 272 УК РФ.

При проведении тщательного анализа приведенных статистических данных необходимо было решить ряд важных частных задач: выделение из всего перечня X1,…., X6 зависимой (выходной) и независимых (входных)переменных; путем проведения конкурса моделей подобрать наиболее адекватную форму связи между независимыми переменными из множества ее альтернативных вариантов (их общее число составляет несколько сотен), оценить численные значения параметров, провести верификацию построенной модели на основе использования известных количественных критериев. При проведении этого анализа были задействованы эффективные регрессионные методы и соответствующие программные средства, описанные, в частности, в работах [1-10].

Результатом проведенных для решения этих задач исследований стала следующая регрессионная модель:

$$X1=0.88+0.034X3X4+0.27X2X5X6, \quad (1)$$

$$R=0.94,\ F=67.8,\ DW=2.2,\ E=1.45,\ ,T=(0.11,\ 11.27,\ 5.23).$$

Здесь R – коэффициент множественной детерминации, F – критерий Фишера, DW – критерий Дарбина-Уотсона, E – средняя относительная ошибка аппроксимации, $K_{СП}$ – критерий согласованности поведения, T – вектор значений критерия Стьюдента для параметров уравнения.

Анализ модели (1) позволяет сделать ряд важных выводов.

Судя по сформированной в результате проведения конкурса моделей правой части регрессионного уравнения (1), независимые переменные X2, X3, X4, X5, X6 не просто оказывают существенное влияние на выходной фактор X1, а это влияние имеет еще и выраженный совместный групповой характер, что позволяет представить весь набор этих переменных в виде совокупности двух групп (X3, X4), (X2, X5, X6). Это обстоятельство указывает на некую «родственность» переменных внутри каждой группы.

Преступление, предусмотренное ст. 273 УК РФ также может выступать в качестве способа для совершения преступлений, предусмотренных ст.ст. 137, 138, 183, 159.6 УК РФ однако в меньшей степени (чем преступление, предусмотренное ст. 272 УК РФ) в силу того, что оно требует от злоумышленника гораздо большей подготовки и знаний в области компьютерных технологий, а также является гораздо более дорогостоящим способом и как правило такой способ используется для более глобальных целей.

Взаимное влияние преступлений, предусмотренных ст. 272 УК РФ и ст. 273 УК РФ представляется незначительным, однако встречаются ситуации, когда каждое из указанных преступлений может выступать по отношению к другому способом достижения конечной цели и/или выполнять вспомогательную функцию. Совершение преступления, предусмотренного ст. 273 УК РФ значительно чаще, чем совершение преступления, предусмотренного ст. 272 УК РФ является самой целью и следовательно в значительно меньшей степени зависит от динамики преступлений, предусмотренных ст.ст. 137, 138, 183, 159.6 УК РФ.

Вместе с тем, необходимо отметить очень важный юридический аспект, заключающийся в следующем, в тех ситуациях, когда преступления, предусмотренные ст. 272 УК РФ и ст. 273 УК РФ с точки зрения механизма совершения преступных действий, выступают в качестве способа совершения других указанных выше преступлений, они подлежат обязательной квалификации как самостоятельные преступление в каждом случае.

1. Положительность параметров модели указывает на возрастание значений зависимой переменной X1 при возрастании каждой из независимых.
2. Модель (1) обладает весьма высокой адекватностью, на что указывают высокие значения верификационных критериев.
3. Последнее обстоятельство предполагает вполне обоснованную возможность эффективного применения модели (1) для решения широкого круга прогнозных задач.

В заключении необходимо отметить, что в России очевидно наблюдается рост компьютерных преступлений в качестве основных причин и условий их совершения можно выделить следующие: внедрение компьютерных технологий почти во всех сферах жизнедеятельности человека; рост числа пользователей информационных технологий; увеличение объемов компьютерной информации; усиление цифрового неравенства; упущения и недочеты организационного характера; фактическая безнаказанность лиц, совершивших компьютерные преступления по причине высокой степени анонимности; высокая латентность и многообразие таких преступлений.

Рост подобных преступлений оказывает негативное влияние на информационную безопасность, которая является составной частью национальной безопасности РФ. Стремительное развитие информационных технологий неизбежно приводит к росту разного рода негативных воздействий (в том числе преступных) на всевозможные информационные системы.

Такая динамика компьютерных преступлений говорит о том, что сегодня необходимо постоянно и своевременно актуализировать, и улучшать средства и методы информационной безопасности для защиты интересов государства, общества и граждан. Перед

правоохранительными органами по указанной причине стоит задача по противодействию всему многообразию компьютерных преступлений, для достижения которой необходимо в полной мере использовать передовые достижения в области информационных технологий.

Для этих целей, а также для полного и всестороннего исследования проблем компьютерных преступлений на наш взгляд представляется необходимым изучение закономерностей, сложившихся в сфере компьютерных преступлений, на основе статистического материала при помощи математической модели.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Дрейпер Н., Смит Г. Прикладной регрессионный анализ. М.: Финансы и статистика. 1981. Т.1. 366 с., Т. 2. 351 с.

2. Носков С.И. Технология моделирования объектов с нестабильным функционированием и неопределенностью в данных. Иркутск: Облинформпечать. - 1996. 320 с.

3. Носков С.И., Баенхаева А.В. Множественное оценивание параметров линейного регрессионого уравнения // Современные технологии. Системный анализ. Моделирование. 2016. № 3 (51). С. 133-138.

4. Носков С.И., Быкова О.В., Некипелова О.Е., Соколова Л.Е. Возможный способ поиска компромиссного решения в задаче линейного программирования с векторной целевой функцией // Фундаментальные исследования. 2014. № 6-3. С. 502-505.

5. Носков С.И. Критерий «согласованность поведения» в регрессионном анализе //Современные технологии. Системный анализ. Моделирование. 2013. № 1 (37). С. 107-110.

6. Лакеев А.В., Носков С.И. Метод наименьших модулей для линейной регрессии: число нулевых ошибок аппроксимации // Современные технологии. Системный анализ. Моделирование. 2012. № 2 (34). С. 48-50.

7. Носков С.И. Проблема единственности Парето-оптимального решения в задаче линейного программирования с векторной целевой функцией // Современные технологии. Системный анализ. Моделирование. 2011. № S-4 (32). С. 283-285.

8. Носков С.И. Точечная характеризация множества Парето в линейной многокритериальной задаче // Современные технологии. Системный анализ. Моделирование. 2008. № 1 (17). С. 99-101.

9. Носков С.И. L-множество в многокритериальной задаче оценивания параметров регрессионных уравнений // Информационные технологии и проблемы математического моделирования сложных систем. 2004. № 1. С. 64-69.

10. Носков С.И. Построение эконометрических зависимостей с учетом критерия «согласованность поведения» // Кибернетика и системный анализ. 1994. № 1. С. 177-181.

11. Родивилин И.П. Преступления в сфере компьютерной информации: состояние, динамика, тенденции, особенности личности преступника // Проблемы современного российского законодательства. 2015. С. 310-312.

12. Родивилин И.П. Цифровое неравенство – угроза безопасности Российской Федерации // Проблемы обеспечения национальной безопасности в контексте изменения геополитической ситуации. 2017. С. 139-143.

REFERENCES

1. Draper N., Smith G. *Applied regression analysis.* M .: Finance and statistics. 1981. T. 1. 66 s., T. 2.351 s.

2. Noskov S.I. *Technology for modeling objects with unstable functioning and data uncertainty.* Irkutsk: Oblinformpechat. - 1996.320 s.

3. Noskov S.I., Baenkhaev A.V. *Multiple estimation of linear regression equation parameters* // Modern technologies. System analysis. Modeling. 2016. No. 3 (51). S. 133-138.

4. Noskov S. I., Bykova O. V., Nekipelova O. E., Sokolova L. E. *A possible way to find a compromise solution in a linear programming problem with a vector objective function* // Fundamental Research. 2014. No. 6-3. S. 502-505.

5. Noskov S.I. *The criterion of "consistency of behavior" in the regression analysis* // Modern technologies. System analysis. Modeling. 2013. No. 1 (37). S. 107-110.

6. Lakeev A.V., Noskov S.I. *The least module method for linear regression: the number of zero approximation errors* // Modern Technologies. System analysis. Modeling. 2012. No. 2 (34). S. 48-50.

7. Noskov S.I. *The uniqueness problem of the Pareto-optimal solution in a linear programming problem with a vector objective function* // Modern Technologies. System analysis. Modeling. 2011. No. S-4 (32). S. 283-285.

8. Noskov S.I. *Point characterization of the Pareto set in a linear multicriteria problem* // Modern Technologies. System analysis. Modeling. 2008. No. 1 (17). S. 99-101.

9. Noskov S.I. *L-set in the multicriteria problem of estimating the parameters of regression equations* // Information technologies and problems of mathematical modeling of complex systems. 2004. No. 1. S. 64-69.

10. Noskov S.I. *Construction of econometric dependencies taking into account the criterion of "consistency of behavior"* // Cybernetics and system analysis. 1994. No. 1. S. 177-181.

11. Rodivilin I.P. *Crimes in the field of computer information: state, dynamics, trends, characteristics of the identity of the offender* // Problems of modern Russian legislation. 2015.S. 310-312.

12. Rodivilin I.P. *Digital inequality is a threat to the security of the Russian Federation* // Problems of ensuring national security in the context of a changing geopolitical situation. 2017.S. 139-143.

Информация об авторах

Глухов Николай Иванович – директор департамента информационной безопасности транспортной инфраструктуры Иркутского государственного университета путей сообщения, кандидат экономических наук, доцент, г. Иркутск, Российская Федерация, e-mail: gni1953@mail.ru.

Носков Сергей Иванович – профессор кафедры «Информационные системы и защита информации» Иркутского государственного университета путей сообщения, доктор технических наук, профессор, г. Иркутск, Российская Федерация, e-mail: sergey.noskov.57@mail.ru.

Попов Павел Юрьевич – магистрант Иркутского государственного университета путей сообщения, г. Иркутск, Российская Федерация, e-mail: legato.irk@mail.ru.

Information about authors

Glukhov, Nikolay I. – Director of the Department of Information Security of Transport Infrastructure of Irkutsk State University of Communications, Ph.D., Associate Professor, Irkutsk, Russian Federation; e-mail: gni1953@mail.ru.

Noskov, Sergey I. - Professor, Department of Information Systems and Information Protection, Irkutsk State University of Communications, Doctor of Technical Sciences, Professor, Irkutsk, Russian Federation, e-mail: sergey.noskov.57@mail.ru.

Popov, Pavel Y. – Undergraduate of Irkutsk State University of Communications, Russian Federation; e-mail: legato.irk@mail.ru.

Для цитирования

Глухов Н.И., Носков С.И., Попов П.Ю. Математическая модель динамики компьютерных преступлений // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №1(6). – С. 1-8. DOI: 10.26731/2658-3704.2020.1(6).1-8 – Режим доступа: http://ismm-

irgups.ru/toma/16-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 20.01.2020)

For citations

Gluchov N.I., Noskov S.I., Popov P.Y. Mathematical model of dynamics computer crimes // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2020. No. 1(6). P. 1-8. DOI: 10.26731/2658-3704.2020.1(6).1-8 [Accessed 20/01/2020]