УДК 519.862.6

А. С. Вергасов[1]

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

ПОВЕДЕНЧЕСКИЕ МОДЕЛИ ЗЛОУМЫШЛЕННИКОВ ПРИ КИБЕРАТАКАХ

Аннотация. В работе рассматривается проблема формирования моделей поведения злоумышленника при кибератаках. Модель поведения злоумышленника учитывает мотив, категорию жертв и объект атак. Классификация производится на основе модели нарушителя. Анализ конъектуры инцидентов, связанных с утечкой данных на территории всего мира, основывается на статистических данных компании InfoWatch.

Ключевые слова: информационная безопасность, модель нарушителя, модель поведения злоумышленника.

A.S. Vergasov[1]

[1] *Irkutsk State Transport University, Irkutsk, Russian Federation*

BEHAVIORAL MODELS OF CRIMINALS AT CYBER ATTACKS

Annotation. The paper considers the problem of forming patterns of behavior of an attacker during cyber attacks. The attacker's behavior model takes into account the motive, the category of victims and the object of attacks. The classification is based on the model of the intruder. Analysis of incidents related to data leakage throughout the world is based on statistics from InfoWatch.

Keywords: information security, intruder model, attacker behavior model.

Введение

Информация с каждым годом становится все более существенных активом в деятельности компаний и государственных учреждений. Ее защита от неконтролируемого распространения, изменения или уничтожения становится приоритетной задачей для служб безопасности.

Для более наглядного понимания роста проблем в данной сфере рассмотрим мировую динамику утечек информации. По аналитическим данным международной компании в сфере информационной безопасности InfoWatch [1] количество утечек информации в период с 2006 по 2018 год многократно увеличилось (рис. 1).

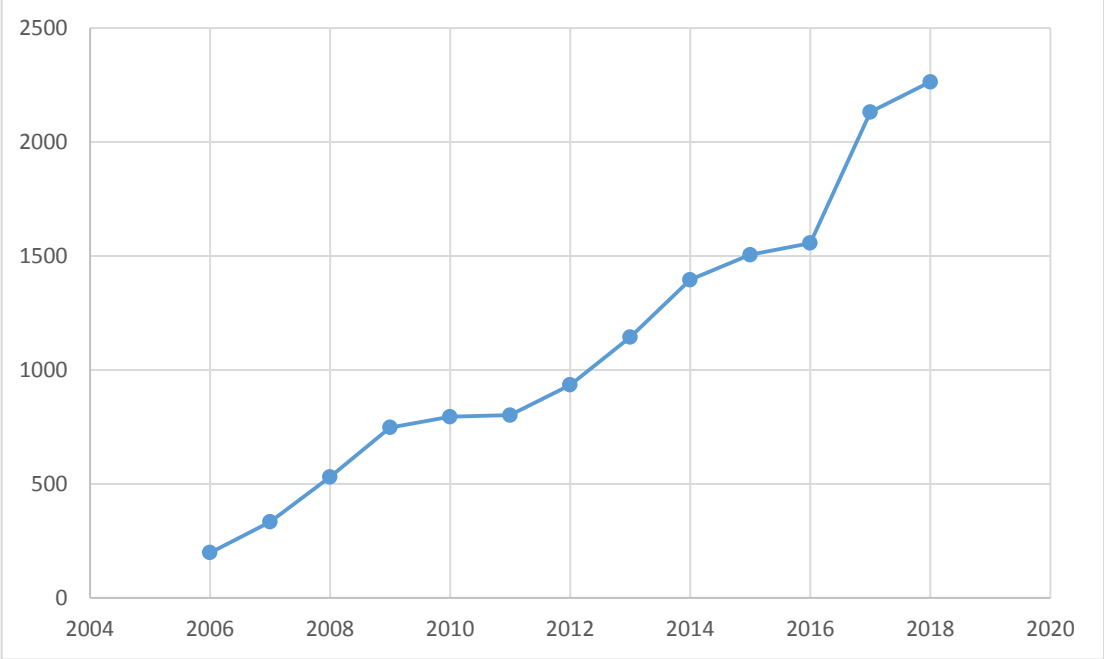

Рис. 1. Количество утечек информации в 2006-2018 гг.

При этом количество утекших данных за один инцидент также заметно выросло (рис.2).

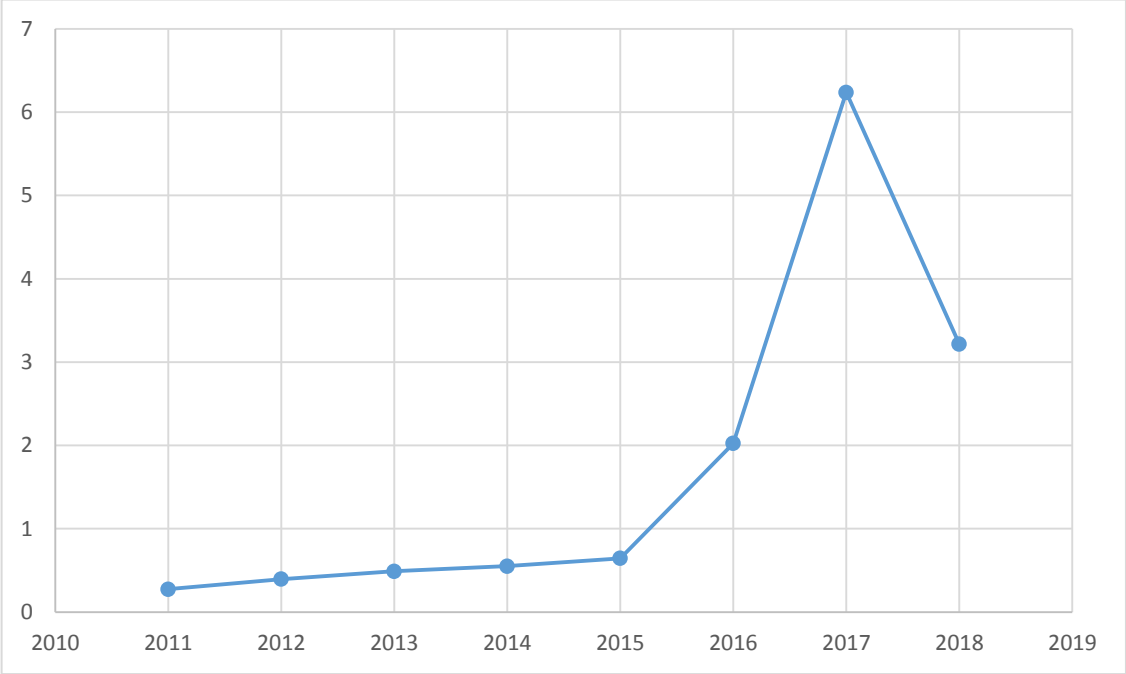

Рис. 2. Среднее количество утекших записей в одном инциденте 2011-2018 гг. (в млн. записей).

Приведенная статистика очевидным образом указывает на рост актуальности исследования данной проблемы.

Анализ статистических данных, приведенных в [2-11], позволяет сформировать факторное пространство при построении поведенческих моделей злоумышленников.

Факторное пространство.

1. Мотивы злоумышленников X1={x1,…,x4}:

x1 – получение данных;

x2 – финансовая выгода;

x3 – хактивизм;

x4 – проявления кибервойны.

2. Категории жертв X2={x5,…,x13}:

x5 – частные лица;

x6 – государственные учреждения;

x7 – финансовая отрасль;

x8 – медицинские учреждения;

x9 – сфера образования ;

x10 – онлайн-сервисы;

x11 – сфера услуг;

x12 – промышленные компании;

x13 – без привязки к конкретной отрасли, здесь учитываются гибридные масштабные атаки, затрагивающие несколько отраслей.

3. Объекты атак X3={x14,…,x19}:

x14 – инфраструктура;

x15 – веб-ресурсы;

x16 – пользователи;

x17 – мобильные устройства.;

x18 – IoT–техника);

x19 – банкоматы и POS-терминалы.

Более подробно каждый фактор рассмотрен в аналитических статьях компании Positive Technologies [2-11].

Модели атак.

Построение моделей возможных атак осуществлялось с использованием методики моделирования нарушителя, описанной в работе [12]. В соответствии с ней одними из существенных параметров в поставленной задаче, описывающими тип и качество нарушителя, являются:

M (motivation) – преднамеренность/случайность совершения преступления:

$$M = \begin{cases} 0, \text{не умышленный характер события} \\ 1, \text{умышленный характер события.} \end{cases}$$

Известно, что в 2018 году соотношение случайных и умышленных утечек составляет 84% и 16% соответственно.

P (place) – внутреннее/внешнее положение нарушителя относительно объекта атаки:

$$P = \begin{cases} 0, \text{внешний нарушитель} \\ 1, \text{внутренний нарушитель.} \end{cases}$$

Общеизвестно, что в 2018 году соотношение внутренних и внешних нарушителей составляет 64% и 36% соответственно.

Q (quality) – уровень нарушителя, принимающий значения от 0 до 7, в зависимости от его возможностей и уровня доступа: 0 – это внешний нарушитель с полным отсутствием знаний об уязвимостях, 7 - внутренний нарушитель с очень высоким уровнем доступа.

Распределение утечек за 2018 год соответствует соотношениям, приведенным на рис.3.

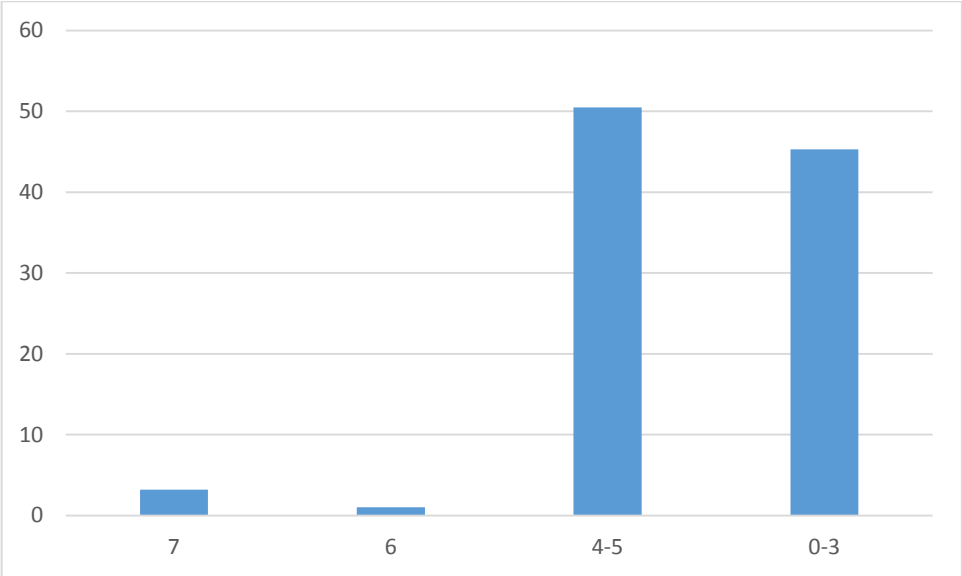

Рис. 3. Распределение утечек по уровню виновника за 2018 год.

Далее приводятся возможные модели атак, сгруппированные по типу нарушителя.

1. «Внешний злоумышленник». Этот тип нарушителя характеризуется следующими параметрами: $M = 1, P = 1, Q \in [0,3]$. Цель атаки такого нарушителя формируется в последнюю очередь после выбора жертвы, исходя из мотива. Может быть построена соответствующая модель:

$$X2 = F_2(X1), \quad (1)$$

$$X3 = F_3(X2, X1), \quad (2)$$

где $F_2(\cdot)$ и $F_3(\cdot)$ - регрессионные вектор-функции.

Известно, что в июне 2019 группа хакеров, предположительно представители китайской организации REDBALDKNIGHT, похитила конфиденциальную информацию компании Mitsubishi Electric. На начальном этапе злоумышленники получили доступ к учетной записи одного из сотрудников китайского филиала компании. Затем они расширили

доступ, подключившись к более чем десятку внутренних сетей компании, в том числе на территории Японии. В результате своей деятельности они повысили свой уровень доступа от 0 до 3 по шкале Q. Итоговая модель нарушителя выглядела следующим образом: $M=1, P=0, Q=3$. Добычей хакеров стала информация о кандидатах на трудоустройство в компанию и деловые документы, исключая информацию о деловых партнерах и оборонных контрактах.

Причинно-следственная цепочка поведения злоумышленника в данном случае, как одно из соотношений (1), (2), может быть представлена в виде:

$$\{x1, x12\} => x16.$$

В ноябре 2019 года группа хакеров взломала элемент инфраструктуры медицинской компании и получила доступ к персональным данным, после чего успешно шантажировала руководство фирмы.

Причинно-следственная цепочка поведения злоумышленника в этом случае имеет вид:

$$x2 => x1 => x8 => x14.$$

2. «Внутренний злоумышленник (инсайдер)». Этот тип нарушителя характеризуется следующими параметрами: $M=1, P=1, Q\in[0,7]$. Цель атаки формируется в последнюю очередь как следствие информированности об уязвимостях компании, в которой работает нарушитель. Может быть построена соответствующая модель:

$$X1 = F_1(X2, X3), \quad (3)$$

где $F_1(\cdot)$ – регрессионная вектор-функция.

Примером может служить продажа персональных данных держателей кредитных карт Сбербанка в сентябре 2019 года. В ходе расследования инцидента выяснилась преднамеренность утечки данных. Инцидент произошел по вине сотрудника банка с использованием санкционированных средств и действий 24 августа 2019 года. Поведение нарушителя укладывается в рассматриваемую модель. Изначально, устроившись на работу, он со временем получил доступ к базе персональных данных, нашел возможность выгрузить ценную информацию, после чего совершил кражу с целью дальнейшей продажи. Исходя из обнародованных данных, злоумышленник характеризуется следующими параметрами: $M=1, P=1, Q\geq 5.$

Причинно-следственная цепочка поведения злоумышленника примет вид:

$$\{x7, x14\} => x2.$$

В мае 2019 года в сеть были выложены базы данных клиентов «ОТП-банка», «Альфа-Банка» и «ХКФ-банка» [3]. Стоить отметить, что наличие открытого доступа свидетельствует о мотиве с не прямой финансовой выгодой. Большая часть базы данных, оказавшейся в открытом доступе, была похищена в 2014 году, предположительно сотрудниками, подвергшимися сокращениям в этих банках. Остальные данные являются более актуальными и датируются 2018-2019 годами. Базы данным содержат персональные данные клиентов. Во всех вышеперечисленных инцидентах тип нарушителя соответствует параметрам: $M=1, P=1, Q\geq 5.$

Причинно-следственная цепочка поведения злоумышленника примет вид:

$$\{x7, x14\} => x1.$$

3. «Внешний нарушитель» Для этого типа нарушителя характерны следующие значения: $M=0, P=0, Q\in[0,3]$.

В силу неумышленности инцидента и отсутствия мотива причинно-следственную связь в этом случае построить невозможно.

4. «Внутренний нарушитель» Здесь имеет место: $M=0, P=1, Q\in[0,7]$.

Сотрудник фирмы неосознанно становится причиной утечки, например потеряв флешку с базой данных клиентов или переслав оную другому сотруднику по незащищенному каналу в открытом виде. В силу неумышленности и такого инцидента и отсутствия мотива, причинно-следственную цепочку событий также выявить невозможно.

В своих последующих публикациях автор намерен при построении поведенческих моделей злоумышленников при кибератаках использовать математический аппарат, описанный в работах [13-25].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. A Study on Global Data Leaks in 2018 [электронный ресурс] // https://infowatch.com/sites/default/files/report/analytics/Global_Data_Breaches_2018.pdf (дата обращения к ресурсу: 08.02.2020).

2. Актуальные киберугрозы I квартал 2017 года [Электронный ресурс] // https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Current-Cyberattacks-rus.pdf (дата обращения к ресурсу: 12.01.2020).

3. Актуальные киберугрозы II квартал 2017 года [Электронный ресурс] // https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf (дата обращения к ресурсу: 12.01.2020).

4. Актуальные киберугрозы: III квартал 2017 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017-q3/ (дата обращения к ресурсу: 12.01.2020).

5. Актуальные киберугрозы: IV квартал 2017 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017-q4/ (дата обращения к ресурсу: 12.01.2020).

6. Актуальные киберугрозы I квартал 2018 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q1/ (дата обращения к ресурсу: 12.01.2020).

7. Актуальные киберугрозы. II квартал 2018 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q2/ (дата обращения к ресурсу: 12.01.2020).

8. Актуальные киберугрозы. III квартал 2018 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q3/ (дата обращения к ресурсу: 12.01.2020).

9. Актуальные киберугрозы. IV квартал 2018 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q4/ (дата обращения к ресурсу: 12.01.2020).

10. Актуальные киберугрозы. I квартал 2019 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ (дата обращения к ресурсу: 12.01.2020).

11. Актуальные киберугрозы: II квартал 2019 года [Электронный ресурс] // https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/ (дата обращения к ресурсу: 12.01.2020).

12. Егошин Н.С., Конев А.А., Шелупанов А.А. Формирование модели нарушителя // Безопасность информационных технологий. – Томск: – 2017. – № 4. – С. 19-26.

13. Базилевский М.П., Вергасов А.С., Носков С.И. Групповой отбор информативных переменных в регрессионных моделях // Южно-сибирский научный вестник. –Барнаул: – 2019. – №4(28). – С. 36-39.

14. Носков С.И., Вергасов А.С. Прогнозирование по регрессионной модели с применением элементов теории сходства // Доклады Томского государственного университета систем управления и радиоэлектроники. – Томск:– 2019. – Т. 22. № 3. – С. 67-70.

15. Носков С.И., Вергасов А.С., Глухов Н.И. Анализ мер сходства при использовании взвешенного метода наименьших квадратов // Информационные технологии и математическое моделирование в управлении сложными системами. – Иркутск: – 2019. – № 2 (3). – С. 12-17.

16. Носков С.И., Вергасов А.С. Реализация взвешенного метода наименьших квадратов с использованием мер сходства // Вестник науки и образования. – Иваново: – 2018. – № 18-1 (54). – С. 29-32.

17. Носков С.И., Удилов В.П. Управление системой обеспечения пожарной безопасности на региональном уровне – Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2003. – 151 с.

18. Kreinovich V., Lakeyev A.V., Noskov S.I.. Approximate linear algebra is intractable // Linear Algebra and its Applications.1996. Т. 232. № 1-3. pp. 45-54.

19. Носков С.И. Точечная характеризация множества парето в линейной многокритериальной задаче // Современные технологии. Системный анализ. Моделирование. – Иркутск: – 2008. – № 1 (17). – С. 99-101.

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

21. Носков С.И. Критерий "согласованность поведения" в регрессионном анализе // Современные технологии. Системный анализ. Моделирование. – Иркутск: – 2013. – № 1 (37). – С. 107-110.

22. Golovchenko V.B., Noskov S.I.. Estimation of an econometric model using statistical data and expert information. Automation and Remote Control. 1991. Т. 52. № 4 pt 2. pp. 542-548.

23. Lakeyev A.V., Noskov S.I.. A description of the set of solutions of a linear equation with interval defined operator and right-hand side. Automation and Remote Control. 1992. № 11. P. 109.

24. Базилевский М.П., Носков С.И. Идентификация неизвестных параметров линейно-мультипликативной регрессии // Современные наукоемкие технологии. – Пенза: – 2012. – № 3. – С. 14.

25. Носков С.И., Базилевский М.П. Построение регрессионных моделей с использованием аппарата линейно-булевого программирования // – Иркутск: Иркутский государственный университет путей сообщения, 2018, – 176 с.

REFERENCES

1. A Study on Global Data Leaks in 2018 [electronic resource] https://infowatch.com/sites/default/files/report/analytics/Global_Data_Breaches_2018.pdf [Accessed 01/12/2020].

2. Actual cyberthreats I quarter of 2017 [Aktual'nyye kiberugrozy I kvartal 2017 goda] [Electronic resource] https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Current-Cyberattacks-rus.pdf [Accessed 01/12/2020].

3. Actual cyber threats II quarter of 2017 [Aktual'nyye kiberugrozy II kvartal 2017 goda] [Electronic resource] https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2017-rus.pdf [Accessed 01/12/2020].

4. Actual cyber threats: III quarter of 2017 [Aktual'nyye kiberugrozy III kvartal 2017 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017-q3/ [Accessed 01/12/2020].

5. Actual cyber threats: IV quarter of 2017 [Aktual'nyye kiberugrozy IV kvartal 2017 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2017-q4/ [Accessed 01/12/2020].

6. Actual cyber threats I quarter of 2018 [Aktual'nyye kiberugrozy I kvartal 2018 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q1/ [Accessed 01/12/2020].

7. Actual cyber threats. II quarter of 2018 [Aktual'nyye kiberugrozy II kvartal 2018 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q2/ [Accessed 01/12/2020].

8. Actual cyber threats. III quarter 2018 [Aktual'nyye kiberugrozy III kvartal 2018 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q3/ [Accessed 01/12/2020].

9. Actual cyber threats. IV quarter of 2018 [Aktual'nyye kiberugrozy IV kvartal 2018 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q4/ [Accessed 01/12/2020].

10. Actual cyber threats. I quarter of 2019 [Aktual'nyye kiberugrozy I kvartal 2019 goda] // [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ [Accessed 01/12/2020].

11. Actual cyber threats: II quarter of 2019 [Aktual'nyye kiberugrozy II kvartal 2019 goda] [Electronic resource] https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/ [Accessed 01/12/2020].

12. Egoshin N.S., Konev A.A., Shelupanov A.A. Formirovaniye modeli narushitelya [Formation of an intruder model]. Bezopasnost' informatsionnykh tekhnologiy [Information Technology Security]. Tomsk, 2017, no. 4, pp. 19-26.

13. Bazilevsky M.P., Vergasov A.S., Noskov S.I. Gruppovoy otbor informativnykh peremennykh v regressionnykh modelyakh [Group selection of informative variables in regression models]. Yuzhno-sibirskiy nauchnyy vestnik [South Siberian Scientific Bulletin]. Barnaul, 2019, No. 4 (28), pp. 36-39.

14. Noskov S.I., Vergasov A.S. Prognozirovaniye po regressionnoy modeli s primeneniyem elementov teorii skhodstva [Prediction by a regression model using elements of the similarity theory] Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki [Reports of Tomsk State University of Control Systems and Radioelectronics]. Tomsk, 2019, T. 22. no. 3, pp. 67-70.

15. Noskov S.I., Vergasov A.S., Glukhov N.I. Analiz mer skhodstva pri ispol'zovanii vzveshennogo metoda naimen'shikh kvadratov [Analysis of similarity measures using the weighted least squares method] Informatsionnyye tekhnologii i matematicheskoye modelirovaniye v upravlenii slozhnymi sistemami [Information technology and mathematical modeling in the management of complex systems]. Irkutsk, 2019, no. 2 (3), pp. 12-17.

16. Noskov S.I., Vergasov A.S. Realizatsiya vzveshennogo metoda naimen'shikh kvadratov s ispol'zovaniyem mer skhodstva [Implementation of the weighted least squares method using measures of similarity”]. Vestnik nauki i obrazovaniya. [Bulletin of science and education]. Ivanovo, 2018, no. 18-1 (54), pp. 29-32.

17. Noskov S.I., Udilov V.P. Upravleniye sistemoy obespecheniya pozharnoy bezopasnosti na regional'nom urovne [Fire safety management system at the regional level]. Irkutsk, Vostochno-Sibirskiy institut Ministerstva vnutrennikh del Rossiyskoy Federatsi [East Siberian Institute of the Ministry of the Interior of the Russian Federation], 2003, 151 p.

18. Kreinovich V., Lakeyev A.V., Noskov S.I .. Approximate linear algebra is intractable Linear Algebra and its Applications,1996, T. 232, no. 1-3. pp. 45-54.

19. Noskov S.I. Vostochno-Sibirskiy institut Ministerstva vnutrennikh del Rossiyskoy Federatsi [The point characterization of the Pareto set in a linear multicriteria problem] Sovremennyye tekhnologii. Sistemnyy analiz. Modelirovaniye. [Modern Technologies. System analysis. Modeling.] Irkutsk, 2008, no. 1 (17), pp. 99-101.

20. Lakeev A.V., Noskov S.I. Metod naimen'shikh moduley dlya lineynoy regressii: chislo nulevykh oshibok approksimatsii [The least module method for linear regression: the number of zero approximation errors] Sovremennyye tekhnologii. Sistemnyy analiz. Modelirovaniye. [Modern Technologies. System analysis. Modeling.] Irkutsk, 2012, no. 2 (34), pp. 48-50.

21. Noskov S.I. Kriteriy "soglasovannost' povedeniya" v regressionnom analize [The criterion of" consistency of behavior "in the regression analysis"] Sovremennyye tekhnologii. Sistemnyy analiz. Modelirovaniye. [Modern technologies. System analysis. Modeling.] Irkutsk, 2013, no. 1 (37), pp. 107-110.

22. Golovchenko V.B., Noskov S.I. Estimation of an econometric model using statistical data and expert information. Automation and Remote Control. 1991,v. 52, no. 4 pt 2, pp. 542-548.

23. Lakeyev A.V., Noskov S.I .. A description of the set of solutions of a linear equation with interval defined operator and right-hand side. Automation and Remote Control. 1992, no. 11, P. 109.

24. Bazilevsky M.P., Noskov S.I. Identifikatsiya neizvestnykh parametrov lineyno-mul'tiplikativnoy regressii [Identification of unknown parameters of linear multiplicative regression] ovremennyye naukoyemkiye tekhnologii. [Modern high technology.] – Penza, 2012, no. 3, pp. 14.

25. Noskov S.I., Bazilevsky M.P. Postroyeniye regressionnykh modeley s ispol'zovaniyem apparata lineyno-bulevogo programmirovaniya [The construction of regression models using the apparatus of linear Boolean programming]. Irkutsk, Irkutskiy gosudarstvennyy universitet putey soobshcheniya [Irkutsk State University of Railway Engineering], 2018, 176 p.

Информация об авторе

Александр Сергеевич Вергасов – ассистент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: tluck@inbox.ru

Author

Aleksandr Sergeevich Vergasov, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: tluck@inbox.ru

Для цитирования

Вергасов А.С. Поведенческие модели злоумышленников при кибератаках // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №1(6). – С. 44-51. DOI: 10.26731/2658-3704.2020.1(6).44-51 – Режим доступа: http://ismm-irgups.ru/toma/16-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 20.01.2020)

For citations

Vergasov A.S. Behavioral models of cybercriminals // 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. 44-51. DOI: 10.26731/2658-3704.2020.1(6).44-51 [Accessed 20/01/2020]