УДК 519.862.6

***А. С. Вергасов*[1]**

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

НЕКОТОРЫЕ МАТЕМАТИЧЕСКИЕ МОДЕЛИ ПОВЕДЕНИЯ ЗЛОУМЫШЛЕННИКА ПРИ КИБЕРАТАКЕ

Аннотация. В работе предлагаются возможные варианты математических моделей поведения злоумышленника при кибератаках. В основе исследования лежит аппарат регрессионного анализа с применением группировки независимых факторов моделей.

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

***A.S. Vergasov*[1]**

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

SOME MATHEMATICAL MODELS OF THE BEHAVIOR OF AN ATTACKER DURING A CYBER ATTACK

Abstract. The paper proposes possible variants of mathematical models of cyber-attack behavior of an intruder. The basis of the research is the apparatus of regression analysis with the use of grouping of independent factor models.

Key words: information security, intruder model, intruder behavior model.

Введение. На протяжении нескольких десятков лет с ростом информатизации экономик развитых и развивающихся стран происходит рост ценности информационных активов. Эта тенденция сопровождается увеличением количества преступлений в информационной сфере (рис. 1) и размера ущерба от них (рис. 2) [1-2].

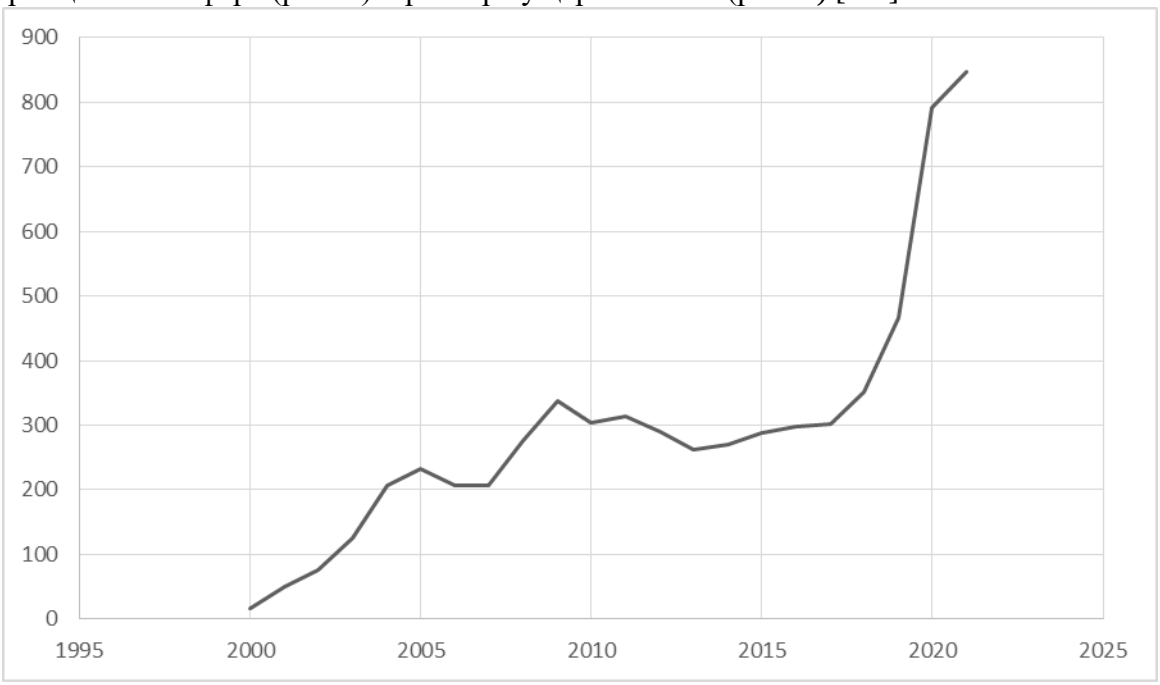

Рис. 1. Количество жалоб об интернет-преступлениях, поданных в IC3 за 2000 – 2021 г. г. (тыс.).

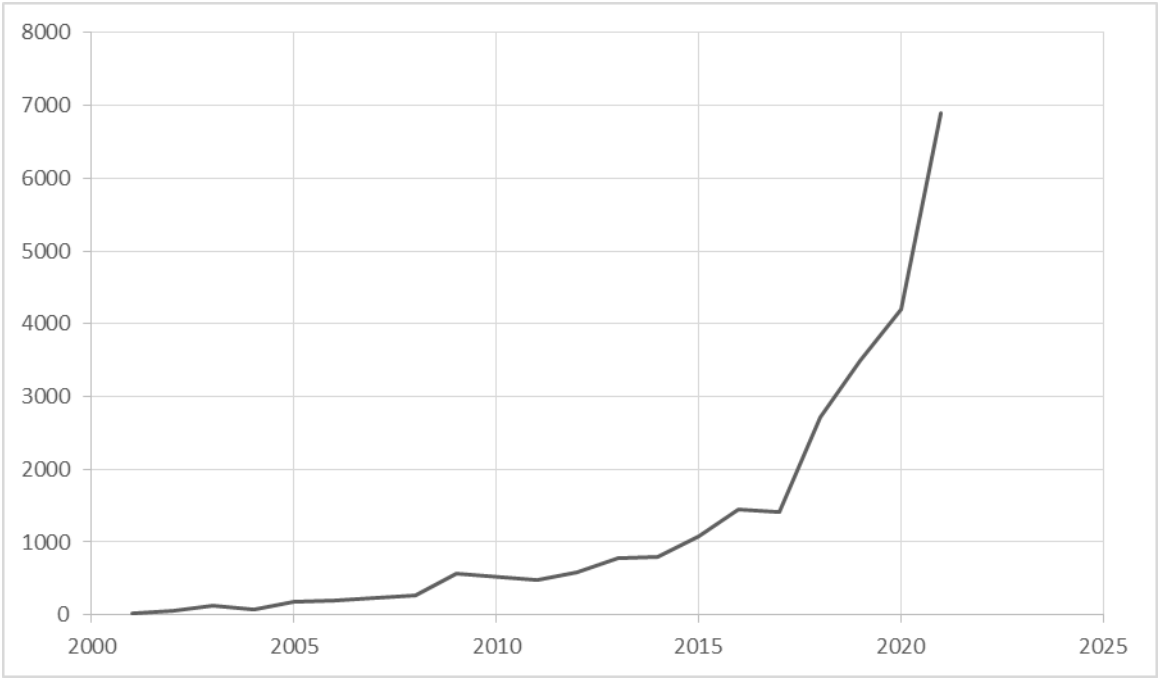

Рис. 2. Ущерб от кибератак по оценкам IC3 2001 – 2021 г.г. (в млн. долл. США).

В следствии этого компании, обеспокоенные возможными финансовыми и репутационными издержками, выделяют значительные средства на поддержание необходимого уровня защиты цифровых активов. Расширяется ассортимент предлагаемых решений в области информационной безопасности (ИБ) и услуг по их внедрению, наблюдается рост рынка информационной безопасности во всем мире и ожидание дальнейшего увеличения мировых ежегодных затрат до более чем шестисот миллиардов долларов к 2030 году [3].

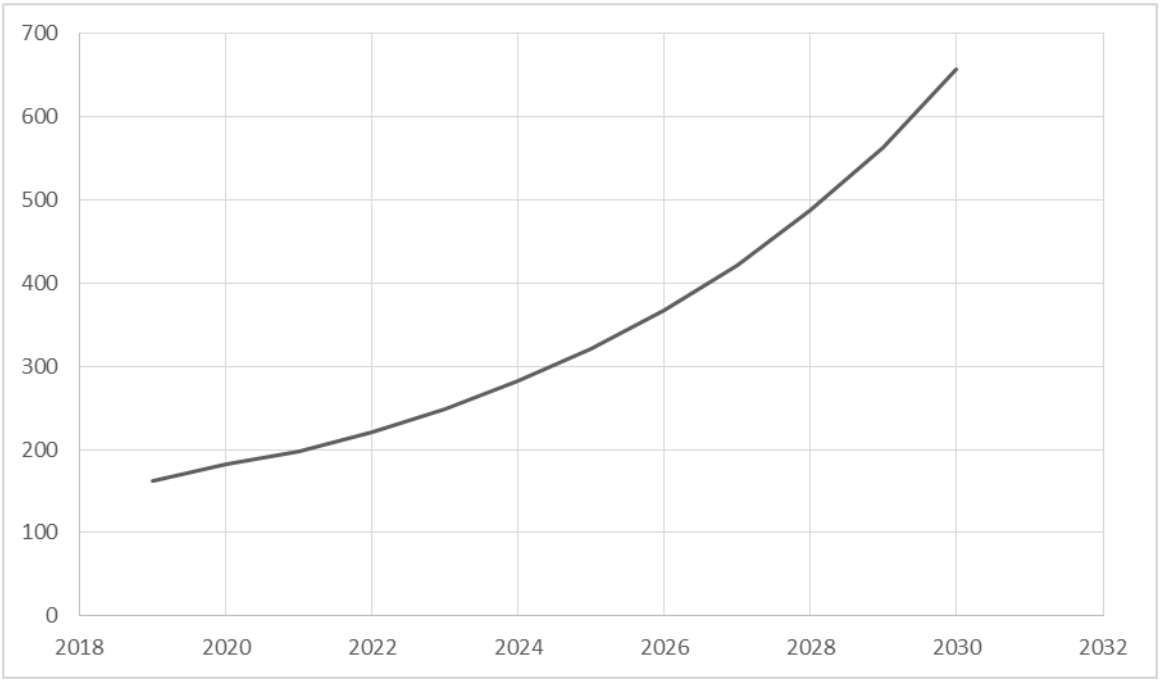

Рис. 3. Размер мирового рынка кибербезопасноти за 2019-2022 гг и прогноз на 2023-2030 гг (в млрд. долл. США)

Самым объемным рынком, по данным Mordorintelligence, остается Северная Америка, однако наиболее динамически развивающимся и перспективным является азиатско-тихоокеанский регион [4]. В частности, по подсчетам PwC (одна из крупнейших компаний в

области аудита), среди ее клиентов в Индии 69 % компаний в 2022 увеличили бюджет на ИБ [5].

Стоит отметить, что принятие ключевых решений в области информационной безопасности в организациях в большинстве случаев возложено на руководителей не из профильных отделов (рис.4.) [6].

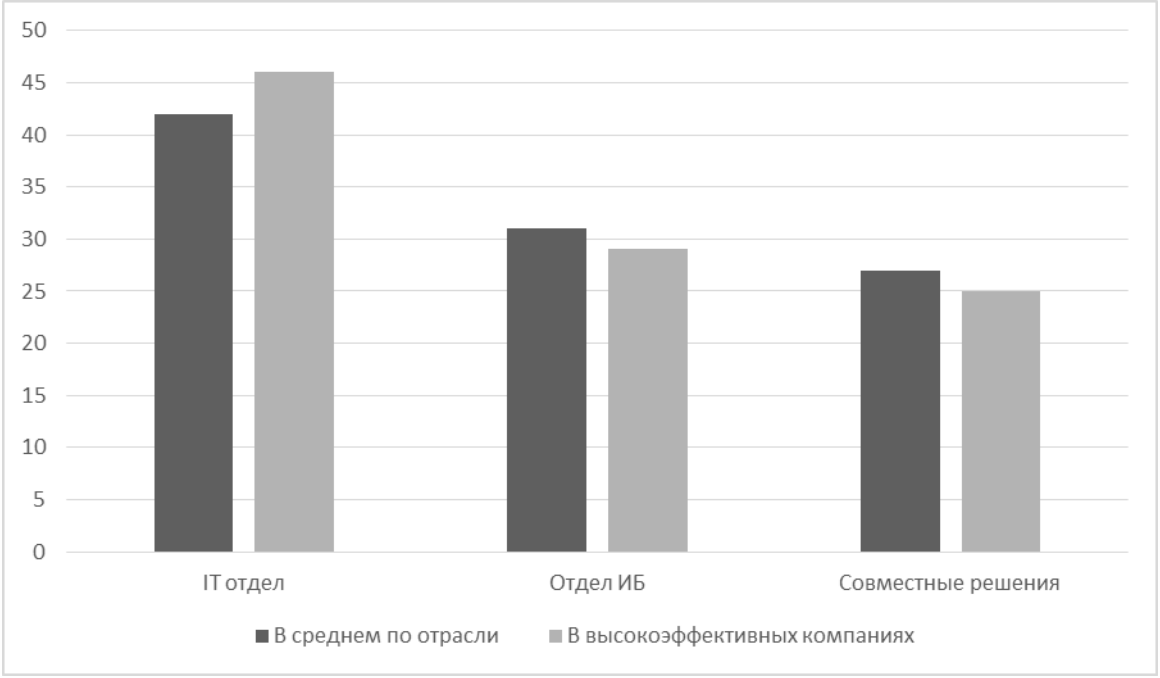

Рис. 4. Распределение ответственных за принятие архитектурных решений в области ИБ по отделам среди компаний (выраженное в процентном соотношении относительно общего количества).

Исходя из вышеперечисленных фактов очевидна необходимость привнесения некоторой формализации в процесс принятия решений в области ИБ. Возможным подходом к решению данной задачи является разработка модели киберугроз, основанной на анализе поведенческих моделей злоумышленников по секторам экономики. Вопросу построения математических моделей поведения злоумышленников как раз и посвящена данная работа.

Описание факторного пространства. В работе [7] рассмотрены формализованные модели поведения злоумышленников при киберпреступлениях, а именно, выделены некоторые направления поведения типа «мотив + категория жертвы → объект атаки». При этом группа эндогенных факторов, характеризующих мотив, включает в себя следующие:

x_1 – получение данных;
x_2 – финансовая выгода;
x_3 – хактивизм;
x_4 – кибервойна.

Факторы группы «категория жертв»:

x_5 – частные лица;
x_6 – государственные учреждения;
x_7 – финансовая отрасль;
x_8 – медицинские учреждения;
x_9 – сфера образования;
x_{10} – онлайн-сервисы;
x_{11} – сфера услуг;
x_{12} – промышленные компании;

x_{13} – без привязки к конкретной отрасли.

Группа объектов атак:

x_{14} – инфраструктура;

x_{15} – веб-ресурсы;

x_{16} – пользователи;

x_{17} – мобильные устройства;

x_{18} – IoT–техника;

x_{19} – банкоматы и POS-терминалы.

Для расширения факторного пространства были применены степенные, логарифмические, аддитивные и мультипликативные преобразования введенных переменных. При построении формальных межфакторных зависимостей использованы методы регрессионного анализа [8-14]. Для выделения наиболее информативных регрессоров при моделировании воспользуемся одной из возможных стратегий, описанных в работе [8], а именно, из каждой группы {мотив, категория жертвы, объект атаки} в модель может входить только одна переменная.

Для построенного отдельных регрессионных соотношений в качестве критериев адекватности применены следующие: множественной детерминации R^2, Фишера F, средней относительной ошибки λ и согласованности поведения Φ [15,16]. Ниже приведены пороговые значения критериев, при которых регрессионная модель может быть признана адекватной:

$$R^2 \geq 0.9,$$
$$F \geq 40,$$
$$\lambda \leq 8,$$
$$\Phi \geq 0.5.$$

Модель внешнего злоумышленника. Рассмотрим модель внешнего злоумышленника, в которой, исходя из его мотива и категории жертвы, формируется объект атаки. Ниже приведены некоторые варианты модели с зависимой переменной x_{16}:

$$x_{16} = 19.038 - 0.051\frac{(x_1)^2}{x_2} - 0.103\frac{(x_8)^2}{x_{11}} \quad (1)$$
$$R^2 = 0.959, F = 82.933, \Phi = 0.555, \lambda = 3.362.$$
$$x_{16} = 21.835 - 218.4\frac{1}{x_2} - 45.338\frac{1}{x_7 * x_{10}} \quad (2)$$
$$R^2 = 0.943, F = 58.503, \Phi = 0.555, \lambda = 4.159$$
$$x_{16} = 12.231 + 0.101x_2 - 5.452\left(\frac{1}{x_7} + \frac{1}{x_{10}}\right) \quad (3)$$
$$R^2 = 0.921, F = 41.272, \Phi = 0.555, \lambda = 4.451$$
$$x_{16} = 18.93 - 0.046\frac{(x_1)^2}{x_2} - 44.673\frac{1}{x_7 * x_{10}} \quad (4)$$
$$R^2 = 0.936, F = 51.762, \Phi = 0.555, \lambda = 3.705$$
$$x_{16} = -25.169 + 4.876(x_2)^{\frac{1}{3}} + 4.712\left((x_{10})^{\frac{1}{3}} + (x_{13})^{\frac{1}{3}}\right) \quad (5)$$
$$R^2 = 0.92, F = 40.429, \Phi = 0.555, \lambda = 4.589$$
$$x_{16} = -18.979 + 1.699(x_2)^{\frac{1}{2}} + 4.648\left((x_{10})^{\frac{1}{3}} + (x_{13})^{\frac{1}{3}}\right) \quad (6)$$
$$R^2 = 0.919, F = 40.051, \Phi = 0.555, \lambda = 4.557$$
$$x_{16} = 19.981 - 0.001(x_1)^2 - 0.028\frac{(x_8)^3}{x_7} \quad (7)$$
$$R^2 = 0.919, F = 40.137, \Phi = 0.555, \lambda = 4.281$$
$$x_{16} = 9.742 + 0.118(x_2 + (x_4)^2) - 19.681\frac{1}{x_9 * x_{10}} \quad (8)$$
$$R^2 = 0.943, F = 58.99, \Phi = 0.555, \lambda = 3.8$$

Исходя из моделей (1) - (8), пользователи выступают в качестве объектов атак в следующих случаях:

– при нападении на предприятия из сферы услуг с целью финансовой выгоды - зависимость (1);

– при атаке на объекты финансовой отрасли для получения финансовой выгоды - модели (2)-(4) или получения данных - (7);

– атакованы онлайн сервисы ради финансовой выгоды - соотношения (2)-(6);

– атакованы объекты предприятий из сферы образования с целью ведения кибервойны - модель (8).

В нападениях на медицинские учреждения с целью получения данных в качестве объекта атак пользователи выступают крайне редко - зависимости (1), (7).

В следующих регрессионных моделях в качестве объекта атак выбраны мобильные устройства.

$$x_{17} = 11.61 - 0.02\frac{(x_3)^3}{x_1} - 4.547\frac{x_6}{x_5} \quad (9)$$

$$R^2 = 0.962, F = 89.272, \Phi = 0.555, \lambda = 6.282$$

$$x_{17} = 16.506 - 2.851 * \left((x_3)^{\frac{1}{3}} + \frac{1}{x_1}\right) - 4.364\frac{x_6}{x_5} \quad (10)$$

$$R^2 = 0.945, F = 60.148, \Phi = 0.555, \lambda = 5.961$$

$$x_{17} = 11.136 - 0.447\frac{(x_3)^2}{x_1} - 0.211\frac{(x_6)^2}{x_5} \quad (11)$$

$$R^2 = 0.944, F = 60.129, \Phi = 0.555, \lambda = 5.785$$

$$x_{17} = 10.996 - 0.00046((x_1)^2 + (x_3)^3) - 0.0000019((x_9)^2 * (x_6)^3) \quad (12)$$

$$R^2 = 0.952, F = 70.189, \Phi = 0.555, \lambda = 5.711$$

$$x_{17} = 15.198 - 1.523\left((x_3)^{\frac{1}{2}} + (x_4)^{\frac{1}{3}}\right) - 0.000000204 * (x_6)^3 * (x_9)^3 \quad (13)$$

$$R^2 = 0.951, F = 68.942, \Phi = 0.555, \lambda = 4.932$$

$$x_{17} = 10.675 - 0.000238 * x_1 * (x_3)^2 - 0.0000019 * (x_9)^2 * (x_6)^3 \quad (14)$$

$$R^2 = 0.951, F = 68.779, \Phi = 0.555, \lambda = 5.444$$

$$x_{17} = 11.441 - 0.261 * x_3 - (2.2e-06) * (x_6)^3 * (x_9)^3 \quad (15)$$

$$R^2 = 0.946, F = 62.123, \Phi = 0.555, \lambda = 5.814$$

Анализ моделей (9)-(15) позволяет сделать следующие выводы:

при нападении на частных лиц с целью получения данных(9)-(11) объектом атаки злоумышленники избирают мобильные устройства;

- во время нападения на государственные учреждения с целью хактивизма (9)-(15), акта кибервойны (13) или получения данных (12)(14) мобильные устройства в виде объекта атак не актуальны.

Злоумышленник, атакуя учреждения из сферы образования для получения данных (12), (14), хактивизма (12)-(15), или в рамках кибервойны (13), как правило, не рассматривает мобильные устройства в качестве объекта атак.

Заключение. В ходе работе построены регрессионные модели, распределенные по отраслям, позволяющие прогнозировать конъектурные изменения в рамках модели внешнего злоумышленника. Автор в дальнейших своих работах намерен значительно расширить перечень поведенческих моделей киберпреступлений и на их основе разработать алгоритм принятия архитектурных решений в ИБ на основе отраслевой принадлежности той или иной компании.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Поступившие жалобы на интернет-преступления на сайте IC3 с 2000 по 2021 год [электронный ресурс] // https://www.statista.com/statistics/267546/number-of-complaints-about-us-internet-crime/ (дата обращения к ресурсу: 28.01.2023).

2. Сумма денежного ущерба, причиненного IC3 сообщениями о киберпреступлениях с 2001 по 2021 год. [электронный ресурс] // https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ (дата обращения к ресурсу: 28.01.2023).

3 Размер рынка кибербезопасности в мире с 2019 по 2030 год [электронный ресурс] // https://www.statista.com/statistics/1256346/worldwide-cyber-security-market-revenues/ (дата обращения к ресурсу: 28.01.2023).

4. Обзор отрасли управляемых служб безопасности [электронный ресурс] // https://www.mordorintelligence.com/industry-reports/security-managed-services-market (дата обращения к ресурсу: 28.01.2023).

5. 2023 Global Digital Trust Insights India edition [электронный ресурс] // https://www.pwc.in/assets/pdfs/consulting/cyber-security/2023-global-digital-trust-insights-v1.pdf (дата обращения к ресурсу: 28.01.2023).

6. Кто принимает решения об архитектуре решений для обеспечения безопасности? [электронный ресурс] // https://www.statista.com/statistics/1238357/it-security-solution-product-decision-team/ (дата обращения к ресурсу: 28.01.2023).

7. 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.

8. 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.

9. 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.

10. 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. 49

11. 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.

12. 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.

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

14. 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.

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

16. Носков С.И., Базилевский М.П. Множественное оценивание параметров и критерий согласованности поведения в регрессионном анализе // Вестник Иркутского государственного технического университета. – Иркутск: –2018. –Т. 22. –№ 4 (135). –С. 101-110.

REFERENCES

1. Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2021 [electronic resource] https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ [Accessed 27/01/2022].

2. Incoming complaints about internet crime on the IC3 website from 2000 to 2021 [electronic resource] https://www.statista.com/statistics/267546/number-of-complaints-about-us-internet-crime/ [Accessed 27/01/2022].

3 Size of cyber security market worldwide from 2019 to 2030 [electronic resource] https://www.statista.com/statistics/1256346/worldwide-cyber-security-market-revenues/ [Accessed 27/01/2022].

4. Managed security services industry overview [electronic resource] https://www.mordorintelligence.com/industry-reports/security-managed-services-market [Accessed 27/01/2022].

5. 2023 Global Digital Trust Insights India edition [electronic resource] https://www.pwc.in/assets/pdfs/consulting/cyber-security/2023-global-digital-trust-insights-v1.pdf [Accessed 27/01/2022].

6. Who makes security solution architecture product decisions? [electronic resource] https://www.statista.com/statistics/1238357/it-security-solution-product-decision-team/ [Accessed 27/01/2022].

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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. 8-1 (54), pp. 29-32.

9. 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.

10. 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.

11. 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.

12. Noskov S.I., Bazilevsky M.P. Mnozhestvennoye otsenivaniye parametrov i kriteriyev soglasovaniya povedeniya v regressionnom analize [Multiple estimation of parameters and criteria for matching behavior in regression analysis] // Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta. [Bulletin of the Irkutsk State Technical University.] Irkutsk, 2018, T. 22, no. 4 (135). pp. 101-110.

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. Некоторые математические модели поведения злоумышленника при кибератаке // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2023. – №1(17). – С.41-48– DOI: 10.26731/2658 3704.2023.1(17).41-48 – Режим доступа: http://ismm-irgups.ru/toma/117-2023, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 31.03.2023)

For citations

Vergasov A.S. Some mathematical models of cyber attacker behavior // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: elektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the man-agement of complex systems: electronic scientific journal], 2023. No. 1(17). P. 41-48. DOI: 10.26731/2658-3704.2023.1(17).41-48 [Accessed 31/03/23]