УДК 519.246.8:34.096

© Сергей Владимирович Поляков
к.т.н., доцент Владимирского филиала РАНХиГС
svp2206@yandex.ru

© Юлия Викторовна Зараева
заместитель начальника 5 отдела Правового управления ГУ МВД России по г. Москве, подполковник внутренней службы,
zaraeva@mail.ru

НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ФАКТОР ИСПОЛЬЗОВАНИЯ КИБЕРПРОСТРАНСТВА ТЕРРОРИСТАМИ И ЭКСТРЕМИСТАМИ

Аннотация: рассматривается динамика преступлений, связанных с неправомерным доступом к компьютерной информации. Дан анализ динамики киберпреступности.

Annotation: The dynamics of crimes related to unauthorised access to computer information is considered. The analysis of cybercrime dynamics is given.

Ключевые слова: неправомерный доступ к компьютерной информации, экстремизм, модель, прогноз.

Keywords: unauthorized access to computer information, extremism, model, forecast.

Самыми распространёнными киберпреступлениями, по мнению Генеральной прокуратуры Российской Федерации, являются неправомерный доступ к компьютерной информации и вредоносные компьютерные программы, а число нераскрытых преступлений с использованием высоких технологий выросло на 30,5%[1]. Неправомерный доступ к компьютерной информации и вредоносные компьютерные программы создают благоприятную обстановку для достижения террористами и экстремистами своих целей.

В настоящее время компьютерные сети могут быть использованы и используются террористами и экстремистами разного толка в качестве средства доступа к системам управления особо охраняемых объектов, а также для координации действий экстремистских и террористических организаций, вербовки новых членов в свои организации, проведения психологических операций, пропаганды своей идеологии и сбора финансовых пожертвований на джихад («священную войну»)[2]. Террористы и их пособники применяют современные программные методы для обеспечения своей анонимности. Кибертеррористы используют современные информационные технологии, компьютерные системы и сети, специальное программное обеспечение с целью несанкционированного проникновения в компьютерные системы и организации, удаленной атаки на информационные ресурсы жертвы.

По данным Генеральной прокуратуры Российской Федерации, самыми «популярными» киберпреступлениями являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и распространение вредоносных компьютерных программ (ст. 273

[1] URL: https://roskomsvoboda.org/40924/ (дата обращения: 15.04.2019).

[2] Портал "Современная армия" [Электронный ресурс]. URL: http://www.modernarmy.ru/article/249 (дата обращения: 15.04.2019).

УК РФ)[3]. Конечно, надо понимать, что неправомерный доступ к компьютерной информации включает в себя любые типы компьютерных преступлений, в том числе кибертерроризм.

Ст. 273 УК РФ соотносится с тем, что вредоносное программное обеспечение – это один из инструментов киберпреступников, и в частности кибертеррористов. С помощью различных видов вредоносных программ злоумышленники стремятся достигать своих целей.

В связи с этим возникает необходимость исследования динамики и взаимосвязи таких видов правонарушений, как неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных компьютерных программ.

В таблице 1 приведены статистические сведения о преступлениях, предусмотренных соответствующими статьями УК РФ в целом по России (источник: ГИАЦ МВД России).

Таблица 1

Количество выявленных преступлений, в том числе зарегистрированных в отчетный период, в целом по России

Период	ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»	ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»
2007	5234	1995
2008	7450	1543
2009	9519	2112
2010	6309	1089
2011	2005	693
2012	1930	889
2013	1799	764
2014	1151	585
2015	1396	974
2016	994	751
2017	1079	802
2018	1761	733

Рассмотрим гипотезу о связи двух типов преступлений, представленных в таблице 1. Для оценки тесноты и направления этой связи факторов, приведенных в таблице 1 (в качестве факторов использовались количественные данные выявленных и зарегистрированных преступлений) используем линейный коэффициент корреляции *r*. Получено его значение $r = 0{,}87$. Это означает, что тесноту связи фактора «Создание, использование и распространение вредоносных компьютерных программ» и фактора «Неправомерный доступ к компьютерной информации» можно оценить как весьма высокую и положительную. Иными словами, неправомерному доступу к компьютерной информации способствует создание, использование и распространение вредоносных компьютерных программ. Статистическую значимость такого вывода подтверждает t-статистика, согласно которой расчетное значение t-критерия Стьюдента больше его критического значения или $t_{расч} = 5{,}47 > t_{кр} = 2{,}23$. Оценка дана с надежностью не хуже 95%.

[3] URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 15.04.2019).

Данные таблицы 1 были использованы и для оценки среднего прогнозирования показателей уровней выявленных преступлений по ст. 272 и ст. 273 УК РФ.

На рис. 1 показана динамика количества зарегистрированных преступлений по неправомерному доступу к компьютерной информации. Обращает на себя внимание то, что в 2007-2010 годах количество таких преступлений составляло порядка 5000-9000, то в последующие годы это количество снизилось до 1000-2000, т.е. примерно в 4-5 раз. За наблюдаемые период 2007-2018 годов уровни зарегистрированных преступлений, квалифицированных как неправомерный доступ к компьютерной информации, описываются экспоненциальной математической моделью вида $y_{теор} = 8487{,}4e^{-0{,}19x}$. Полученная модель объясняет 71,8% зарегистрированных преступлений, квалифицированных как неправомерный доступ к компьютерной информации, фактором времени. Модель позволяет оценить изменение среднего значения результирующего фактора на 2019 и 2020 годы. Получено, что при сохранении такой тенденции выявления преступлений по ст. 272 УК РФ ожидается в 2019 и в 2020 годах снижение количества зарегистрированных преступлений до 718 и 594 соответственно. При этом отметим, что полученная экспоненциальная математическая модель описывает исследуемые уровни (показатели) наиболее качественно по сравнению с иными моделями (степенная, полиномиальная, логарифмическая, линейная и т.д.).

Рис. 1. Изменение количества зарегистрированных преступлений, квалифицированных как неправомерный доступ к компьютерной информации за период 2007-2018 годов.

На рис. 2 показана динамика количества зарегистрированных преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ за период 2007-2018 годов.

Рис. 2. Изменение количества зарегистрированных преступлений, квалифицированных как создание, использование и распространение вредоносных компьютерных программ, за период 2007-2018 годов

Динамика данного вида преступлений описывается полиномом второй степени вида $y_{теор} = 20{,}365x^2 + (-373{,}49)x + 2401{,}1$. Эта модель показала наилучшие качества из ряда иных моделей. Модель объясняет 75,7% количества зарегистрированных преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ по годам. Прогноз среднего значения количества преступлений на 2019 и 2020 годы показал их рост, а именно, в 2019 году ожидается их количество ожидается 988, а в 2020 году 1165.

Таким образом, получаем, что при сохранении нынешней тенденции к выявлению преступлений количество зарегистрированных преступлений, связанных с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), в ближайшие годы будет снижаться, а количество выявленных преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ, будет расти. Это означает, что связь этих двух типов преступлений изменится с положительного на отрицательное направление.

В свою очередь это не означает, что количество рассматриваемых преступлений действительно будет слабо расти или даже снижаться. Обращает на себя внимание то, что динамика зарегистрированных преступлений по ст. 272 и ст. 273 УК РФ (см. таблицу 1) в последние3-4 года меняется слабо. Это может говорить об эффективной работе правоохранительных органов или, наоборот, о слабой их работе по преступлениям данного направления. Учитывая рост технического оснащения киберпреступности, высокий уровень их профессиональной подготовки, а также тот факт, как было отмечено выше, что число нераскрытых преступлений с использованием высоких технологий выросло на 30,5%, можно сделать вывод о том, что правоохранительные органы должны усилить работу по выявлению подобного вида преступлений. Это касается как профессиональной подготовки сотрудников, так и технической оснащенности соответствующих подразделений и служб.

Список литературы

1. URL: https://roskomsvoboda.org/40924/ (дата обращения: 15.04.2019).
2. Портал "Современная армия" [Электронный ресурс]. URL: http://www.modernarmy.ru/article/249 (дата обращения: 15.04.2019).
3. URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/ (дата обращения: 15.04.2019).
4. Поляков С. В. Использование Excel в моделировании, оценке деятельности и управлении: учебно-методическое пособие. – Владимир : Владимирский филиал РАНХиГС, 2015.
5. Поляков С. В., Кисляков А. Н. Основы математического моделирования социально-экономических процессов: учебно-методическое пособие. – Владимир : Владимирский филиал РАНХиГС, 2017.