УДК 004
JEL коды: D89
08.00.13

Моделирование правовых информационно-логических отношений и угроз

Modeling legal information and logical relations and threats

Хотов Азамат Лионович,
старший преподаватель кафедры «Программирование и инфокоммуникационные технологии», факультет информационных технологий ФГБОУ ВО «Чеченский государственный университет», Грозный, Россия.
Hotov Azamat Lyonovich,
Senior Lecturer of the Chair "Programming and Infocommunication Technologies", Faculty of Information Technologies of the Federal State Educational Establishment of Higher Education "Chechen State University", Grozny, Russia

Аннотация
Правовая поддержка ИКТ, информационных услуг, систем комплексно должна быть проработана, особенно, веб-услуг. Правовые сетевые отношения субъектов регулируются законодательством, но есть особенности. В ИКТ-средах гражданские правоотношения различаются, запаздывают по развитию. Необходимы механизмы релевантного правового регулирования отношений в компьютерных средах. Их можно выработать с помощью системного анализа, моделирования процессов, ситуаций. В работе проделано соответствующее системное исследование. Приведены методические примеры-ситуации.
Abstract
Legal support of ICT, information services, systems should be comprehensively developed, especially, web services. Legal network relations of subjects are regulated by law, but there are features. In ICT environments, civil law relations are different, they are delayed in development. The mechanisms of the relevant legal regulation of relations in computer environments are needed. They can be developed with the help of systems analysis, modeling processes, situations. The work done the appropriate system study. The methodical examples-situations are given.
Ключевые слова: моделирование, право, система, отношения, правовые, угрозы, компьютерные, терроризм, взлом, угроза, интернет, сети.
Keywords: modeling, law, system, relations, legal, threats, computer, terrorism, hacking, threat, Internet, networks.

Введение

Правовая поддержка информационных услуг комплексно не определена (особенно, веб-услуг). Считается, информационная система, Интернет, сеть – без правосубъектности (важный признак системы) не имеет обязанностей, прав, за правоотношения в ней ответственен лишь правоспособный субъект [4].

Правовые сетевые отношения субъектов регулируются законодательством, хотя есть значимые в праве особенности. Провайдеры, владельцы информационных систем – поставщики услуг доступа к ресурсам, их размещения: хостинг-провайдер сайта с вредной информацией может судом признан быть ее распространителем (обеспечивает же третьим лицам доступ) [3].

В ИКТ-средах гражданские правоотношения различаются по правоотношениям (потребительские, коммерческие), форме их реализации (виртуальные, частично виртуальные),

субъект правоотношений здесь по ГК – посетитель (потребитель ресурса) среды. Идентифицировать дееспособность посетителя сложно, процедура нечеткая, неопределенная, плохо структурируемая. Отношения в сетях всегда запаздывают по развитию [11].

Действия, моделируемые и координируемые в правовом поле для снижения рисков, ущерба должны включать:

1. анализ деструктивных действий;
2. оценку возможного ущерба;
3. обмен информацией, ее верификацию;
4. практические меры против угрозы.

Рисунок 1. Распределение угроз ИБ

Все это невозможно без сценариев, моделей развития конфликтов. Необходим механизм релевантного правового регулирования, пока же оформляются лишь договора (с хостинг-провайдером, маркетингом, рекламной компанией и др.).

Такой механизм (такие процедуры) можно выработать с помощью системного анализа, моделирования процессов, ситуаций. Покажем это на методических примерах-ситуациях.

Пример 1. Террористическая угроза

Как измерять, рассматривать в меняющемся мире динамику развития угроз террора. С целью измерения таких связей создаются соответствующие математические модели. Для выявления скрытых корреляций полезна процедура: объектам (характеристикам),

представляющим особый правовой интерес придаются веса («взвешиваются» и затем строятся соответствующие взвешенные вектора).

Терроризм, уже глобально координируемый, способен разрушить связи, оптимальные конструкции в ряде стран. Готовность населения противостоять ему, можно прогнозировать при помощи математического прогнозирования, с помощью «искусственного интеллекта» (СИИ). Ученые полагают, что население, подготовленное с помощью Интернет, ИКТ, математических прогнозов сможет помогать силовым структурам.

У отечественных силовых структур «рук не хватит» предотвращать терроризм в условиях развития высоких технологий, интернет-сообществ, идет ведь накопление латентного террористического потенциала (терророгенность) [7,8]. Защитные меры от угроз терроризма – ужесточение режимов безопасности, технологических барьеров, усиление охранных (по периметру) функций и др. Такие мероприятия препятствуют террористам, вынуждают отклоняться от намеченных целей, действовать на менее критически направлениях, участках, объектах.

Рисунок 2. Действия при разных уровнях угроз терроризма

Превентивные меры включают моделирование, прогнозирование, которые часто приравниваемы к прямым ударам спецподразделений. Узаконенные превентивные меры призваны, как минимум, нанести ущерб инфраструктуре террористической организации на

территориях нескольких стран, являются ответом на замыслы нарушить сложившиеся экономико-социальные отношения.

Чаще применяется методика анкетирования, например, по региону [13]. Цель, в частности, выявить склонность к терроризму, лояльность к нему. Анкетирование анализируется, результаты шкалируются (например, от «нет напряженности» до «высокая напряженность», не забываем и «не знаю») или переносятся в интервальную арифметику. Получается числовая мера оценки респондентом состояния проблемы [11]. Затем на основе квалиметрии, социологии, математической статистики, теории измерений, индивидуальные мнения респондентов объединяются во мнение опрашиваемой группы. Гипотеза: групповое мнение в целом объективно описывает реальное состояние проблемы.

Можно использовать метод Дельфи или другой экспертно-эвристический метод. Например, в методе Дельфи в анкетирование включаем вопросы социального, административного, пропагандистского, этнического, охранного, психологического, конфликтологического плана. Затем интегрируем парциальные индексы с весовыми коэффициентами, нормируем, получая интегральный индекс угрозы, который может включать:

1. средства внешнего воздействия;
2. контакты, меры снижающие общую эффективности контртерроризма;
3. протестные, организованные формы террористической деятельности и др [1-3].

Интегрированный индекс динамически пополняется данными, освобождается от несущественной информации, «белого шума».

Пример 2. Компьютерная угроза

Понятие «компьютерное преступление» пока не является понятием УК, но ежегодный прирост таких преступлений – более 200%, ежегодный ущерб – сотни миллионов рублей, ущерб – миллиарды, а обвинительные приговоры - лишь для примерно 40% от возбужденных дел. Годовой абсолютный рост – более 20%.

Около 16% «компьютерных злоумышленников» – молодые, до 18, около 60% – 18-26 лет. Тот возраст, в котором наиболее активно посещают Интернет. Более половины - со специальной ИКТ-подготовкой, подавляющее большинство - сотрудники госучреждений [9].

Компьютерное преступление – акт, предусмотренный УК государства общественно-опасным, совершаемым с применением компьютера, средства актуализации информации. Злоумышленник учитывает возможности сервера (скорость, память, обработку и др.), ищет уязвимости, использует их [17].

«Развиваются» программы-вымогатели, теперь и с привлечением криптовалютных систем.

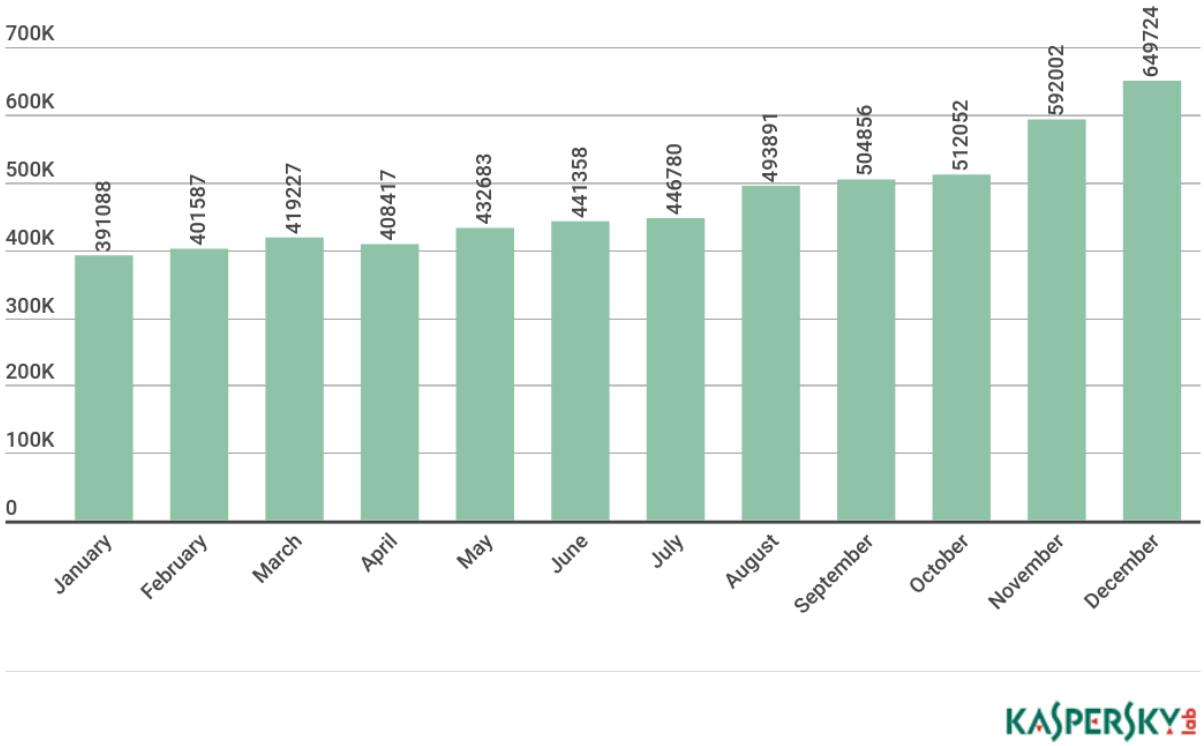

Рисунок 3.Рост компьютерных преступлений.

Полезны идентификационные «образы», «модели» таких преступлений, важно иметь «модели», «портреты» и преступника:

1. «любитель» – программист (пользователь), причина преступления – спортивный азарт и, возможно, правовая неграмотность (обычно осуществляется без особой преступной цели);
2. «профессионал» - программист со стойкой тягой к компьютерным преступлениям (имеется преступная, корыстная цель);
3. «фобы» – пользователи, подверженные фобиям, психозу, вызванным систематическими информационными перегрузками или «недогрузками» (обычно осуществляется без умысла, но сознательно);
4. «инсайдеры» – имеющие (имевшие) доступ к конфиденциальной информации организации и могущие передать (передавшие) ее «на сторону» в преступных, политических целях (например, сообщающие легко запоминаемую служебную информацию – курс акций, предмет торгов, архитектура сети, система доступа, политика безопасности и др.);
5. «хулиганы» – пользователи, программисты, которые нарушают правила поведения в компьютерных системах, архитектуру из хулиганства;
6. «домушники» – лица, которые воруют компьютерные средства (например, диски с информацией);

7. «перехватчики» – лица, которые перехватывают информацию с помощью определенных компьютерных, электронных средств перехвата;
8. «мусорщики» – лица, собирающие и использующие содержимое физических или электронных корзин, восстановление информации и др.;
9. «за дураком» – использующие физический или электронный доступ из-за грубых нарушений, неквалифицированности персонала (оставления компьютера или документов в свободном доступе, неудаление паролей и логинов и др.); критически опасна ситуация, когда роль «дурака» исполняет администратор;
10. «маскарадники» – пользователи, которые проникают в систему из компьютеров, аккаунтов законных, зарегистрированных пользователей (например, логина, пароля полученных подкупом, вымогательством, шантажом и др.);
11. «аналитики» – пользователи, программисты, считывающие незащищённые или защищённые данные системы, затем анализирующие любые параметры систем безопасности, доступа, архитектуры с доступа;
12. прочие.

Заключение

Ценно знание законов, но и нюансов правоприменения, позволяющих принимать эффективное решение в рамках законодательства. Противодействие терроризму строится с опорой на науку, образование, общественность. Необходимо изучение конкретных проблем предотвращения глобального терроризма, привлекая к этому компьютерные и иные информационно-аналитические возможности [6].

Также для компьютерных преступлений пока нет релевантной системы мер антипреступлений, законодательства, методик расследования. «Модели», «портреты» при всей их условности, перекрываемости, могут быть полезны. При «облачных» связях, вычислениях – это преимущество [15].

Работа в этом направлении продолжаемая.

Литература

1. Алексеева Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере Ленинградский юридический журнал. 2016. № 4 (46). С. 97-103.
2. Гулов В.П., Хвостов В.А., Попов А.С. Метод нормирования требований к информационной безопасности основных элементов медицинской информационной системы при заданном общем уровне безопасности Вестник новых медицинских технологий. 2015. Т. 22. № 2. С. 7-11.
3. Ищенко А.Н., Прокопенко А.Н., Страхов А.А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности россии в информационной сфере Проблемы правоохранительной деятельности. 2017. № 2. С. 55-62.
4. Крупко А.Э. Политика информационной безопасности: состав, структура, аудит информационной безопасности ФЭС: Финансы. Экономика. 2015. № 8. С. 27-32.
5. Лившиц И.И. Актуальность применения метрик информационной безопасности для оценки результативности проектов систем менеджмента информационной безопасности Менеджмент качества. 2015. № 1. С. 74-81.
6. Мартынов, И. (2018). Адаптивное тестирование бизнес-решений. Экономика. Бизнес. Информатика, 4(1), 1-8. Получено из https://internetnauka.com/index.php/journal/article/view/265

7. Минзов А.С., Невский А.Ю., Баронов О.Ю. О новой доктрине информационной безопасности России (размышления о совершенствовании системы профессионального образования в сфере информационной безопасности) ИТНОУ: Информационные технологии в науке, образовании и управлении. 2017. № 3 (3). С. 80-85.

8. Соляной В.Н., Сухотерин А.И. Становление направления "радиоэлектронная безопасность функционирования информационных объектов" в системе дополнительного профессионального образования по информационной безопасности Информационное противодействие угрозам терроризма. 2015. Т. 2. № 25. С. 255-260.

9. Федосеев А.А., Прохоров С.А., Иващенко А.В. Комплексное управление безопасностью в едином информационном пространстве предприятия Программные продукты и системы. 2008. № 4. С. 44.

10. Филькин К.Н., Филькин С.Н., Шелупанов А.А. Информационно-управляющая система поддержки принятия решений при управлении информационной безопасностью территориально-распределенной организации Безопасность информационных технологий. 2007. № 4. С. 83-86.

11. Филяк П.Ю., Шварев В.М. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности Информация и безопасность. 2015. Т. 18. № 4. С. 580-583.

12. Чашкин В.Н. Управление информационной безопасностью как элемент системы управления информационно-технологической деятельностью организации Безопасность информационных технологий. 2009. Т. 16. № 1. С. 123-124.

13. Чеботарева А.А. Обеспечение информационной безопасности личности: роль международной информационной безопасности и стратегического партнерства Вестник Академии права и управления. 2016. № 1 (42). С. 48-51.

14. Шамилев, Р., Шамилев, С., & Науразова, Э. (2018). Интранет-среда, соцсети, менеджмент компаний и некоторые проблемы международной экономики. Электронный междисциплинарный научный журнал с порталом международных научно-практических конференций Интернетнаука, 4(2), 133-139. Получено из https://internetnauka.ru/index.php/journal/article/view/588

15. Шамилев, Р., Шамилев, С., & Науразова, Э. (2018). Социально-экономические и правовые аспекты региональных и муниципальных систем противодействия коррупции. Экономика. Бизнес. Информатика, 4(3), 320-327. Получено из https://internetnauka.com/index.php/journal/article/view/288

16. Шамилев, С. (2018). Нечетко-множественная поддержка решения о покупке ценных бумаг. Электронный междисциплинарный научный журнал с порталом международных научно-практических конференций Интернетнаука, 4(1), 72-83. Получено из https://internetnauka.ru/index.php/journal/article/view/581

17. Якубова, И. (2018). Аудит информационной безопасности коммерческого веб-ресурса. Экономика. Бизнес. Информатика, 4(2), 194-201. Получено из https://internetnauka.com/index.php/journal/article/view/275

References

1. Alekseeva E.V. The doctrine of the information security of the Russian Federation as a key aspect of the legal support of national security in the information sphere The Leningrad legal journal. 2016. № 4 (46). Pp. 97-103.

2. Gulov V.P., Khvostov V.A., Popov A.S. Method of rationing the requirements for information security of the basic elements of a medical information system for a given general level of security. Herald of new medical technologies. 2015. Vol. 22. No. 2. P. 7-11.

3. Ishchenko A.N., Prokopenko A.N., Strakhov A.A. A new doctrine of information security of the Russian Federation as the basis for countering threats to the security of Russia in the information sphere Problems of law enforcement. 2017. No. 2. S. 55-62.

4. Krupko A.E. Information security policy: composition, structure, audit of information security of FES: Finance. Economy. 2015. No. 8. P. 27-32.

5. Livshits I.I. The relevance of the use of information security metrics for assessing the effectiveness of information security management systems projects Quality management. 2015. No. 1. S. 74-81.

6. Martynov, I. (2018). Adaptive testing of business solutions. Economy. Business. Computer Science, 4 (1), 1-8. Obtained from https://internetnauka.com/index.php/journal/article/view/265

7. Minzov A.S., Nevsky A.Yu., Baronov O.Yu. On the new doctrine of information security in Russia (reflections on improving the system of vocational education in the field of information security) ITNOU: Information technology in science, education and management. 2017. No. 3 (3). Pp. 80-85.

8. Solyarnoy V.N., Sukhoterin A.I. Formation of the direction "electronic safety of information objects functioning" in the system of additional professional education in information security Information countering the threats of terrorism. 2015. Vol. 2. No. 25. P. 255-260.

9. Fedoseev, A.A., Prokhorov, S.A., Ivashchenko, A.V. Integrated security management in a single information space of an enterprise Software products and systems. 2008. № 4. S. 44.

10. Filkin, K.N., Filkin, S.N., Shelupanov, A.A. Information management decision-making support system for managing information security of a geographically distributed organization Information technology security. 2007. No. 4. P. 83-86.

11. Filyak P.Yu., Shvarev V.M. Ensuring the information security of the organization based on the information security management system Information and security. 2015. Vol. 18. No. 4. P. 580-583.

12. Chashkin V.N. Information security management as an element of the organization's information technology management system Information technology security. 2009. V. 16. No. 1. P. 123-124.

13. Chebotareva A.A. Ensuring personal information security: the role of international information security and strategic partnership. Vestnik of the Academy of Law and Management. 2016. № 1 (42). Pp. 48-51.

14. Shamilev, R., Shamilev, S., & Naurazova, E. (2018). Intranet-environment, social networks, company management and some problems of the international economy. Electronic interdisciplinary scientific journal with a portal of international scientific-practical conferences Internet science, 4 (2), 133-139. Received from https://internetnauka.ru/index.php/journal/article/view/588

15. Shamilev, R., Shamilev, S., & Naurazova, E. (2018). Socio-economic and legal aspects of regional and municipal anti-corruption systems. Economy. Business. Computer Science, 4 (3), 320-327. Obtained from https://internetnauka.com/index.php/journal/article/view/288

16. Shamilev, S. (2018). Fuzzy-multiple support for the decision to purchase securities. Electronic interdisciplinary scientific journal with a portal of international scientific conferences Internet Science, 4 (1), 72-83. Received from https://internetnauka.ru/index.php/journal/article/view/581

17. Yakubova, I. (2018). Information security audit of a commercial web resource. Economy. Business. Computer Science, 4 (2), 194-201. Obtained from https://internetnauka.com/index.php/journal/article/view/275