УДК 343.9:004.056
ББК Х518.9+Х401.114

Ч.Ш. КУПИРОВА, Ю.А. КУЗЬМИН

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОБЪЕКТ КИБЕРПРЕСТУПНОСТИ

Ключевые слова: *криминология, объект преступного посягательства, киберпространство, информационная безопасность, киберпреступность, компьютерные преступления, защита информации.*

Проведен анализ понятия «киберпространство» как виртуального информационного пространства, моделируемого с привлечением компьютерных систем, хранящего некоторую информацию, которая распространяется по глобальным сетям. Проведен анализ понятия «киберпреступность» как преступного деяния, совершенного в киберпространстве, создающего круг проблем по совершенствованию защитных мер от нелегального доступа к информации в глобальной сети Интернет, использования сведений с целью нанесения вреда с помощью распространения различных программ вирусного характера. Определен объект киберпреступления, который весьма обширен и кроме общественных отношений включает как право на информацию, так и саму информацию не как предмет, а как явление. Важнейшим из таких объектов киберпреступности является информационная безопасность, являющаяся одной из важных составляющих глобальной безопасности.

Обоснована актуальность вопросов по организации процессов обработки, хранения, распространения и защиты информации в глобальных информационно-коммуникационных системах. Выделено особое значение и необходимость тесного взаимодействия информационной безопасности с экономической и национальной безопасностью. Информационная безопасность включает в себя защиту информационных сетей, ресурсов, программных средств, объектов интеллектуальной собственности и других нематериальных активов, включая имущественные интересы участников различного рода правоотношений.

Актуальность темы защиты информационной безопасности киберпреступности вызвана тем, что сегодня наблюдаем рост таких явлений, как киберпреступность и кибертерроризм, появляются определенные виды информационного оружия, с помощью которого против России могут вестись глобальные информационные войны, информационно развитые государства нацелены на стимулирование «утечки интеллекта» и капиталов из нашей страны, осложняется решение вопросов сохранения государственной, коммерческой, служебной и персональной тайны, так как низкий уровень отечественных информационных технологий обуславливает построение информационной инфраструктуры России на базе импортной техники и технологий.

Под киберпреступностью понимается преступная деятельность, совершаемая с использованием компьютерных систем и сетей. Такая деятельность главным образом направлена против безопасности информации, хранящейся на электронных носителях (например, на компьютере).

Понятия «киберпреступления» и «компьютерные преступления» вполне можно считать тождественными, поскольку оба они применяются для обозначения группы одних и тех же преступных деяний.

Термин «киберпреступность» можно определить как преступное деяние, совершенное в киберпространстве. «Киберпространство» – это виртуальное информационное пространство, моделируемое с привлечением компьютерных систем, хранящее некоторую информацию, которая распространяется по глобальным сетям. Так как применение защитных мер борьбы против киберпреступности невозможно без понимания смысла этого термина, исследователи, детально рассмотрев данное явление, дали ему пространственное определение. Киберпреступность – это правонарушения, совершаемые в сфере информационных технологий. Киберпреступностью является любая преступная активность, где объектом в качестве цели и/или инструмента является компьютер или сетевое устройство. Согласно Европейской Конвенции по киберпреступлениям, киберпреступления – это правонарушения, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерное использование указанных систем, сетей и данных [2]. С целью борьбы с киберпреступностью необходимо совершенствовать защитные меры от нелегального доступа к информации в глобальной сети Интернет, использования сведений с целью нанесения вреда с помощью распространения различных программ вирусного характера [3. С. 192].

Объект «киберпреступления» весьма обширен и кроме общественных отношений включает как право на информацию, так и саму информацию не как предмет, а как явление. Одним из таких объектов киберпреступности является информационная безопасность. Информационная безопасность является одной из важных составляющих глобальной безопасности. В процессе глобализации, в условиях построения информационного общества роль информационной безопасности активно возрастает и, наоборот, глобальные процессы оказывают влияние на информационную безопасность и взаимосвязанные с ней иные виды безопасности, такие, как экономическая, национальная и глобальная.

Вследствие стремительного технологического прогресса закономерно возникают важные вопросы по организации процессов обработки, хранения, распространения и защиты информации в глобальных информационно-коммуникационных системах. Не секрет, что именно информационные технологии и развитая инфраструктура телекоммуникаций имеют сегодня важное значение в обеспечении роста производительности производства, административного и хозяйственного управления, в расширении информационного взаимодействия между людьми, распространении массовой информации, интеллектуализации общества и повышении его правовой культуры.

Информационная безопасность приобретает особое значение и вследствие тесного взаимодействия с экономической и национальной безопасностью вносит значительный вклад в глобальную безопасность. Под глобальной безопасностью можно понимать состояние глобальных процессов и форм их реализации, содействующих решению проблем, стоящих перед отдельными

государственными, региональными и местными администрациями, всестороннему развитию и обеспечению потребностей каждого человека.

Особенности распространения информации, возможности неограниченного и неконтролируемого их влияния, несанкционированный доступ, компьютерные вирусы остро поставили перед обществом проблемы информационной безопасности. Информационная безопасность должна осуществляться комплексно и систематически с использованием полного набора организационных, технических, аппаратно программных и иных средств. Становление общества нового информационного формата остро ставит вопрос информационной безопасности пространства государства, человека, общества.

Данный вопрос невозможно обойти или игнорировать, тем более что он становится очень актуальным и для нашей страны.

Информационная безопасность является более узким понятием и рассматривается как составляющая национальной безопасности. Информационная безопасность охватывает защиту информационных сетей, ресурсов и других активов, включая имущественные интересы участников различного рода правоотношений. В условиях глобализации усиливается значимость проблем, связанных с информационной безопасностью:

– возникновение и рост таких явлений, как киберпреступность и кибертерроризм;

– возникновение отдельных видов информационного оружия и ведение глобальных информационных войн;

– потеря национальной культуры или слияние ее с другими культурами и менталитетом других наций;

– стимулирование информационно развитыми государствами «утечки интеллекта» и капиталов;

– возникновение явлений «информационного взрыва», «информационного голода» и «информационных войн»;

– осложнение решения вопросов сохранения государственной, коммерческой, служебной и персональной тайны, так как низкий уровень отечественных информационных технологий обусловил построение информационной инфраструктуры России на базе импортной техники и технологий и др.

Проблему информационной безопасности невозможно решить без обновленной политики в области информатизации. Тенденции развития современного мира характеризуются созданием единого глобального информационного пространства на планете, так что проблема информационной безопасности становится проблемой коллективной, а не отдельно взятой страны.

Понятие информационной безопасности может рассматриваться в широком и в узком смысле [1. С. 68].

Информационная безопасность (в узком смысле) – необходимая и неотъемлемая составная часть других видов безопасности. Информационная безопасность – это неотъемлемая часть политической, экономической, военной, социальной и других составляющих национальной безопасности. Информационная безопасность вполне может рассматриваться как информационная безопасность предприятия (организации) – это состояние защищенности ин-

формации предприятия (организации) от дестабилизирующего влияния как внешних, так и внутренних угроз.

Информационная безопасность (в широком смысле) – самостоятельный вид безопасности наряду с национальной, экономической, военной, социальной и политической. Информационная безопасность может рассматриваться как информационная безопасность государства – это составляющая национальной безопасности, характеризующая состояние защищенности национальных интересов в информационной сфере от внешних и внутренних угроз.

Информационная безопасность обеспечивается:

– комплексом нормативных документов по всем аспектам использования средств вычислительной техники для обработки и хранения информации ограниченного доступа;

– комплексом государственных стандартов по использованию программных средств защиты информации;

– банком средств диагностики и профилактики компьютерных вирусов, новых технологий защиты информации и др.

В условиях распространения информационных воздействий справедливо следующее определение: информационная безопасность человека, общества, государства – это состояние их информационной вооруженности, способной активно противостоять преступности в сфере современных информационных технологий.

Информационная безопасность рассматривается также как единство концептуальных, теоретических и технических основ обеспечения на информационном уровне безопасности всех сфер государственной и общественной деятельности, а также сфер формирования, циркуляции, накопления и использования информации. В организационно-управленческом аспекте понятие «информационная безопасность» рассматривается как состояние защищенности жизненно важных интересов личности, общества и государства, при котором сводятся к минимуму отрицательное информационное воздействие, негативные последствия функционирования информационных технологий, нанесение ущерба из-за неполноты, несвоевременности и недостоверность информации, а также из-за несанкционированного распространения информации.

Мы согласны с мнением профессора А.С. Шаталова, который утверждает, что борьба с киберпреступностью представляет собой проблему международного масштаба [4. С. 80]. Непрекращающееся увеличение численности пользователей сети Интернет закономерно делает их зависимыми от информсообщества и уязвимыми от возможных киберпосягательств. Вместе с тем возрастает и вероятность пополнения числа жертв киберпреступников. В силу этого один из принципов Стратегии развития информационного общества в России на 2017–2030 гг. провозглашает обеспечение государственной защиты интересов россиян в информационной сфере. Острая необходимость в такой защите вызвана большим числом факторов, среди которых особо следует выделить:

– значительное увеличение объема информации, обрабатывающейся и хранящейся в киберпространстве;

– особую «привлекательность» для киберпреступников;

– наличие объективных сложностей, связанных с выявлением, раскрытием и расследованием киберпреступлений;

– нестандартность, сложность и постоянное обновление способов совершения киберпреступлений;

– длительную неосведомленность потерпевших о факте совершения киберпреступлений;

– отсутствие возможностей предотвращения, профилактики и пресечения киберпреступлений традиционными правовыми средствами.

Литература

1. *Городнов О.А.* Информационное право. М.: Проспект, 2018. 226 с.

2. Киберпреступность – определение, классификация интернет угроз [Электронный ресурс]. URL: http://elcomrevue.ru/kibeoprestupnost-chto-eto.

3. *Кириллова А.С.* Киберпреступность в Российской Федерации: основные проблемы и способы их решения // Евразийская юридическая конференция: сб. ст. междунар. науч.-практ. конф. Пенза: Наука и Просвещение, 2018. С. 190–193.

4. *Шаталов А.С.* Феноменология преступлений, совершенных с использованием современных информационных технологий // Право. Журнал Высшей школы экономики. 2018. № 2. С. 68–83.

КУПИРОВА ЧУЛПАН ШЕУКАТОВНА – кандидат юридических наук, доцент кафедры уголовно-правовых дисциплин, Чувашский государственный университет, Россия, Чебоксары (chulpan27@bk.ru).

КУЗЬМИН ЮРИЙ АНАТОЛЬЕВИЧ – старший преподаватель кафедры уголовно-правовых дисциплин, Чувашский государственный университет, Россия, Чебоксары (kya70@mail.ru).

Ch. KUPIROVA, Yu. KUZMIN

INFORMATION SECURITY AS AN OBJECT OF CYBERCRIME

Key words: *criminology, object of criminal encroachment, cyberspace, information security, cybercrime, computer crimes, information protection.*

The article analyses the concept of "cyberspace" as a virtual information space, simulated with the use of computer systems, storing some information that is distributed over global networks. It analyses the concept of "cybercrime" as a criminal act committed in the cyberspace, creating a range of problems to improve protective measures against illegal access to information in the global Internet, the use of information for the purpose of harming through the spread of various viral programs. The object of cybercrime is defined, which is very extensive and in addition to public relations includes both the right to information and the information itself not as an object, but as a phenomenon. The most important of these objects of cybercrime is information security, which is one of the important components of global security.

The urgency of issues on organizing the processes of processing, storage, distribution and protection of information in global information and communication systems is substantiated. A special importance and necessity of close interaction between information security and economic and national security is emphasized. Information security includes protection of information networks, resources, software, intellectual property objects and other intangible assets, including property interests of participants in various legal relations.

The relevance of protecting information security from cybercrime is due to the fact that today the growth of phenomena such as cybercrime and cyber terrorism is observed, certain types of information weapons are developed, using which global information wars can be waged against Russia, information-oriented states are aimed at encouraging "leakage of intelligence" and assets from our country, which is compounded by issues of

preserving the state, commercial, official and personal secrets, as the low level of domestic information technology results in creating informational infrastructure of Russia on the basis of imported equipment and technologies.

References

1. Gorodnov O.A. *Informatsionnoe pravo* [Information right]. Moscow, Prospekt Publ., 2018, 226 p.

2. *Kiberprestupnost' – opredelenie, klassifikatsiya internet ugroz* [Cybercrime definition, classification of Internet threats]. URL: http://elcomrevue.ru/kibeoprestupnost-chto-eto

3. Kirillova A.S. *Kiberprestupnost v Rossiyskoy Federatsii: osnovnyie problemyi i sposobyi ih resheniya* [Cybercrime in the Russian Federation: major challenges and solutions]. *Evraziyskaya yuridicheskaya konferentsiya: sb. st. Mezhdunar. nauch.-prak. konf.* Penza, Nauka i Prosveschenie Publ., 2018, pp. 190–193.

4. Shatalov A.S. *Fenomenologiya prestupleniy, sovershennyih s ispolzovaniem sovremennyih informatsionnyih tehnologiy* [Phenomenology of crimes committed using modern information technologies]. *Pravo. Zhurnal Vyisshey shkolyi ekonomiki*, 2018, no. 2, pp. 68–83.

KUPIROVA CHULPAN – Candidate of Legal Sciences, Associate Professor of Criminal Law Department, Chuvash State University, Russia, Cheboksary (chulpan27@bk.ru).

KUZMIN YURIY – Senior Lecturer of Criminal Law Department, Chuvash State University, Russia, Cheboksary (kya70@mail.ru).