Бураева Людмила Александровна
канд. физ.-мат. наук, доцент
Северо-Кавказский институт повышения квалификации (филиал)
ФГКОУ ВО «Краснодарский университет МВД России»
г. Нальчик, Кабардино-Балкарская Республика

ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЯМИ

***Аннотация**: в данной статье рассмотрена проблема киберпреступлений. В работе четко выделены типы возможных киберпреступлений.*

***Ключевые слова**: информатизация, информация, информационное общество, технологии, информационная безопасность, киберпреступления.*

Характерной чертой развития современного общества является информатизация практически всех сфер его жизнедеятельности. Сегодня информация выступает в качестве основного ресурса общества, наряду с природными и энергетическими. В качестве средств информационное общество широко использует компьютерные технологии, телекоммуникационные сети, электронные библиотеки, банки данных, автоматизированные системы, системы искусственного интеллекта. Основная проблема, возникающая при этом перед обществом – как обеспечить безопасность информации, то есть предупредить совершение так называемых компьютерных преступлений или преступлений в глобальной сети. Анализ криминологической обстановки в области информационной безопасности показывает, что злоумышленные действия над информацией во всемирной сети не только не уменьшаются, а имеют достаточно устойчивую тенденцию к росту, а способы и формы совершения киберпреступлений множатся в своем разнообразии [4].

Лидируют среди киберпреступлений преступления экономической направленности, при их совершении злоумышленники стараются получить доступ к конфиденциальным коммерческим данным: о клиентах банков, их счетах и операциях, которые затем можно использовать для хищения денежных средств. По

данным аналитиков, ущерб от мошенников, взламывающих программы дистанционного банковского обслуживания – интернет-банкинга, доходит до десятков миллионов рублей [10].

Среди остальных видов киберпреступлений все большие обороты набирают преступления террористической и экстремистской направленности в сети Интернет. Современные религиозно-экстремистские организации все чаще выставляют свои обращения через сайты экстремистской направленности, которые играют роль «пресс-центров» для лидеров боевиков, террористов, повстанцев, религиозных радикалов. Можно сказать, что «всемирная паутина» стала одним из рупоров экстремистов и террористов в информационной войне [3]. Исследованием данной проблемы современности занимаются многие ученые [2; 5–7; 9]. В целях обеспечения надёжной защиты стран СНГ от пропаганды со стороны террористических и религиозно-экстремистских организаций необходимы значимые финансовые затраты. В такой ситуации целесообразным является либо формирование общего информационного центра, финансирующегося всеми странами-членами Содружества, либо обеспечение активного информационного обмена между государствами по данному вопросу.

Все чаще глобальное пространство используется для организации массовых беспорядков [1], в настоящее время стремительно распространяются новые формы социальной организации, так называемые флешмоб-акции, то есть заранее спланированные массовые акции, как правило, организуемые через современные социальные сети, в которой большая группа людей внезапно появляется в общественном месте, в течение нескольких минут выполняет заранее оговоренные действия, которые называются сценарием, и затем быстро расходится.

Среди компьютерных преступлений выделяется так называемый компьютерный терроризм, ставший приемлемой альтернативой традиционным террористическим актам, по следующим причинам: анонимность, низкий риск обнаружения и возможность действия террориста практически в любой местности. По сведениям аналитиков, наибольший интерес для террористов представляют:

энергетическая сфера, военная и ядерная структура государства, сфера транспортных перевозок (особенно воздушный транспорт) и финансовая сферы государства. Так, Израильская армия уже опробовала форму ведения кибервойны в 2007 году, при нападении на секретный строительный объект в Сирии. Израильским военным хакерам удалось тайно внедрить «троянский вирус» в код программного обеспечения сети сирийской противовоздушной обороны, после чего израильтяне смогли управлять системой противовоздушной обороны противника. Противодействие проявлениям кибертерроризма требует комплексного подхода, объединяющего силовые, политико-дипломатические, экономические и гуманитарные формы и методы действий, в сочетании с эффективными антитеррористическими мерами, как на национальном, так и на международном уровнях.

В России борьбой с киберпреступлениями занимается Управление «К» МВД РФ и отделы «К» региональных управлений внутренних дел. Однако, в связи с растущей угрозой киберпреступности и в целях более эффективного противодействия кибершпионажу, президентом России Владимиром Путиным в январе 2013 года было дано поручение ФСБ РФ создать систему защиты от хакерских атак. Целью данной системы будет обнаружение, предупреждение и ликвидация последствий компьютерных атак на информационные ресурсы, системы и ИКТ-сети, находящиеся на территории страны, а также в дипломатических представительствах и консульских учреждениях России за рубежом. В 2013 году утверждены «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» [8].

Список литературы

1. Абазов И.С. Особенности и специфика тактических действий подразделений ОВД при обеспечении охраны общественного порядка на массовых мероприятиях // Теория и практика общественного развития. – 2016. – №2. – С. 75–78.

2. Аккаева Х.А. Основные проблемы борьбы с терроризмом на современном этапе // Теория и практика общественного развития. – 2015. – №9. – С. 114–116.

3. Бураева Л.А. Информационные войны и информационный терроризм в современном мире: методы и поле действия // Известия Кабардино-Балкарского научного центра РАН. – 2014. – №1. – С. 7–11.

4. Бураева Л.А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. – 2015. – №13. – С. 96–99.

5. Гаужаева В.А. Признаки терроризма, формирующие его понятие в нормативных и научных источниках // Актуальные вопросы юридических наук в современных условиях: Сборник научных трудов по итогам международной научно-практической конференции (г. Санкт-Петербург, 2015). – Инновационный центр развития образования и науки. – С. 69–72.

6. Карданов Р.Р. Роль судебно-криминалистических экспертиз в антитеррористической деятельности // Доклады Адыгской (Черкесской) Международной академии наук. 2014. – №1. – Т. 16. – С. 92–96.

7. Манукян А.Р. Проблемы противодействия терроризму и экстремизму на территории Российской Федерации // Образование. Наука. Научные кадры. – 2015. – №2. – С. 194–197.

8. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 №Пр-1753) // СПС «Консультант Плюс».

9. Токбаев А.А Некоторые аспекты противодействия экстремизму в условиях современной России // Теория и практика общественного развития. – 2016. – №2. – С. 79–81.

10. Хакеры украли миллиард долларов в ходе крупнейшей атаки на банки [Электронный ресурс]. – Режим доступа: http://lenta.ru/news/2015/02/16/yardhack/ (дата обращения: 12.08.2016).