Краснодарский университет МВД России

ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
II Всероссийской научно-практической
конференции

(21 мая 2015 г.)

Краснодар
2015

УДК 004
ББК 67.410.212
И74

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

И74 **Информационное противодействие** экстремизму и терроризму : материалы II Всероссийской научно-практической конференции, 21 мая 2015 г. / редкол.: А. Б. Сизоненко, С. Г. Клюев, Е. В. Запорожец, А. Г. Александров, В. Н. Цимбал. – Краснодар : Краснодарский университет МВД России, 2015. – 120 с.

ISBN 978-5-9266-0977-3

Представлены доклады и тезисы выступлений участников II Всероссийской научно-практической конференции «Информационное противодействие экстремизму и терроризму», в которых рассмотрены наиболее острые вопросы обеспечения информационной безопасности при организации противодействия экстремизму и терроризму.

Для профессорско-преподавательского состава, докторантов, адъюнктов, курсантов, студентов и слушателей образовательных организаций, сотрудников правоохранительных органов, повышающих уровень своих знаний.

УДК 004
ББК 67.410.212

ISBN 978-5-9266-0977-3

Н.И. Журавленко,
к.ю.н., доцент, Крымский филиал
Краснодарского университета МВД России,
ibiubp@mail.ru

ПРИЧИНЫ И УСЛОВИЯ РАЗВИТИЯ ТЕРРОРИЗМА В РОССИИ

В статье исследованы особенности терроризма в России и основные факторы, влияющие на рост преступлений террористического характера. На основе проведенного анализа делается вывод о необходимости объединения усилий законодательной, исполнительной и судебной властей, различных ведомств, средств массовой информации и населения в борьбе с терроризмом.

Среди факторов, способствующих росту терроризма в России, в научной литературе обычно выделяют следующие: увеличение количества террористических проявлений в странах ближнего и дальнего зарубежья; социально-политическая и экономическая нестабильность в сопредельных государствах, наличие вооруженных конфликтов в некоторых из них, а также территориальных претензий; стратегические установки некоторых иностранных спецслужб и зарубежных (международных) террористических организаций на эскалацию социально-политической напряженности в России; отсутствие надежного контроля за въездом и выездом граждан из России, а также сохраняющаяся «прозрачность» ее границ; наличие каналов нелегального поступления в Россию из-за рубежа оружия, взрывчатых веществ и других, запрещенных для оборота веществ и предметов; образование российской диаспоры (расселение граждан РФ за пределами России); наличие в стране значительного нелегального «рынка» оружия и относительная легкость его приобретения; наличие значительных контингентов лиц, прошедших «школу войны» в Афганистане, Приднестровье, Таджикистане, Чечне и других «горячих точках», их недостаточная социальная адаптированность в обществе; ослабление целого ряда административных режимов; деятельность ряда экстремистских группировок; обостренное чувство социальной неуверенности, незащищенно-

сти у значительных контингентов граждан; слабая работа по защите прав граждан правоохранительных и государственных органов, общественных организаций; низкий уровень правовой и политической культуры в обществе; утрата многими людьми идеологических и духовных жизненных ориентиров, чувства национальной гордости; рост социальной агрессивности; чувство отчаяния и общественная фрустрация; падение авторитета закона и власти, веры в возможность позитивных изменений; широкая пропаганда в кино, на телевидении, в прессе и литературе культа жестокости и насилия, чуждого образа жизни, духовных ценностей и мировоззрения [1, 88].

Перечисленные причины довольно полно раскрывают основные факторы, влияющие на рост преступлений террористического характера в России. Изучение этих причин позволяет вычленить наиболее важные из них – социальные противоречия, не получившие своевременного разрешения и достигающие конфликтной формы, особенно на ее конфронтационной стадии.

Для их решения необходим комплексный межведомственный подход, сориентированный на нейтрализацию и устранение причин и факторов, порождающих социальную, в том числе межнациональную и криминальную, напряженность, различные проявления политического и иного экстремизма. В их числе такие социально-экономические факторы, как свертывание производства; рост вынужденной скрытой и явной безработицы; падение жизненного уровня населения; последствия длящихся межнациональных конфликтов, а также порожденные ими проблемы беженцев и вынужденных мигрантов, нарушение привычных социальных и экономических связей; наличие в стране сил, в том числе националистических, криминальных и внешних, заинтересованных в сохранении и эскалации напряженности.

Ученые-террологи и специалисты-практики выделяют достаточно широкий спектр социальных противоречий, обусловливающих возникновение и развитие терроризма. К ним относятся социально-экономические, идеологические, политические, межгосударственные, национальные, религиозные и иные противоречия и конфликты.

В научной литературе имеются многочисленные суждения о причинах возникновения и распространения современного терро-

ризма, которые, как правило, сводят их к тем или иным внешним воздействиям либо связывают с природой современной западной демократии, якобы беззащитной перед лицом терроризма. Среди различного рода условий, которые характеризуют социальную обстановку в той или иной стране или регионе, отечественные ученые-террологи выделяет следующие причины и условия.

К первой группе относят: большую остроту или непримиримость межгосударственных или внутренних противоречий; распространение идеологии насилия как метода решения общественных проблем; глубокую социальную дифференциацию и разрыв в уровне материальных условий жизни различных слоев населения; идеологический раскол общества; резкое снижение социальной защищенности населения, процессы его маргинализации; невозможность защиты социальных интересов отдельных групп общества и др.

Ко второй группе факторов относят: неэффективность международной или внутригосударственной системы борьбы с преступностью, в том числе с терроризмом; низкую политическую и правовую культуру населения, отдельных его групп; ухудшение межгосударственных отношений, рост социальной напряженности и другие причины [2, 40-41].

Как справедливо замечает С.А. Гончаров, говоря о терроризме как об одной из крайних форм политического экстремизма, необходимо постоянно иметь в виду эту родовую связь, а также понимать то, что особенности терроризма в России определяются специфическими глубинными причинами, лежащими в основе политического экстремизма, прежде всего теми факторами, которые влияют на его развитие [2, 181-190].

Безусловно, терроризм нельзя рассматривать отдельно, вне экстремизма. Именно этим было продиктовано принятие Федеральных законов от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» и № 112-ФЗ «О внесении изменений и дополнений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О противодействии экстремистской деятельности» [4].

Поскольку рассматривая проблемы терроризма в отрыве от экстремизма можно впасть в серьезное принципиальное заблуждение, а именно – иллюзию возможности подавления терроризма

не затрагивая при этом причин, его порождающих. Поэтому при рассмотрении таких взаимосвязанных явлений необходимо учитывать причины и условия появления не только политического и уголовного экстремизма в целом, но и терроризма как его конкретной формы.

Как отмечалось выше, коренные причины терроризма лежат в углубляющемся социальном и политическом кризисе, в ослаблении правопорядка, что в свою очередь и порождает новые противоречия, для разрешения которых отдельные лица и организации все чаще прибегают к насилию. Таким образом, через призму противоречий, порождающих политический экстремизм и прямо воздействующих на расширение его сферы, более подробно выделим и сформулируем особенности, присущие терроризму в России на современном этапе.

Во-первых, необходимо учитывать зависимость применения террора от всех социальных, политических, экономических и других процессов, происходящих в стране. Усиление терроризма в стране, как правило, происходит тогда, когда утрачены старые ценности и еще не сформировались новые, когда разрушена бывшая государственная система, в том числе и система обеспечения общественной и государственной безопасности. В сложившейся ситуации становится совершенно очевидным, что не решив радикальным образом социальные, экономические, национальные, управленческие проблемы, не удастся ликвидировать социальную основу терроризма.

Вторая особенность заключается в тесной взаимосвязи между уголовным и политическим терроризмом. Именно в уголовной среде чаще всего вербуются исполнители политического терроризма, о чем свидетельствуют все крупные акции политического террора. Вдохновители и организаторы подобного рода преступлений предоставляют исполнителям из числа уголовных элементов своеобразную «идеологическую нишу», позволяющую им осуществлять свою преступную деятельность, рассматривая ее как служение «высшим», чаще всего националистическим, целям. В этом плане уголовная деятельность, прежде всего деятельность групп организованной преступности, построенных на этнической основе, связывает свои акции с добыванием финансовых, материально-технических средств, в том числе вооружения, не только

для своих непосредственно уголовных нужд, но и для нужд политического экстремизма. Таким образом, благодаря такой тесной взаимосвязи происходит своеобразное воспроизводство преступной деятельности.

Кроме того, на развитие терроризма работает и прямая пропаганда насилия в средствах массовой информации. Поэтому террористы часто предстают в глазах общества как «борцы» за национальную или какую-либо социальную идею. Это связано и с культивированием политического радикализма как способа достижения политических целей – прежде всего захвата власти.

Еще одной особенностью терроризма в России является его современная вооруженность, включающая новейшие виды оружия. Этому способствовали, с одной стороны, распад в 90-е годы прошлого века на территории бывшего СССР одной из самых мощных армий в мире, а с другой стороны – сложные социальные процессы, происходившие в эти годы в армии и вокруг нее. Именно эти условия, по существу, открыли военные арсеналы как для уголовных элементов, так и для представителей политического экстремизма. Более того, крупные финансовые средства, имеющиеся в руках политических радикалов, сторонников крайних форм и методов политической борьбы, позволяют сейчас оснащать террористов-боевиков, да и просто бандитов, самым современным техническим оборудованием, экипировкой, не только не уступающим, но нередко и более совершенным, чем те средства, которые есть у армии и правоохранительных органов.

Другая причина внутрироссийского терроризма – в усилении социально-политической несправедливости, в углублении социальной незащищенности граждан, в обострении межнациональных отношений, которые в значительной степени являются питательной средой политического и экономического террора. Здесь сталкиваются политико-криминальные группировки в борьбе за власть и перераспределение народных богатств.

По мнению ряда ученых, значительно реже возникают причины терроризма на религиозной почве. Как правило, они дополняют националистические и политические причины, способствуя размежеванию людей. Эти причины все чаще стали проявляться на территории России, что вызывает особую тревогу за целост-

ность страны и может вызвать новые военные действия со стороны религиозных фанатиков. Однако не только религиозные, но и все другие вышеуказанные причины не имеют первостепенного значения при совершении террористических акций. Главную роль здесь, как и при совершении любых других умышленных преступлений, играют причины социально-психологического плана, т.е. личностные качества и свойства преступников, которые непосредственно влияют на формирование мотива преступления.

В настоящее время набирает силу международный терроризм антигосударственного характера. Исследователи отмечают его устойчивость и приходят к выводу, что никакие бомбардировки стран – «спонсоров международного терроризма» – не уничтожат это явление, потому что за его появлением стоят до сих пор не замеченные нами изменения [5, 9].

Думается, правы те политологи, которые считают, что всем нам надо учиться не только точности бомбардировки тренировочных лагерей какой-либо очередной «Аль-Каиды», но и учиться понимать друг друга. Действительно, мы пока еще даже не пытаемся понять, что движет террористами, мы просто их даже не знаем. В представлении большинства людей террористы – это «экстремисты», «фанатики», «бандиты» либо просто психически ненормальные люди. Наше незнание людей, с которыми идет непримиримая борьба, и наше нежелание знать их проблемы и мнения – это тоже одно из условий обострения и глобализации как российского, так и международного терроризма.

Подводя итог проведенному анализу причин и условий развития терроризма в России следует сделать вывод, что в нынешних условиях государство должно иметь целостную программу по борьбе с терроризмом, объединяющую усилия законодательной, исполнительной и судебной властей, различных ведомств, средств массовой информации и населения. При этом, развертывая и усиливая борьбу против терроризма, необходимо пресекать создание различных незаконных вооруженных групп, предпринимать еще более активные меры по подавлению организованной преступности, пресечению противоправных действий против личности и имущества граждан.

Литература

1. Хлобустов О.М., Гончаров С.Г. Терроризм: реальность сегодняшнего состояния // Современный терроризм: состояние и перспективы. – М.: Эдиториал УРСС, 2000.

2. Авдеев Ю.И. Терроризм как социально-политическое явление // Современный терроризм: состояние и перспективы. – М.: Эдиториал УРСС, 2000.

3. Гончаров С.А. Особенности терроризма в России // Актуальные проблемы Европы / Проблемы терроризма: Проблемно-тематический сборник. – М., РАН, Институт научной информации по общественным наукам. № 4. 1997.

4. Федеральный закон от 25 июля 2002 г. «О противодействии экстремистской деятельности» № 114-ФЗ // Российская газета. № 138–139. 2002. 30 июля.

5. Ольшанский Д.В. Психология терроризма. – СПб.: Питер, 2002. С. 9.

Н.И. Журавленко,
к.ю.н., доцент, Крымский филиал
Краснодарского университета МВД России,
ibiubp@mail.ru
Л.Е. Шведова,
к.т.н., Крымский филиал
Краснодарского университета МВД России,
larisashvedova@yandex.ru

ИСПОЛЬЗОВАНИЕ ТЕРРОРИСТАМИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ТЕХНИЧЕСКИХ СРЕДСТВ

В статье рассмотрены как традиционные «летальные», так и нетрадиционные «информационные» технологии современного терроризма, дана правовая и криминологическая характеристика этому явлению, проанализированы его основные виды и направления, изучены методы и средства совершения терактов шахидами-смертниками.

В качестве способов терроризма российский уголовный закон называет «совершение взрыва, поджога и иные действия». Как следует полагать, в числе иных действий могут быть массовые и единичные отравления людей, радиоактивное заражение, захват транспортного средства, применение оружия и др. Соответственно орудиями террора могут выступать взрывчатые, радиоактивные, ядовитые вещества, огнестрельное оружие и другие средства, пригодные для лишения жизни людей в террористических целях.

Следует отметить, что приведенный перечень способов и орудий террора ни в коем случае нельзя считать исчерпывающим, так как человеческая изобретательность по части насилия поистине безгранична. По мере развития науки и техники появляются все новые способы совершения террористических актов. Например, в настоящее время существует реальная угроза широкомасштабного использования террористами радиоактивных веществ. Взорвав с помощью обычной взрывчатки радиоактивные вещества или отходы их производства, спровоцировав тепловой выброс (как в Чернобыле) на захваченной атомной электростанции, осуществив взрыв на перерабатывающем радиоактивные вещества предприятии, разбрызгав с помощью поливальной машины или распылив из самолета, предназначенного для обработки ядохимикатами сельскохозяйственных угодий, радиоактивные изотопы по улицам города, террористы смогут осуществить высокотоксичное заражение огромной территории, что вызовет катастрофические последствия [1, 8-10].

В соответствии со ст. 3 Федерального закона «О противодействии терроризму» терроризм – это «идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий» [2]. В ст. 3 ранее действовавшего ФЗ «О борьбе с терроризмом» 1998 г. под этим понятием подразумевались «насилие или угроза его применения в отношении физических лиц или организаций… и т. д.», что приводило к смешению его с понятием «террористическая акция», которое определялось как «непосред-

ственное совершение преступления террористического характера», т. е. факт проявления терроризма [2].

В последнее время основными исполнителями террористических акций все чаще выступают шахиды-камикадзе – особо жестокая каста террористов, представителями которой за последние 20 лет было совершено более трехсот актов суицидного терроризма. Если в 80-х годах случаи суицидного терроризма отмечались лишь в Ливане, Кувейте и Шри Ланке, то в 90-х годах они происходили уже в Израиле, Индии, Панаме, Алжире, Аргентине, Пакистане, Хорватии, Турции, Танзании и Кении.

Как правило, шахиды – это молодые мужчины, но жертвуют собой и женщины. Однако в фундаменталистских террористических группах слабый пол в качестве смертниц не используется – запрещает ислам. Но чем меньше террористическими группами провозглашается религиозных лозунгов, тем выше процент использования ими женщин-смертниц.

Использовать женщин-смертниц легче. Традиционно они вызывают меньше подозрений. Кроме того, возникают определенные проблемы с проведением их обыска, особенно, когда они маскируются под беременных. Женщин удобно использовать в качестве своеобразной «медовой ловушки», «любовной наживки».

Совершенствуются и сами нательные пояса с самодельными взрывными устройствами (СВУ). Они стали меньше по размерам, и в них начали использовать взрывчатое вещество, которое не обнаруживается приборами досмотра. Более того, взрыватели стали электронными, зачастую соединенными с датчиками кровяного давления и пульса. Именно они приведут СВУ в действие если террорист будет ранен и не сможет его применить самостоятельно. Например, при захвате школы в Беслане один из террористов постоянно стоял на книге, удерживая в нажатом состоянии кнопку, соединенную с цепью инициирования взрыва. Его ранение или смерть неизбежно должны были привести к подрыву боезарядов, установленных в спортзале с 1200 заложниками. Это также исключает его попадание в плен и дачу им показаний. Подобными взрывателями некоторые организации оснащают и террористов на машинах, начиненных взрывчаткой.

Мировой опыт свидетельствует о том, что предотвратить действия террориста-смертника почти невозможно, но все-таки

при своевременном проведении контрмер есть шанс. Самым действенным способом здесь является агентурное проникновение в террористические организации для выявления планов по подготовке суицидных терактов и их исполнителей. Ведь, несмотря на самые строгие меры конспирации, предпринимаемые террористами, в подготовке таких терактов участвует много людей: ведется разведка объекта, изучается обстановка вокруг него, готовятся места укрытия для смертников перед проведением теракта. Исполнителей обеспечивают питанием, одеждой, документами, изготавливаются и доставляются к месту теракта СВУ, проводятся тренировки, обеспечивается проникновение на объект. Только маршруты отхода для смертников не предусматриваются, да они им и ни к чему.

События последнего времени показывают, что деятельность международных террористических организаций, приобретая принципиально новые черты, становится все более изощренной и циничной. Изменяются стратегические направления ударов, совершенствуется тактика современных террористических группировок.

Чтобы любой ценой добиться своих целей, террористы все чаще делают своими мишенями не государственные и военные объекты, не крупных политических лидеров, а гражданское население, туристов, посетителей крупных зрелищных мероприятий, рынков, ресторанов. Все это приводит к растущему числу невинных человеческих жертв (достаточно вспомнить масштабные теракты в США, на Филиппинах, в Индонезии, Израиле и России) [4, 78].

Теракт, все больше становясь самоцелью террористов, имеет основную задачу – стать новостью номер один, психологически поразить огромные массы населения. Поэтому террористы, расширяя практику использования смертников-самоубийц, по своей сути не заинтересованы в переговорах о тактических уступках.

В настоящее время все чаще отмечаются факты освоения информационных технологий и компьютерных сетей транснациональными террористическими и экстремистскими организациями, что обусловило появление наиболее опасной разновидности компьютерной преступности – кибертерроризма. По заявлениям западных спецслужб и правоохранительных органов, такие террористические организации, как «Аль-Каида», «Хезболла», «Абу

Нидаль» и другие активно используют возможности Интернета. С применением его возможностей ими осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой, религиозной и других форм нетерпимости, а также вовлечение в свои ряды новых членов, осуществление незаконных финансовых операций и т. д.

Серьезная угроза подобных действий со стороны международных террористов стоит в настоящее время перед США, Великобританией, Германией и рядом других стран Запада. По данным экспертов, в настоящее время в них резко возросло количество кибератак на государственные информационные системы, последствия которых не менее опасны, чем традиционные террористические акты с использованием смертников, взрывчатки и т. д. Такие преступные деяния могут выводить из строя системы управления и функционирования атомных и других важных объектов, нефте- и газопроводов, электростанций, железных дорог, аэропортов, объектов водоснабжения. Поэтому кибертерроризм порою сравнивают по эффекту применения с воздействием ядерного, бактериологического и химического оружия. Например, в 2000 г. в России неизвестные злоумышленники взломали компьютерную сеть РАО «Газпром» и на некоторое время получили полный контроль над центральным пунктом распределения газовых потоков. События 11 сентября 2001 г. в США сопровождались кибератаками на навигационные системы Нью-Йоркского аэропорта, а позже последовали атаки на систему энергообеспечения нескольких штатов.

В недавнем прошлом «Ирландская Республиканская Армия» в Великобритании создавала специальные группы хакеров, в задачи которых входили взлом банковских счетов и похищение денег для финансирования этой террористической организации, а также сбор информации в Сети для будущих терактов.

Многие хакерские группы, такие, как югославская «Черная рука», пакистанская «G-Force» или палестинская «Unix Security Guard», не сделав ни единого выстрела, своими кибератаками наносили столь серьезный ущерб институтам государственной власти ряда стран, что заняли «достойное» место в списках террористических организаций [5].

Наряду с угрозами информационной безопасности растущая широкая доступность современных технологий резко усиливает угрозу ядерного, химического, биологического, информационного и других видов высокотехнологичного терроризма. Но все же против «черных» технологий, используемых террористами, всегда найдутся «белые» технологии, методы и средства антитеррора. Разум и интеллект в конечном итоге сломят человеконенавистническую парадигму и злой гений террористов.

Угрозы терроризма могут быть нейтрализованы только путем консолидации всего мирового сообщества для ликвидации социальных, экономических и идеологических корней этого явления. Понятно, что столь масштабная задача потребует много времени и существенных затрат. Пока же степень взаимодействия в рамках международной антитеррористической коалиции оставляет желать лучшего, так как взаимодействие подчас носит откровенно декларативный характер. Это определяется стремлением США продолжать действовать в одностороннем порядке, используя двойные стандарты и не особенно считаясь с мнением и интересами других стран.

Подводя итог проведенному анализу современных технологий терроризма следует сделать вывод, что предотвращение террористических актов в настоящее время представляет весьма сложную задачу, требующую объединения усилий стран и межгосударственных организаций, спецслужб и полиции, служб безопасности государственных организаций и коммерческих структур, общественных организаций и граждан.

Литература

1. Агапов М.А. Ядерная и радиационная безопасность. Готовность к ЧС // Системы безопасности, связи и телекоммуникаций. 2003. № 2. С. 8-10.

2. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (с изменениями на 31 декабря 2014 года).

3. Федеральный закон «О борьбе с терроризмом» в редакции Федеральных законов от 07.08.2000 № 122-ФЗ, от 21.11.2002 № 144-ФЗ. Отменен Федеральным законом от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму».

4. Журавленко Н.И., Клюев А.В. . Детерминанты терроризма и организация его профилактики: Монография. – Уфа: ОН и РИО УЮИ МВД РФ, 2005. – 245 с.

5. Арас Дж. Терроризм вчера, сегодня и навеки. URL: http://www.gumer.info/bibliotek_Buks/Polit/Aras/31.php. Дата обращения 18.03.2015.

Н.С. Хохлов,
д.т.н., профессор,
Воронежский институт МВД России
Д.А. Жайворонок,
к.т.н., доцент,
Воронежский институт МВД России
С.В. Канавин,
к.т.н.,
Воронежский институт МВД России

ОСОБЕННОСТИ ПРИМЕНЕНИЯ КОМПЛЕКСОВ РАДИОМОНИТОРИНГА КАК СРЕДСТВ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ

Массовое применение телекоммуникационного оборудования и развитие технологий беспроводного доступа, рост загруженности радиочастотного спектра и плотности размещения действующих радиоэлектронных средств привели к усложнению электромагнитной обстановки. Возникает также проблема того, что частоты, закрепленные ГКРЧ за конкретным пользователем, могут быть использованы злоумышленником. Кроме того, загруженность радиочастотного спектра может приводить к ухудшению электромагнитной совместимости радиоэлектронных средств и систем. В сложившейся обстановке возможных угроз экстремизма и его негативного влияния на уровень национальной безопасности России, одной из актуальных задач, которые возникают перед центрами связи информационных технологий и защиты информации МВД России, является обеспечение радиомониторинга.

Радиомониторинг – это деятельность по изучению, контролю, накоплению и хранению данных о радиообстановке в заданном

районе, поиску и обнаружению легальных (зарегистрированных) и нелегальных (незарегистрированных) радиопередатчиков и источников других радиоизлучений. Перед сотрудниками ОВД, применяющими средства радиомониторинга в своей служебной деятельности, возникают следующие задачи: постоянный или периодический контроль загруженности частотного спектра; обнаружение и анализ новых излучений, определение местоположения их источников; выявление непреднамеренных или специально организованных каналов утечки информации [1].

По своему эксплуатационному назначению средства радиомониторинга подразделяются на 5 типов: стационарные, мобильные, портативные, переносные и дополнительное оборудование (измерительные средства). Для качественного контроля радиообстановки необходимо использовать систему разнесенных станций радиомониторинга. Это достигается путем использования одной стационарной и нескольких мобильных станций радиомониторинга. Центральная станция мониторинга осуществляет обнаружение и прием радиоизлучений, а мобильные станции осуществляют пеленгование и вычисление местоположения источника радиоизлучения. Передвижные станции радиомониторинга дополнительно укомплектовываются переносным оборудованием для дослеживания источников радиоизлучений на местности где прием стационарными и мобильными станциями затруднен.

Мобильные средства радиомониторинга по своим конструктивным особенностям уступают стационарным постам в функциональности, так как антенная система монтируется на автотранспортном средстве, что приводит к уменьшению рабочей зоны наблюдения за радиосредствами.

Носимые средства радиомониторинга предназначены для работы в полевых условиях и должны быть оборудованы источниками резервного питания. Особенности эксплуатации накладывают на них ограничения по массогабаритным характеристикам, так как оборудование предназначено для открытого и скрытого применения [2].

В настоящее время используются различные средства радиомониторинга, включающие в себя антенны, приемные устройства, анализаторы и измерители параметров сигналов, программ-

ное обеспечение, а также автоматизированные комплексы различного назначения.

В органах внутренних дел (ОВД) применяется комплекс «Барс-МПИ2», который предназначен для поиска, обнаружения, экспресс-анализа радиоизлучений в диапазоне 20…3000 МГц и пеленгования их источников (рис.1).

Рис. 1 Комплекс пеленгования источников радиоизлучений «Барс-МПИ2» на базе автомобиля УАЗ Патриот, развернутый в Воронежском институте МВД России

Состав технических средств изделия позволяет решать задачи: поиска, радиопеленгования и технического анализа радиоизлучений.

Комплекс обеспечивает:

- ввод и оперативное изменение данных, необходимых для решения задач радиоконтроля, как с клавиатуры управляющего компьютера, так и из файлов заданий в формате XML, в том числе получаемых по каналам связи;
- вывод результатов радиоконтроля на дисплей управляющего компьютера и сохранение в файле результатов радиоконтроля в формате XML, в том числе для передачи по каналам связи;
- определение занятости полос радиочастот, а также радиочастот и радиочастотных каналов;
- регулирование уровня порога сигнала на входе оборудования, превышение которого регистрируется как занятость канала, с шагом 1 дБ;

- построение и вывод на дисплей панорамы спектра в координатах «частота-время» для интервала времени одни сутки с отображением уровней сигнала в цвете.

- измерение частоты радиоизлучений;

- измерение уровня радиоизлучений;

- прослушивание и/или запись сигналов (слуховой контроль) с формированием временных меток продолжительностью не менее 72-х часов;

- запись демодулированных звуковых сигналов с использованием методов сжатия;

- передачу демодулированных звуковых сигналов с использованием методов сжатия по каналам связи;

- отображение спектра сигнала;

- определение направления (пеленгование) на источник излучения (в том числе помех), с отображением информации на картографическом фоне;

- определение координат источников радиоизлучений при работе радиопеленгаторов в составе пеленгаторной группы и отображение местоположения источников радиоизлучений на картографическом фоне;

- определение координат и курса в движении;

- возможность работы в составе АСРК;

- многопользовательский и многозадачный режим работы;

- функционирование как в автоматическом, так и автоматизированном режимах как на стоянке, так и в движении;

- дистанционное управление РКО с внешней ПЭВМ через беспроводное соединение для решения задач обнаружения, экспресс-анализа и пеленгования, технического анализа на картографическом фоне.

Носимый комплекс поиска, обнаружения и пеленгования источников радиоизлучений «Барс-Н» обеспечивает:

- обнаружение и оценку уровня принимаемого радиосигнала на фиксированных частотах;

- обнаружение и оценку уровня принимаемого радиосигнала на произвольной частоте;

- определение направления на источник радиоизлучения с использованием направленных свойств антенн по максимуму (минимуму) сигнала;

- визуальную индикацию направления на источник излучения;

- визуальную индикацию спектра принимаемого радиосигнала;

- визуальную индикацию грубой и точной шкалы уровня принимаемого радиосигнала;

- визуальную индикацию режимов работы и настроек радиоприемного устройства;

- скрытую индикацию точной шкалы уровня принимаемого сигнала;

- скрытую индикацию направления на источник радиоизлучения;

- прослушивание сигнала демодулятора.

РКО тракта пеленгования комплекса обеспечивает:

поиск, энергетическое и пространственное обнаружение радиоизлучений в диапазоне рабочих частот - 30 ÷ 3 000 МГц;

скорость сканирования при анализе загрузки частотного диапазона – не менее 500 МГц/с при частотном разрешении 10 кГц;

инструментальная погрешность пеленгования (средняя квадратическая ошибка) в секторе 360º во всем диапазоне частот - 4,0 градуса;

Характеристики двухканального устройства аналого-цифрового приема и обработки мобильного комплекса представлены ниже (таблица 1):

Таблица 1

№ п/п	Параметр	Значение
1	Диапазон рабочих частот	30…3000 МГц
2	Полоса одновременного обзора	до 20 МГц
3	Дискретность настройки по частоте, не более аналоговой части цифровой части	 1000 кГц 1 Гц
4	Время настройки синтезатора	10 мс
5	Погрешность по частоте опорного генератора	$5x10^{-9}$
6	Ослабление помех по побочному каналу приема (для промежуточных и зеркальных частот)	80 дБ
7	Точка пересечения по интермодуляции второго порядка IP_2 (относительно 1 мВт)	40 дБм

Продолжение таблицы

8	Точка пересечения по интермодуляции третьего порядка IP_3 (относительно 1 мВт)	10 дБм
9	Коэффициент шума	12 дБ (-162 дБм/Гц)
10	Фазовый шум гетеродина при отстройке по частоте 20 кГц	-100 дБ/Гц
11	Диапазон действия АРУ	нет
12	Диапазон действия АТТ	0;5;10;15;20;25;30 дБ
13	Антенный вход: входное сопротивление при КСВ не более 2,5	50 Ом
14	Максимальное допустимое напряжение на входе	1 В
15	Коэффициент прямоугольности полос пропускания по уровням 60/6 дБ	2 дБ
16	Неравномерность АЧХ в полосе пропускания (после коррекции)	± 2дБ

Характеристики носимого комплекса «Барс-Н»:

- диапазон рабочих частот (обнаружения и пеленгования) от 20 МГц до 3000 МГц с разрешением 100 Гц;

- ошибка пеленгования источников радиоизлучений с инструментальной погрешностью (среднеквадратической ошибкой) в диапазоне:

20…200 МГц - не хуже 15 градусов;

200…500 МГц - не хуже 10 градусов;

500…3000 МГц - не хуже 7 градусов.

Электропитание комплекса осуществляется от однофазного источника переменного тока с номинальным напряжением 220 В ± 10 % частотой 50 Гц ± 1 Гц через преобразователь напряжения 220/=13,8 В, от буферных аккумуляторных батарей или внутренней сети автомобиля.

Мощность, потребляемая от источника питания – не более 600 Вт. Диапазон рабочих температур для аппаратуры внутри салона от плюс 10 до плюс 40^0С. Комплекс функционирует в режиме непрерывной круглосуточной работы с учетом 30 минут на ежедневное техническое обслуживание. Комплекс готово к работе в нормальных условиях через 30 мин. после подачи на него электропитания.

Использование сотрудниками ОВД для решения практических задач комплексов радиомониторинга позволит успешно осуществлять радиоконтроль и обнаружение незарегистрированных радиоизлучений в интересах противодействия экстремизму и его негативному влиянию на уровень национальной безопасности России.

Литература

1. Дятлов А.П. Радиомониторинг излучений спутниковых радионавигационных систем/А.П. Дятлов, Б.Х. Кульбикаян М.: Радио и связь, 2006. – 272 с.

2. Рембовский А.М. Радиомониторинг – задачи, методы и средства / А.М. Рембовский, А.В. Ашихмин // Под ред. А.М. Рембовского, 2-е изд., пере-раб. и доп. – М.: Горячая линия – Телеком, 2010. – 624 с.

К.С. Ткаченко,
ФГБОУ ВО «Севастопольский государственный университет», tkachenkokirillstanislavovich@mail.ru, tkachenkokirillstanislavovich@gmail.com

МОДЕЛЬ И МЕТОД ОБЕСПЕЧЕНИЯ ПОДДЕРЖКИ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В УЗЛЕ СЕТИ

Предлагаются модель и метод обеспечения информационного противодействия экстремизму и терроризму в узле распределенной среды или однородной сети на основе алгоритмов стохастической аппроксимации. Реализуется программное средство информатизации поддержки принятия решений.

Важной научной и практической задачей, возникающей в процессе поисков методов борьбы с экстремизмом и терроризмом, является использование адаптивных систем управления как распределенными средами и однородными сетями, так и их от-

дельными узлами. В последних исследованиях и публикациях по этой тематике [1-3] начато построение методов реструктуризации. Нерешенной прежде частью является разработка метода, пригодного для противодействия экстремизму и терроризму при атаках на узлы сетей и сред.

Целью данной работы является разработка и исследование модели и метода обеспечения информационного противодействия экстремизму и терроризму в узле сети (среды), а также программно-инструментального комплекса на их основе.

Широко известно, что использование средств вычислительной техники при управлении атомными электростанциями, транспортно-логистическими системами, водоснабжением, водоотведением и прочим, приводит к наличию возможности порождения катастрофических последствий нарушения их процессов работоспособности злоумышленниками. Это происходит вследствие атак несанкционированного доступа и вирусных воздействий, которые могут проводиться экстремистами и террористами. Любая подобная атака может обозначаться как возмущающее событие, которое обладает некоторой априори неизвестной интенсивностью.

Полагается, что обращение к интенсивность обращений к узлу для решения полезных вычислительных задач является стационарным, потери за невыполнение заданий накапливаются. В этих предположениях представляется возможным адаптировать стохастический вариант модели экономического размера заказа [4] к задаче информационного противодействия экстремизму и терроризму.

Пусть $f(x)=\mu e^{-\mu x}$ – плотность распределения времени обработки заявок и пакетов заданий на обслуживание в узле по экспоненциальному закону, где μ – производительность узла. $D=D[x]=\mu^{-2}$ – дисперсия значений производительности узла. h – оценка затрат на потери от ожидания в очереди. p — оценка затрат на потери от отказа в обслуживании. K – оценка затрат на постановку пакета заявок в очередь. y – увеличение мощности узла администратором в директивном порядке. A – уровень, при котором происходит данное увеличение. В соответствии с [4, 16.1.2] функция потерь выражается как:

$\xi(y,A)=\frac{DK}{y}+h\left(\frac{y}{2}+A-M[x]\right)+\frac{pD}{y}\int_A^B(x-A)f(x)dx$, причем $M[x]=\mu^{-1}$ для потока, а $B-$ наибольшая мощность функционирования системы. То есть

$$\xi(y,A)=\frac{\mu^{-2}K}{y}+h\left(\frac{y}{2}+A-\mu^{-1}\right)+\frac{p\mu^{-2}}{y}\int_A^B(x-A)\mu e^{-\mu x}dx,$$ откуда

$$\xi(y,A)=\frac{K}{\mu^2 y}+h\left(\frac{y}{2}+A-\frac{1}{\mu}\right)+\frac{pe^{-\mu(A+B)}\left(e^{\mu A}(\mu A-\mu B-1)+e^{\mu B}\right)}{\mu^3 y}, \qquad (1)$$

поскольку $\int(x-A)\mu e^{-\mu x}dx=\mu^{-1}e^{-\mu x}(\mu(A-x)-1)$.

На основании (1) получается, что моделью задачи является

$$\arg\min_{y,A\in R}\xi(y,A). \qquad (2)$$

Метод обеспечения информационного противодействия заключается в решении (2) рандомизированным алгоритмом глобального поиска [5]. Модификация этого алгоритма для данной задачи включает в себя следующие шаги:

Шаг 1. Ввод величин μ, h, p, K, B, a_1, b_1, a_2, b_2, таким образом, чтобы $y\in[a_1,b_1]$, $A\in[a_2,b_2]$, N.

Шаг 2. Задание начальных значений и выполнение расчетов: $f^{\min}:=10^{100}$, $y^{\min}:=f^{\min}$, $A^{\min}:=f^{\min}$.

Шаг 3. N раз выполняются шаги (4) – (5).

Шаг 4. Расчет $y:=\omega(a_1,b_1)$, $A:=\omega(a_2,b_2)$, где $\omega(x,y)$ – генератор равномерно распределенных на $[x,y)$ псевдослучайных чисел, $f:=\xi(y,A)$ (1).

Шаг 5. Если $f<f^{\min}$, то присвоить $f^{\min}:=f$, $y^{\min}:=y$, $A^{\min}:=A$.

Шаг 6. Вывод $y^{\min}$, $A^{\min}$, $f^{\min}$.

Разрабатывается программное средство поддержки принятия решений на языке программирования высокого уровня *Python*, реализующее шаги (1) – (6). При разработке, проводившейся в соответствии с требованиями *PEP-8*, учтено использование возможностей современной версии *Python3*.

Перспективой дальнейших изысканий по данной тематике станет детализация модели по числу критериев.

Литература

1. Назин А.В. Адаптивный выбор вариантов. Рекуррентные алгоритмы / А.В. Назин, А.С. Позняк. – М.: Наука, 1986. – 288 с.
2. Скаткова Н.А. Гарантоспособные технологии реконфигурации автоматизированных транспортно-производственных систем / Н.А. Скаткова // Радиоэлектронные и компьютерные системы. Вып. 6. – Харьков, 2008. – С. 52–57.
3. Ткаченко К.С. Программная система адаптивного принятия решений при априорной неопределенности входных данных / К.С. Ткаченко // Вестник СевНТУ: сб. науч. тр. Вып. 131/2012. Серия: Информатика, электроника, связь. – Севастополь: Изд-во СевНТУ, 2012. – С.78–81.
4. Таха Х.А. Введение в исследование операций / Х.А. Таха. – М.: Издательский дом «Вильямс», 2005. – 912 с.
5. Бейко И.В. Методы и алгоритмы решения задач оптимизации / И.В. Бейко, Б.Н. Бублик, П.Н. Зинько. – К.: Вища школа, 1983. – 512 с.

О.И. Бокова,
д.т.н., профессор,
Воронежский институт МВД России
Н.С. Хохлов,
д.т.н., профессор,
Воронежский институт МВД России
А.В. Сидоров,
Воронежский институт МВД России

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ СРЕДСТВ РАДИОСВЯЗИ И УПРАВЛЕНИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ К ДЕСТРУКТИВНЫМ ЭЛЕКТРОМАГНИТНЫМ ВОЗДЕЙСТВИЯМ, КАК СРЕДСТВО ПРОТИВОДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОМУ ТЕРРОРИЗМУ

Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г. [1] определяет экстремизм как «какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства,

а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них, и преследуемые в уголовном порядке в соответствии с национальным законодательством Сторон».

Российская Федерация, в том числе другие страны, такие как: Казахстан, Узбекистан, Таджикистан, Кыргызстан, Китайская Народная Республика подписали данную конвенцию в январе 2003 г.

Инструментом для совершения противоправных деяний террористами экстремистами, сепаратистами, является террористический акт. В последние годы интенсивно развивается одна из ветвей информационного терроризма, а именно, электромагнитный терроризм. При этом средства радиосвязи и управления органов внутренних дел (СРС и У ОВД) могут быть подвержены деструктивному поражающему воздействию электромагнитного характера со стороны сепаратистов, криминальных структур или же представителей враждебных государств. Современные технические средства (ТС) деструктивного электромагнитного воздействия являются по существу электромагнитным оружием, способным дистанционно поразить информационную систему. Основным поражающим фактором при этом является электромагнитный импульс, воздействующий на систему или ее элементы по цепям питания и (или) каналам связи [2].

В настоящее время получены научные результаты по отдельным направлениям оценки стойкости технических средств к подобным импульсным излучениям. Результатом целенаправленного и системного применения технологий безопасности в этой сфере стало создание как защищенных информационных систем, так и соответствующих испытательных средств. Большой вклад в исследования в этой области внесли В.Е. Фортов, В.И. Борисов, В.Б. Авдеев, Н.В. Балюк, О.И. Бокова, Л.О. Мырова, Л.Н. Кечиев, А.И. Куприянов, В.А. Михайлов, Ю.В. Парфенов, В.А. Плыгач, В.А. Сикарев, А.А. Сикарев, Н.Н. Толстых, А.П. Ярыгин, и др.

В то же время, оценка устойчивости СРС и У ОВД к воздействию мощных электромагнитных излучений (ЭМИ), представляет пока недостаточно исследованную научную задачу. Существующие методы и средства оценки устойчивости радиотехнических средств в основном ориентированы на обеспечение элек-

тромагнитной совместимости, электромагнитных воздействий естественного, техногенного характера или электромагнитного импульса высотных ядерных взрывов, и не учитывают возможности современного электромагнитного оружия, базирующегося на генерации сверхкоротких импульсов высокой мощности.

Так, в настоящее время отсутствуют как экспериментальные данные по стойкости современных технических средств связи и управления ОВД к действию поражающих электромагнитных излучений, так и методы расчетных оценок результатов воздействия на устройства СРС и У, а также не сформулированы требования к параметрам испытательных воздействий при проведении испытаний на имеющихся средствах испытаний. Это не позволяет делать оценки устойчивости современных СРС и У к деструктивным электромагнитным воздействиям.

Деструктивное сверхкороткоимпульсное электромагнитное излучение, оказывающее поражающее воздействие по проводным (кабельным) линиям связи, по металлоконструкциям, по сетям питания, по радиоканалу, является в руках злоумышленников электромагнитным оружием [3]. Это оружие характеризуется высокой эффективностью воздействия и масштабными последствиями его применения, в частности функциональным поражением средств радиосвязи и управления ОВД. С развитием радиоэлектронной аппаратуры активно развиваются средства электромагнитного поражения радиоэлектронных систем и устройств [4]. Для защиты инфокоммуникационных систем связи и управления ОВД должен применяться комплексный подход.

Методической основой защиты от деструктивных электромагнитных воздействий (ДЭМВ) является анализ уязвимости элементов инфокоммуникационной системы связи и управления и передаваемой по каналам связи информации к деструктивным электромагнитным воздействиям.

Уязвимость – это параметр или совокупность параметров средств радиосвязи и управления, характеризующих возможность нанесения СРС и У повреждений различными видами внешних воздействий. Повреждения в результате этих воздействий могут привести к нарушению целостности системы, к сбоям и неправильной работе системы, да и вовсе к полному физическому выходу из строя. Применительно к СРС и У ОВД это ведет к полной

или частичной замене средств радиосвязи и управления, программированию и конфигурированию этих средств, а зачастую перезапуску системы в целом [5].

Исходя из этого, с учетом потенциальных параметров воздействия, вырабатываются требования к их защите.

Систему защиты формируют на основе разработанных требований. Ее необходимо рассматривать как совокупность организационных, программно-технических и правовых мер, направленных на комплексное противодействие угрозе и ликвидацию ее последствий [3, 6].

Правовые меры подразумевают создание нормативно-правового обеспечения для защиты СРС и У от преднамеренного электромагнитного воздействия.

На федеральном уровне данный вопрос регулируется системой государственных стандартов, которые определяют технические требования необходимой помехозащищенности технических средств, испытательные воздействия, критерии оценки работоспособности средств и систем при испытаниях. Данные критерии не учитывают специфику и важность выполняемых функций.

Поэтому на уровне министерств и ведомств требуется разработка отраслевых стандартов и правил, которые бы учитывали их специфику, требования к стойкости используемого оборудования, параметры электромагнитных воздействий и т. д.

К таким ведомственным нормативным актам относится отраслевой стандарт ОСТ 78.01.0004-2000 «Наземные радиостанции с угловой модуляцией, стационарные, возимые и перевозимые автомототранспортом, носимые и переносные, предназначенные для работы в радиосетях ОВД и ВВ МВД РФ. Виды, основные параметры, технические требования». Данный документ определяет виды, основные параметры, технические требования к средствам радиосвязи, обязательность проведения испытаний по видам воздействия, виды испытаний на внешние воздействия. При этом среди воздействующих факторов данный ОСТ выделяет: вибрацию, механические повреждения, температуру, атмосферное давление, влажность, соляной туман, пыль и песок, атмосферные осадки, росу, иней, но не рассматривает влияние электромагнитного излучения на средства радиосвязи и управления, хотя ДЭМВ является не менее опасным среди перечисленных внешних воз-

действий. Учитывая специфику ведомственных систем радиосвязи и управления, необходимо разработать требования, предъявляемые к ним по стойкости к ДЭМВ.

Организационные меры должны быть направлены на соблюдение норм и правил по электромагнитной совместимости (ЭМС) ТС, созданию системы физической защиты средств связи и управления ОВД, объекта, где они расположены, интеграции различных систем: информационной безопасности, физической защиты, защиты от ДЭМВ.

Программно-технические меры заключаются в своевременном обнаружении, а при возможности и нейтрализации угрозы; применении специальных технических средств и программных продуктов для повышения стойкости и защиты оборудования к электромагнитным воздействиям и достоверности, качества передаваемой информации [7].

В связи с этим необходим анализ СРС и У ОВД с целью выработки критериальных уровней устойчивости СРС и У к ДЭМВ. Оценка уязвимости основывается на этих критериальных уровнях, которые должны быть определены в отраслевом стандарте, а для проверки необходимы испытания используемого оборудования на стойкость к ДЭМВ.

На основе разработанной модели деструктивного электромагнитного воздействия на системы радиосвязи и управления ОВД [8] авторами предложены рекомендации по повышению устойчивости средств радиосвязи и управления ОВД к ДЭМВ. Вот некоторые из них:

1. Для повышения устойчивости СРС и У ОВД целесообразно использовать ложные пункты электромагнитного излучения для дезинформации противника о действительном месте сосредоточения средств связи.

2. Применение в качестве ДЭМВ помехи с хаотической импульсной модуляцией приводит к срыву работы устройств синхронизации СРС и У. Для снижения эффективности воздействия помех данного типа рекомендуется выполнять реализацию приемной аппаратуры ОВД на электронной компонентной базе, соответствующей требованиям военных стандартов, а также применять специальные алгоритмы защиты преселекторов приемников.

3. При использовании в СРС и У ОВД каскадных и сверточных кодов в сочетании с многопозиционными сигналами с фазовой модуляцией (манипуляцией) и амплитудно-фазовой модуляцией, устойчивость системы при ДЭМВ повышается, что позволяет применить способ демодуляции и декодирования всего информационного блока как единого многопозиционного элемента с вынесением единого решения о всей принятой *k*-й элементной информационной последовательности.

4. В СРС и У целесообразно использовать модемы сигналов с относительной фазовой манипуляцией, а не с частотной модуляцией.

5. На основании анализа специализированной нормативной документации и технических характеристик существующих имитаторов электромагнитного излучения предложены следующие параметры ДЭМВ для проведения экспериментальной оценки устойчивости СРС и У ОВД (табл. 1):

Таблица 1

Экспериментальные параметры ДЭМВ
для оценки устойчивости СРС и У ОВД

Параметр	Значение параметра	Единица измерения
Напряженность электрического поля	от 0,3 до 30	кВ/м
Напряжение на нагрузке сопротивлением 50 Ом	от 50 до 150	кВ
Напряжение на нагрузке сопротивлением 10 кОм	от 50 до 80	кВ
Длительность фронта импульса	от 0,1 до 50	нс
Длительность импульса	от 0,2 до 250	нс
Длительность пачки импульсов	1	с
Частота следования импульсов	от 10 до 1000000	Гц
Время воздействия	Менее 30	с

Реализация предложенных мер позволит повысить защиту аппаратуры СРС иУ ОВД к ДЭМВ, и тем самым снизить возможные риски поражения электромагнитным оружием аппаратуры ОВД представителями экстремистских формирований, что позволит эффективнее выполнять, стоящие перед ОВД, задачи.

Литература

1. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (заключена в г. Шанхае 15.06.2001 г.) // СПС «КонсультантПлюс», 2015 г.
2. Сидоров А.В. Электромагнитный терроризм как источник угроз инфокоммуникационным системам связи и управления / А.В. Сидоров, О.И. Бокова, Н.С. Хохлов // Вестник Воронежского института высоких технологий. 2014. – №13. – С. 106–109.
3. Акбашев, Б.Б. Защита объектов телекоммуникаций от электромагнитных воздействий: монография / Б.Б. Акбашев, Н.В. Балюк, Л.Н. Кечиев. – М.: Грифон, 2014. – 472 с.
4. Хохлов, Н.С. Современные средства деструктивного силового электромагнитного воздействия на системы радиосвязи и управления органов внутренних дел / Н.С Хохлов, А.В. Сидоров // Математические методы и информационно-технические средства: сборник материалов всероссийской научно-практической конференции. – Краснодар: КрУ МВД России, 2013. – С. 343–346.
5. Сидоров, А.В. Оценка уязвимости средств радиосвязи и управления ОВД при деструктивных электромагнитных воздействиях / А.В. Сидоров, Н.С. Хохлов // Общественная безопасность, законность и правопорядок в III тысячелетии: сборник материалов международной научно практической конференции. – Ч. 2. – Воронеж: Воронежский институт МВД России, 2013. – С. 145–149.
6. Хохлов, Н.С. Моделирование и оптимизация противодействия разрушению информации в системах управления и связи органов внутренних дел при электромагнитных воздействиях: монография / Н.С. Хохлов. – Воронеж: Воронежский институт МВД России, 2005. – 181 с.
7. Хорошко, В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков / под ред. Ю.С. Ковтанюка. – К.: Юниор, 2003. – 504 с.
8. Хохлов Н.С. Оценка устойчивости системы радиосвязи и управления к деструктивным электромагнитным воздействиям / Н.С. Хохлов, А.В. Сидоров // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. – 2013. – № 2(18). – С. 27–35.

О.И. Бокова,
д.т.н., профессор,
Воронежский институт МВД России
Д.А. Жайворонок,
к.т.н., доцент,
Воронежский институт МВД России
О.С. Сластникова,
Воронежский институт МВД России

ОСОБЕННОСТИ РЕАЛИЗАЦИИ УСТРОЙСТВА АНАЛОГО-ЦИФРОВОГО ПРИЕМА И ОБРАБОТКИ КОМПЛЕКСА ПЕЛЕНГОВАНИЯ ИСТОЧНИКОВ РАДИОИЗЛУЧЕНИЙ

В условиях нарастающей угрозы экстремизма во всем мире и его негативного влияния на уровень национальной безопасности России в частности, в последнее время для осуществления постоянного или периодического контроля загруженности частотного спектра, обнаружения и анализа новых излучений, определения местоположения их источников, а также выявления непреднамеренных или специально организованных каналов утечки информации все большую актуальность приобретает использование устройств аналого-цифрового приема и обработки (АЦПО) радиосигналов.

Устройство АЦПО представляет собой двухканальный программно управляемый радиоприемник супергетеродинного типа с тремя преобразованиями частоты. Перестройка приемника осуществляется изменением частот гетеродинов. Антенные входы рассчитаны на подключение антенн несимметричным коаксиальным кабелем с волновым сопротивлением 50 Ом. Цифровая обработка принимаемых сигналов осуществляется в устройстве цифровой обработки.

Основные технические характеристики представлены в таблице 1.

Таблица 1

Наименование параметра	Значение параметра	
Диапазон рабочих частот, МГц	30…1000	1000…3000
Полоса аналоговой части, МГц	20	
Дискретность настройки по частоте (аналоговая часть), МГц	1	
Относительная нестабильность не хуже	$\pm 1*10^{-8}$	
Полосы пропускания цифровых фильтров, кГц	0,5; 1; 2,5; 5,0; 10; 12,5; 25	
Коэффициент шума, дБ, не более	12	
Точка пересечения по интермодуляции второго порядка IP_2, дБ (отн. 1 мВт), не менее	25	
Точка пересечения по интермодуляции третьего порядка IP_3, дБ (отн. 1 мВт), не менее	5	0
Затухание, вносимое аттенюаторами на входе канала, дБ	0…30 дБ с шагом 5 дБ	
Уровень фазового шума гетеродина относительно основного излучения дБ/Гц при отстройке на 20 кГц, не более	-95	
Частота дискретизации АЦП, МГц	120	
Количество разрядов АЦП	16	
Питание от источника постоянного тока напряжением, В	+ 10…+15 В.	
Дистанционное управление, интерфейс	Ethernet 100/1000BASE-T	
Время готовности к работе с момента включения, минуты, не превышает	10	

Конструктивно приемник выполнен в виде одного блока (рис. 1), в котором размещены: аналоговая часть и цифровая часть – устройство цифровой обработки сигналов (ЦОС). Аналоговый приемный тракт оканчивается выходами на частоте 88 МГц. Цифровой тракт, состоящий из устройства ЦОС и ЭВМ со специальным программным обеспечением, имеет выходы для подключения внешней ПЭВМ (порты Ethernet).

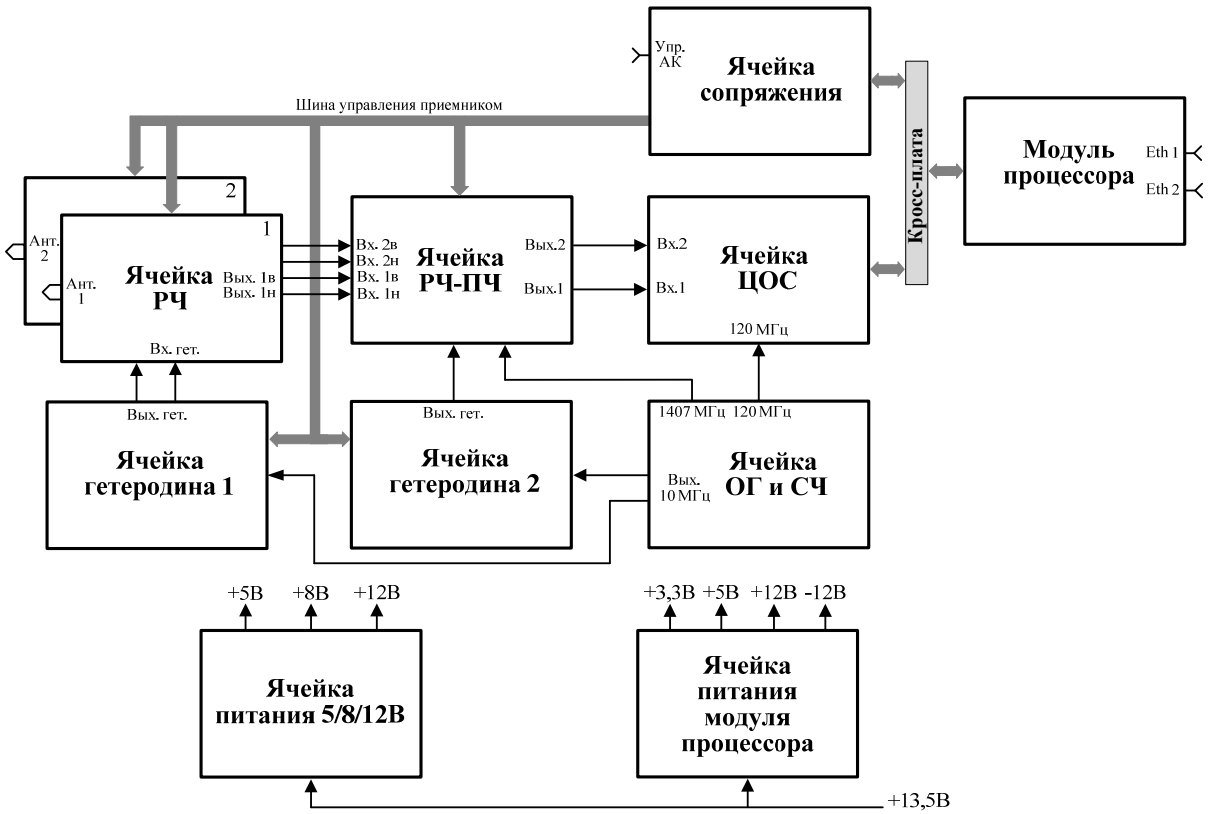

Рис. 1. Структурная схема двухканального устройства АЦПО

Ячейка РЧ и гетеродин 1 образуют встроенный в приемник конвертер, принимающий сигналы в диапазоне 1000…3000 МГц и осуществляющий линейный перенос их спектров в диапазон 325…775 МГц (рис. 2).

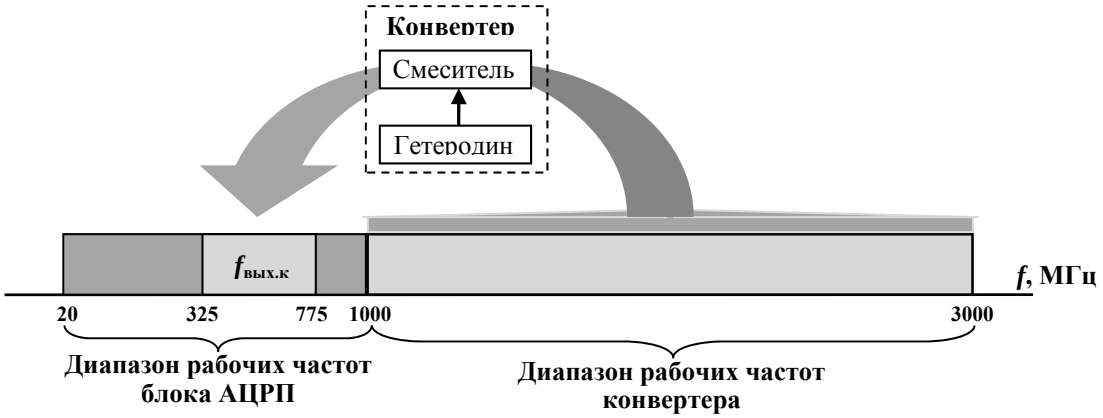

Рис. 2. Конвертирование спектров сигналов

Ячейка РЧ – смеситель конвертера, который осуществляет прием сигналов в диапазоне частот 1000…3000 МГц и линейный перенос их спектров в диапазон 325…775 МГц. Преобразование обеспечивается с помощью гетеродина конвертера, работающего в диапазоне 1500…2200 МГц. При работе конвертера в диапазоне 1000…1800 МГц используется «верхняя» настройка гетеродина ($f_{вых.к.}=f_{гет}-f_{с}$), а в диапазоне 1800…3000 – «нижняя» ($f_{вых.к.}=f_{с}-f_{гет}$).

В диапазоне частот 30…1000 МГц преобразований принимаемых сигналов в ячейке РЧ не происходит, поскольку сигналы со входа ячейки РЧ коммутируются на ее выход.

На входе ячейки РЧ имеются аттенюаторы, дискретно регулирующие уровни входных сигналов и позволяющие снизить уровни интермодуляционных помех. Пределы регулирования ослабления аттенюаторов 0…30 дБ, шаг регулирования 5 дБ.

Ячейка РЧ/ПЧ выполняет избирательно-усилительную и преобразовательную функции. Ширина полосы пропускания ячейки по входу соответствует диапазону рабочих частот приемника (30…1000 МГц).

Смесители ячейки с помощью внешних гетеродинов обеспечивает два преобразования несущих частот сигналов: одно на промежуточную частоту 1495 МГц (ПЧ1), а втрое – на промежуточную частоту 88 МГц (ПЧ2). Как при первом, так и при втором преобразовании осуществляется линейный перенос спектров принимаемых сигналов на соответствующие промежуточные частоты. Ширина полосы пропускания по промежуточной частоте 1495 МГц около 40 МГц, по промежуточной частоте 88 МГц – 20 МГц.

Гетеродинирующие колебания с частотами первого гетеродина формируются в ячейке гетеродина 1, а с частотой второго гетеродина – в ячейке ОГ и СЧ.

В радиоприемнике применена кварцевая стабилизации частот гетеродинов, формируемых методом косвенного цифрового синтеза. Опорной частотой во всех схемах формирования частот гетеродинов служит частота опорного генератора. В качестве опорного генератора используются термостатированный рубидиевый стандарт частоты с номинальной частотой 10 МГц, относительной температурной нестабильностью $\pm 3 \times 10^{-11}$ в интервале

температур -5…+50°С и долговременной относительной нестабильностью ±2.0x10^{-9}/год.

Ячейка гетеродина 1 является генератором синусоидальных колебаний в диапазоне частот 1500…2250 МГц. Перестройка конвертера в диапазоне рабочих частот осуществляется перестройкой гетеродина 1 с шагом 1 МГц.

Ячейка гетеродина 2 аналогична ячейке гетеродина 1 и обеспечивает формирование колебаний ($f_{Г2}$) в диапазоне частот: 1500…2500 МГц. Перестройка в диапазоне частот 30…1000 МГц осуществляется изменением частоты гетеродина 2 с шагом 1 МГц.

Управление частотами гетеродина 1, гетеродина 2 и аттенюаторами ячейки РЧ осуществляется по 3-х проводной шине от ячейки сопряжения приемника.

Ячейка СЧ. В состав ячейки входят два гетеродина-синтезатора частот: один из них формирует колебания с частотой 1407 МГц (гетеродин 3), а второй (гетеродин 4) – колебания с частотой 120 МГц, используемые в устройстве ЦОС для дискретизации принимаемых аналоговых сигналов при их преобразовании в цифровую форму. Ячейки ЦОС с АЦП преобразуют аналоговые сигналы в цифровую форму с последующей цифровой фильтрацией сигналов и представлением их к виду удобному для хранения и анализа. Модуль процессора – процессорная плата в формате CompactPCI 3U является программируемым логическим контроллером, отвечающим за выполнение операций, заданных программой. Программное обеспечение в оперативную память загружается с флэш-диска, устанавливаемого в специальный разъем модуля. Ячейка сопряжения формирует сигналы управления для ячеек РЧ, РЧ/ПЧ (управление аттенюаторами), ячеек 1-го и второго гетеродинов (управление перестройкой 1-го и 2-го гетеродинов по частоте) и антенного коммутатора комплекса. Плата импульсного преобразователя напряжения 15 В формирует питающее напряжение + 15 В для рубидиевого стандарта частоты. Ячейка питания 5/8/12 В предназначена для питания модуля ККРЧ, рубидиевого стандарта частоты, ячеек РЧ, РЧ/ПЧ, гетеродинов и синтезатора частот. Ячейка питания модуля процессора обеспечивает формирование напряжений +3,3 В, +5 В, +12 В и -12 В, необходимых для функционирования модуля процессора.

Кросс-плата обеспечивает соединение по шине PCI модуля процессора с ячейкой цифровой обработки, а через LINK-порты взаимодействие ячеек сопряжения и ЦОС.

Устройство цифровой обработки сигналов включает: модуль процессора (микро-ЭВМ); ячейку ЦОС; ячейку сопряжения.

Вне зависимости от диапазона частот работы приемника на вход блока ЦОС поступает групповой сигнал на промежуточной частоте 88 МГц в полосе 20 МГц.

Аналого-цифровое преобразование входного аналогового сигнала осуществляется 16-разрядным АЦП с динамическим диапазоном около 96 дБ. Частота дискретизации сигнала составляет 120 МГц.

Цифровая обработка и фильтрация осуществляется в реальном масштабе времени с использованием квадратурных составляющих сигнала.

Модуль процессора приемника и ЭВМ комплекса соединяются посредством интерфейса Ethernet 100/1000. Для подключения используется 8-контактный разъем RJ-45.

Литература

1. Бокова О.И., Жайворонок Д.А., Хохлов Н.С., Медведев И.И. Устройства приема и обработки сигналов: учебное пособие – 2-е изд. перераб. и доп. – Воронеж: Воронежский институт МВД России, 2013. – 228 с.

2. Сети и системы радиосвязи ОВД и средства их информационной защиты: учебное пособие / Бокова О.И. [и др.]; под ред. Н.С. Хохлова. – Воронеж: Воронежский институт МВД России, 2012. – 228 с.: ил.

3. Квадратурные формирователи радиосигналов: монография / Попов П.А., Жайворонок Д.А., Ромашов В.В. и др.; Под Ред. П.А. Попова. – Воронеж: Воронежский институт МВД России, 2001. – 200 с.: ил.

А.Е. Журавлев,
к.т.н., ФГБОУ ВО «Государственный университет морского
и речного флота имени адмирала С.О. Макарова»,
zhuravlev.a.e@yandex.ru

СРЕДСТВА АВТОМАТИЗИРОВАННОГО ОПЕРАТИВНОГО ОБНАРУЖЕНИЯ И МЕТОДЫ БОРЬБЫ С УГРОЗАМИ НЕСАНКЦИОНИРОВАННОЙ ПОДМЕНЫ ИНФОРМАЦИИ В СЭД

В работе рассматриваются вопросы организации автоматизированной системы обнаружения и предотвращения различного рода несанкционированных внедрений в базу данных системы электронного документооборота. Разобран основной комплекс проблем, связанных с мониторингом и сигнализацией об угрозах вторжения в объект контроля.

Современная система электронного документооборота (СЭД) является неотъемлемой частью большинства актуальных автоматизированных информационно-справочных систем (АИСС) различных служб и организаций. Такие СЭД могут быть задействованы на всех уровнях автоматизации АИСС, от небольшой коммерческой организации до огромных вузов, НИИ и электронного правительства.

Комплексное обеспечение информационной безопасности таких систем является задачей во многом нетривиальной, а реализацию технологий предотвращения угроз безопасности можно назвать оптимальной стратегией управления. Комплекс АИСС состоит из множества компонентов, каждый из которых, как и система коммуникаций между ними, является потенциальной целью злоумышленника. Одним из основных компонентов этого класса является СЭД как среда концентрации наиболее ценных ресурсов всей системы, именно поэтому СЭД часто является целью злоумышленников. Наиболее типичными видами угроз для СЭД можно назвать:

- нарушение работоспособности;
- несанкционированный доступ;
- подмена информации.

За обнаружение попыток получения несанкционированного доступа к СЭД обычно отвечает специализированные компоненты защиты. В рассматриваемом случае эти функции выполняет модуль «Тоннель», отвечающий за контроль доступа к компонентам АИСС. Однако, данный модуль становится бессилен, если доступ к компоненту получен условно-правомерно с точки зрения системы, например, при помощи (незаконно) полученных данных для авторизации или же используя физическое подключение к серверу. В таких случаях незаменимым становится рассматриваемый в рамках данной работы модуль «Паутина». Целью его разработки и внедрения в действующую СЭД стала необходимость автоматизированного мониторинга и контроля изменений в базе данных документов на самом низком уровне, т.е. вне рамок контроля самой СЭД. Особенности модуля «Паутина»:

– полная автономность;

– динамическая масштабируемость;

– универсальность механизмов;

– поддержка сторонних алгоритмов.

Модуль «Паутина» является полностью автономным, это значит, что, будучи единожды инициализированным (т.е. корректно настроенным и запущенным), модуль становится неуправляемым из других компонентов АИСС, что гарантирует невозможность осуществления несанкционированного воздействия на его механизмы.

В системе «Паутина» предусмотрено ранжирование документов по трем группам:

– ранг «A»: внешние входящие и исходящие документы организации, а также документы, имеющие визы или точки маршрутов (например, для оценки или согласования содержания) связанные с лицами, не являющимися сотрудниками организации;

– ранг «B»: внутренние документы организации, проходящие исключительно через собственных сотрудников;

– ранг «C»: внутренние документы подразделений организации, не выходящие за их пределы;

Внутри каждой группы имеется несколько подгрупп, уточняющих некоторые аспекты конкретного документа. Так, например, к подгруппе «A01» относятся входящие документы, источ-

ником которых являются партнерские или дружественные организации; к подгруппе «A16» принадлежат документы, требующие внешней экспертной оценки и т.д. Вся группа «А» является наиболее уязвимой по причине невозможности контроля документа в некоторые моменты времени, а также наибольшей потенциальной ценности, потому для этой группы уровни допуска для системы оценки угроз несколько отличны от прочих. Так, например, компонент паутины «Песочница» присваивает в несколько большее время жизни объектам категории «А».

Песочница является своеобразным хранилищем для объектов СЭД, в которые помимо документов, также входят пользователи, маршруты (с их собственными объектами), роли, интерфейсы и т. п. По принципу функционирования, песочница является синергией реляционной базы данных и виртуальной интегрированной среды, что позволяет реализовать интеллектуальную систему заполнения таблицы соответствия типа «файл-хранение». Этот факт означает, что система сама определяет, как хранить каждый конкретный файл. В системе реализовано хранение файлов в виде архивов, а также раздельное хранение ключевых особенностей (слов, фраз, изображений, стилей, встроенных объектов, ссылок, связей и т.п.) документов, их хеш-сумм (CRC32, MD5, SHA-1, TTH), сигнатуры (совокупности характеристик), электронной цифровой подписи (ЭЦП) и любых их сочетаний. Песочница предназначена условно-временного хранения подозрительных объектов, а также на ее основе реализуется база данных для действующих алгоритмов обнаружения изменений в файлах.

Модулем «Паутина» используются два собственных встроенных метода обнаружения несанкционированных изменений в объектах СЭД:

– модельно-суффиксный метод, который на основании группы алгоритмов, осуществляет сопоставление входящего массива данных объекта СЭД с имеющейся коллекцией, сформированной на основании рассмотренных механизмов песочницы;

– дактилоскопический метод, сравнивающий небольшие фрагменты входящего массива с эталонными фрагментами коллекции.

Особенность первого метода является возможность использования в «дежурном» режиме, т. е. благодаря минимальной нагрузке на АИСС он может постоянно выполняться в реальном времени, не создавая коллизий и тем самым обеспечивая общую «разведку». Второй метод имеет управляемую глубину анализа, благодаря чему может демонстрировать 94-96% точность анализа, т. е. практически не имеет ложных срабатываний, и, соответственно, не создает избыточной нагрузки на ответственных лиц. Метод используется для «точечной» обработки подозрительных объектов.

По факту обнаружения потенциального вредителя и объекта его воздействия, паутина локализует угрозу, помещая пользователя (иногда, вместе с его ролью и интерфейсом, если причина возникновения угрозы может крыться в них) и документы в песочницу, составляет развернутый отчет о его действиях, формирует один из типовых бизнес-процессов «Обнаружение угрозы», выставляя, в зависимости от типа и ранга документа, а также точности (вероятности), ответственных лиц в качестве узловых точек и запускает его на исполнение прилагая составленный отчет. До устранения угрозы система собирает и хранит информацию обо всех действиях целевого пользователя и смежных исполнителей, а также контролирует состояние как целевого документа, так и всех прочих документов, имеющихся в истории работы данного пользователя. Таким набором действий не только локализуется текущая угроза, но и строится «база знаний», на основе которой вырабатываются рекомендации по профилактике угроз подобного рода.

Рассмотренный модуль «Паутина», а точнее, его «Песочница», закладывает в систему предотвращения угроз базу для перспективной автономной самообучающейся системы комплексной организации информационной безопасности в АИСС. Так, пополняя «базу знаний», и адаптируя алгоритмы под ее более интенсивное и рациональное использование имеется возможность добиться непревзойденной эффективности защиты информации.

Литература

1. Жеребенкова А. В. Документооборот на предприятии. СПб: Вершина, 2005.

2. Журавлев А. Е. Об автоматизации системы контроля знаний в вузе в соответствии с положениями Болонского процесса // Новые информационные технологии в образовании: Сборник научных трудов четырнадцатой международной научно-практической конференции «Применение технологий «1С» для повышения эффективности деятельности организаций образования» 28-29 января 2014 г. Часть 2. М.: ООО «1С-Паблишинг», 2014. С. 77.

3. Журавлев А. Е. Автоматизация системы оценки качества освоения учебной программы // Материалы XXV международной конференции «Применение новых технологий в образовании», «ИТО-Троицк-2014». М.: БАЙТИК, 2014. С. 412–413.

4. Майкл Дж. Д. Саттон Корпоративный документооборот. Принципы, технологии, методология внедрения. СПб: БМикро, Азбука, 2002.

А.С. Лукьянов,
к.т.н., Воронежский институт МВД России
С.В. Канавин,
к.т.н., Воронежский институт МВД России

АНАЛИЗ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕГАТИВНОГО ВЛИЯНИЯ ЭКСТРЕМИЗМА НА УРОВНЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

В настоящее время в мире география экстремизма расширяется, он начал распространяться по всем континентам, появляясь на территориях, которые ранее отличались внутриполитической стабильностью. За многие века своего существования экстремизм и терроризм сильно эволюционировали. Разворачиваясь в условиях глобализации и информационной революции, они гораздо более гибко, нежели государственные структуры, принимают се-

годня приспособленные к новым условиям организационные формы деятельности. Поэтому, несмотря на масштабные международные усилия по борьбе с этим злом, количество террористических актов по всему миру продолжает расти [3].

Экстремизм как негативный социальный феномен не является чем-то абсолютно новым, присущим исключительно нашему времени и современному обществу. Насколько позволяет судить писаная история общества, в той или иной форме они существовали во все века и у всех народов и обществ. Однако в современную эпоху экстремизм, с одной стороны, приобрел совершенно иной масштаб, и многократно умножился негативный эффект от экстремистской деятельности, а, с другой — он стал восприниматься и оцениваться обществом с гораздо большей остротой и неприятием. Цивилизованное общество, умудренное опытом долгих веков исторического развития, воспринимает сегодня это негативное явление, прежде всего как проявление дикости и варварства, как пережиток ранних эпох развития человечества и его политической и духовной культуры. Поэтому противодействие этому негативному феномену принимает, сегодня не локальный и частный, а общецивилизационный, международный характер, но такой, же характер приобретают сегодня, к сожалению, и сам экстремизм.

Современный политический экстремизм хорошо оснащен как интеллектуально, так и инструментально. Высокий интеллектуальный уровень как признак экстремизма не является чем-то новым, появившимся только в условиях Интернета и информационной глобализации. Отцами идеологии экстремизма всегда были неординарные и даже выдающиеся люди. Можно вспомнить в этой связи имена Бакунина, Кропоткина, Троцкого, Муссолини, Мао, Че Гевары, Маркузе и т.д. Молодежные бунты шестидесятых годов XX века в западных странах прошли, как известно, под знаком трех «М» – Маркс, Мао, Маркузе. Хотя разрыв между бедностью и богатством и сегодня является одной из главных причин социальных и политических конфликтов, тем не менее, идеологическое позиционирование на социально-классовой основе в международном экстремистском движении сегодня отодвинуто на второй план. Идеологическая борьба возвращается в со-

временный мир, но возвращается уже на иной, культурно-ценностной и культурно-этнической, основе [3].

Рассмотрим предупреждение экстремизма в нескольких аспектов. Во-первых, предупреждение экстремизма и повышение эффективности борьбы с ним – одна из первостепенных задач любого современного государства. Во-вторых, предупреждение экстремизма – есть комплексная система мер социально-экономического, политического и юридического характера, направленная на предотвращение: возникновения экстремизма и террористических организаций (группировок), совершения экстремизма и террористических актов, последствий экстремизма и терроризма; целью которой, является обеспечение общественной безопасности населения, защита политических, экономических и международных интересов государства. К ним, в настоящее время, относятся следующие: 1) борьба с преступностью экстремистской и террористической направленности ведется в основном в ходе реагирования на уже совершенные преступления; 2) отсутствие совместной работы по предупреждению преступных посягательств, разрушению международных и межрегиональных связей преступных группировок, и как следствие, ликвидации экстремистских и террористических организаций; 3) в настоящее время еще не создан совместный и полноценный информационный банк данных обо всех ранее совершенных экстремистскими и террористическими группами преступлениях и участниках этих групп.

Следует признать, что в XXI веке экстремизм как весьма эффективный инструмент нелегитимного насильственного достижения политических целей, что сказывается на уровне национальной безопасности России и вообще получает широкое распространение в мире. При этом организаторы экстремистской деятельности стремятся извлекать максимальную выгоду из процесса глобализации, ставя себе на службу новейшие информационные технологии, делая все менее уязвимыми для правоохранительных органов элементы своей инфраструктуры, создавая мощную финансовую базу для преступной деятельности. Возникают террористические организации нового типа, построенные по принципу сетевой структуры, обладающей наибольшим потенциалом в современных информационно-коммуникативных

условиях. Для них характерны единые центры и информационно-коммуникативные каналы, автономный способ существования входящих в сообщество периферийных преступных группировок, взаимодействующих как с центром, так и между собой. Сторонники экстремистских действий, противоречащих общечеловеческим ценностям, используют достижения новейших технологий с целью пропаганды собственной идеологии и ведения информационных войн. Так, в настоящее время насчитывается более 500 Интернет-сайтов, направленных на разжигание национальной вражды, более 2000 сайтов – религиозной вражды и т. д.

Одним из основных направлений стоит отметить защиту данных на интернет-сайтах, информационных систем обрабатывающих информационные ресурсы, т.к. имея возможности свободного действия для направлений экстремизма и терроризма может быть нанесен ущерб разного уровня для национальной безопасности России. Существуют, различные методы и средства защиты информационных ресурсов, выступающие неотъемлемым компонентом комплексной системы обеспечения информационной безопасности и способствующей минимизации существующих угроз информации. Результаты аналитических исследований являются основой построения и регулярной актуализации комплексной технологической системы защиты информации.

Под системой защиты информации (СЗИ) понимается рациональная совокупность направлений методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, а также ее утечке [1]. Главными требованиями эффективного функционирования системы являются: персональная ответственность начальников и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений, подлежащих защите, регламентация порядка доступа сотрудника к конфиденциальным документам, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности данной службы.

Ценность информации и требуемая надежность ее защиты находятся в прямой зависимости. Важно, что структура системы защиты должна охватывать не только электронные информационные системы, а весь управленческий комплекс подразделения в

единстве его реальных функциональных отделений, документационных процессов. Отказаться от бумажных документов и часто рутинной, исторически сложившейся управленческой технологии не всегда представляется возможным, особенно если вопрос стоит о безопасности ценной, конфиденциальной информации под которой понимается состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право [2].

Основной характеристикой системы является ее комплексность, т.е. наличие в ней обязательных элементов, охватывающих все направления защиты информации, что обеспечивает трудность ее преодоления [4]. Конкретную систему защиты информации можно представить в виде кирпичной стены, состоящей из множества разнообразных элементов.

Элементами СЗИ являются: правовой, организационный, инженерно-технический, программно-аппаратный и криптографический, представлено на рис. 1. В каждом элементе защиты могут быть реализованы на практике только отдельные составные части в зависимости от поставленных задач защиты. Структура системы, состав и содержание элементов, их взаимосвязь зависят от объема и ценности защищаемой информации, характера возникающих угроз безопасности информации, требуемой надежности и стоимости системы.

В различных государственных организациях множеством информационных систем и значительными объемами защищаемых сведений формируется многоуровневая система защиты информации, характеризующаяся иерархическим доступом к информации. Сложные, технически насыщенные системы не всегда рациональны, т.к. защита информации может произойти по непредсказуемому организационному каналу.

Содержание составных частей элементов, методы и средства защиты информации в рамках любой СЗИ должны регулярно изменяться с целью предотвращения их раскрытия злоумышленником.

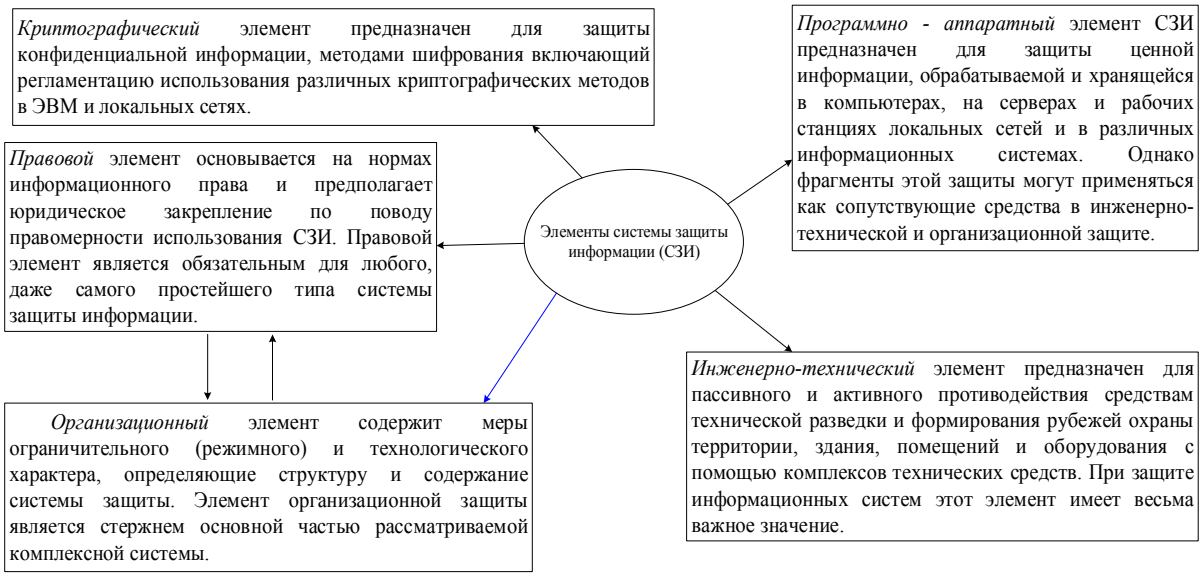

Рис. 1. Элементы систем защиты информации

Следовательно, основным условием безопасности информационных ресурсов ограниченного доступа от различных видов угроз (экстремизма и терроризма) является, прежде всего, организация в подразделении аналитических исследований, построенных на современном научном уровне и позволяющих иметь постоянные сведения о необходимой структуре и эффективности системы защиты и направлениях ее совершенствования в соответствии с возникающими ситуационными проблемами. Задачи обеспечения безопасности информации реализуются комплексной системой защиты информации, которая по своему назначению способна решить множество проблем, возникающих в процессе работы с информационными ресурсами.

Литература

1. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Архитектура защиты информации.

2. Рекомендации по стандартизации Р 50.1.053. – 2005. Информационная технология. Основные термины и определения в области технической защите.

3. Аршинов С.Ф. «Исламский фактор» в общественно-политической жизни современной России: диссертация политических наук: 23.00.02. – Саратов, 2005. – 231 с.: ил.

4. Романец Ю.В. Защита информации в компьютерных системах и сетях. / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин– М.: Радио и связь, 2001. – 376 с.

К.Л. Костюченко,
к.т.н., доцент,
Уральский юридический институт МВД России,
kkost2@yandex.ru

3D-ПЕЧАТЬ: КРИМИНАЛЬНЫЕ И ТЕРРОРИСТИЧЕСКИЕ АСПЕКТЫ

В статье дана общая характеристика технологии 3D-печати. Определены криминальные, террористические, экстремистские и др. проблемы, выявляющиеся при реализации 3D-технологий. Намечены правовые, информационные, организационные и морально-воспитательные пути решения проблем.

Как известно из истории, многие открытия, изобретения, конструкторские разработки не только способствовали прогрессивному развитию человечества, но и служили во вред ему. Так, некоторые технические и технологические новинки последнего времени (роботы, беспилотные летательные аппараты, дроны, радиоуправляемые машинки, программные продукты и др.) были использованы как криминальные и террористические средства. Похожая участь, скорее всего, ожидает и технологии 3D-печати (3D-принтеры, 3D-сканеры, 3D-редакторы и т. п.).

3D-печать (трехмерная печать, «объемная» печать) – это большой шаг вперед в науке, образовании, инженерии, дизайне и т. д. Сегодня 3D-принтеры работают не только с пластмассами, но и с металлами, керамикой, биоматериалами и множеством различных их сочетаний, характеризующимися уникальными свойствами и высоким качеством поверхностей, производя достаточно большие объекты (размером до нескольких метров). Наиболее распространенными областями применения являются: архитектура (макеты зданий, городов и т. п.) [1]; строительство (первые примеры «распечатанных» домов, а в планах – создание жилых модулей на Луне методом распечатки из имеющегося там грунта); машиностроение (концепт-модели и прототипы будущих изделий и деталей); медицина (протезы, ортопедические изделия, муляжи и макеты органов пациента); образование (самые разнообразные наглядные пособия); легкая и текстильная промышлен-

ность (бытовая техника, одежда и обувь по индивидуальным характеристикам); пищевая сфера (кондитерские изделия и блюда самых сложных видов и вкусов); ювелирное дело; оборонная промышленность; военная топография; правоохранительная сфера (оперативная распечатка макетов зданий и местности при тактическом планировании); театр, кино, хобби (различные предметы, декорации, муляжи редких музейных экспонатов, мелкосерийное производство, штучные и коллекционные изделия) и др.

Однако быстрое развитие 3D-печати порождает и проблемы: экономические (падение спроса на товары из-за распечатки в домашних условиях практически любой понравившейся вещи, трансформирование мирового производства и инфраструктуры) [2]; социальные (закрытие некоторых промышленных предприятий, повышение уровня безработицы); правовые (несоблюдение при 3D-печати авторских прав и неуплата компенсации автору).

Не исключение и криминальные проблемы. Они появились после того, как 3D-принтер «распечатал» с высокой точностью макет реального пистолета, который можно использовать при совершении преступлений (ограблений).

По мере того как материалы и аппаратура будут совершенствоваться при одновременном снижении стоимости, 3D-принтеры, как и их предшественники – 2D-принтеры, достаточно скоро станут привычными бытовыми устройствами. Массовая доступность 3D-печати может составлять серьезную угрозу общественной безопасности, потому что с помощью новой технологии можно довольно просто создать (распечатать) стреляющее огнестрельное пластиковое оружие, не замечаемое металлодетекторами. В будущем при наличии 3D-принтера любой человек сможет наладить производство оружия у себя дома. А это оружие (и даже точные копии) наиболее вероятно будет использовано в криминальных, террористических, экстремистских целях.

Американский оружейный мастер Хэйв Блу (Have Blue) стал первым в мире, кто собрал огнестрельное оружие, ствольная коробка которого напечатана на 3D-принтере. Естественно, ствол, боек и другие механизмы невозможно сделать из пластика, так что в этом пистолете используются оригинальные металлические детали от винтовки M16.

Еще один американец – студент Коди Уилсон (Cody Wilson), успешно протестировал первый в мире пистолет «The Liberator», распечатанный на 3D-принтере [3]. При этом его затраты на материалы составили всего $25, а печать длилась не более суток. С сайта, где он выложил чертежи, их тут же скачали более 100 тысяч раз. Создалась ситуация, когда любой пользователь без каких-либо специальных знаний в области проектирования и разработки оружия может распечатать все детали и собрать полностью работоспособную модель пистолета.

Последователи только увеличивали опасность: подбирали материалы и режимы изготовления для увеличения прочности ствола (для производства нескольких десятков выстрелов), распечатывали винтовку, создавали пластиковые пули со свинцовой дробью внутри, научились создавать металлические образцы оружия, приближая по характеристикам распечатки к боевому оружию.

Журналисты пошли дальше. В Израиле они провели эксперимент, дважды проникнув в здание парламента с распечатанным на 3D-принтере пистолетом сквозь охрану и рамки металлодетекторов. После того как они побывали на совещании, где присутствовал премьер-министр, оружие было испытано в тире стрельбой боевыми патронами. Журналисты Daily Mail смогли проехать на поезде Eurostar из Лондона в Париж с распечатанным пистолетом «The Liberator». Следовательно, явно проявляется тот факт, что распечатка неотслеживаемого правоохранительными органами оружия может быть проведена скрытно (в домашних или подобных условиях) с высоким качеством, с постоянно повышающейся точностью и мощностью выстрела. Легкость же одновременного получения чертежей стреляющих устройств (и других опасных приборов и механизмов) в разных географических точках с последующим созданием большого количества копий становится острой криминальной и террористической угрозой, превращающейся в угрозу национальной безопасности.

С помощью 3D-принтера можно создать и огнемет. Дизайнер Иван Оуэн решил подготовиться, как говорится «на всякий случай», и с помощью 3D-принтера самостоятельно собрал надежное оружие для отталкивания зомби – Flamethrower. Используя листовой вентилятор на батарейках, пропановую горелку

и 3D-печатные детали, создано оружие, которое работает на основе кукурузного крахмала, который вспыхивает при контакте с пропаном. Пока огнемет против зомби еще воспринимается как курьез, но при определенной доработке может стать страшным оружием.

Техническая мысль создателей не стоит на месте. Поэтому могут быть придуманы самые разнообразные опасные изделия летального и нелетального действия. При этом тому, кто будет собирать оружие, специальных умений и знаний по производству оружия не требуется – чертежи и документацию можно будет получить по сети Интернет. Уже сейчас там достаточно комментариев типа: «Дайте мне 3D-принтер! Я найду чертежи АК-47 и пойду грабить банк!».

В ближайшее время обозначенные проблемы только усугубятся. Число «потребительских» домашних 3D-принтеров у россиян уже подобралось к 100 тыс. Следовательно, теоретически появляется возможность оперативной и скрытной распечатки большого количества оружия (или иных «стреляющих» и опасных устройств). Такое оружие будет характеризоваться высоким качеством, адаптацией под конкретного человека, маскировкой под различные предметы. Нельзя оставлять в стороне и такой фактор, как эстетическая привлекательность оружия для потребителя – потенциального нарушителя (преступника).

Эти криминальные и террористические проблемы нужно решать. Какие-то – уже сейчас, какие-то – в скором будущем.

Возможно, придется внести в некоторые нормативные правовые акты корректировки, связанные с уточнением формулировок описаний деталей оружия. Прежде всего, в Федеральный закон «Об оружии» (по аналогии с добавлением оружия, произведенного с помощью 3D-принтера, в перечни огнестрельного оружия некоторых штатов США). Учитывая длительный характер принятия нормативных правовых актов, информационная подготовительная работа должна начинаться уже сейчас.

Пресечение бесконтрольной распечатки оружия ляжет на плечи правоохранительных органов и спецслужб государства. Основной путь решения – информационно-поисковая работа и методы оперативно-разыскной деятельности.

Теоретически возможен и административно-правовой путь – поставить под контроль органами внутренних дел приобретение и эксплуатацию 3D-принтеров. Подобный пример уже был – в начале 90-х годов XX века лицензионно-разрешительная система МВД России регистрировала цветные принтеры с целью пресечения попыток фальшивомонетничества. Однако должный эффект контроля достигнут не был из-за стремительного роста количества и разнообразия принтеров.

Проблема выявления случаев быстрого распространения чертежей для распечатки оружия в телекоммуникационных системах – также сфера совместной организационной деятельности правоохранительных органов и некоторых гражданских ведомств, например, Роскомнадзора.

Вероятно, придется усилить профилактическую составляющую, которая состоит в целенаправленной морально-воспитательной работе (совместно со СМИ) по снижению привлекательности «распечатки оружия» и информировании потенциального нарушителя (преступника) об уголовно-правовой ответственности за данное деяние.

Таким образом, можно заключить, что 3D-печать не только является технологическим прорывом, но и несет серьезные угрозы национальной безопасности. Поэтому уже в самое ближайшее время государству и его правоохранительным органам необходимо создавать организационно-правовые, программно-технические и информационные средства нейтрализации указанных угроз.

Литература

1. Канесс Э. Доступная 3D-печать для науки, образования и устойчивого образования / Э. Канесс, К. Фонд, М. Зеннаро. – М., 2013. – 194 с.

2. Даер Э. Авто из принтера / Э. Даер // Популярная механика. – 2014. – № 12. – С. 72–74.

3. Официальный сайт «Военное обозрение». – URL: http://topwar.ru/ (дата обращения: 05.05.2015).

И.С. Рекунков,
к.т.н., Московский государственный университет
информационных технологий, радиотехники и электроники,
rekunkov_ivan@mail.ru

МЕТОДИКА ПРОВЕДЕНИЯ СПЕЦИАЛЬНОГО ОБСЛЕДОВАНИЯ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ ПЕРЕД ПРОВЕДЕНИЕМ СОВЕЩАНИЯ С ОБСУЖДЕНИЕМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В статье описана методика проведения специального обследования защищаемого помещения перед проведением совещания с обсуждением конфиденциальной информации.

Специальные обследования защищаемого помещения – это комплекс инженерно-технических мероприятий, проводимых с использованием необходимых, в том числе и специализированных технических средств, проводимых с целью выявления возможно внедренных электронных средств съема информации в ограждающих конструкциях, предметах мебели и интерьера выделенных помещений [3].

Подготовка к проведению специальных обследований:

Учитывая то, что специальные обследования защищаемых помещений являются комплексом мероприятий, которые проводятся, как правило, таким образом, чтобы не привлечь внимания вероятного противника, заинтересованного в получении информации ограниченного пользования, циркулирующей в выделенном помещении, специальные обследования проводятся в виде поисковой операции. Проведение поисковой операции тщательно готовится и легендируется под проведение комплекса ремонтно-строительных работ.

Рассмотрим общий вариант выполнения подготовки и проведения поисковой операции, проводимой специализированной группой.

В рамках подготовки операции необходимо, прежде всего, провести оценку обстановки, складывающейся в районе проведения поисковой операции

Оценка угроз:

При подготовке к проведению поисковой операции, как правило, противник нам неизвестен, поэтому построение модели вероятного противника и моделирование его действий зачастую приходится выполнять со слов заявителя. Так, анализируя причины, побудившие заявителя обратиться за помощью, можно получить представление о планах противника.

В результате оценки противника необходимо сделать промежуточные выводы, которые должны позволить получить предварительный облик противника:

характер его действий позволит оценить его потенциальные возможности;

расположение и вид закладных устройств (если они обнаружены до проведения поисковой операции) позволит определить его реальные возможности и выявить связи с работниками вашей организации и т. д.

Здесь представлен один из возможных вариантов выводов. Конкретные выводы можно сделать, только получив реальную задачу [2].

Оценка условий, в которых решается поставленная задача:

После предварительной оценки противника и прикидки его модели действий, оценивают условия, в которых придется решать поставленную задачу:

анализируется расположение объекта на местности с учетом окружающей его территории и размещенных на ней посторонних объектов;

оценивается контролируемая зона и возможности по снятию информации из-за ее пределов;

обследуется сам исследуемый объект.

При непосредственном знакомстве с объектом прежде всего выясняют:

взаимное расположение контролируемых и смежных помещений, режимы их посещения;

устанавливают факты и сроки ремонтных работ, монтажа и демонтажа коммуникаций, замены предметов мебели и интерьера;

изготовляют планы помещений, на которые наносят все входящие и проходящие коммуникации;

изучают конструктивные особенности ограждающих поверхностей, материалы покрытий.

Анализ вероятного противника и объекта действий позволяет сделать выводы и наиболее полно оценить свои возможности и необходимые условия для выполнения поисковых мероприятий.

Базируясь на выводах о возможном противнике и данных об объекте, определяют:

виды и объем поисковых действий;

состав измерительной техники и вспомогательного имущества;

необходимое количество специалистов и подсобных рабочих;

временной диапазон проведения операции.

При подготовке работ особое внимание необходимо уделить анализу уязвимости коммуникаций, имеющих выход за пределы объекта (силовая сеть, телефония, сигнализация). Помимо того, что по этим линиям может передаваться информация от закладных устройств, на телефонных линиях на всем их протяжении присутствует передаваемая штатно речевая или цифровая информация (факс, модем).

Проверка данных коммуникаций обычно проводится с участием специалистов, эксплуатирующих эти линии. При разработке легенды на проведение работ необходимо учитывать возможность участия этих специалистов в несанкционированном съеме информации. Перечисленные мероприятия проводит руководитель поисковой операции.

В результате оценки обстановки и уяснения поставленной задачи, руководитель должен иметь пакет документов для формирования замысла решения на проведение поисковой операции.

Пакет документов должен включать:

согласованную с заказчиком легенду проведения поисковой операции;

план прилегающей территории с указанием принадлежности и назначения строений;

поэтажный план строения с обозначением смежных с обследуемым помещений;

отчет об организациях или частных лицах, работающих в смежных помещениях;

протокол, содержащий характеристики ограждающих поверхностей, материалов покрытий;

схему жизнеобеспечивающих сооружений с привязкой к плану помещения;

схему входящих и проходящих проводных коммуникаций;

план (фотографии) размещения мебели, предметов интерьера на объекте;

план-график работ с указанием ответственных исполнителей;

перечень необходимой исследовательской аппаратуры [1].

Замысел решения на проведение поисковой операции:

В результате уяснения задачи и оценки обстановки у руководителя операции формируется замысел выполнения поставленной задачи. В нем руководитель намечает порядок и последовательность решения проблем, влияющих на выполнение основной задачи, при этом он определяет:

ответственных за выполнение основных этапов работ;

последовательность и сроки их выполнения;

порядок материального обеспечения;

порядок и последовательность действий при отклонениях и несоблюдении сроков решения основных вопросов;

порядок взаимодействия между исполнителями;

порядок управления и контроля за действиями подчиненных.

После оформления решения отрабатывается план-график выполнения работ, в котором отражаются основные вопросы решения:

начало и окончание основных работ;

ответственные исполнители;

последовательность выполнения основных этапов, их взаимосвязь между собой;

организация контроля качества и сроков выполнения основных видов работ.

Выполнение поисковых мероприятий:

Рассмотрим вариант проведения поисковых мероприятий непосредственно на объекте.

Первым этапом проводятся исследования, которые условно можно разделить на четыре вида:

радиообнаружение;

осмотр помещения;

обследование электрических и электронных приборов;

проверка проводных коммуникаций.

Для их выполнения используют металлодетекторы, нелинейные локаторы, индикаторы электромагнитного поля, сканирующие приемники и радиочастотомеры, переносные рентгеновские и теплови-зионные приборы, программно-аппаратные комплексы и прочие имеющиеся в наличии поисковые средства. Досмотр труднодоступных позиций осуществляют с применением зеркал или волоконно-оптических эндоскопов.

Радиообнаружение:

Для эффективного проведения радиообнаружения желательно наличие карты загрузки радиодиапазона (в виде файла или распечатки), полученной на расстоянии от 300 до 1000 м. от объекта. Это позволит при нахождении в ближней зоне действия возможных радиозакладных устройств (непосредственно на объекте) упростить решение задачи с помощью сравнительного анализа загрузки диапазонов. В процессе работы составляют карту загрузки радиочастотного диапазона, отсортировывают сигналы известных станций, идентифицируют источники нелегальных излучений, регистрируя наличие составляющих на частотах второй и третьей гармоник. Не стоит забывать, что с развитием элементной базы, появлением новых методов кодирования и модуляции вероятность использования противником РЗУ с открытым каналом падает, но полностью исключать ее из рассмотрения нельзя [2].

Первичный осмотр и техническая проверка:

Второй вид работ, касающийся осмотра помещений, условно можно подразделить на: первичный осмотр и техническую проверку.

Первичный осмотр. На этом этапе осуществляют визуальный контроль помещения и находящихся в нем предметов. Во избежание пропуска зоны или предмета осмотр проводят по определенной схеме, двигаясь по часовой стрелке и от периферии к центру. При наличии плана или фотографии предварительно сличают истинное размещение вещей и предметов с зафиксированным документально.

Техническая проверка:

Аппаратурную проверку предметов мебели и интерьера проводят с применением нелинейного локатора и переносного рентгеновского аппарата на подготовленной площадке, предварительно проверенной на наличие помеховых сигналов [3].

Проверка электрических и электронных приборов:

К следующему виду относится проверка электрических и электронных приборов.

Электрические приборы (настольные лампы, нагревательные приборы, электрические удлинители) перед проверкой включают в сеть и индикатором поля определяют наличие в них источников радиоизлучения.

При установлении подозрительных излучений прибор проверяют с помощью комплекса радиообнаружения. Затем обесточивают, разбирают и осматривают.

После проверки электроприборы опечатывают специальными пломбами или маркируют ультрафиолетовыми метками [3].

Проверка проводных коммуникаций:

Затем проводят проверку проводных коммуникаций. Осмотр каждой линии начинают с установления трассы ее прохождения в помещении, используя монтажные схемы, трассо и металлоискатели. Целесообразно проверить электросеть, затем абонентские телефонные линии и кабели сигнализации, а также распределительные коробки, щиты и т. д.

В начале линии проверяют на наличие в них высокочастотных сигналов, модулированных информационным сообщением. Слаботочные линии дополнительно проверяют на присутствие в них информационных низкочастотных сигналов.

Организуется проверка информационных коммуникаций на всех участках их прохождения (включая линейные устройства вне защищаемого здания), где нельзя исключить появление противника [3,4].

Подготовка отчетных материалов:

После проведения обследования, полученные материалы оформляют в виде отчетных документов, в состав которых должны входить:

протоколы с указанием мест срабатывания исследовательских приборов, участков вскрытий ограждающих поверхностей, описанием подозрительных предметов мебели и интерьера;

протоколы изъятия средств съема информации;

заключение о степени защищенности объекта от несанкционированного съема информации;

рекомендации по устранению и нейтрализации технических каналов утечки конфиденциальных сведений.

Документы согласовывают с заказывающей стороной и передают в службу безопасности объекта [1].

Следовательно, подготовка и проведение совещаний и переговоров по конфиденциальным вопросам, оформление их результатов связаны с выполнением ряда обязательных процедур, необходимых для правильной организации работы организаторов и участников этих мероприятий. При несоблюдении изложенных требований возникает серьезная опасность разглашения или утечки ценных сведений и секретов фирмы, ее партнеров и клиентов. Контроль за выполнением этих требований возлагается на секретаря-референта, который обеспечивает информационную безопасность деятельности фирмы, сохранение ее деловых и производственных секретов.

Список использованных источников:

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.

2. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации. Учебник для вузов. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

3. Хорев А.А. Техническая защита информации. Учебное пособие. М.: «Аналитика», 2008. – 435 с.

4. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие. – СПб.: ГУАП, 2006. – 188 с.

А.М. Любичев,
ФГАОУ ВО «Национальный исследовательский университет
«Московский институт электронной техники»,
andreymelaman@gmail.com
О.Б. Малежин,
к.т.н., доцент,
ФГАОУ ВО «Национальный исследовательский университет
«Московский институт электронной техники»,
omal@elvis.ru

АНАЛИЗ СПОСОБОВ ОЦЕНКИ ВЕРОЯТНОСТИ РИСКА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье анализируются основные способы оценки вероятности риска в сфере информационной безопасности. Выделяются основные их особенности, преимущества и недостатки.

В современном мире в сфере информационной безопасности очень велико многообразие определений слова «риск». Но практически во всех дефинициях слова «риск» ключевыми являются слова «вероятность» и «последствия» (или «ущерб»). Например, ГОСТ Р 51901.1-2002 «Менеджмент риска. Анализ риска технологических систем» дает определение риска как «сочетание вероятности события и его последствий» [1]. Еще один пример – в стандарте ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» приводится вот такая дефиниция – «риск (risk): потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов» [2]. Таким образом, хоть все трактовки и отличаются между собой, но, при этом, имеют практически одинаковый смысл. Если попробовать обобщить и объединить все существующие определения, то получается, что «риск – это сочетание вероятности осуществления определенного события и негативных последствий (то есть нанесение потенциального или реального ущерба активу или группе активов), связанных с этим событием».

Если разложить риск на компоненты, то основными его составляющими будут являться тяжесть возможного ущерба (последствия) и вероятность нанесения ущерба (которая состоит из частоты и продолжительности воздействия угрозы, вероятности возникновения угрозы и возможности избегания угрозы или ограничения ущерба от нее). Стоит отметить, что эффективность управления рисками напрямую зависит от того, насколько правильно и корректно будут оценены эти элементы.

Необходимо правильно оценивать вероятность того или иного риска, чтобы грамотно и эффективно управлять рисками. Существует несколько подходов измерения вероятности риска. Первый из них – это собственная статистика того, кто оценивает вероятность риска. Это один из самых эффективных методов, где главным условием является постоянность (неизменность) среды оценки. Статистическая (историческая) оценка позволяет прогнозировать будущее на основании информации, полученной за прошлые (прошедшие) периоды времени. Для успешной реализации данного метода требуется мониторинг и сбор данных на протяжении определенного периода времени (срок каждый раз варьируется в зависимости от конкретной ситуации). Стоит отметить, что при отсутствии адекватных инструментальных средств данный процесс является довольно ресурсоемким – необходим сбор, нормализация, хранение и анализ данных.

Ко второму способу измерения вероятности риска можно отнести анализ отчетов и использование статистики сторонних организаций (которые специализируются в данной сфере). Например, при таком подходе можно анализировать и извлекать полезную информацию из отчетов таких организаций как Computer Security Institute (CSI), Federal Bureau of Investigation (FBI), KPMG, PricewaterhouseCoopers (PwC), Ernst & Young (EY), МВД, Perimetrix, Infowatch и других. Но при использовании данного метода стоит отметить, что не всегда можно полагаться на такую статистику. Во многих случаях специалисты, использующие такой подход для измерения вероятности риска, не знают всех условий, при которых была реализована та или иная угроза информационной безопасности, представленная в отчете, или то каким образом произошел определенный инцидент, приведенный в статистике. Также обычно неизвестны все детали и методы сбора,

нормализации, анализа и обработки данных, которые применяет организация в своих исследованиях. Собираемая статистика во многом зависит от применяемых способов опроса, аудитории, желания респондентов сообщать точные данные, а также от масштаба опроса. Не стоит забывать, что следует делать поправку на тип организации для которой применяется данная статистика – это тоже немаловажный аспект при измерении вероятности риска.

К третьему способу относят самостоятельный подсчет вероятности риска. Схематично данный метод представлен ниже (рис.1).

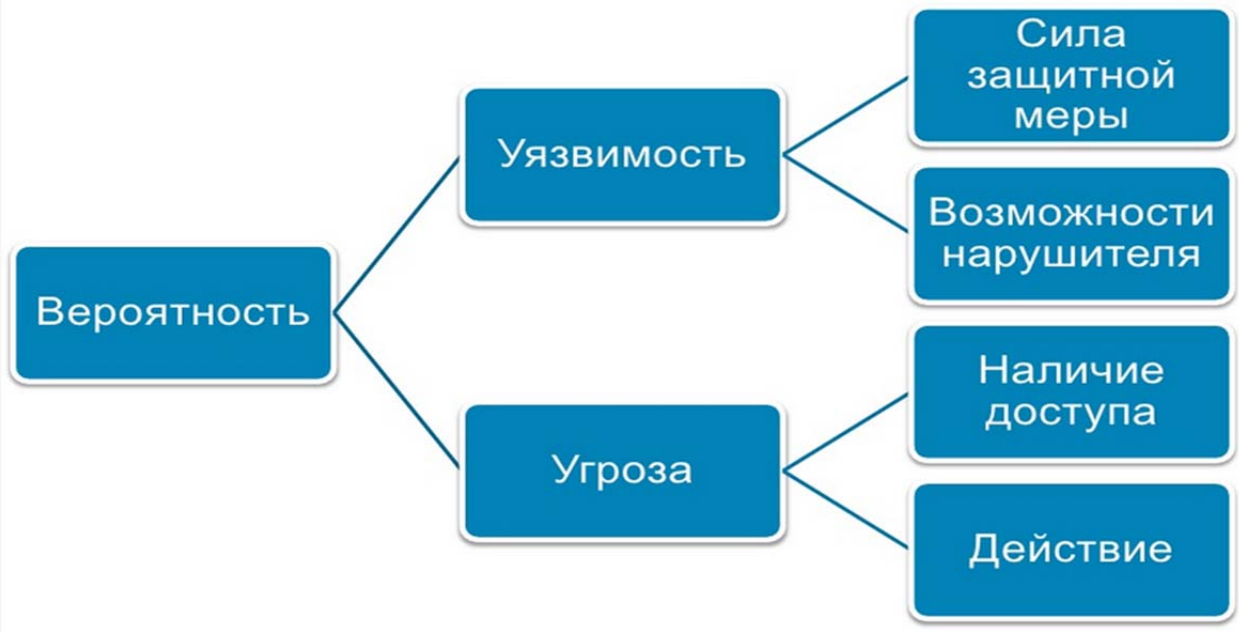

Рис. 1 – Самостоятельный подсчет вероятности риска

Здесь следует отметить, что для подсчета вероятности риска следует произвести оценку вероятности эксплуатации той или иной уязвимости (вероятность определяется силой защитной меры, направленной на защиту того или иного актива, и возможностями, которыми обладает нарушитель), а также подсчет вероятности реализации какой-либо угрозы (которая зависит от наличия или отсутствия доступа у атакующего, а также от действий, которые нарушитель предпринимает).

К четвертому способу относят сравнение (сопоставление) риска с другими аналогичными рисками. При сравнении рисков следует учитывать несколько факторов. Такой метод возможен

только на аналогичных решениях по информационной безопасности и когда:

- установлены аналогичные средства безопасности;
- назначение систем и технологии у двух сторон сравнимы;
- угрозы и компоненты риска могут быть сопоставимы;
- технические условия сравнимы;
- условия использования сравнимы.

Также при таком подходе необходимо иметь в виду вспомогательные условия (например, потенциал нарушителя и вид защищаемой информации) [3].

Пятый способ представляет собой прогнозирование, которое можно осуществлять с помощью аналитических методов, таких как:

- «Дерево неисправностей» (Fault Tree Analysis) – диаграмма всех возможных последствий инцидента в системе;
- «Дерево событий» (Event Tree Analysis) - диаграмма всех возможных последствий данного события;
- имитационное моделирование отказов или инцидентов.

Данный подход в сфере информационной безопасности не используется или практически не используется (применяется только в критических областях).

Шестой способ – подсчет бинарной вероятности риска. В данном случае вероятность считается равной 1 в том случае, если угроза реализуема, и 0 – если нет (при отсутствии средств защиты). Данный подход можно рассматривать при оценке вероятности только для узкого круга систем (так как он весьма ресурсоемкий) или для очень распространенных угроз. Этот метод используется в методиках ФСТЭК и ФСБ.

Для определения риска информационной безопасности различные методы могут использовать количественные или качественные шкалы. В первом варианте все компоненты риска и сам риск измеряются в числовых значениях. При применении количественных шкал вероятность атаки может измеряться числом в интервале, ущерб – в виде денежного эквивалента материальных потерь, которые возникают у организации, если атака успешно реализована. При использовании качественных шкал числовые значения меняются на эквивалентные им понятийные уровни. В этом случае каждому понятийному уровню будет соответство-

вать определенный интервал количественной шкалы оценки. Число уровней может быть различным в зависимости от используемых методик оценки вероятности риска [4].

При этом стоит отметить, что количественная оценка не всегда применима из-за:

- нехватки данных о системе;
- нехватки данных о деятельности, которая подвергается оценке;
- отсутствия или недостатка информации об инциденте (инцидентах);
- зависимости от человеческого фактора;
- того, что зачастую такие измерения риска требуют значительных затрат ресурсов.

Также стоит уточнить, что для качественной оценки необходимо:

- четкое объяснение всех терминов, которые используются (должна быть определена дефиниционная база);
- обоснование всех классификаций частот и последствий;
- понимание всех преимуществ и недостатков качественной (или экспертной) оценки и психологии восприятия риска.

Последний рассматриваемый (и наиболее распространенный) способ измерения вероятности риска в данной статье – это экспертная оценка. Частично она была описана выше. Стоит отметить, что при отсутствии статистических (исторических) данных экспертная оценка является единственным методом определения частоты (вероятности) реализации угрозы (или угроз). При данном подходе эксперты ранжируют вероятность возникновения того или иного события, опираясь на свой опыт и знание анализируемой системы. К достоинствам такого метода стоит отнести простоту его реализации, а к недостаткам (ограничениям) – возможность воздействия заинтересованных лиц на экспертное мнение, невозможность применения общих моделей для оценки всех рисков (всегда существуют случайные события, которые невозможно предугадать с помощью экспертной оценки), необходимость наличия достаточного количества экспертов, а также соответствующей квалификации каждого эксперта, психология восприятия риска [5].

Все способы и методы, рассмотренные в этой статье, применимы для различных частных случаев подсчета вероятности риска. Специалист, занимающийся построением системы управления рисками информационной безопасности, должен четко осознавать, когда следует использовать тот или иной способ. При этом стоит отметить, что построение системы управления рисками информационной безопасностью – это более сложная задача, чем выбор способа подсчета вероятности риска и требует хорошей теоретической подготовки, а также опыта проектирования и внедрения таких систем.

Литература

1. ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем [Электронный ресурс]. – Режим доступа: http://vsegost.com/Catalog/62/6283.shtml
2. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электронный ресурс]. – Режим доступа: http://vsegost.com/Catalog/27/271.shtml
3. ГОСТ Р 51901.13-2005 (МЭК 61025:1990) Менеджмент риска. Анализ дерева неисправностей [Электронный ресурс]. – Режим доступа: http://docs.pravo.ru/document/view/20841595/19930857/
4. Аудит информационной безопасности – основа эффективной защиты предприятия [Электронный ресурс]. – Режим доступа: http://www.dialognauka.ru/press-center/article/4753/
5. Как считать риски? Личный блог Лукацкого А. В. [Электронный ресурс]. – Режим доступа: http://lukatsky.blogspot.ru/2012/04/blog-post_18.html

А.А. Бодрова,
ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники»,
decaff24@gmail.com

АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СВОБОДНО ДОСТУПНЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, РАСПРОСТРАНЕННЫХ В СЕТИ ИНТЕРНЕТ

В статье приведен анализ свободно доступных в сети Интернет программных средств криптографической защиты информации, рассмотрены их функциональные возможности и используемые алгоритмы. Даны рекомендации по применению.

В сети Интернет растет число свободно доступных средств криптографической защиты информации (СКЗИ). Это программные СКЗИ, имеющие несвободные (proprietary software), открытые (open-source software) или свободные (free software) лицензии, дающие пользователю широкий спектр возможностей по применению. Большинство СКЗИ можно получить и использовать бесплатно. Они не имеют сертификатов ФСБ и ФСТЭК, однако для индивидуальных, корпоративных и коммерческих задач защиты информации такие средства применять на территории России не запрещается (законодательно ограничивается использование СКЗИ только в государственных и муниципальных учреждениях).

В информационном пространстве информация подвергается большому числу угроз – нарушение конфиденциальности, целостности, приписывание авторства или отказ от него, блокирование. Целью работы является анализ спектра задач по защите информации от угроз, которые можно решить, используя СКЗИ, распространенные и свободно доступные в глобальной сети.

Исторически, первым свободным СКЗИ был программный комплекс PGP (Pretty Good Privacy) - разработал Ф.Циммерман (США) в 1991 году, права принадлежат Symantec corp.

Бесплатная версия (PGP Desktop) позволяет выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том

числе прозрачное шифрование данных на запоминающих устройствах, на жестком диске. Дополнительные функции предоставляет платная версия программного комплекса: создание виртуального диска, шифрование физического диска, шифрование электронной почты.

Существуют реализации PGP для всех наиболее распространенных операционных систем (Windows, Mac).

Симметричное шифрование производится по одному из алгоритмов: AES, CAST5, 3DES, IDEA,Twofish, Blowfish, Camellia - на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal.

PGP поддерживает аутентификацию и проверку целостности посредством цифровой подписи по асимметричным алгоритмам RSA или DSA. При этом сначала создается хеш открытого текста по одному из алгоритмов: MD5, SHA-1, RIPEMD-160, SHA-256, SHA-384,SHA-512.

СКЗИ GNU Privacy Guard (GnuPG, GPG) – свободная программа для шифрования информации, электронной почты и создания электронных цифровых подписей. Разработана В. Кохом (Германия) в 1997. Является бесплатной программой с открытым исходным кодом - работает на большинстве операционных систем (Microsoft Windows, GNU/Linux, Mac OS X, FreeBSD, OpenBSD, NetBSDи т. д.).

Симметричное шифрование по алоритмам AES, CAST5, 3DES, IDEA (с помощью плагина), Twofish, Blowfish, Camellia.

Асимметричное шифрование по алгоритмам ElGamal и RSA (длина ключа от 1024 до 4096 бит).

DiskCryptor является СКЗИ с открытым исходным кодом. Программа была создана анонимным разработчиком. Она доступна только для платформы Windows на английском языке. Программа осуществляет прозрачное шифрование всех дисковых разделов, в том числе и системного, съемных дисков. Для увеличения скорости шифрования в программе предусмотрено аппаратное AES ускорение.

Программа осуществляет асимметричное шифрование по алгоритмам: AES, Twofish, Serpent.

СКЗИ FreeOTFE(Free On-The-Fly disk Encryption) это свободная бесплатная программа с открытым кодом, предназначенная для шифрования «на лету». Автор программы - Сара Дин.

Выпускается для операционных систем Windows и Windows Mobile. FreeOTFE может использоваться в «портативном режиме», который позволяет хранить программу на флеш-накопителе или другом портативном устройстве вместе с зашифрованными данными.

Шифрование файлов, папок, съемных носителей, жесткого диска, виртуальных дисков осуществляется по симметричным алгоритмам: AES, Blowfish, CAST5/CAST6 , DES / 3DES (data encryption standard), MARS, RC6 (Rivest Cipher 6) , Serpent, Twofish.

OpenVPN – свободная реализация технологии виртуальной частной сети VPN (Virtual Personal Network) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер – клиенты между компьютерами. OpenVPN была создана Джеймсом Йонаном и используется в операционных системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Mac OS X, QNX, Microsoft Windows, Android. Программы доступны в том числе и на русском языке.

Для шифрования в программе используется криптографическая библиотека OpenSSL, в которой реализованы симметричные алгоритмы: Blowfish, Camellia, DES, RC2, RC4, RC5, IDEA, AES, ГОСТ 28147-89. И асимметричные RSA, DSA, Diffie-Hellman key exchange, ГОСТ Р 34.10-2001 (34.10-94).

KeePass – это свободный менеджер паролей с открытым исходным кодом. Его официальная реализация есть только для Windows, но, т.к. исходный код открыт, есть огромное количество реализаций, в том числе для Linux и под OS X, например, KeePassX. Также есть приложения и для мобильных ОС. Программа доступна на русском языке.

Продукт можно использовать как портативное средство, сохранив его на флэш-накопителе USB для работы с общедоступными компьютерами. Помимо управления паролями, программа позволяет их генерировать на основе случайных нажатий пользователя по клавиатуре и перемещений мыши.

Для шифрования используются симметричные алгоритмы AES, Twofish.

Cloudfogger программа для автоматического шифрования данных, отправляемых в облачные хранилища. Это проприетарная программа, которую можно получить бесплатно. Права на нее принадлежат Cloudfogger GmbH. Программа доступна для Windows, Mac OS X, iOS и Android. Русскоязычной версии нет. Cloudfogger поддерживает большинство популярных облачных сервисов Dropbox, SkyDrive, Google Drive и др. Так же программа позволяет обмениваться зашифрованными файлами.

Данные шифруются алгоритмом AES с ключом 256 бит.

Права на программу Hotspot Shield принадлежат AnchorFree, Inc. Эта программа обеспечивает безопасность во время подключения к открытым точкам доступа Wi-Fi. Ее можно использовать на платформах Windows, Mac OS X, Android, iOS. Программа доступна на русском языке. Программа производит шифрование входящего и исходящего трафика алгоритмом AES и направляет его через собственные серверы.

У программы есть платная Elite версия, которая в добавление может работать на платформе Kindle и в ней отсутствует рекламный модуль.

Таким образом, свободно доступные СКЗИ позволяют решить практически все задачи защиты информации в информационной среде, реализуя широкий спектр криптографических функций: шифрование файлов (PGP Desktop, Diskcryptor, FreeOTFE, GnuPG, Cloudfogger), цифровая подпись (PGP Desktop, GnuPG), шифрование электронной почты (GnuPG), шифрование съемных носителей (Diskcryptor, FreeOTFE), шифрование жесткого диска (Diskcryptor, FreeOTFE), шифрование виртуального диска (Diskcryptor, FreeOTFE), разделение секрета (PGP Desktop, GnuPG), удаление остаточной конфиденциальной информации (PGP Desktop, Diskcryptor), создание скрытых дисков (FreeOTFE), организация защищенного туннеля в общедоступном канале связи (OpenVPN, Hotspot Shield), хранение паролей, генерация паролей (KeePass), шифрование данных в облачных хранилищах (Cloudfogger).

Литература

1. Официальный сайт программы Diskcryptor. [Электронный ресурс]. Дата обновления: 21.10.2014. URL:https://diskcryptor.net/wiki/Main_Page (дата обращения: 04.05.2015).

2. OpenPGP в России. [Электронный ресурс]. URL: https://www.pgpru.com/ (дата обращения: 11.05.2015).

3. Официальный сайт программы OpenVPN. [Электронный ресурс]. URL: https://openvpn.net/(дата обращения: 04.05.2015).

4. Официальный сайт программы KeePass. [Электронный ресурс]. URL: http://keepass.info/ (дата обращения: 04.05.2015).

5. Официальный сайт программы GnuPG. [Электронный ресурс]. URL: https://www.gnupg.org/ (дата обращения: 04.05.2015).

6. Официальный сайт программы Cloudfogger. [Электронный ресурс]. URL: https://www.cloudfogger.com/en/ (дата обращения: 04.05.2015).

7. Официальный сайт программы Hotspot Shield. [Электронный ресурс]. http://www.hotspotshield.com/ru/ (дата обращения: 04.05.2015).

8. PGP Desktop for Windows. User’s Guide. Symantec. – 2012. – 307 p.

С.Г. Федоров,
ФГБОУ ВПО «Московский государственный индустриальный университет», btrst2@ya.ru
Т.А. Ситников,
ФГБОУ ВПО «Московский государственный индустриальный университет», sitnikov_t@mail.ru
Н.Г. Бутакова,
к.ф.-м.н., доцент, ФГБОУ ВПО «Московский государственный индустриальный университет», Nat_Butakova@rambler.ru

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОЙ СРЕДЕ НА ПРИМЕРЕ КРИПТОВАЛЮТЫ

Проведен обзор действующих криптовалют, проанализированы особенности их использования в виртуальной среде, рассмотрены угрозы безопасности криптовалюты и меры противодействия им; описан ряд успешно проведенных атак и их последствий.

Защита информации в информационном пространстве, которое активно формирует интернет, и криптография, как главное направление защиты, приобретают все большее значение в современном обществе. Интернет представляет собой новую среду обитания человека, деятельности личности, общества и государства. Эта среда - виртуальная, и информация – основной объект этой среды – физически уязвима. Рассмотрим проблемы обеспечения информационной безопасности на примере криптовалют.

Всеобщая компьютеризация, недостатки и нестабильность принятых монетарных систем, а так же особенности человеческой психологии, подтолкнули общественность к поиску новых возможностей для совершения торговых операций. В 2009 на основе концепций Дэвида Чома, Вэя Дая и Ника Сзабо появилась первая успешно функционирующая криптовалюта – Bitcoin (Биткоин). В настоящее время в данной системе сгенерировано более 13 миллионов монет; торговый оборот криптовалюты Биткоин составляет более 800 тысяч биткоинов в сутки.

Криптовалюта (англ. Cryptocurrency) – вид цифровой валюты, эмиссия и учет которой основаны на криптографических методах (например, методе защиты Proof-of-work и асимметричном шифровании). Функционирование системы происходит децентрализовано в распределенной компьютерной сети. По состоянию на июнь 2014 года программное обеспечение всех криптовалют базировалось на открытом исходном коде системы Bitcoin. У криптовалют по умолчанию не предусмотрен принудительный возврат платежей, однако имеются возможности сделок с участием посредника, когда для завершения или отмены сделки требуется согласие всех трех или произвольных двух сторон, средства не могут быть принудительно заморожены или изъяты без доступа к приватному ключу владельца, однако участники сделки могут добровольно временно взаимно блокировать свои средства в качестве залога. Как правило, имеется верхний предел общего объема эмиссии. Однако у некоторых криптовалют, таких как PPCoin, Novacoin, Sifcoin и других отсутствует фиксированный верхний предел общего объема эмиссии и возможна как эмиссия за счет имеющихся накоплений, так и демиссия путем обязательного уничтожения небольшой фиксированной суммы в каждой транзакции. Все существующие на данный момент криптовалюты используются псевдонимно – все транзакции публичны, но привязки к конкретному человеку по умолчанию нет, однако личность пользователя может быть установлена, если известна необходимая дополнительная информация. Ведется разработка Zerocoin, где планируется заменить псевдонимность на анонимность. С момента появления первой криптовалюты было создано множество форков (*англ. fork – ответвление - использование кодовой базы программного проекта в качестве старта для другого*) и их количество постоянно растет.

В настоящее время популярность криптовалют продолжает расти, появляются новые сервисы упрощающие прием криптовалют для компаний. Примером такого сервиса является компания BitPay, среди ее клиентов virgin, microsoft, shopify. В начале 2015 г. число компаний работающих с сервисом BitPay возросло до 100 тыс. [1] Помимо коммерческой деятельности криптовалюты активно используются для благотворительности и спонсирования. В апреле 2014 года Dogecoin Foundation спонсировал одного

из пилотов гонок NASCAR [2], помимо этого была проведена благотворительная акция doge4water в ходе которой были собраны средства для борьбы с засухой в Кении. [3]

С ростом популярности криптовалют возросло и количество атак использующих особенности алгоритмов криптовалют, и веб-ресурсов, обрабатывающих данные счетов.

Основное различие криптовалют заключается в принципе генерации монет.

Proof-of-Work (POW) – принцип, согласно которому любая операция требует достаточно сложных вычислений, но которые легко и быстро проверяются обслуживаемой стороной, что является основой для создания защитной системы. При использовании этого принципа вероятность сгенерировать новый блок в системе у майнера пропорциональна вычислительной мощности аппаратных средств. Данный принцип первоначально предлагался как средство для борьбы с почтовым спамом. Отправителю письма предлагалось решить задачу занимающую некоторое процессорное время, незначительное для обычного пользователя, но существенно замедляющего массовую рассылку. Это основной принцип сети Bitcoin и подобных ему форков, обеспечивающий генерацию новых блоков системы. Сложность генерации блоков в системе биткоин пересчитывается раз в две недели и зависит от общей вычислительной мощи майнеров. [4]

Proof-of-Stake (POS) – принцип обеспечивает генерацию блоков монето-годами - количеством монет, умноженных на их «возраст» или время, которое они лежат нетронутыми. В данном случае майнер имеет возможность сгенерировать новый блок для системы при условии наличия у него монет в кошельке. Основное преимущество такого подхода - отсутствие необходимости в затратах электроэнергии для поддержания работоспособности валюты. Данный принцип позволяет избежать резких изменений некоторых ключевых параметров системы, таких как сложность и награда за генерацию блока. Впервые данный метод был показан в криптовалюте NxtCoin и впоследствии был использован при в разработке таких форков как: NovaCoin, YaCoin, PeerCoin. [5]

Некоторые из используемых в настоящее время валют используют гибридную систему генерации блоков, включающие в себя сочетание принципов **Proof-of-Work** и **Proof-of-Stake**.

Bitcoin (BTC) – первая криптовалюта запущенная в 2009 году, автором которой является человек, или группа лиц под псевдонимом Сатоши Накамото, который покинул проект в 2010 году оставив открытый исходный код системы и последователей, которые поддерживают ее работоспособность и продолжают ее развитие. В настоящее время рыночная капитализация Биткоин составляет около 3,2 миллиардов долларов США и суточный оборот более 800 тысяч монет в сутки. Среднее время генерации блока составляет 10 минут; максимально возможное количество монет в системе приближается к 21 миллиону; первоначальная награда за нахождение блока составляла 50 монет и уменьшается вдвое каждые 210 тысяч блоков, т.е. каждые 4 года. В качестве алгоритма хеширования используется SHA-256. Первоначально вычисление новых блоков происходило с помощью CPU, немногим позднее вычисление начали производить с использованием мощностей GPU, на смену которым пришли FPGA. В настоящее время для майнинга (*процесса выполнения математических вычислений для подтверждения транзакций, с наградой за выполненную работу)* используют оборудование в основе которого лежит ASIC - интегральная схема специального назначения. Данное оборудование существенно повлияло на рост сложности вычисления новых блоков и в начале их появления остро стала проблема осуществления «атаки 51%». [6]

Litecoin (LTC) – вторая по популярности криптовалюта в мире созданная в 2011 году; имеет рыночную капитализацию более 60 миллионов долларов США. Блоки в данной системе генерируются раз в две с половиной минуты. Максимально возможное количество монет составляет 84 миллиона. Сложность пересчитывается каждые 2016 блоков. Первоначальная награда за найденный блок составляет 50 монет и уменьшается вдвое каждые 840 тысяч блоков. Использует алгоритм хеширования «scrypt», который активно использует оперативную память, что усложняет разработку специального оборудования для вычисления этих блоков. [7]

Namecoin (NMC) – создана в 2011 году как средство обслуживания криптографически защищенной доменной зоны .bit. Монеты системы используются для приобретения доменов. Срок аренды домена истекает после генерации 36 тысяч блоков. Рас-

пределенная вычислительная сеть гарантирует невозможность создания двух одинаковых доменных имен и невозможность присвоения или изменения записи посторонним лицом. Данная криптовалюта основана на концепции Bitcoin, так же как и родительская валюта, использует алгоритм хеширования SHA-256. Рыночная капитализация, по данным на начало 2014 года, составляла более 29 миллионов долларов США, а суточный оборот монет более 35 тысяч монет или более 100 тысяч долларов. Общее количество монет и падение награды такие же, как и у сети Bitcoin. [8]

К числу наиболее вероятных угроз для криптовалют и возможных способов их парирования относятся:

«Атака 51%». В случае появления в сети майнера, сконцентрировавшего в своих руках большую часть вычислительной мощи сети, он получает возможность расщепить цепочку блоков и подтвердить легитимность контролируемой им ветви, как следствие того, что она имеет большую совокупную сложность. Это дает злоумышленнику возможность полностью контролировать любые операции в сети. Данная угроза, в первую очередь, актуальна для новых криптовалют, использующих метод POW для генерации блоков, как следствие низкой сложности и малого количества майнеров на начальном этапе. Для таких валют как Bitcoin или Litecoin вероятность реализации такой угрозы имеется, но экономически не целесообразна. В настоящее время стоимость проведения такой атаки будет выше, чем стоимость проданных атакующим монет, контроль над которыми он получит. Единственными источниками данной угрозы для этих криптовалют могут быть только поставщики специализированного оборудования, но даже в этом случае прибыль от реализации оборудования будет выше стоимости монет проданных злоумышленником из-за неминуемого падения биржевого курса. Кроме получения прибыли путем продажи монет, злоумышленник может ввести цензуру, но в этом случае наиболее вероятным развитием ситуации видится крах атакуемой криптовалюты ввиду ухода из нее пользователей.

Для снижения вероятности «атаки 51%» было предложено использование метода POS. В случае использования данного метода для реализации атаки необходимо иметь более 51% монет

криптовалюты, что автоматически превращает злоумышленника в главную жертву; [9]

Double-spending. Данная угроза актуальна для веб-ресурсов предоставляющих какие-либо товары или услуги за монеты криптовалют. Она основана на том, что продавец убеждается в создании транзакции на оплату и передает товар. В это время злоумышленник создает новую транзакцию из тех же монет, и при условии, что данная транзакция попадает в блок содержащий большее количество транзакций, она принимается системой. В итоге атакующий получает товар, а монеты уходят на адрес, включенный в наиболее полный блок. Для снижения этого риска продавцам не следует принимать транзакции с нулевым количеством подтверждений. Получение системой 6-ти подтверждений снижает вероятность реализации угрозы до 0.1%; [10]

Transaction malleability. Реализация данной угрозы возможна за счет особенностей протоколов некоторых криптовалют, которые дают возможность добавить мусорные данные в транзакцию на момент пока она не получила подтверждений. В результате этого искажается хеш транзакции и, как следствие, отправитель не может отследить ее статус. Сама транзакция не искажается и монеты доходят до получателя. Для снижения рисков рекомендуется использовать альтернативные пути подтверждения, например, проверять зачисление средств по адресу получателя, а не по хеш адресу транзакции. [11]

В июне 2013 года была реализована «атака 51%» на криптовалюту Feathercoin. Злоумышленник, используя имеющиеся в его распоряжении огромные вычислительные мощности, превышающие совокупную мощность сети более чем в 600 раз, захватил контроль над всеми вновь вычисленными блоками. В результате атаки злоумышленником было найдено около 180 блоков. В настоящее время неизвестно, была ли данная атака санкционирована создателями системы как средство ее популяризации, либо действовал сторонний злоумышленник. Цепочка блоков не была раздвоена и в конечном счете, атака не явилась критической для сети. [12]

В сентябре 2013 года, используя уязвимость Double-spending, была произведена атака интернет-казино BetCoin Dice. Атакующий, делая ставки, отправлял транзакцию без комиссии,

что понижало вероятность их скорого включения в блок, но не мешало распространению данных о самой транзакции в сети. Казино, видя неподтвержденную транзакцию, создавало ответную транзакцию, либо с выигрышем, либо с мелкой суммой означавшей проигрыш. По результатам ответной транзакции злоумышленник определял выигрышные ставки и включал соответствующие транзакции в свой блок. Это произошло за счет наличия у атакующего больших вычислительных мощностей. [13]

В феврале 2014 года была реализована угроза Transaction malleability, которая явилась причиной блокирования вывода с одной из крупнейших бирж MtGox, что повлекло за собой краткосрочную панику и обвал курса на всех основных биржах. Администрация биржи, несмотря на рекомендации сообщества, использовала для обработки выплат программное обеспечение собственной разработки, особенностью которого была автоматическая отправка незавершенных транзакций. В результате этого биржа понесла убытки на сумму в 650 тысяч биткоинов, в последствии чего компания подала заявление на ликвидацию. В то же время, подобная атака была проведена и на другую крупную биржу криптовалют Bitstamp, но в отличии от MtGox, биржа Bitstamp не понесла прямых финансовых потерь.

В июле 2012 года была проведена атака на биржу BTC-E. С помощью компрометации секретного ключа для доступа к API биржи. В результате этого злоумышленник сымитировал пополнение внутренних счетов различных аккаунтов биржи и скупил все имеющиеся на бирже криптовалюты, после чего, произвел их вывод. Результатом данной атаки явилась потеря со стороны биржи суточного объема торгов, что составило около 4500 биткоинов. [14]

В марте 2012 года, в результате взлома облачного хостинга, были похищены резервы биржи Bitcoinica, которые составили более 40 тысяч монет. [15]

Таким образом, рассмотрев некоторые возможные угрозы безопасности криптовалют и осуществленные атаки, с учетом принципов генерации монет и организационно-технических мероприятий, можно сделать вывод, что на практике реализация угроз безопасности криптозащищенных объектов, является достаточно ресурсоемкой и технически сложной задачей и не несет

катастрофических потерь для системы в целом. Большую угрозу представляют атаки связанные с инфраструктурой веб-ресурсов, обрабатывающих данные счетов криптовалют. В настоящее время нет четких требований к безопасности подобных веб-ресурсов. Требуется разработка стандартов безопасности, подобных PSI DSS и проведение регулярного аудита безопасности подобных веб-ресурсов.

Литература

1. http://blog.bitpay.com/
2. http://www.nascar.com/en_us/news-media/articles/2014/5/22/josh-wise-dogecoin-sponsorship-talladega-sprint-fan-vote.html
3. http://doge4water.org/
4. http://ru.wikipedia.org/wiki/Proof-of-work
5. http://en.wikipedia.org/wiki/Proof-of-stake
6. https://bitcoin.org/en/faq
7. https://litecoin.info/Litecoin
8. http://dot-bit.org/FAQ
9. http://ru.wikipedia.org/wiki/Bitcoin
10. http://en.bitcoinwiki.org/Double-spending
11. https://en.bitcoin.it/wiki/Transaction_Malleability
12. http://feathercoin.ru/ataka-51-na-feathercoin/
13. https://forum.bits.media/index.php?/topic/2688-double-spending-i-ghashio/
14. https://btc-e.com/news/81
15. http://status.linode.com/2012/03/manager-security-incident.html

С.А. Фалкина,
Крымский юридический институт (филиал)
Академии Генеральной прокуратуры
Российской федерации,
svetafalkina@mail.ru

ПРОБЛЕМА ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПОДРОСТКОВ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

В статье приводится анализ научных работ, посвященных изучению интернет-угроз. Автор рассматривает склонность к виктимному поведению личности как одну из предпосылок получения вреда в реальной жизни и угрозе психологической безопасности.

Учитывая стремительное развитие информационных технологий, их внедрение во все сферы жизнедеятельности, а также увеличение числа детей и молодежи, для которых интернет-сеть является ведущим институтом социализации, актуальным вопросом становится решение проблемы влияния угроз и рисков Интернета на становление личности подрастающего поколения. Одним из важных условий успешного развития информационного общества является обеспечение информационной безопасности в процессе использования интернет-технологий. Однако на сегодняшний день в интернет-пространстве представлено множество угроз, которые могут наносить вред и оказывать негативное влияние на формирование личности, образцов поведения, установок, социальных норм и ценностей в процессе интернет-социализации подростков и юношей. В связи с эти возникает необходимость рассмотрения проблемы безопасности личности через анализ современных интернет-угроз и оценку их влияния на причинения вреда пользователям интернет-сети.

Проблема безопасности личности рассматривается в нескольких направлениях: психологическая и социальная безопасность как состояние защищенности личности (Прокофьев В.Ф., Еремина О.И., Рассоха Н.Г., Петрушина О.В.); рассмотрение психологической безопасности с точки зрения безопасности (Баева И.А., Дашкова Н.В. Петрушина О.В., Brown S.P., Leigh T.W.,

Edmonson); информационно-психологическая безопасность личности и среды (Грачев Г.В., Смолян Г.Л., Решетина С.Ю., Мельницкая Т.Б.); психофизическая безопасность (Абдурахманов Н. И., Баришлолец В.А., Макилов В.П., Пирумов В.С.). Исследователи в качестве центрального понятия в теории безопасности выделяют понятие «угроза». Г.В. Грачев выделяет внешние и внутренние источники угрозы. И если внешние угрозы находятся в самой среде, то внутренние относятся к личностным характеристикам ребенка [2].

Одними из первых проблемой безопасного поведения в сети Интернет стали заниматься западные ученые. Так, американский исследователь Palfrey John выделяет три группы угроз психологической безопасности детей и подростков в Интернете: нежелательные контакты (которые могут привести к сексуальному насилию); кибербуллинг: оскорбления, агрессивные нападки, преследования в Сети; «опасные» материалы (порнография, видеоролики, изображения и тексты сексуального, экстремистского характера, призывы к насилию) [9]. Федоренко С.В. анализируя негативные влияния информационно-коммуникативных технологий, отмечает, что к ним, прежде всего, относят: 1) потребление суррогатной информации (ужасов, порнографии, коммерческой рекламы, другой информации сомнительного качества), вследствие чего происходит «инфляция» интеллектуально-познавательной деятельности, формируются фрагментарные, бессистемные знания и представления и ошибочные, неадекватные модели мира; 2) «искусственное» общение, которое мало-помалу вытесняет коммуникацию с близкими людьми, друзьями на пользу виртуальных взаимоотношений, вследствие чего у человека формируются искаженные социальные ценности и установки, теряется ориентация на традиции и авторитеты (обесценивается авторитет родины, родителей, власти, закона и т.д.); 3) виртуализация жизненного пространства пользователей Интернета, признание приоритета виртуальной реальности над реальностью повседневной социальной жизни; 4) увлечения виртуальным насилием, жестокими видеоиграми; 5) опасности для психического здоровья: аддиктивный синдром (интернет-зависимость), разрушение социальных связей и социальной активности [7].

В. Плешаков в теории киберсоциализации рассматривает следующие опасности для детей и подростков в Интернете: эксплуатация доверия, доступ к порнографии, сайты с деструктивным содержанием, увлечение жестокими играми, троллинг, кибербуллинг, киберхарасмент [4]. Г. Солдатова выделяет следующую классификацию рисков для детей в Сети: 1) контентные (материалы, которые содержат незаконную, неэтическую, вредную информацию: насилие, эротику, порнографию и т. д.); 2) коммуникативные (кибербуллинг, груминг); 3) потребительские (риск приобретения товара низкого качества, фальсификации, утрата денежных средств); 4) технические (угроза повреждения программного обеспечения, нарушение конфиденциальности, разглашение информации) [6].

Так, исследователями были отмечены общие характеристики, которые создают определенное поле для возникновения проблем утраты психологической безопасности. Украинские ученые Кочарян А.Б., Гущина Н.И. выделяют следующие интернет-угрозы: вирусы; нелегальные и вредные материалы, которые не соответствуют возрастным особенностям и негативно влияют на физическое и психическое здоровье детей (нежелательный контент); кибер-хулиганство (кибер-булинг, кибер-гумлинг, гриферы); получение информации о ребенке и ее семье (фишинг, фарминг); онлайн-хищники; создание профайлов для выявления интересов ребенка; спам; недостоверная информация [2]. Также внешние источники угрозы безопасности личности в Интернете исследованы С.Д. Максименко, С.И. Болтивцом, М.А. Чепой, И.В. Литовченко. Однако программы, построенные по результатам этих исследований, направлены на психологическое просвещение родителей и не учитывают личностные особенности самих детей. Г.Л. Смолян указывает в качестве факторов риска, присущих самому человеку: незрелость личности, выражающаяся в неспособности к самостоятельному осознанному выбору информации, релевантной своим интересам, убеждениям и планам; установки личности на конформизм, подражательство, на готовность к восприятию манипулятивного информационного воздействия; состояния социума, способствующие повышенной внушаемости, массовому заражению идеями [5]. Несмотря на значимость проведенных исследований, исследователями не учитываются отли-

чия виртуальной и реальной среды, а личностная незрелость исследуется в направлении конформности. Британские ученые, во главе с С. Ливингстон, анализируя риски, которые упоминали дети во время исследования «Дети Европы онлайн», указывают на то, что столкновения с риском ни одно и то же, что получение вреда. Риск может принести вред, а может, и нет – это зависит от множества факторов [8].

Таким образом, на данный момент остро стоит вопрос о новых типах и способах взаимодействия между подростками и различными социальными группами, характеризующимися, в том числе, и социально опасными проявлениями. В свою очередь, негативными последствиями могут считаться общение с носителями форм девиантного поведения в Сети, а именно, к которому относится хакерство, нарушение режима секретности, диффамация, кибертерроризм, компьютерная педофилия [1]. При этом сами подростки могут иметь как антисоциальную направленности деятельности в Сети и быть причиной преступных действий, так и сами попадать в статус жертвы преступления. В данном случае подростки, как наиболее уязвимая и восприимчивая возрастная категория, могут неумышленно провоцировать по отношению к себе свершение противоправных действий. Тот факт, что многие люди становятся жертвами преступлений, не является случайным событием, а чаще предопределен наличием определенных личностных особенностей (возрастных, индивидуально-психологических), стереотипов поведения, опытом реагирования в определенных ситуациях, что говорит о викимных склонностях. Определенные приобретенные социальные, физические, психические черты и признаки человека, способствующие дезадаптивному стилю реагирования субъекта, которые делают его предрасположенным оказаться жертвой преступления, называют виктимностью. [3].Так, возрастающее количество научных работ, посвященных разным аспектам проблемы взаимодействия подростков в сети Интернет, указывает на актуальность проблемы. Однако одновременно анализ литературы показал, что множество важных вопросов остаются не раскрытыми. На наш взгляд, необходимым является изучение особенностей виктимного поведения подростков в Интернете как одного из факторов риска нарушения психологической безопасности в интернет-сети.

С целью определения представлений подростков о рисках, с которыми они встречаются в сети Интернет, было проведено эмпирическое исследование. На первом этапе исследования подростки с помощью методики исследования склонности к виктимному поведению (О.О. Андронниковой) были определены в 2 группы: подростки, склонные к виктимному поведению и подростки, не имеющие склонности к виктимному поведению. На рис. 1 представлены результаты представлений интернет-пользователей о рисках, с которыми они сталкиваются в киберпространстве.

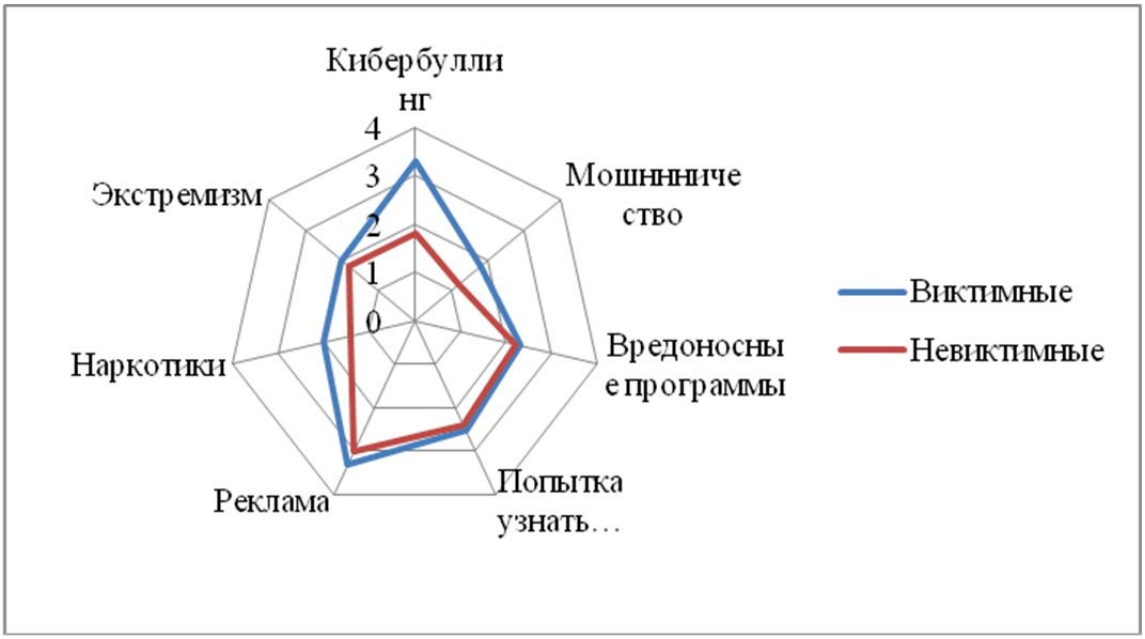

Рис. 1. Оценка рисков в интернет-пространстве

Подростки, имеющие склонность к виктимному поведению, отметили, что наиболее частой и опасной угрозой в Сети является кибербуллинг. При этом подростки второй группы данную угрозу отнесли на 4 место. Данные результаты могут указывать на наличие реализованной виктимности в интернет-пространстве связанной с кибербуллингом (преследования, запугивания, агрессивное поведение, направленное против жертвы с целью унижения ее достоинства). Такие угрозы, как «неэтичная и навязчивая реклама», «попытки посторонних узнать личную информацию», «угрозы вредоносных программ» получили достаточно высокую оценку в обеих группах. Также было отмечено, что виктимные подростки,

на их взгляд, сталкиваются в Интернете с угрозами пропаганды наркотиков и экстремизмом.

Таким образом, исследователи классифицируют различные аспекты негативного влияния использования Интернета: опасности для детей и подростков в Интернете и негативные последствия киберсоциализации, риски в Интернете; риски, связанные с опасным медиасодержанием; риски онлайн-среды для детей; группы негативных факторов, которые влияют на пользователя персонального компьютера; различные направления негативных влияний Интернета на «детей цифровой эпохи»; совокупность социальных рисков, которые вызваны появление Интернета; виды интернет-мошенничества. Однако необходимо учитывать то, что сами подростки, находясь в интернет-пространстве, могут вести себя виктимно, провоцируя по отношению к себе свершение противоправных или преступных действий. В силу определенных социально-психологических аспектов деятельности человека в Интернете (анонимность, физическая непредставленность партнера по общению и т. п.) у пользователей может создаваться ощущение безопасности и отсутствия какой-либо угрозы, что может приводить к реализации в интернет-пространсве виктимных склонностей подрастающего поколения и нести угрозу социально-психологическому благополучию подростков.

Литература

1. Бондаренко С.В. Профилактика девиантного поведения молодежи Дона и Юга России /Л.А. Погосян, С.В. Бондаренко, В.В. Черноус. – Ростов н/Д.: СКНЦ ВШ, 2003. -134с.
2. Виховання культури користувача Інтернету. Безпека у всесвітній мережі. Навчально-методичний посібник / А.Б. Кочарян, Н.І. Гущина. - Київ, 2011. - 100 с.
3. Малкина-Пых И.Г. Психология поведения жертвы. Справочник практического психолога / И.Г. Малкина-Пых. – К.: Издательство «Эксмо», 2006. – 1008 с.
4. Плешаков В. А. Теория киберсоциализации человека / В.А. Плешаков // Монография. Под общ. ред. чл.-корр. РАО,

д.п.н., проф. А.В. Мудрика. – М.: МПГУ; «Homo Cyberus», 2011. – 400 с.

5. Смолян Г.Л. Проблемы обеспечения гарантий безопасности информационного общества / Г.Л. Смолян, А.А. Кононов // Научно-техническая информация, № 8, Сер. 1, 2003. – С. 13–18.

6. Солдатова Г.В. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об интернете/ Г.В. Солдатова, Н.Ю. Зотова, А.И. Чекалина, О.С. Гостимская. – М., 2011. – 176 с.

7. Федоренко С.В. Глобалізація розвитку комп'ютерних технологій: інтернет, досягнення та наслідки / С.Федоренко // Проблеми та перспективи наук в умовах глобалізації: матеріали VI Всеукраїнської наукової конференції. – Ч. ІІ: фізичне виховання, фізика, інформатика, математика, техніка, біологія, хімія. – Тернопіль, 2010. – С. 50–54.

8. Livingstone S. In the own words: what bothers children online? S. Livingstone, L. Kirwil, C. Ponte & E. Staksruud // EU Kids Online, London School of Economies & Political Science, London, UK. – 2013. – Режим доступа: http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx

9. Palfrey John Gasser. Interop: The Promise and the Perils of Highly Interconnected Systems. Basic Books, 2012.

И.К. Гаврилов,
Краснодарский университет МВД России
С.Г. Клюев,
к.т.н., Краснодарский университет МВД России

ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ КАК ЭЛЕМЕНТ ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОЙ ПРИЕМНОЙ ОРГАНА ВНУТРЕННИХ ДЕЛ

Создание электронной приемной органа внутренних дел – одно из перспективных направлений в развитии органов внутренних дел в сфере информатизации и информационно-коммуникационных технологий (ИКТ). Одной из фундаментальных задач при создании электронной приемной органа внутренних дел (ЭП ОВД) является задача обеспечения возможности взаимодействия граждан и бизнеса с органами внутренних дел всех уровней, взаимодействия между государственными органами и учреждениями путем широкого использования ИКТ. Информационное взаимодействие требует построения системы отношений доступа, обеспечивающей гарантированную авторизацию взаимодействующих субъектов и объектов и подтверждение взаимно однозначного адреса устанавливаемого взаимодействия. Это осуществляется с помощью реализации функций идентификации и аутентификации. С одной стороны, это функции назначения систем обеспечения информационной безопасности (СОИБ), реализующие санкционированный доступ к ресурсам. С другой стороны, в рамках электронного правительства это инфраструктурные функции гарантии образования связных процессов (транзакционных инициатив) взаимодействия субъектов, ресурсов (сервисов) и автоматизированных систем, участвующих в реализации государственных или муниципальных заданий (заказов) и исполнении государственных и муниципальных функций (информационно-технологическое взаимодействие). При этом санкционированный доступ должен предоставляться с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие. Для решения задачи идентификации и аутентификации в составе инфраструктуры ЭП ОВД предлагается выде-

лить специальную систему – ГИС «Единая система идентификации и аутентификации в инфраструктуре органов внутренних дел» (далее – ЕСИА ОВД).

К основным функциям ЕСИА ОВД относятся:

обеспечение ведения регистров участников информационного взаимодействия, таких как регистры физических и юридических лиц, регистр государственных организаций, регистры должностных лиц и их полномочий, регистр информационных систем;

обеспечение идентификации и аутентификации участников информационного взаимодействия при их доступе к ресурсам информационных систем;

предоставление информационным системам идентификационных данных (в том числе сведений о полномочиях – в рамках авторизации) участников информационного взаимодействия [1].

Отметим некоторые существенные особенности, связанные с реализацией этих функций.

Идентификационные данные, используемые при реализации функций идентификации, аутентификации и авторизации, являются персональной информацией, накопление, хранение и использование которой должно осуществляться в соответствии с законодательными нормами. Следовательно, системные и технические решения относительно этого специфичного информационного ресурса должны быть сбалансированными и эффективными с позиций правовых норм [2] и операционных характеристик [3].

Масштабируемость системы и интероперабельность процессорных решений по ЕСИА ОВД распространяются как по горизонтали взаимодействия (федеральный, региональный или муниципальный уровни), так и по вертикали (межуровневое взаимодействие). Эту особенность необходимо иметь в виду, несмотря на тот факт, что в настоящее время использование ЕСИА ОВД на федеральном уровне имеет обязательный характер, а на региональном и муниципальном – рекомендательный [1] . Тем не менее идентификационные данные в механизмах реализации в любом случае должны быть совместимыми.

Исходя из рассмотренных предпосылок формировались подходы к выбору решений при разработке ЕСИА ОВД.

При реализации функции обеспечения ведения регистров рассматривалось два возможных подхода:

использовать уже существующие государственные регистры и выполнять к ним запросы из ЕСИА ОВД – практически неприменимый подход, так как существующие регистры органов внутренних дел в настоящий момент не обладают полнотой информации, необходимой для обеспечения идентификации субъекта, зачастую содержат противоречивую информацию о субъекте и не всегда предоставляют уникальные идентификаторы записей регистра для возможности их однозначного сопоставления друг с другом при получении информации из различных регистров;

создать в составе ЕСИА ОВД свои регистры физических лиц, организаций, должностных лиц организаций, информационных систем. Связать эти регистры ЕСИА ОВД с наиболее значимыми существующими государственными регистрами, такими как регистры ФНС (реестры ЕГРЮЛ, ЕГРИП, реестр индивидуальных номеров налогоплательщиков), регистры Пенсионного фонда РФ (реестр страховых номеров индивидуальных лицевых счетов граждан РФ – СНИЛС), регистры ФМС (реестр паспортов граждан РФ).

Был выбран второй подход. Ввод и актуализация информации обеспечиваются субъектами, владеющими наиболее актуальной информацией и мотивированными в поддержании информации о себе в актуальном виде, а именно участниками информационного взаимодействия.

Заинтересованные в использовании сервисов ЭП ОВД лица регистрируют в регистрах ЕСИА ОВД свои учетные записи, учетные записи организаций и их информационных систем. В процессе регистрации вводимые данные подвергаются проверке по существующим государственным регистрам (для исключения возможности создания в ЕСИА ОВД записей о не существующих в реальности субъектах, а также для подтверждения правомочности действий субъектов, которые определены при регистрации ими организаций и информационных систем).

При регистрации в ЕСИА ОВД физических лиц (прежде всего, граждан РФ) используется процедура подтверждения учетной записи, в процессе которой осуществляющее регистрацию лицо подвергается проверке на то, что именно оно является за-

конным владельцем своей учетной записи. В настоящий момент предусмотрено два способа подтверждения учетной записи:

получение кода активации учетной записи лично в руки в центре регистрации (отделения Почты России, центры регистрации ОАО «Ростелеком», иные уполномоченные организации);

подтверждение учетной записи с помощью квалифицированной электронной подписи, установленной с использованием средства электронной подписи, содержащего квалифицированный сертификат ключа проверки подписи, выпущенный аккредитованным удостоверяющим центром.

При регистрации организаций и информационных систем выполняется проверка факта, что записи об этих сущностях регистрируются в ЕСИА ОВД субъектами, имеющими подтвержденные полномочия. Первичные полномочия субъектов на действия от имени организации подтверждаются благодаря проверке прав субъектов через ЕГРЮЛ. Далее ЕСИА предоставляет механизмы присоединения должностных лиц организаций и делегирования им полномочий на действия от имени организаций и принадлежащих организации информационных систем.

При реализации функции обеспечения идентификации и аутентификации участников информационного взаимодействия в ЕСИА ОВД в качестве основы решения по взаимодействию информационных систем и ЕСИА ОВД были выбраны распространенные в мире стандарты и технологии взаимодействия, широко поддержанные производителями прикладного программного обеспечения и программного обеспечения промежуточного уровня. данные стандарты и технологии относятся к области, называемой федеративным управлением идентификационными данными (в зарубежных материалах используется термин Federated Identity Management). Следование этим стандартам и технологиям позволило обеспечить высокую интероперабельность ЕСИА ОВД.

ЕСИА ОВД обеспечивает расширение поддерживаемого ею перечня механизмов аутентификации. В настоящий момент предполагается, что ЕСИА ОВД будет поддерживать возможность аутентификации пользователей с использованием следующих методов:

аутентификация с использованием логина/пароля;

аутентификация с использованием отправляемых по SMS кодов подтверждения (разновидность one-time password аутентификации);

аутентификация с использованием квалифицированной электронной подписи.

Возвращаемый от ЕСИА ОВД в информационную систему набор идентификационных данных определяется зарегистрированными в ЕСИА ОВД настройками информационной системы. Каждой системе доступно только определенное для нее разрешенное подмножество атрибутов. В настоящий момент ЕСИА ОВД обеспечивает ведение более двух десятков атрибутов идентификационных данных пользователя. Набор ведущихся в регистрах ЕСИА ОВД атрибутов со временем расширяется.

Литература

1. Требования к федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». Постановление Правительства РФ от 28 ноября 2011 г. № 977.

2. Закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Положение о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме». Приказ Министерства связи и массовых коммуникаций Российской Федерации от 13 апреля 2012 г. № 107.

4. Методические рекомендации по использованию Единой системы идентификации и аутентификации. URL: http//minsvyaz.ru/Metodicheskie_rekomendatsii_ESIA.pdf (дата обращения: 02.04.2015).

В.В. Поляков,
к.ю.н., Алтайский государственный университет,
vvpagu@rambler.ru,
А.С. Мананников,
Алтайский государственный университет,
manannikovanton35@mail.ru

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

Разработано авторское понятие кибертерроризма. Рассмотрены актуальные проблемы борьбы с кибертерроризмом. Предложены методы противодействия данному явлению оперативно-розыскными силами.

XXI век – век информационных технологий, которые динамично развиваются и способствуют улучшению жизнедеятельности общества. Несмотря на многочисленные преимущества современных компьютерных технологий, они создали новые условия, которые содействуют совершению преступлений на национальном и международном уровнях. [1, с. 114–116]

Высокая компьютерная оснащенность и созданные человеком мощные вычислительные сети, включая глобальную мировую сеть Интернет, породили, с одной стороны, колоссальные возможности для эффективного обладания человечеством фактически неисчерпаемыми информационными ресурсами, а с другой – возник целый спектр новых опасностей и угроз, в том числе и террористического характера». [2, с. 179]

В настоящее время, терроризм перестал существовать только лишь в привычной форме, он перешел в иное глобальное пространство.

В этой связи, появилось такое явление, как информационный терроризм.

В отличие от традиционного этот вид терроризма связан с использованием современных информационно-коммуникационных технологий экстремистскими и террористическими организациями, как в целях организации своей деятельности, так и непосредственно для подготовки и совершения актов терроризма. [3, с. 28]

В научной литературе предлагается определенное понимание информационного терроризма. В частности В.Ю. Осипов и Р.М. Юсупов под информационным терроризмом предлагают понимать вид террористической деятельности, ориентированный на принуждение к реализации политических, экономических, религиозных, идеологических и других целей через деструктивные действия в сфере информации. [4, с. 36]

Д.В. Фатхи в общих чертах определяет информационный терроризм как достаточно хорошо освоенные формы и приемы действий, применяемых для решения довольно широкого круга задач как локального, так и стратегического характера. [5, с. 241]

Понятие «информационный терроризм» являясь обобщающим понятием, включает в себя иные составляющие, среди которых можно выделить «кибертерроризм», который является одним из наиболее опасных видов компьютерной преступности.

Считаем, что для правового регулирования рассматриваемого вопроса необходимо определять кибертерроризм как разновидность преступления предусмотренного ст. 205 УК РФ.

Таким образом, на наш взгляд кибертерроризм – это совершение умышленных действий заключающихся в атаке на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях.

Проявляется кибертерроризм во вмешательстве в работу компонентов телекоммуникационных сетей, функционирующих в их среде компьютерных программ, несанкционированной модификации компьютерных данных, что вызывает дезорганизацию работы критически важных элементов инфраструктуры государства и создает опасность гибели людей, значительного имущественного ущерба или иных общественно опасных последствий. [6, с. 85]

Дальнейшее развитие новых информационных технологий с простотой доступа к ним, относительно низкой их стоимостью и

предоставляемыми ими широкими возможностями открывает для терроризма новые границы, переводя кибертерроризм в разряд серьезных опасных угроз для человечества, сравнимых, по оценкам специалистов, с ядерным, бактериологическим и химическим оружием. При этом степень опасности угрозы кибертерроризма, в силу своей новизны, не до конца еще осознана. Кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. [6, с. 86]

Учитывая серьезную опасность как информационного терроризма в целом, так и кибертерроризма в частности считаем необходимым предложить комплекс мер направленных на предупреждение и противодействие рассматриваемым негативным явлениям.

Необходимо совершенствование уголовно-процессуального законодательства, направленное на создание условий, способствовавших правоохранительным органам оперативно и эффективно действовать в случаях угроз безопасности, осуществляемых с использованием информационно коммуникационных технологий, единообразное оформление доказательств, полученных с использованием компьютерных систем и телекоммуникаций, так как в настоящее время отсутствуют четкие механизмы проведения предварительного расследования и судебного разбирательства по фактам противоправных действий в информационной сфере, связанных с актами кибертерроризма, а также порядок предупреждения и ликвидации последствий этих противоправных действий. Очевидно, что уголовно-процессуальное законодательство изменить в кротчайшие сроки невозможно, а борьбу с кибертерроризмом необходимо вести сейчас. В связи с этим, стоит отметить, что практика показала ведущую роль оперативно-розыскной деятельности (далее – ОРД), способной наиболее эффективно обеспечивать предупреждение информационного и кибертерроризма.

Объективная необходимость ОРД предопределена самим существованием преступности, особенно организованной. Ее роль и социальная значимость обуславливается широкими потенциальными возможностями использования ее результатов в решении различных задач, в т.ч. и задач уголовного судопроизводства [7, с. 13–14].

Осуществление ОРД должно идти в ногу со временем и затрагивать новые области человеческой деятельности. Прежде всего, это касается распространения ее возможностей на сеть Интернет. Борьба с преступностью в телекоммуникационных системах невозможна без применения специальных оперативно-разыскных сил, средств и методов, например снятия информации с технических каналов связи.

Эффективное осуществление оперативно-разыскных мероприятий (далее – ОРМ) в сетевом пространстве невозможно без корректировки методов ОРД. Необходимость модернизации ОРД в данном случае, вызвана уникальностью сетевого пространства, которая заключается в том, что преступления в сети, могут совершаться различными нетипичными способами, в том числе:

– удаленно (когда пользователь с одного компьютера с помощью информационных сетей подключается к другому компьютеру, получая при этом возможность непосредственно воздействовать на содержащуюся в нем компьютерную информацию); [8, с. 7]

– динамически (выполнение действий с помощью мобильных устройств, при перемещении их оператора в физическом пространстве);

– трансгранично (преступное действие выполняется в одном государстве, общественно опасные последствия наступают в другом, при этом физического пересечения преступником границ государства не происходит). [9, с. 25];

Для обеспечения информационной безопасности и предупреждения преступлений в сфере высоких информационных технологий оперативным сотрудникам целесообразно в рамках реализации гл. IV ФЗ об ОРД привлекать граждан к содействию ОРД. При этом стоит отметить, что особенности сетевого пространства предполагают специфичные формы привлечения граждан к содействию ОРД. Так, например, используя сеть Интернет, граждане могут заполнять на соответствующих сайтах формы сообщений о совершенных или готовящихся преступлениях, о потенциальных преступниках, их связях и т.п. Полагаем, что повысить эффективность ОРД в рассматриваемом направлении может проведение опроса в электронной форме. Из тактических соображений предпочтение стоит отдавать легендированной форме

опроса, при которой оперативник скрывает свои истинные цели и профессиональную принадлежность. При осуществлении указанных ОРМ возможно выявление лиц, готовых оказывать содействие оперативно-разыскным органам (далее – ОРО) на конфиденциальной основе. При наличии признаков достаточной осведомленности таких лиц важным становится укрепление доверительных отношений с ними и выход на непосредственное общение. Привлечение граждан к содействию ОРО позволяет не только получать достоверную информацию о состоянии оперативной обстановки на контролируемых сетевых объектах, но и изучать способы совершения и сокрытия следов сетевых компьютерных преступлений, ранее не встречавшихся в следственной и оперативно-разыскной практике. [10, с. 335]

Представляется, что в рамках оперативно-разыскной деятельности положительную роль сыграло бы внедрение ресурса «honeypot», нацеленного на выявление криминальной активности в сети Интернет. Его суть сводится к установке в телекоммуникационной сети своеобразной ловушки, приманкой в которой служит возможность относительно простым способом взломать чужой сервер или сетевой сервис. Профессиональные преступники, используя свои знания и криминальный опыт, собственные программные средства и уникальные способы совершения неправомерного доступа к компьютерной информации, взломав защиту такого сервера, оставили бы следы, которые бы выявлялись и фиксировались специальным, заранее установленным на сервер программным обеспечением. В результате использования «honeypot» у ОРО появилась бы возможность собирать ценный эмпирический материал о преступниках, конкретных преступлениях, способах и средствах их совершения, физических и виртуальных местах их нахождения, а также потенциальных жертвах преступных посягательств. Использование «honeypot» наиболее эффективно было бы при осуществлении оперативного эксперимента, контроля сообщений и снятия информации с технических каналов связи. [11, с. 102].

Помимо осуществления ОРМ и внедрения ресурса «honeypot» необходимо использование и иных методов противодействия информационному и кибертерроризму.

Предложенные методы исследования и противодействия информационного терроризма и кибертерроризма поспособствуют их предупреждению, и обеспечению информационной безопасности Российской Федерации.

Литература

1. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2.
2. Сидоренко А.Г., Тихомиров Ю.В. Терроризм и антитеррористическая безопасность в контексте истории и современной геополитики. – М.: Кучково поле. 2011.
3. Клементьев А.С. Организационно-правовые аспекты противодействию терроризму в информационной сфере // Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2010. № 1 (14).
4. Осипов В.Ю., Юсупов Р.М. Информационный вандализм, криминал и терроризм как современный угрозы обществу // Труды СПИИРАН. 2009. № 8.
5. Фатхи Д.В. Информационный терроризм как новая форма терроризма // Известия южного федерального университета. Технические науки. 2007. № 2 (74).
6. Медов М.У. Кибертерроризм: новая угроза // Научный портал МВД России. 2014. № 3 (27).
7. Маркушин А.Г. Оперативно-розыскная деятельность. М.: Изд-во Юрайт, 2013.
8. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. ... канд. юрид. наук. Омск, 2008.
9. Мананников А.С. Оперативно-розыскная деятельность в сети интернет как средство правового обеспечения информационной безопасности и предупреждения компьютерных преступлений // Проблемы правовой и технической защиты информации – 2014 / Материалы междисциплинарной межвузовской конференции студентов, магистрантов и аспирантов. – Барнаул. 2014.

10. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. М.: Изд-во ИНФРА-М. 2014.

11. Поляков В.В., Мананников А.С. Оперативно-разыскная деятельность в сети Интернет как средство предупреждения компьютерных преступлений // Алтайский юридический вестник. 2014. № 8.

А.В. Ширяев,
Алтайский государственный университет,
mr.toni.soprano@mail.ru
В.В. Поляков,
научный руководитель, к.ю.н.,
Алтайский государственный университет,
vvpagu@rambler.ru

ОБЪЕКТ И ПРЕДМЕТ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Проанализированы объект и предмет неправомерного доступа к компьютерной информации. Рассмотрены понятия информации, компьютерной информации, ее значение в современном мире.

Компьютерная информация в современном мире стала одним из предметов преступного посягательства[1]. целью подобных действий нередко является неправомерный доступ к интересующей преступников компьютерной информации. Федеральный закон «Об информатизации, информации и защите информации» определяет информацию, как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы представления[2]. Из приведенной нормы закона видно, что законода-

[1] Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний / С.В. Воронцова // Российская юстиция / Адм. Президента Рос. Федерации. – М., 2011. – № 2. – С. 14–15.

[2] Иванова И.Г. Выявление и расследование неправомерного доступа к компьютерной информации: автореф. дис. на соиск. учен.степ. канд. юрид. наук / Иванова Инна Геннадьевна. – Красноярск; Барнаул: БЮИ МВД России, 2007. – 22 с.

тель не сформулировал понятия компьютерной информации, но при этом привел несколько отправных точек и определений, которые могут позволить определиться с понятием компьютерной информации[1]. Если связать компьютерную информацию со средствами хранения и передачи, можно утверждать, что компьютерная информация – это информация, которая передается, обрабатывается, хранится с использованием ЭВМ[2]. Представляется удачным определение, сформулированное В.В. Крыловым, который обозначает ее, как «сведения, знания, набор команд, программ, предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях,- идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования[3].

Исходя из приведенных определений можно выделить следующие особенности компьютерной информации:

- объемность и быстрота обработки данной информации;
- легкость и быстрота уничтожения;
- обезличенность, т.е. между ней и лицом, которому она принадлежит, нет жесткой связи[4].

Традиционно классификация преступлений начинается с анализа объекта и предмета преступного посягательства. По мнению Н.Г. Кадникова, благодаря этому возможно установить сходство или различие между совершенным деянием и юридической моделью, а также между смежными деяниями, внешне не похожими по ряду признаков[5]. Отталкиваясь от определения Н.Г. Кадникова, рассмотрим объект наиболее распространенного

---

[1] Стельмах А.П. Кибернетическая безопасность: понятие и сущность феномена/ А.П. Стельмах, А.В. Тонконогов // Социально-гуманитарные знания: научно-образовательное издание / учредитель: М-во образования и науки РФ, ред. журн. – М., 2013. – № 2. – С. 103–115.

[2] Крылов В.В. Информационные компьютерные преступления: [квалификация, методика расследования, основные нормативные акты]: учеб. ипракт. Пособие / В.В. Крылов. – М.: Изд. группа ИНФРА-М – НОРМА, 1997. – 276 с.

[3] Мандиа К. Защита от вторжений: расследование компьютерных преступлений: [пер. с англ.] / Кевин Мандиа, Крис Просис. – М.: Лори, 2005. – 476 с.

[4] Салтевский М. В. Проблемы противодействия преступности в сфере компьютерных технологий: науч.-практ. изд. / М. В. Салтевский, А. Н. Литвинов, Н. Г. Чернец. – М.: Юркнига, 2006. – 96 с.

[5] Крылов В.В. Информационные компьютерные преступления: [квалификация, методика расследования, основные нормативные акты] : учеб. и практ. пособие / В.В. Крылов. – М.: Изд. группа ИНФРА-М – НОРМА, 1997. – 276 с.

вида киберпреступлений – неправомерного доступа к компьютерной информации.

Родовым объектом неправомерного доступа к охраняемой законом компьютерной информации является совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка. Именно поэтому рассматриваемый вид преступлений находится в разделе «Преступления против общественной безопасности и общественного порядка» УК РФ[1]. Одним из квалификационных критериев объединения компьютерных преступлений в единую главу является видовой объект посягательства, который составляет совокупность общественных отношений в части правомерного и безопасного использования компьютерной информации и информационных ресурсов. Непосредственным объектом анализируемого преступления являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ или их сети. Дополнительный объект неправомерного доступа к компьютерной информации факультативен и его наличие будет зависеть от того вреда, который был причинен правам и законным интересам личности, общества, государства. В качестве дополнительного объекта в данном случае может, например, выступать собственность, авторское право, право на неприкосновенность частной жизни, экологическая безопасность и т. д. Наличие дополнительного объекта повышает степень общественной опасности преступного деяния и подлежит обязательному учету при назначении наказания виновному[2].

Объект посягательства является необходимым элементом любого общественно опасного и противоправного деяния. По мнению некоторых исследователей, если в процессе расследования неправомерного доступа к компьютерной информации будет установлено, что действия лица не причинили и не создали реальной угрозы причинения вреда личности, обществу или госу-

---

[1] «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 04.08.2014) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

[2] Герке М. Понимание киберпреступности – явление, задачи и законодательный ответ [Электронный ресурс]. – Режим доступа: www.itu.int/ITUD/cyb/cybersecurity/legislation.html Заглавие с экрана. – (Дата обращения: 18.05.2015).

дарству, то состав преступления отсутствует, так как в данном случае отсутствует объект преступного посягательства[1]. Представляется, что правильнее в данном случае было бы также иметь ввиду наличие умысла на совершение преступления, поскольку не всегда не наступление вреда личности, обществу или государству происходит по причине, зависящей от преступника. Иногда лицо осознает, допускает и желает наступление общественно опасных последствий или относится к этому безразлично, что указывает на покушение или приготовление к преступлению.

По вопросу предмета неправомерного доступа к компьютерной информации у ученых имеются различные точки зрения. Многие авторы под предметом неправомерного доступа к компьютерной информации понимают саму компьютерную информацию, информационные ресурсы, которые являются нематериальными ценностями, на которые непосредственно оказывает воздействие киберпреступник, осуществляя преступное посягательство на общественные отношения по обеспечению безопасности такой информации и нормальной работы ЭВМ, системы ЭВМ или их сети[2]. Правильнее говорить не о любой компьютерной информации, а только об охраняемой законом, так как несанкционированный доступ к общедоступным данным не причиняет вреда их владельцу и поэтому, согласно ст. 272 УК РФ, не является преступным.

Предмет преступного посягательства является отличительным признаком общественно опасных и противоправных деяний. Знание предмета компьютерных преступлений позволяет отграничить данные преступления от других, имеющих сходство с компьютерными, например, когда происходит кража компьютера или видео-перехват компьютерной информации[3]. Так, некоторыми авторами предлагалось в предмет, рассматриваемой группы преступлений, относить компьютер, как информационную систе-

---

[1] Салтевский М.В. Проблемы противодействия преступности в сфере компьютерных технологий: науч.-практ. изд. / М.В. Салтевский, А.Н. Литвинов, Н.Г. Чернец. – М.: Юркнига, 2006. – 96 с.

[2] Федотов Н.Н. Форензика – компьютерная криминалистика. – М.: Юридический Мир, 2007. – 360 с.

[3] Россия и вызовы цифровой среды: рабочая тетр. / [В.С. Овчинский и др.]; [гл. ред. И.С. Иванов]; Российский совет по междунар. делам (РСМД). – М.: Спец-книга, 2014. – 40 с.

му, носитель информации[1]. Вряд ли такую позицию можно признать справедливой, поскольку она не соответствует букве закона и существенно расширяет пределы уголовной ответственности за неправомерный доступ к компьютерной информации. Полагаем, что общественно опасные и противоправные посягательства, имеющие своим предметом не компьютерную информацию, а электронно - вычислительную технику, объединяются в совершенно другую группу преступлений, нарушающую охраняемые законом отношения собственности. Объясняется это тем, что электронно - вычислительная техника является материальным предметом внешнего мира, имеет материальную ценность, стоимость, представляет собой движимую вещь, являющуюся чужой, то есть не принадлежащей виновному лицу и, следовательно, соответствует всем необходимым признакам, характеризующим предмет преступлений, направленных против собственности (глава 21 Особенной части УК РФ)[2].

Таким образом, общественно опасные и противоправные посягательства, имеющие своим предметом компьютерную информацию, а родовым объектом неправомерного доступа к охраняемой законом компьютерной информации - совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка, являются преступлениями в сфере высоких технологий.

Литература

1. Иванова И.Г. Выявление и расследование неправомерного доступа к компьютерной информации: автореф. дис. на соиск. учен. степ. канд. юрид. наук/ Иванова Инна Геннадьевна. – Красноярск; Барнаул: БЮИ МВД России, 2007. – 22 с.

2. Крылов В.В. Информационные компьютерные преступления: [квалификация, методика расследования, основные норма-

[1] Расследование неправомерного доступа к компьютерной информации: Учеб. пособие / [Ю.В. Гаврилин, А.В. Пушкин, Е.А. Соцков, Н.Г. Шурухнов]; под ред. Н.Г. Шурухнова; Моск. ун-т МВД России. – 2-е изд., перераб. и доп. – М.: Щит-М, 2004. – 351 с.

[2] «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 04.08.2014) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

тивные акты] : учеб. ипракт. пособие/ В. В. Крылов. - М.: Изд. группа ИНФРА-М - НОРМА, 1997. – 276 с.

3. Мандиа К. Защита от вторжений: расследование компьютерных преступлений: [пер. с англ.] / Кевин Мандиа, Крис Просис. - М.: Лори, 2005. – 476 с.

4. Салтевский М.В. Проблемы противодействия преступности в сфере компьютерных технологий: науч.-практ. изд./ М.В. Салтевский, А.Н. Литвинов, Н. Г. Чернец. - М.: Юркнига, 2006. – 96 с.

5. Расследование неправомерного доступа к компьютерной информации: Учеб. пособие / [Ю.В. Гаврилин, А.В. Пушкин, Е.А. Соцков, Н.Г. Шурухнов]; Под ред. Н.Г. Шурухнова; Моск. ун-т МВД России. – 2-е изд., перераб. и доп. – М.: Щит-М, 2004. – 351 с.

6. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 21.07.2014) (с изм. и доп., вступ. в силу с 04.08.2014) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

7. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний / С.В. Воронцова // Российская юстиция / Адм. Президента Рос. Федерации. – М., 2011. – №2. – С. 14–15.

8. Герке М. Понимание киберпреступности – явление, задачи и законодательный ответ[Электронный ресурс]. – Режим доступа: www.itu.int/ITUD/cyb/cybersecurity/legislation.html Заглавие с экрана. – (Дата обращения: 18.05.2015).

9. Россия и вызовы цифровой среды: рабочая тетр. / [В.С. Овчинский и др.]; [гл. ред. И.С. Иванов]; Российский совет по междунар. делам (РСМД). – М.: Спец-книга, 2014. – 40 с.

10. Стельмах А.П. Кибернетическая безопасность: понятие и сущность феномена / А.П. Стельмах, А.В. Тонконогов // Социально-гуманитарные знания: научно-образовательное издание/ учредитель: М-во образования и науки РФ, ред. журн. – М., 2013. – № 2. – С. 103–115.

11. Федотов Н.Н. Форензика – компьютерная криминалистика. – М.: Юридический Мир, 2007.– 360 с.

К.Н. Горюн,
Краснодарский университет МВД России
С.Г. Клюев,
к.т.н., Краснодарский университет МВД России

СОЦИАЛЬНЫЕ СЕТИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Развитие человечества не стоит на месте. Разрабатываются и создаются новые товары и новые технологии, чтобы облегчить и упростить нашу жизнь, особенно если это общения.

С развитием сети Интернет появилось множество вариантов решения любых задач в любых сферах деятельности, это не только удобный способ получения информации, но и важный инструмент для общения. Так, стали появляться различные средства социальных сервисов Интернета, начиная с привычной для нас электронной почты и заканчивая социальными сетями, форумами и блогами.

В мире современных технологий наиболее успешно развиваются социальные сети, направленные на построение в Интернете сообществ людей со схожими интересами, деятельностью, взглядами на те или иные события. Поэтому, как и любой другой ресурс сети Интернет, социальные сети имеют не только достоинства, но и недостатки, которые влияют как на отдельных лиц, так и на общество в целом.

На сегодняшний день в России порталы социальных сетей содержат персональные данные миллионов пользователей, тем самым обеспечивая возможность разнообразного общения между участниками и поиска друг друга на портале и представляя собой огромные онлайн-директории, которые при желании доступны каждому.

Таким образом, возникает ряд вопросов, касающихся обеспечения информационной безопасности (ИБ) данных ресурсов и правового регулирования отношений в области соблюдения законодательства РФ.

Важнейшая задача в деле обеспечения информационной безопасности России – осуществление комплексного учета инте-

ресов личности, общества и государства в данной сфере. Доктрина ИБ РФ эти интересы определяет следующим образом:

интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность;

интересы общества в информационной сфере заключаются в обеспечении интересов общества в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России;

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека (гражданина) в области получения информации. Одновременно требуется использование этой сферы только в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, безусловного обеспечения законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества.

Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование различных форм общественного контроля над деятельностью федеральных органов государственной власти и органов государственной власти.

Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности [1].

Данная иерархия затрагивает различные сферы деятельности сотрудника органов внутренних дел, в том числе его пребывание в социальных сетях, так как для многих людей это стало

незаменимым источником общения, новостей, развлечения, отдыха.

Также следует отметить, что каждая ступень иерархии «человек – организация – государство» может так или иначе воздействовать на всю цепочку в целом и являться мощным рычагом как для манипулирования конкретными людьми, так и для разжигания скандалов национального характера. В данной статье рассмотрена «золотая середина» вышеизложенной иерархии, а именно использование социальных сетей в органах внутренних дел со стандартной архитектурой сети и системными характеристиками при использовании сервисов социальных сетей.

Как показывает статистика компании ЗАО «Лаборатория Касперского» [2], с каждым годом растет количество фишинговых атак и спама именно в социальных сетях, которые пока остаются бесспорным лидером среди общеизвестных источников коммуникации. Поэтому руководителям органов внутренних дел стоит задуматься о защите данных, а также об осведомленности сотрудников о безопасной работе в социальных сетях и о внедрении и усилении мер обеспечения защиты информации в плане предотвращения ее утечки, защиты репутации, сохранения всех видов информации ограниченного доступа.

Повышенный интерес к сервису социальных сетей находит отражение в деятельности ОВД и имеет двойственную природу. С одной стороны, чаще всего в ОВД очень строго относятся к работе сотрудников, простоям и потере репутации из-за некачественного выполнения ими своих обязанностей, результатом чего является блокировка выхода на развлекательные сайты, с том числе сайты данной категории. Такой запрет использования социальных сетей на рабочем месте, в свою очередь, приводит к тому, что сотрудники прибегают к помощи непроверенных продуктов, скачанных на мошеннических сайтах, переходят по непроверенным ссылкам, тем самым увеличивая риск потери данных. С другой стороны, возможность получения более подробной и систематизированной оперативной информации о сотрудниках, гражданах и организациях растет по мере расширения использования социальных сетей. Следует отметить, что подобные сервисы широко применяются продвинутыми сотрудниками для поис-

ка необходимых контактов и выхода на нужных людей, минуя бюрократический аппарат и социальные барьеры.

Несмотря на вышеописанные проблемы, большинство органов внутренних дел не задумывается о потенциальной возможности утечки информации посредством социальных сетей, а обращает внимание на потерю рабочего времени сотрудниками и снижение производительности, что также является заблуждением. Существует немало других факторов, которые снижают производительность работы сотрудников, например, сотрудник зашел в соседний отдел и заговорился с коллегами, пропустив важный звонок, вследствие чего было упущено оперативное превосходство, в то время как он мог обсудить тот же вопрос в сети, онлайн, находясь на своем рабочем месте рядом с телефоном.

Можно выделить некоторое количество потенциальных угроз, связанных с возможными потерями для ОВД. Предотвращение данных угроз является неотъемлемой частью общих стратегий построения систем управления информационной безопасностью, таких как политика информационной безопасности ОВД, анализ и оценка рисков информационной безопасности, поэтому для защиты от утечки данных стоит рассматривать такие угрозы наряду с другими актуальными угрозами ИБ.

Самый простой пример угрозы утечки данных: сотрудник, пользуясь социальной сетью, меняет статус, который каким-то образом компрометирует организацию, например, раскрывает конфиденциальную информацию, которая еще не была допущена в средства массовой информации или рассылку. Подобного рода действия могут носить как случайный, так и умышленный характер. Ярким примером причины умышленного действия могут служить массовые забастовки, сокращения, когда недовольство некоторой группы людей может вызвать массовые рассылки различной информации, грозящей репутации ОВД посредством клеветы. Стоит отметить, что владельцы социальной сети не несут ответственности за персональные данные пользователя, а также за распространение и удаление размещенной информации, что указано в пользовательском соглашении. Соответственно, действие Федерального закона «О персональных данных» не распространяется на нее. Поэтому следует четко понимать, что вся ответственность лежит на пользователях интернет-ресурса.

Другой непредсказуемой угрозой ИБ ОВД является собранная инсайдером совокупность данных о конкретном пользователе (человеке) с нескольких ресурсов с целью построения полного портрета: образование, карьера, интересы, семья, личные данные и другое. При этом подопытный становится персонализированной целью злонамеренных действий, в то время как для работодателя возрастает риск целевых атак. Хорошим примером является использование злоумышленником социальной инженерии.

Еще один яркий пример – это халатное использование социальных сетей большинством пользователей. Ведь люди сами добровольно выкладывают информацию о себе, об учреждениях, в которых они работают, что чаще вредно сказывается на самих пользователях. Например, социальные сети могут легко использоваться руководством для проверки сотрудников, при этом профиль пользователя может сыграть как положительную, так и отрицательную роль.

Но самой актуальной угрозой использования социальных сетей была и остается возможность заражения вирусами. Большинство рассматриваемых сервисов используют огромное количество приложений и дополнительных ресурсов для привлечения и заинтересованности участников – музыка, видео, фотографии, изображения, что требует от пользователя установки дополнительного ПО или плагина для ПО. Тем самым под видом безобидного приложения скачивается вирус, троянская программа, шпион или делается переадресация на идентичный сервис с целью выявления аутентификационной информации.

Для обеспечения ИБ ОВД основными мерами защиты от утечки данных являются организационные меры, начинающиеся с построения системы управления ИБ, анализа и оценки рисков, выявления наиболее ценной информации и активов, с последующим моделированием убытков, вызванных утечкой информации, а также выявлением и разработкой оптимальных мер по защите. Существует ряд таких мер, например инженерно-технические меры защиты – комплексные средства мониторинга, анализа и фильтрации входящего и исходящего трафика на уровне шлюзов, а также средства анализа поведения приложений и сетевых коммуникаций. Или организационные меры – управление доступом к потенциально опасной среде, то есть диверсифицированные по-

литики «белых списков» и фильтрации контента для различных групп пользователей [3]. Еще одним важным аспектом является работа с человеческим фактором в направлении усиления рабочей дисциплины, корпоративной этики, а также донесение до сотрудников понимания, что политики ИБ служат не для вторжения в их частную жизнь и ущемления достоинств или прав, а являются мерой предотвращения потерь и утечки данных компании, особенно если речь идет об информации ограниченного доступа. Следует проводить такие мероприятия, как тренинги и обучение персонала, в том числе риторика и деловое общение, что демонстрирует заинтересованность работодателя в повышении мер защиты информации.

Стоит еще раз отметить, что проблемы утечки информации грозят репутации ОВД. Неважно, каким образом ОВД решает взаимодействовать с таким явлением, как социальная сеть, важно, чтобы была разработана стратегия решения проблем утечки данных и политика ИБ ОВД.

Литература

1. Доктрина информационной безопасности Российской Федерации.

2. Аналитика фишинговых атак. URL: http://www.securelist.com/ru/analysis (дата обращения: 23.01.2015).

3. Журнал «Information Security/ Информационная безопасность». URL: http://www.itsec.ru (дата обращения: 02.02.2015).

4. Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д. А. Новикова. М.: Издательство физико-математической литературы, 2010. – 228 с.

А.А. Селина,
ФГБОУ ВПО «Алтайский государственный университет»,
annet_the_best@mail.ru

КИБЕРТЕРРОРИЗМ: МЕЖДУНАРОДНО-ПРАВОВОЙ ДИСКУРС

В статье раскрывается понятие «кибертерроризма», его виды, а также рассматриваются актуальные проблемы международного сотрудничества в противодействии киберпреступности, предлагаются пути их решения.

Сегодня интернет широко используется не только обычными гражданами, но различными террористическими и экстремистскими организациями и играет большую роль в их деятельности, которая не ограничивается лишь пропагандистской и разъяснительной работой, публикацией материалов определенной направленности и др.

Глобализация информационных процессов вызвала ряд качественно новых глобальных угроз, в том числе уязвимость мирового сообщества перед преступными посягательствами в сфере информационной безопасности. Посредством интернет-ресурсов осуществляется привлечение к подобной деятельности, вербовка новых членов, сбор финансовых средств, планирование и координация совместных действий.

Не вызывает сомнения, что компьютерные преступления во всем мире имеют устойчивую тенденцию к росту, поскольку растет и аудитория пользователей высокими технологиями и Интернет-ресурсами. Ключевым положением борьбы с кибертерроризмом является интеграция правовых систем различных стран (например, сближение уголовного законодательства стран Евросоюза). На первый план, по сравнению с национальным законодательством, выходят инструменты межгосударственного (международного) регулирования, поскольку данная проблема не носит, как правило, каких-либо географических или политических границ.

Кибертерроризм также в полной мере можно отнести к так называемым технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористиче-

ских акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии.[1]

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением к традиционному виду терроризма. Исследователи выделяют два вида кибертерроризма: совершение с помощью компьютеров и компьютерных сетей террористических действий (условно назвав это терроризмом в «чистом виде»), а также использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов. Первому виду кибертерроризма можно дать определение с помощью соединения понятий «киберпространство» и «террористический акт». «Террористический акт (205 УК РФ) - совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях».[2] Таким образом, кибертерроризм «в чистом виде» определяется как умышленная атака на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Это деяние должно быть совершено в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти. К этому виду терроризма можно отнести также угрозу совершения подобных действий для достижения вышеуказанных целей.[3]

В свою очередь результаты анализа поступающей в Антитеррористический центр государств-участников СНГ информации позволяют сделать вывод об активизации попыток использования террористическими организациями для достижения своих

преступных целей возможностей глобальной сети Интернет и о возрастании потенциальной опасности совершения актов так называемого кибертерроризма .

В последние годы активно прорабатываются вопросы совершенствования нормативной правовой базы стран СНГ в данном направлении. Так, Указ Президента России «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» запрещает государственным органам пользоваться Интернетом без средств защиты и регламентирует, какие специальные службы должны за это отвечать. Указ направлен главным образом на обеспечение защиты российского сегмента сети Интернет, в первую очередь - сетевых ресурсов государственных органов, от внешних угроз несанкционированного воздействия. При этом речь идет, в первую очередь, о предотвращении возможных попыток компьютерного «взлома» и получения контроля над сетевыми ресурсами органов власти России с террористическим умыслом. [4]

При этом речь идет не столько о включении международных актов в национальное законодательство путем их ратификации, сколько о добровольном и рациональном учете рекомендаций международных (межправительственных) организаций (ЕС, ООН, АТР и др.) и опыта развития специального законодательства в других странах.

Для совершенствования российского законодательства это особенно важно, поскольку объективную проблему представляет новизна сферы правового регулирования, отсутствие устоявшейся теоретической основы, что прежде всего сказывается на понятийном аппарате по рассматриваемому вопросу.

Между тем, мировым сообществом в данное время наработан определенный положительный опыт борьбы с кибертерроризмом. На международном и межгосударственном уровне принят ряд нормативных правовых актов, регламентирующих данную проблему.

Так, Генеральной Ассамблеей ООН в резолюции 53/70 от 4 декабря 1998 года были затронуты вопросы целесообразности разработки общепринятых международных принципов организации противодействия кибертерроризму, предусматривающих

усиление безопасности глобальных информационных и телекоммуникационных систем и борьбу с информационным терроризмом и преступностью.

Значительным шагом в формировании международной правовой базы в данном направлении стало подписание 23 ноября 2001 года представителями стран - членов Совета Европы, США, Канады и Японии Конвенции Совета Европы «О киберпреступности». Она определяет приблизительный перечень преступлений, совершенных в информационной сфере, против информационных ресурсов или с помощью информационных средств и признает их киберпреступлениями. На сегодняшний день Конвенция подписана 43 членами ЕС и 15 другими странами, включая США. Российская Федерация не вошла в число государств, подписавших Конвенцию, поскольку считает один из пунктов возможностью вмешательства в собственный суверенитет: «Сторона может без согласия другой Стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему».[5]

В настоящее время это единственный международный акт, содержащий закрепление основ по защите прав человека в киберпространстве. Россия, по всей видимости, пока не готова к полноценному сотрудничеству в данном направлении с зарубежными партнерами. При этом следует отметить, что мировое сообщество также еще находиться в процессе выработки единой политики в указанном вопросе, о чем свидетельствует непрекращающаяся работа представителей различных государств в борьбе с киберпреступностью.

Россией также была разработана концепция Конвенции об обеспечении международной информационной безопасности 2011 г., которая предполагает полное сохранение государственных суверенитетов и границ национального регулирования в виртуальном пространстве.

Резюмируя изложенное необходимо подчеркнуть, киберпреступность представляет собой глобальную проблему, для решения которой необходима международная координация усилий.

Наиболее эффективный способ борьбы с компьютерными преступлениями сегодня - объединение опыта на международном уровне, как правоохранительных органов, так и компаний, специализирующихся в области информационной безопасности, и их активное тесное сотрудничество. Государствам необходимо активно налаживать контакты друг с другом по всем основным вопросам киберугроз. Даже если пока не говорить о глобальном соглашении по сотрудничеству в сфере информационной безопасности, широкие двусторонние контакты в любом случае будут способствовать формированию устойчивого и безопасного информационного пространства.

В настоящее время в совершенствование международной стратегии борьбы с киберпреступностью ведут более сорока стран мира. Из этого следует, что международному сообществу необходимо прийти к решению проблем унификации законодательства. В противном случае, с учетом трансграничности киберпреступности, определенные несоответствия в законодательстве и несогласованность уголовной политики позволят лицам, совершившим общественно опасные действия, уйти от ответственности.

Литература

1. Петрищев В.Е Заметки о терроризме / В.Е. Петрищев – М.: Эдиториал УРСС. 2001. 288 с.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.03.2015) // Собрание законодательства РФ. 17.06.1996. № 25. ст. 2954.
3. Голубев В. Электронный терроризм проблемы противодействия / В. Голубев // Компьютерная преступность и кибертерроризм. Исследования, аналитика. Вып. 2. Запорожье. 2004. С. 13–17.
4. О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена: Указ Президента России от 17. 03. 2008 г. № 351 (ред. от 25.07.2014) // Собрание законодательства РФ. № 43. 27.10.2008.
5. Конвенция о преступности в сфере компьютерной информации (ETS № 185) Будапеште 23.11.2001 ред. от 28.01.2003 http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

К.А. Журтов,
Краснодарский университет МВД России
С.Г. Клюев,
к.т.н., Краснодарский университет МВД России

О РЕПУТАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ВСЛЕДСТВИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные технологии претерпевают стремительное развитие на протяжении последних десятилетий и предоставляют все больше возможностей, связанных с их использованием. Органы внутренних дел (ОВД), а также их сотрудники имеют неограниченный доступ в сеть Интернет – если не из сети ОВД, то из дома или с личного мобильного устройства. Соответственно, в сети Интернет обрабатывается колоссальное количество информации, которая попадает туда нередко вследствие нарушений информационной безопасности. В настоящее время ОВД уделяют недостаточно внимания учету рисков потери репутации вследствие инцидентов информационной безопасности.

Под термином «информационная безопасность» довольно часто понимается защита информации с использованием программных, аппаратных и программно-аппаратных решений. Но не менее важно учитывать вероятность возникновения событий иного характера, от которых трудно предотвратить, используя только технические средства защиты, такими событиями могут быть:

публикация в интернет-блоге о внутренних проблемах ОВД;

размещение на официальном сайте ОВД посторонней информации.

Все подобные ситуации объединяет фактор влияния общественного мнения. Злоумышленники применяют ряд способов воздействия на репутацию ОВД, основным из которых являются несанкционированные операции с информационными активами ОВД, в том числе нарушение конфиденциальности, целостности и доступности защищаемой информации.

Зачастую в ОВД отсутствуют регламентированные мероприятия по управлению основными видами взаимоотношений в

части обеспечения информационной безопасности. Под основными видами взаимоотношений понимаются взаимоотношения с сотрудниками, с общественностью, с государственными органами, с организациями. Виды взаимоотношений характерны не для каждой организации, но взаимоотношения с сотрудниками и с общественностью присутствуют всегда.

Взаимоотношения с сотрудниками – это основной вид взаимоотношений, который присутствует в любом ОВД. Опасность наличия внутреннего нарушителя (инсайдера) крайне велика, поскольку полноценной защиты от его деятельности в настоящее время не существует. Понимание сотрудниками необходимости обеспечения информационной безопасности в большинстве случаев отсутствует, что приводит к неумышленным действиям сотрудника, допускающим утечку важной для ОВД информации. Невозможно запретить сотруднику действовать «не по инструкции», распространять противоречивые, ложные сведения о своей деятельности или деятельности организации, а также соответствующие действительности сведения о проблемах в ОВД среди знакомых, в сети Интернет и т. д. Потеря репутации ОВД из-за взаимоотношений с работниками может возникать в результате следующих инцидентов информационной безопасности:

разглашение работником важной информации организации внутри коллектива. К этому может привести недостаточное понимание сотрудниками важности соблюдения правил информационной безопасности, пренебрежение политикой информационной безопасности ОВД. Рассматриваемый инцидент может спровоцировать ухудшение внутренних взаимоотношений в коллективе, разлад, уход ценных сотрудников (что влечет за собой издержки по нахождению новых квалифицированных кадров).

заявление работника в уполномоченные органы о нарушении ОВД трудового или иного законодательства, что провоцирует проверки с их стороны. В результате ОВД теряет свой статус добросовестного работодателя, что отталкивает потенциальных кандидатов от вступления в трудовые правоотношения с ним.

распространение работником информации о недостаточно хороших условиях труда в ОВД в своей профессиональной среде (как правило, среди бывших однокурсников). Инцидент приводит

к потере репутации ОВД, который считался работодателем с приемлемыми условиями работы.

Взаимоотношения с государственными органами власти – это выстраивание и налаживание взаимоотношений с государственными органами власти, в том числе с правительством, региональными и местными органами власти.

Для поддержания хорошей репутации ОВД в государственном секторе, как правило, необходимо выстраивать свою деятельность в соответствии с множеством требований федеральных законов. В контексте информационной безопасности существует как перечень законодательных актов, положения которых необходимо учитывать любым организациям, вне зависимости от рода их деятельности, так и отдельные статьи отраслевых законов, регламентирующих различные аспекты информационной безопасности. Подробно нормативные правовые акты Российской Федерации в области обеспечения информационной безопасности (в том числе и требования отраслевого законодательства), а также мероприятия по защите информации ограниченного доступа были рассмотрены в работах [1] и [2].

Невыполнение требований по информационной безопасности, как правило, влечет санкции со стороны государственных структур, которые приводят к потере репутации ОВД, например:

приостановка, а также запрет на обработку некоторых видов информации (невыполнение требований № 152-ФЗ «О персональных данных» и его подзаконных актов, статьи 13.12, 19.20 КоАП РФ). Данная санкция в отношении ОВД свидетельствует о том, что обработка информации в ОВД ведется недолжным образом и допускает ее утечку, а также незаконное распространение. В итоге, ОВД подвергается явному риску потери репутации.

В каждом рассмотренном случае возникают разной степени негативные последствия, связанные с влиянием на репутацию ОВД. Вследствие этого предлагается ввести следующую формулировку для понятия «репутационный риск», определяемого в соответствии с проблемами обеспечения информационной безопасности:

Репутационный риск ОВД – относительная величина, определяющая убытки ОВД, возникающие вследствие отсутствия подходящих организационных и технических мероприятий по

нейтрализации угроз информационной безопасности, приводящих к потере репутации ОВД для основных видов взаимоотношений.

В результате проведенного анализа можно сделать вывод о важности правильно выстроенных взаимоотношений с сотрудниками, поскольку ряд их действий, возможных вследствие недостаточности организационных мероприятий в области обеспечения информационной безопасности, влечет за собой потерю репутации ОВД и, как следствие, различного рода убытки.

Литература

1. Дорохов В.Э., Моисеев А.В. Обзор нормативно-правовых актов Российской Федерации в области информационной безопасности // Безопасность информационных технологий. 2013. № 3. С. 106–110.

2. Дорохов В.Э. Мероприятия по защите информации ограниченного доступа на основе нормативно-правовых актов Российской Федерации с учетом их отраслевой направленности в информационной безопасности // Сборник тезисов докладов конференции «Обеспечение комплексной безопасности предприятий: проблемы и решения», 4-6 июня 2013 г. С. 82–83.

СОДЕРЖАНИЕ

Научное издание

ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
II Всероссийской научно-практической
конференции

(21 мая 2015 г.)

В авторской редакции
Компьютерная верстка *Н. А. Никитиной*

ISBN 978-5-9266-0977-3

Подписано в печать 02.09.2015. Формат 60х84 1/16.
Усл. печ. л. 6,9. Тираж 100 экз. Заказ 327.

Краснодарский университет МВД России.
350005, Краснодар, ул. Ярославская, 128.