Министерство внутренних дел
Российской Федерации

Краснодарский университет

# ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
I Всероссийской научно-практической конференции

(16 мая 2014 г.)

Краснодар
КрУ МВД России
2015

УДК 004
ББК 67.410.212
И74

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России



**Информационное противодействие** экстремизму и терроризму : материалы I Всерос. науч.-практ. конф., 16 мая 2014 г. / редкол.: А. Б. Сизоненко, С. Г. Клюев, А. Г. Александров, М. Н. Андрющенко, В. Н. Цимбал. – Краснодар : Краснодарский университет МВД России, 2015. – 134 с.

И74

ISBN 978-5-9266-0855-4

В сборнике содержатся материалы, представленные на I Всероссийской научно-практической конференции «Информационное противодействие экстремизму и терроризму», посвященной наиболее острым вопросам обеспечения информационной безопасности при организации противодействия экстремизму и терроризму.

Для профессорско-преподавательского состава, докторантов, адъюнктов, курсантов, студентов и слушателей высших учебных заведений, а также сотрудников правоохранительных органов, повышающих уровень своих знаний.

УДК 004
ББК 67.410.212

ISBN 978-5-9266-0855-4

# ТЕРРОРИЗМ В ГЛОБАЛЬНОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

*Бураева Л.А., к.ф.-м.н., Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, Luda_n1@mail.ru*

*В статье рассмотрены проявления терроризма в глобальном информационном пространстве, предоставляющем злоумышленникам все свои мощные ресурсы, включая сетевую анонимность, свободу доступа, невысокую стоимость связи, быструю передачу информации, огромную международную аудиторию, множественность воздействия через различные сайты и блоги, возможность действия террориста практически в любой местности и низкий риск обнаружения.*

Сегодня Россия является лидером по количеству пользователей всемирной паутины среди европейских стран. По оценкам аналитиков число пользователей Интернет в мире уже превысило 2,5 миллиарда человек, из них 44% проживают в Азии, 23% – в Европе, 13% – в Северной Америке, 6% – в Африке, 3% – в Ближнем Востоке, 1% – в Австралии [1]. Однако, широкое использование компьютерных технологий и глобальных компьютерных сетей во всех сферах жизнедеятельности, создает предпосылки, облегчающие совершение преступных деяний в киберпространстве, которые, зачастую, остаются безнаказанными. Среди известных видов киберпреступлений, как против личности, так и против государства, следующие: хакерские атаки, разработка и распространение компьютерных вирусов, распространение детской порнографии, мошенничество с пластиковыми платежными карточками, кража денежных средств с банковских счетов, а также компьютерный или кибертерроризм [2].

На современном этапе, всемирная паутина активно используется террористическими организациями для пропаганды общественно опасных взглядов, вербовки новых членов, размещения руководств по организации терактов, психологического терроризма, сбора информации о предполагаемых целях и объектах

шантажа, пропаганды расовой, религиозной и других форм нетерпимости. По утверждению аналитиков, в скором времени терроризм в глобальном информационном пространстве может стать приемлемой альтернативой традиционным террористическим актам, по многим причинам, среди которых: сетевая анонимность, свобода доступа, невысокая стоимость связи, быстрая передача информации, огромная международная аудитория, множественность воздействия через различные сайты и блоги, возможность живого общения пользователей на форумах и чатах, возможность действия террориста практически в любой местности и низкий риск обнаружения.

Особая опасность проявлений терроризма в глобальном информационном пространстве заключается в том, что в своих преступных целях злоумышленники могут совершать кибератаки на компьютерные системы управления объектами жизнеобеспечения, целыми отраслями промышленности и обороны. К примеру, в июне 2010 года был обнаружен вирус в компьютерной системе Иранского центра по обогащению урана, который изменил скорости вращения центрифуг и впоследствии вывел их из строя. После данного инцидента большинство развитых стран начало укреплять защиту жизненно важных промышленных объектов, в частности, в энергетике и водоснабжении. Известны кибератаки на сайты инфраструктурных и оборонных предприятий. В течение 2012 года правительственные ресурсы США подверглись кибератакам 12 млн. раз, компьютерные правительственные системы Ирана испытали на себе 28 миллионов атак, информационные ресурсы Израиля были атакованы 44 миллиона раз. За время президентских выборов в России в 2012 году компьютеры правительственных структур подверглись кибератакам 1,2 миллиона раз [3].

По словам основателя интернет-ресурса «WikiLeaks», скандально известного похитителя секретных материалов Джулиана Ассанжа, опубликовавшего на своем сайте 150 тысяч секретных документов, общество до сих пор не осознало тот факт, что сегодня нужно бояться не бомб, а взлома компьютеров, управляющих ими.

Следует отметить, что сегодня все действующие террористические организации используют в своих преступных целях гло-

бальное информационное пространство, проводя пропаганду расовой, религиозной и других форм нетерпимости через интернет-сайты. На них они ведут активную агитацию за вооружённую борьбу с религиозным инакомыслием [4], осуществляют призывы к свержению светских режимов и установлению теократических государств, контролируют информационную и социально-психологическую обстановку разных стран мира. В большинстве случаев, сайты террористических организаций имеют версии на разных языках, что позволяет им вербовать новых членов с разных стран. Кроме того, террористическая пропаганда активно ведется в социальных сетях, например: «Фейсбук», «Твиттер», «YouTube», которые часто являются не только источниками непроверенной провокационной информации, но и организаторами и координаторами народных волнений. Указанный факт изложен в докладе «Использование Интернета в террористических целях» [5], подготовленном членами целевой группы ООН по осуществлению контртеррористических мероприятий.

Террористы используют широкие возможности глобальной сети в двух аспектах: технологическом и информационном. В первом случае террористы используют компьютерные технологии для совершения террористических действий: они могут атаковать или проникнуть внутрь компьютерных систем различных учреждений, в результате чего могут пострадать военные, разведывательные, медицинские службы, транспортные и финансовые системы и т.д. Для второго, информационного аспекта, характерно оказание посредством компьютерной информации воздействия на психику и сознание людей. Причем данное воздействие направленно на формирование общественно опасных мыслей и суждений, провоцирующих к совершению определенных действий в интересах террористов, а в дальнейшем – преступлений террористической направленности. Интернет активно используется террористами для сбора средств на поддержку террористической деятельности; распространения агитационно-пропагандистской информации о деятельности террористических организаций; осуществления организационной деятельности, например, рассылки сообщений о встречах заинтересованных лиц; анонимного привлечения к террористической деятельности соучастников, например, хакеров и представи-

телей бизнеса, которые предоставляют различные информационные услуги на коммерческой основе; осуществления информационно-психологического воздействия на население с целью шантажа, создания паники и распространения дезинформации и т.д.

К практическим шагам борьбы с проявлениями терроризма в глобальном информационном пространстве, в России следует отнести ставший традиционным Форум Международного Дня безопасного Интернета, основными организаторами которого являются Центр безопасного Интернета в России и Региональный общественный Центр Интернет-технологий под патронатом Общественной Палаты Российской Федерации. Президент Российской Федерации В.В. Путин перед правительством и силовыми структурами РФ активно ставит задачу продолжать борьбу с экстремизмом и терроризмом. В своем докладе на расширенной коллегии ФСБ РФ В.В. Путин отметил, что только за 2013 год была пресечена деятельность более 400 сайтов террористической и радикальной направленности, и такая антиэкстремистская работа в информационном пространстве должна последовательно продолжаться. Также в своем выступлении В.В. Путин сообщил, что граждане РФ, завербованные террористами и радикалами, сегодня принимают участие в боевых действиях в Афганистане, Сирии, других регионах, по сути, проходят там террористическую подготовку и идеологическую обработку [6].

Главная особенность проблемы борьбы с терроризмом в глобальном информационном пространстве заключается в том, что одно государство не в состоянии противостоять данному явлению самостоятельно, используя только собственный государственно-властный механизм. Только благодаря постоянному тесному сотрудничеству мировое сообщество может противостоять такому фактору международных угроз, как киберпреступность и кибертерроризм.

**Литература**

1. Официальный сайт сетевого здания ФГУП РАМИ «РИА Новости». [Электронный ресурс]. Электрон. дан. – Режим доступа: www. URL: http://ria.ru/technology/20120119/543870925.html#ixzz2LEdsyXVE http://ria.ru/technology/20120119/543870925.html (дата обращения: 12.05.2014).

2. Бураева Л.А. Киберпреступность и кибертерроризм – новая глобальная угроза мировому сообществу // Материалы XVI Международной научно-практической конференции «Современные тенденции и направления оптимизации борьбы с преступностью в новейшей России». – Нальчик: Издательство М. и В. Котляровых (ООО «Полиграфсервис и Т»), 2013г. – С.280-288.

3. Официальный сайт «Армейский Вестник». [Электронный ресурс]. Электрон. дан. – Режим доступа: www. URL: http://army-news.ru/2013/01/kiberataki-2013-goda-prognozy-ekspertov/ (дата обращения: 12.05.2014).

4. Тарчоков, Б.А. Мотивация преступных проявлений экстремистского характера // Наука и бизнес: пути развития. –2013. –№ 6 (24). –С. 77-81.

5. Использование Интернета в террористических целях / Организация объединенных наций. Нью-Йорк: Издат. Организации объединенных наций, 2013. 148 с.

6. В.В. Путин призвал бороться с экстремизмом и терроризмом в интернете. [Электронный ресурс]. Электрон. дан. – Режим доступа: www. URL: http://kavkazpress.ru/archives/44964 (дата обращения: 12.05.2014).

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ

*Згадзай О.Э., к.ф.-м.н, доцент, Казанский юридический институт МВД России, zgadzai_oleg@mail.ru*
*Казанцев С.Я., д.п.н., профессор, Казанский юридический институт МВД России, vestnikkui@mail.ru*

Аннотация. В условиях становления гражданского общества проблемы, связанные с использованием криптографических средств защиты информации, приобретают особую актуальность. Проведенный в работе анализ свидетельствует о тенденции усиления законодательного контроля над криптографией со стороны государства. Наиболее актуальной является проблема криптографической защиты персональных данных.

Ключевые слова: криптография, криптология, криптографические средства, лицензирование, депонирование ключей, персональные данные

Актуальность взаимоотношения криптологии и права в эпоху «цифровых технологий» ни у кого не вызывает сомнений. Внедрение компьютеров и телекоммуникационных технологий радикально изменило способы обмена информацией. Наряду с быстродействием, эффективностью и экономией средств – качествами, которые принесла «цифровая революция» – появились и новые угрозы неприкосновенности коммуникаций и данных.

До недавнего времени средства криптографии были практически не востребованы среди неправительственных организаций, а технологии шифрования стояли на страже лишь военных и дипломатических тайн. С переходом к информационному обществу возник новый рынок криптографических средств. Электронные коммуникации широко распространились в гражданском секторе и стали частью глобальной экономики. Компьютеры используются для хранения и передачи персональных данных, включая медицинскую и финансовую информацию. Как следствие, растет потребность в защите личной конфиденциальной информации, безопасных средствах шифрования и аутентификации.

Нормативно-правовая база правового регулирования использования криптографических средств основана на двух типах источников: международных нормативно-правовых актах и актах национального законодательства. В первую очередь, следует выделить ряд международных документов и договоров в области правового регулирования криптографии. Один из них – Вассенаарское соглашение [1]. Это документ, подписанный 19 декабря 1995 года 33 странами мира, в том числе и Россией, преследует цель ограничения экспорта обычных видов вооружения и «товаров двойного применения» в некоторые нестабильные страны или, в определенных случаях, в те государства, которые находятся в состоянии войны. К «товарам двойного применения» относятся и криптографические продукты и высоконадежные системы обеспечения информационной безопасности [2]. В большинстве случаев положения Вассенаарского соглашения обязательны для исполнения странами-участницами.

Вторым важнейшим международным документом, определяющим принципы использования криптографии, является комплекс положений Организации по экономическому сотрудничеству и

развитию (ОЭСР) – «Privacy&Crypto 2000» [3]. Положения представляют собой рекомендации, которые страны должны учитывать при осуществлении политики в области криптографии. В соответствии с положениями вводится восемь основных правил в области криптографии:

1. Методы криптографии должны пользоваться доверием, чтобы таким же доверием пользовались информационные и коммуникационные системы;

2. Пользователи должны иметь право выбирать любой метод криптографии, не запрещенный законом;

3. Развитие криптографических средств должно определяться потребностями частных лиц, коммерческих организаций и государственных структур;

4. Технические стандарты, критерии и криптографические протоколы должны разрабатываться и поддерживаться на национальном и международном уровне;

5. Основные права человека на неприкосновенность частной жизни, включая тайну коммуникаций и защиту персональных данных, должны уважаться в национальных правилах в области криптографии и в практике использования криптографических средств;

6. Национальная политика в области криптографии может предусматривать доступ к зашифрованным данным или ключам. Эта политика должна строиться с учетом всех остальных принципов;

7. Ответственность частных лиц и организаций, предлагающих криптографические услуги или услуги по сохранению ключей, определяется законом или договором и должна быть четко определена;

8. Государства должны сотрудничать с целью координации политики в области криптографии.

Несмотря на значимую роль международных договоров, главное место в системе источников правового регулирования криптографических средств занимают нормативно-правовые акты национального законодательства. Основополагающим нормативно-правовым актом, определяющим порядок лицензирования и регистрации криптографических средств на территории Российской Федерации, является Постановление Правительства от 16.04.2012 № 313.

Необходимо выделить некоторые особо значимые с правовой, научной и практической точек зрения моменты рассматриваемого документа.

Во-первых, любое криптографическое средство, прошедшее процедуру государственного лицензирования, при необходимости может быть использовано уполномоченными правительственными структурами, чтобы прочитать сообщение, зашифрованное криптографическим средством, прошедшим процедуру лицензирования.

Во-вторых, в положениях приводится перечень криптографических средств, которые можно не лицензировать. В частности, к ним относятся:

1. симметричные криптографические алгоритмы с ключом, длина которого не больше 56 бит;

2. ассиметричные криптографические алгоритмы с максимальной длиной ключа – 512 бит.

Почему выделены такие алгоритмы и такая длина ключей? По информации специалистов-экспертов, современные правительственные системы криптоанализа вскрывают такие алгоритмы за считанные минуты, так что в их лицензировании нет никакой необходимости.

Другим нормативно-правовым актом, осуществляющим регулирование использования криптографических средств, является Федеральный закон «Об электронной подписи» от 06.04.2011 № 63. Данный закон регламентирует деятельность по использованию криптографических средств электронной подписи. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. Принципы, заложенные в основу использования криптографических средств, распространяются и на средства электронной подписи.

Одной из наиболее актуальных проблем использования криптографических средств является проблема обеспечения доступа к закрытым криптографическим ключам государственных структур. По данному вопросу в настоящее время в мире сформировались две четкие позиции:

1. депонирование ключей;
2. «законный доступ» правительственных структур.

Суть депонирования заключается в том, что пользователи имеют право использовать сильную криптографию в своих системах, однако третья сторона, в лице государственной структуры, получает ключи на хранение в депозитарий и имеет право предоставить их государственным органам по запросу. Таким образом, в систему отправитель – получатель включается третье лицо в лице государства.

Идея о депонировании ключей была заложена в качестве основополагающей концепции США в области правового регулирования криптографии [4]. США оказывали давление на многие страны и международные организации, включая Организацию по экономическому сотрудничеству и развитию и Вассенаарское соглашение. Однако страны, входящие в ОЭСР, отказались от предложенной концепции.

Эксперты в области безопасности настроены критически по отношению к надежности систем депонирования. Они отмечают множество проблем, которые создает централизованная схема хранения ключей. Европейская Комиссия опубликовала доклад [5], в котором рассматривались проблемы систем депонирования ключей:

- Любая схема доступа к ключам открывает ряд дополнительных возможностей для вторжения в криптографическую систему;
- Стоимость внедрения схем доступа к ключам может быть неоправданно высокой;
- Схемы доступа к ключам можно легко обойти (обмануть), даже если предположить, что всех пользователей обязали принять эти схемы.
- Всякое участие третьей стороны в процессе связи делает этот процесс более уязвимым.

Ощутимый удар по концепции депонирования ключей нанесло заседание участников Вассенаарского соглашения в декабре 1998 года, на котором они не пришли к общему соглашению, и американский план не был принят. Таким образом, мировым сообществом официально отвергнута концепция правового регулирования криптографии с помощью системы депонирования ключей.

Однако начиная с 2000 года Агентство Национальной Безопасности США получило из федерального бюджета США более 150 млрд. долларов на реализацию проекта «Bullrun» [6]. Суть проекта сводится к созданию информационной системы поиска закрытых ключей через протоколы передачи данных TCP/IP, FTP, UDP, TCMP, WiFi с целью их последующего помещения в централизованный депозитарий криптографических ключей. Если эта информация подтвердится, то США придется либо вносить очередные поправки в Конституцию и тем самым признать, что интересы государства превыше интересов личности, либо отказаться от данного проекта, что маловероятно.

После официального отказа от депонирования ключей правительства разных стран рассматривают в качестве основной концепцию «законного доступа». Суть ее заключается в законодательно разрешенном доступе к ключам третьих лиц. По замыслу авторов концепции, юридическим и физическим лицам следует предоставлять криптографические ключи по требованию правоохранительных органов, в противном случае им может быть предъявлено обвинение в препятствии правосудию.

На саммите в Денвере, прошедшем в июне 1997 года, страны «Большой восьмерки» поддержали идею «законного доступа». Решение гласило, что каждая страна должна обеспечить «законный доступ государства к ключам в целях предотвращения и расследования случаев терроризма, а также выработать механизм международного сотрудничества в данной области» [7].

Следует отметить, что к настоящему времени лишь немногие страны приняли соответствующие законы. Законы, по которым лицу может грозить уголовное наказание, если оно откажется предоставить свои ключи следствию, приняты пока только в Сингапуре и Малайзии. В обеих странах полиция имеет право налагать штрафы и брать под стражу пользователей, которые не предоставляют ключи или оригинальный текст сообщений.

Законодательством Российской Федерации не предусмотрены никакие из рассмотренных вариантов доступа к ключам. Однако федеральным законом «Об оперативно-розыскной деятельности» в статье 6 в перечне оперативно-розыскных мероприятий упомянуты следующие мероприятия:

- контроль почтовых отправлений, телеграфных и иных сообщений;
- прослушивание телефонных переговоров;
- снятие информации с технических каналов связи.

Таким образом, в ходе проведения оперативно-розыскных мероприятий могут быть использованы средства для доступа к закрытым ключам. В ст. 6 ФЗ «Об оперативно-розыскной деятельности» говорится также, что проведение указанных оперативно-розыскных мероприятий может производиться с использованием оперативно-технических сил и средств органов федеральной службы безопасности, которая располагает необходимыми специалистами в области криптографии.

Подводя итог обсуждению вопроса о доступе к криптографическим ключам необходимо отметить, что приемлемого решения в настоящий момент не существует, и это является серьезным пробелом как иностранного, так и отечественного законодательства.

В сфере использования криптографических средств наиболее актуальной является проблема защиты персональных данных. В связи с возросшей необходимостью защиты персональных данных Государственной Думой РФ в 2006 году был принят федеральный закон «О персональных данных». В соответствии с законом персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания. Хранение персональных данных

должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Одним из основных значимых аспектов в области защиты конфиденциальности персональных данных является использование криптографических средств. В соответствии со статьей 19 закона «О персональных данных» оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Правительством Российской Федерации принято постановление N 781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Постановление устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в

информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации. При этом под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под контрольными тематическими исследованиями – периодически проводимые тематические исследования.

В заключение хотелось бы еще раз отметить, что криптография защищает государственную, служебную и коммерческую тайны [8]. Проведенный анализ правовых актов международного и российского законодательства свидетельствует о тенденции усиления законодательного контроля над криптографией со стороны государства. Однако следует помнить, что криптография стоит на страже личной и национальной безопасности только до тех пор, пока она подчиняется грамотному правовому регулированию.

**Литература**

1. Den Tourin. Krypto & Science. URL: http://www.privacyinternational.org/

2. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Initial Elements, Press Statement, 12 July 1996.

3. Доклад о контроле над криптографическими технологиями. 28 января 2000 г. URL: http://appli1.oecd/olis/1998doc.nsf

4. EPIC. «Белый Дом о новой политике в области крипто», 16 сентября 1998 г. URL: http://www.epic.org/crypto/announce_9_16.html

5. Доклад Европейской комиссии по проблемам krypto&privacy, 1997. URL: http://www.jya.com/mitizeal.txt

6. Сноуден пролил свет на ситуацию со взломом криптографии. Все плохо. URL: http://www.habrahabr.ru/post/192722/

7. Правительственный форум по шифрованию и укреплению правопорядка URL: http://www.homeoffice.gov.uk/oicd/ecu/partind.htm

8. Жельников В.С. Криптография от папируса до компьютера. М., 1998.

# ИНФОРМАЦИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ КАК ОДИН ИЗ ЭЛЕМЕНТОВ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

*Алескеров В.И., к.ю.н., доцент, ОТМ ОВД ВИПК МВД России,*
*Куц Ф.А., управление «К» БСТМ МВД России*

*Преступления в сфере компьютерной информации являются новеллами в отечественном уголовном законодательстве. Компьютерная информация до настоящего времени остается наиболее уязвимой. Компьютерные преступления, носят специфичный характер и в настоящее время, – это новации в системе уголовного права, так как способы их совершения настолько многогранны и носят изощренный характер, что порой сотрудникам управлений «К» при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями, в связи с чем разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности.*

Преступления в сфере компьютерной информации являются новеллами в отечественном уголовном законодательстве. Необходимость установления уголовной ответственности за причинение вреда в связи с незаконным использованием компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности современного общества. Однако, к сожалению, до настоящего времени, во многих организациях, предприятиях, учреждениях и отраслях народного хозяйства по сравнению с информацией, зафиксированной на бумажных носителях [1], компьютерная информация остается наиболее уязвимой.

Анализ положений действующего Уголовного кодекса РФ позволяет сделать вывод о том, что законодатель в гл. 28 «Преступления в сфере компьютерной информации» ввел ряд понятий, не содержавшихся ранее не только в понятийно-терминологическом аппарате уголовного права, но и в «информационном» законодательстве, так как ранее не было практических наработок и теоретических рекомендаций по раскрытию и расследованию пре-

ступлений в этой сфере. В целях своевременного документирования преступной деятельности данного вида преступлений и получения необходимой доказательной базы в отношении лиц их совершивших в 2001 году в структуре МВД России создано специализированное подразделение – Управление «К» БСТМ МВД России, у которого основными направлениями оперативно-служебной деятельности являются:

1. борьба с преступлениями в сфере компьютерной информации;
2. борьба с преступлениями в сфере телекоммуникаций;
3. борьба с незаконным оборотом РЭС и СТС;
4. борьба с нарушением авторских и смежных прав;
5. борьба с распространением детской порнографии;
6. борьба с преступлениями в электронных платежных системах.

Компьютеризация всех слоев населения носит социально значимое веяние, но, его достижения могут быть использованы не только в хороших намерениях, но, и при совершении преступлений компьютерной направленности. Компьютерные преступления, носят специфичный характер и в настоящее время, – это новации в системе уголовного права, так как способы их совершения настолько многогранны и носят изощренный характер, что порой сотрудникам управлений «К» при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями, в связи с чем, разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности. Необходимо заметить, что одним из важнейших составляющих элементов криминалистической характеристики в ходе раскрытия компьютерных преступлений, является субъективная особенность личности преступника, который на начальном этапе раскрытия преступлений характеризуется лишь скудной информацией, в связи, с чем мы абсолютно согласны с мнением, высказанным Т.В. Ворошиловой, которая предлагает учитывать такие составляющие как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре.[2] Иными словами, немаловажное значение в раскрытии любого вида компьютерного преступления, играет характерологическая особенность психологии

личности преступника, которая позволяет при глубоком анализе определить и сузить круг подозреваемых лиц, мотив преступления, способ его совершения, а также выдвинуть версии, что естественно приблизит оперативных работников и следователей к осуществлению выполнения оперативно-розыскных мероприятий и следственных действий, способствующих раскрытию данного вида преступлений.

Уголовно-правовой анализ преступлений в сфере компьютерной информации невозможно провести без предварительного уяснения родового понятия информации. Она выступает в качестве сравнительно нового предмета исследования и особого объекта правового регулирования. Именно поэтому необходимо обратиться не только к законодательным понятиям информации, но и к научным ее толкованиям.

Понятие «информация» имеет как минимум четыре основных значения:

- как сведения, передаваемые людьми любым способом;
- как общенаучное понятие;
- как обмен сигналами в животном и растительном мире;
- информация как кибернетический термин.

Само слово «информация» происходит от латинского «information» и означает «разъяснение» или «осведомленность»[3]. Начальные шаги в теории информации были сделаны еще в первой половине XX в.: в 1928 г. Р. Хартли впервые дал количественное определение информации, а в 1948 г. вышла знаменитая книга К. Шеннона «Математическая теория связи», где информация и дается уже как статистическое определение.

Н. Винер, один из основателей кибернетики, определил информацию как «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств»[4]. К. Шеннон, который сыграл не меньшую роль в развитии кибернетики, рассматривал информацию как сигнал (сообщение), устраняющий или снижающий неопределенность[5].

А.Л. Фатьянов полагает, что «информация есть воспринимаемая живым организмом через органы чувств окружающая действительность в виде распределения материи и энергии во времени и в пространстве и процессов их перераспределения».

Таким образом, информация с точки зрения кибернетики представляется не как общественный феномен, то есть информация, производимая и потребляемая обществом, а более узком, техническом аспекте – как информация, циркулирующая по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем.

Информационная сфера сегодня – это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающаяся в адекватном правовом регулировании. С этой целью создается «информационное» законодательство, а также система мер уголовно-правовой защиты данной группы отношений. Последние изменения в главу 28 УК РФ вступили в силу 7 декабря 2011 года.

Основное различие правового режима информации состоит в степени ее доступности для пользователей. Так, в зависимости от категории доступа к ней, информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)[6]. В соответствии со ст. 5 ФЗ №149 от 27.07.2006г. «Об информации, информационных технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствий с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Так, например, правовой режим информации, составляющей государственную тайну, определяется Законом РФ №5485-1 от 21.07.1993г. «О государственной тайне» (с изменениями от 06.10.1997г.)[7]. Перечень сведений, составляющих государственную тайну, определен ст. 5 Закона и включает в себя три основных раздела:

1. сведения в военной области,
2. сведения в области экономики, науки и техники,

3. сведения в области внешней политики и экономики.

Как указывалось ранее, законодателю в каждом нормативно-правовом акте требуется найти баланс между обеспеченным Конституцией РФ правом граждан на информацию и обеспечением ее конфиденциальности. Не стал исключением в этом смысле и Закон «О государственной тайне», который содержит перечень сведений, не подлежащих отнесению к государственной, тайне и засекречиванию.

В соответствии со ст. 7 Закона таковыми являются: сведения о чрезвычайных происшествиях, катастрофах, стихийных бедствиях; о состоянии экологии, здравоохранения, санитарии, демографии, а также о состоянии преступности; о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам; о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах РФ; о состоянии здоровья высших должностных лиц РФ; о фактах нарушения законности органами государственной власти и их должностными лицами.

Основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации заложены ФЗ «Об информации, информационных технологиях и о защите информации», в ст. 3 которого четко установлено, что правовое регулирование рассматриваемых отношений основывается на принципах:

1) свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установления ограничений доступа к информации только федеральными законами;

3) открытости информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправия языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечения безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверности информации и своевременность ее предоставления;

7) неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимости установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Понятие «компьютерной информации» является не менее многозначным, чем понятие информации. Ее место в системе правоотношений, возникающих в информационной сфере, до сих пор является предметом научных дискуссий, которые пока не завершились формированием общепризнанного научного и законодательного определения, поскольку многообразие его толкования отображает весьма сложный характер реального мира.

Проблемы в правоприменительной практике связаны с тем, что, несмотря на важность точного формализованного представления о сущности и свойствах компьютерной информации (как предмета преступления), на законодательном уровне так и не появилось определения «компьютерной информации». Однако, в специальной и учебной литературе предложено множество определений рассматриваемого термина. Так, например, одними из первых понятие «компьютерной информации» дали: Т.Г. Смирнова, определив компьютерную информацию как «совокупность сведений, представляющих особую ценность для государства, общества и отдельных граждан, производство, хранение и использование которых осуществляется посредством компьютерной техники», и А. Петров, предложивший понимать под данным термином «информацию, содержащую сведения, составляющие государственную или коммерческую тайну, сведения конфиденциального характера и общего пользования».

Отметим, что предложенные определения не лишены недостатков. Из определения Т.Г. Смирновой следует, что информация и ее материальный носитель («компьютерная техника») не отде-

лимы друг от друга, а исходя их такого подхода, компьютерная информация, циркулирующая в сети ЭВМ, не будет являться предметом данной категории преступлений, а, следовательно, останется без надлежащей уголовно-правовой защиты. Из содержания понятия «компьютерная информация», данного А.А. Петровым, вообще невозможно выделить отличительные признаки компьютерной информации как таковой[8].

Более корректным представляются определения, предложенные С.А. Пашиным и В.С. Комиссаровым. По утверждению первого автора, «компьютерная информация – это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ»[9]. В.С. Комиссаров справедливо указал, что «компьютерная информация может находиться или на машинном носителе (магнитном диске, магнитной ленте, дискете, магнитно-оптическом диске (CD-ROMe), или непосредственно в ЭВМ (в постоянном или оперативном запоминающих устройствах), либо в системе ЭВМ или их сети»[10]. По нашему мнению предложенные С.А. Пашиным и В.С. Комиссаровым понятия наиболее точные, четко отражают критерии предмета преступлений в сфере компьютерной информации. Так же нельзя не согласиться и с определением «компьютерного преступления», предложенным авторами В.А.Дуленко, Р.Р. Мамлеева, В.А. Пестрикова, где ими сказано, что компьютерное преступление как уголовно-правовое понятие – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства [11]

Поэтому с учетом представленных позиций авторов понятие «компьютерной информации» как предмета преступления можно сформулировать как организационно упорядоченную совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информационно-телекоммуникационной сети с реквизитами, позволяющими их идентифицировать, имеющую собственника либо иного законного владельца.

Полагаем, что уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести

ущерб ее собственнику (владельцу, пользователю). При закреплении предложенного определения в базовом для этой сферы законодательстве, например в Федеральном законе «Об информации, информационных технологиях и о защите информации», оно позволит, на наш взгляд, существенно сократить ошибки в правоприменении рассматриваемых уголовно-правовых норм.

**Литература**


1. Винер Н. Кибернетика и общество. М., 2003. С. 31.
2. Т.В. Ворошилова. Социальная и психологическая характеристика личности компьютерного преступника. М., 2009 г., стр. – 5.
3. Большой энциклопедический словарь. М., 2004. С. 421.
4. Винер Н. Кибернетика и общество. М., 2003. С. 35.
5. Шеннон К. Работы по теории информации и кибернетики. М., 1963. С. 59.
6. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации: Учеб. пособие. М., 2001. С. 10.
7. СЗ РФ 1997г., № 41. Ст. 4673.
8. Петров А.А. Компьютерная информация как предмет уголовно-правовой защиты реформированного уголовного законодательства // Российское право в период социальных реформ. Н.Новгород. 1998. Вып. 2. С. 132.
9. Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. Ю.И. Скуратова, В.М. Лебедева. М., 2001. С. 696.
10. Уголовное право России / Под ред. В.С. Комисарова. М., 2006. С. 307.
11. В.А.Дуленко, Р.Р. Мамлеев, В.А. Пестриков.,. Учебное пособие. «Преступление в сфере высоких технологий» – М. – 2010 г., С.- 196.


## О БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ


*Дуденков А.В., к.ю.н., Ростовский юридический институт МВД России,*
*Петрищева Е.Н., Ростовский юридический институт МВД России,*
*mayor_ledi@mail.ru*



*В статье рассматриваются вопросы безопасности персональных данных при использовании сети Интернет. Говорится о том, что всё затруднительнее становится скрыть от государственных служб, корпораций и не в меру любопытных «просто граждан» информацию персонального характера.*

С каждым годом в Интернете всё затруднительнее становится скрыть от государственных служб, корпораций и не в меру любопытных «просто граждан» информацию персонального характера. Принятие разных ограничивающих законов и персональная осторожность самых продвинутых пользователей мало помогают сохранить свои секреты в неприкосновенности.

Скрытность не спасает. Говоря о безопасности, часто первым делом поминают социальные сети, куда множество граждан выкладывают личные фото, имена, адреса, и так далее, так что и искать ничего не приходится. Между тем, это хоть и самый широкий, но совсем не единственный путь, который персональные данные попадают в чужие руки, так что прекращение общения в социальных сетях не станет панацеей.

В глобальной сети нельзя кликнуть ни по одной ссылке так, чтобы об этом не стало известно. Сначала об этом узнаёт провайдер, посредством которого вы выходите в Интернет. Не стоит об этом забывать когда кажется, что можно остаться в сети совершенно анонимным: правоохранительным органам узнать имя анонима не составит труда, сделав запрос к провайдеру. Сайты, на которые пользователи заходят, также получают о них некоторые данные. У веб-серверов часто имеются журналы обращений, где хранится информация из браузеров пользователей. Не стоит забывать и о файлах куки, которые сайты ставят на браузеры посетителей.

Самые популярные сайты могут раскинуть свои щупальца по всей сети: например, часто приходится видеть на самых разнообразных сайтах кнопки популярных социальных сетей, таких как «Одноклассники», «Вконтакте», Twitter, Facebook и прочих. Эти кнопки, располагаясь на страницах каких-либо сайтов, на самом деле находятся на тех же серверах, что и соответствующие соцсети. Самое же интересное, что даже если не кликать на них, соцсети будут знать о вашем посещении тех страниц, где расположены их кнопки. Про рекламные баннеры, в том числе текстовые, можно сказать то же самое. Такие баннеры находятся на крупных серверах рекламных сетей, к которым обращаются тысячи сайтов. Кроме них, существуют специализированные инструменты, которые созданы для анализа посещаемости, такие как Google

Analytics, которые фиксируют посещение пользователей страниц при помощи HTML-кода.

Все эти получатели информации протоколируют её у себя, накапливают и при случае готовы использовать в своих или в чужих интересах. Как же все эти данные можно использовать? Каждый пользователь в отдельности в таких случаях не представляет интереса, а вот изучение особенностей поведения больших групп является уже полезным, например, для рекламодателей.

В прошлом году в газете New York Times была опубликована статья о магазинах торговой сети Target. В ней рассказывается, как данная сеть использует собранные о покупателях данные с целью выявления группы будущих матерей. Маркетологи компании были уверены, что во время беременности покупательские привычки претерпевают изменения, и на основе этого можно превратить их в своих постоянных клиентов – нужно только знать, когда.

В США, как известно, чрезвычайно распространена оплата кредитными картами, а также дисконтными. Естественно, при их использовании информация о совершении покупки попадает в базы данных, которую можно проанализировать. Определив покупательниц, у которых дети уже есть, маркетологи взялись сравнить их покупки до беременности и во время. Не станем приводить конкретные результаты, скажем только, что они есть: во время беременности покупательницы уделяют повышенное внимание некоторым группам товаров, на основе чего можно вести их усиленную рекламу.

Проблемы с утечкой данных есть не только в Интернете! Приведённая выше история подтверждает этот факт, и таких примеров можно привести немало. Если говорить о мобильных телефонах, то номер аппарата привязан к паспорту пользователя, так что ничего менее приватного и представить себе нельзя. Местоположение телефона, а вместе с ним и его владельца, известно 24 часа в сутки.

При перемещении аппарат ищет базовые станции оператора мобильной связи и подключается к ним. Каждое подключение фиксируется, так что где телефон находится сейчас, а где он был год назад в такой-то час такого то дня, записывается. Опять-таки, правоохранительные органы и спецслужбы всегда могут этим воспользоваться.

Добавляют проблем используемые алгоритмы геопозиционирования. Определение положения смартфона на основе данных спутников GPS не является быстрым делом, так что помогают в этом ещё и триангуляция на основе данных от вышек сотовой связи и беспроводных сетей. Список таких сетей не хранится в смартфонах, а загружается из Интернета в случае необходимости, при этом выдавая местоположение аппарата тому сервису, с которого эти данные загружаются.

Платёжные карты, как уже показано выше, тоже являются отличным средством рассказать о себе и своих пристрастиях. Причём рассказать сразу и платёжной системе, и банку, и компании, у которой делается покупка. Здесь данные также привязаны к фамилии и паспорту, так что об анонимности речи не идёт.

Новые опасения относительно приватности зарождаются с появлением очков дополненной реальности Google Glass. Точнее, они ещё даже не появились, а продаются только разработчикам программного обеспечения для них, а страхи уже растут. Просто нажав на дужку, можно будет включить видеозапись, которая тут же попадёт в Интернет. Так что если у вас нет анкеты в соцсетях, это не значит, что там не будет видео с вашим участием. Утечка информации неудержима.

Правительства ряда стран пытаются решить вопрос утечки данных запретами. Год назад Европейский Союз наложил строгие ограничения на использование куки-файлов, а в британских провинциях решили перегородить улицы, чтобы не дать проехать машинам Google, которые ведут съёмки для сервиса Street View. В Германии пытаются запретить использовать в Facebook технологию лицевого распознавания, а в Далласе вести съёмку с беспилотников без разрешения владельцев территории. Все эти запреты мало мешают всему вышеназванному.

Часто простым пользователям дают такие рекомендации, как не пользоваться соцсетями, отключить в своих браузерах JavaScript и куки, блокировать всплывающую рекламу при помощи аддонов, не выкладывать фотографий, не называть настоящее имя. Однако ваше имя или адрес корпорации и социальные сети могут вовсе не интересовать. Неверное представление о приватности помогает быстрее лишиться её.

Рассмотрим пример из информатики. С помощью 33-х битов можно записать число, превышающее 8,5 млрд., что больше численности населения нашей планеты. Значит 33-битного числа достаточного для присвоения каждому человеку уникального идентификационного номера. Не зная о человеке ничего, придётся для его поиска перебрать все 7 млрд., что является невыполнимой задачей. Но если на какой-то вопрос о человеке можно ответить да или нет, это уже сужает круг поиска. Если знать его пол, это уже сужает круг поиска вполовину. Если знать, что он регулярно посещает веб-сайт с числом посетителей в полмиллиона человек, поиск уменьшается до этого значения [2]. Браузер передаёт серверу своё название, версию, версию используемой на компьютере пользователя операционной системы, язык, поддерживаемые форматы и куки. JavaScript и Flash дают доступ к часовому поясу и установленным плагинам. Круг сужается ещё сильнее, число неизвестных битов сокращается.

Отключение кук и JavaScript может только навредить, поскольку выделяет человека: в Рунете всего 0,5% пользователей отключают их. Помимо данных из браузера можно вести лингвистический анализ пользователей, фиксировать часто употребляемые ими выражения, анализировать выкладываемые пользователем фотографии с технической точки зрения, и т.д. Чтобы избежать всего этого, придётся вернуться в докомпьютерную эпоху.

Всегда есть желающие получить информацию о вас. Многие считают, что у них нет ничего ценного, из-за чего стоило бы за ними следить. Между тем, эта слежка сейчас происходит просто автоматически, не разбирая простых людей или важных персон.

Реклама – двигатель прогресса. Прогресса Google и Facebook, которые, как сказано выше, ведут групповой поведенческий анализ с целью повышения эффективности рекламы. В Германии идея внедрения в Facebook технологии распознавания лиц пришлась очень не по душе. Сейчас необходимо наличие текстовой подписи, чтобы узнать, кто изображён на фотографии, но технология распознавания позволит обойтись без неё. Это даст доступ к огромному источнику лежащей в Интернете, но не распознанной пока информации.

Является ли утечка информации проблемой? Потеря приватности представляет собой побочный эффект передовых технологий, которыми мы пользуемся каждый день. Многие удаляют свои

профили в социальных сетях, как недавно сделали 11 млн. пользователей Facebook после разоблачений Эдварда Сноудена [1]. Кто-то считает, что отключение JavaScript и Flash в браузере поможет им. В будущем передовых технологий станет только больше, и доступ к ним могут получить не только корпорации, но и простые люди. Вряд ли кто-то решиться пойти на отказ от использования технологий, чтобы избежать утечки информации.

Для утешения можно сказать, что анализ всех таких данных ведут не люди, а специальные программы, и от получения точечной рекламы на сайтах ещё никто не пострадал. Конечно, могут быть и весьма негативные последствия потери приватности, например, компрометирующие фотографии способны испортить личную жизнь или карьеру, политические взгляды привести к репрессиям, а данные о местоположении навести нежелательных людей. Всё это, впрочем, лишь следствие несовершенства человеческого общества в целом, его трудового законодательства, политических систем и т.д.

Остаётся только наблюдать, как технологии сбора данных и методы использования этих данных будут развиваться в дальнейшем.

**Литература**

1. http://www.vesti.ru/doc.html?id=1100824
2. http://www.rg.ru/sujet/5027/

# О БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВУЗОВ МВД РОССИИ

*Карпика А.Г., к.т.н., доцент, Ростовский юридический институт МВД России, akarpika@yandex.ru*
*Арбузов П.В., к.ф-м.н., доцент, Ростовский юридический институт МВД России, arbuzovp@gmail.com*
*Гуде С.В., к.т.н., доцент, Ростовский юридический институт МВД России, gud56@mail.ru*

*В статье рассматриваются фундаментальные и прикладные вопросы безопасности информационно-аналитических ресурсов вузов МВД России. Особое внимание уделено составу периметра информационной безопасности и возможным уязвимостям информационных ресурсов.*

Современный этап развития системы высшего образования Российской Федерации и осуществленный переход на новые образовательные стандарты потребовал от ведомственной системы образования МВД России пересмотреть вопросы организации информационно-аналитического обеспечения образовательного процесса вузов. Подготовка сотрудников полиции к выполнению служебных обязанностей проходит на фоне динамично меняющейся экономической и геополитической ситуации в евроазиатском регионе вообще и в Российской Федерации в частности.

Несомненно, подобные изменения оказывают серьезное влияние на российское общество, часть которого находится под влиянием со стороны внешних деструктивных сил. В сложившихся условиях дальнейшее развитие ведомственной системы образования целесообразно проводить в направлении повышения ее готовности к упреждающему парированию экономических, политических и демографических вызовов. Безусловно, противостоять перечисленным вызовам не представляется возможным без применения инновационных методов управления системой образования, проведения экспериментов в этой области, а также открытого обсуждения полученных результатов [1].

Современные информационные технологии расширили круг участников образовательного процесса, подключив к нему посредством сетевых технологий удаленных пользователей. К подобным технологиям относится электронная информационная образовательная среда, успешно функционирующая в Ростовском юридическом институте МВД России.

Электронная информационная образовательная среда (далее ИОС, среда) относится к системам массового обслуживания и в идеале требует организации периметра безопасности, позволяющего решить следующие задачи:

1. Затруднение несанкционированного доступа к среде.
2. Противодействие возможным локальным (с рабочего места пользователя среды) и сетевым информационным атакам.
3. Минимизация времени ликвидации последствий информационной атаки.

4. Исключение возможных недружественных действий со стороны разработчиков программного обеспечения (выявление программных закладок, ошибок программного кода).

Большинство перечисленных задач может быть решено путем изоляции сети передачи данных, на базе которой функционирует ИОС, от сетей общего пользования. Именно такой принцип используется во многих информационно-управляющих системах, задействованных в контуре управления стратегическими объектами во многих странах мира.

В рассматриваемом случае подобное решение представляется невозможным в силу ряда обстоятельств:

Во-первых, ИОС предназначена для повышения эффективности образовательного процесса, что само по себе предполагает активное взаимодействие всех участников процесса с образовательными ресурсами и друг с другом вне зависимости от места жительства и времени обращения.

Во-вторых, наличие широкого и динамично меняющегося состава пользователей (слушателей, профессорско-преподавательского и инженерно-технического состава) делает невозможным организацию максимально контролируемого доступа к изолированной информационной сети.

В-третьих, изолированная сеть сама по себе является структурой консервативной и самодостаточной, что не способствует эффективному внедрению новых образовательных технологий в педагогический процесс.

В-четвертых, необходимо учитывать склонность современных обучающихся к использованию мобильных устройств, постоянно подключенных к глобальной сети. Учет этого фактора, несомненно, стимулирует слушателей использовать ресурсы ИОС в процессе самостоятельного выполнения учебных заданий и подготовки к промежуточной аттестации по изучаемым дисциплинам [2].

Таким образом, возникает противоречие между необходимостью обеспечить гарантированный и свободный доступ пользователей среды к образовательным ресурсам с одной стороны и обеспечить достаточную безопасность и устойчивость ИОС с другой.

Организация безопасности информационной образовательной среды является комплексной задачей, в состав которой входит обеспечение (рис.1):

– программной безопасности (1);
– аппаратной безопасности (2);
– безопасности персонала (администратора сервера, среды) (3).

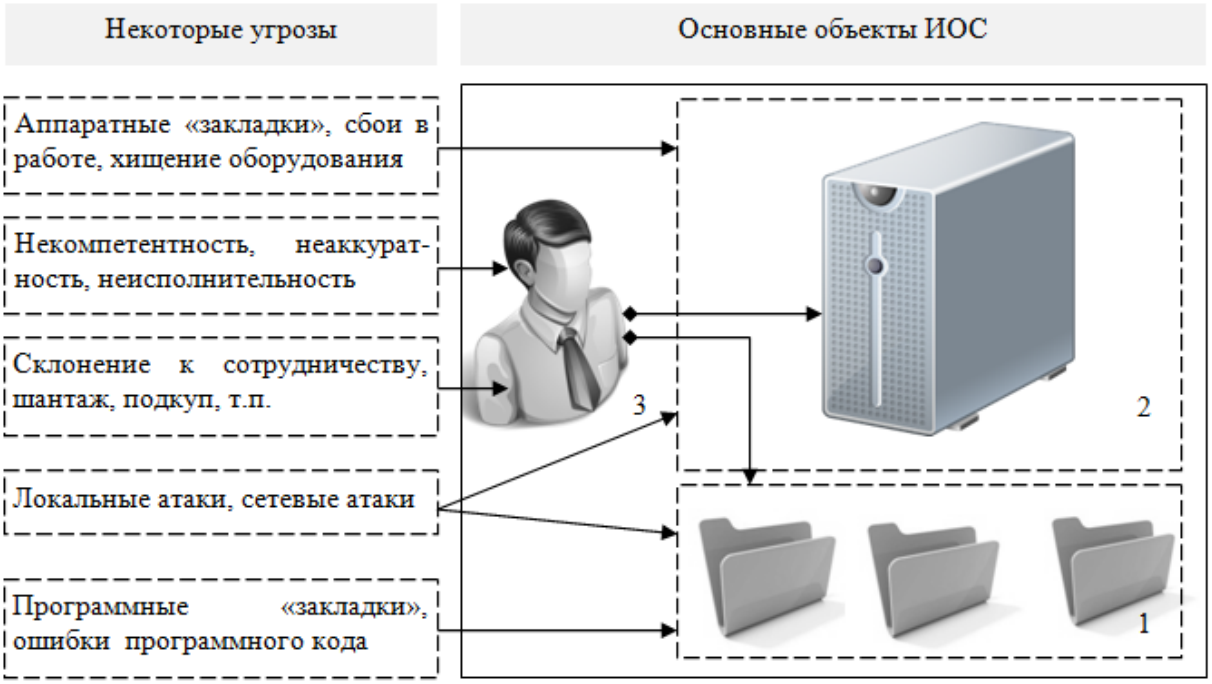



Рис. 1. Основные объекты ИОС и некоторые характерные угрозы

В идеале, если все три составляющих правильно организованы и функционируют надлежащим образом, то ИОС обладает достаточной устойчивостью и хорошим потенциалом сопротивления большинству видов информационных атак.

Рассмотрим подробнее некоторые составляющую периметра безопасности.

Программная безопасность в общем плане включает в себя как минимум, следующие составляющие:

– безопасность базовой программно-аппаратной платформы;

– безопасность программного обеспечения «сервера приложений», в котором установлена среда (как правило это связка: веб сервер + сервер баз данных + интерпретатор скриптового языка);

– безопасность скриптов (программных модулей) ИОС.

Надежность программной части подразумевает отсутствие уязвимостей, позволяющих злоумышленнику получить доступ к базе данных, файловой системе или средствам администрирования среды.

Отсутствие уязвимостей в программной части является в настоящее время скорее желанием, чем объективной реальностью. Чтобы в программной части не было уязвимостей, разработчики должны разрабатывать скрипты с оглядкой на безопасность, что выполняется не всегда. Правда жизни такова, что практически в каждом сервере приложений (веб сервере) системе управления сайтом, или в скрипте, существуют уязвимости. Часть из них выявлена и опубликована в открытом доступе (публичные уязвимости), другая не доступна широкой аудитории и используется злоумышленниками для целевых атак на сайты. Здесь острой необходимостью является своевременное обновление программного обеспечения до последней доступной версии.

В том случае, если разработка системы проводилась собственными силами, то рекомендуется выполнить сканирование доступными средствами поиска уязвимостей (XSpider'ом, Acunetix Web Vulnerability Scanner'ом, утилитами для поиска SQL инъекций, XSS, RFI и другими), проверить исходный код сайта средствами статического анализа исходного кода (RIPS) и, если обнаружатся уязвимости, исправить их [3].

Кроме того, правильное конфигурирование сервера приложений и ИОС администратором среды является зачастую решающим фактором, усиливающее им безопасность и устойчивость к информационным атакам.

Вторым важным элементом, определяющим политику безопасности ИОС в целом, является программно-аппаратная платформа, на котором размещаются программные модули среды. Обычно определяют следующие виды хостинга: «shared» («разделяемый», или «общий» для ряда сайтов) и «dedicated» («выделенный» для конкретного проекта). В первом случае ответственность за безопасную настройку сервера лежит на администраторе компании – «хостера». Для «dedicated»- сервера эта ответственность лежит на его владельце. В обоих случаях конфигурация программно-аппаратной платформы должна обеспечивать только минимально необходимую свободу действий, не нарушающих работоспособность среды. То есть на сервере должны быть разрешены только самые необходимые функции, а все остальные – запрещены. Например, если проект не выполняет внешних подключений к другим серверам, должны быть отключены опции внешних

соединений. Кроме того, должна быть ограничена область видимости файловой системы из скриптов и другое. Создание и поддержание правильной конфигурации является основной задачей системного администратора сервера. На этом сходство « shared « и « dedicated» заканчивается.

Как правило, на одном сервере «shared» размещается множество сайтов, каждому из которых требуется свой набор функций. Поэтому «хостеры» максимально лояльно подходят к вопросам настроек сервера, разрешая практически все. Это негативно сказывается на общем уровне безопасности всех сайтов, размещенных на сервере. Настройку «dedicated»-сервера обычно проводит квалифицированный системный администратор, который в 9 случаях из 10 изолирует сайт от остальной части системы, максимально ограничивая «свободу» программных модулей и область их видимости, а также организует механизмы контроля целостности файловой системы, систему резервного копирования и логгирования (ведение журнала системных событий).

Перечислим некоторые уязвимости, характерные для сетевых проектов, и поясним возможные способы борьбы с ними. Некоторые из них известны широкому кругу пользователей сети, другие не настолько явны, но от этого не менее опасны. Для большей наглядности представим результат в виде таблицы (табл.1).

Таблица 1

| Уязвимость | Описание | Способы борьбы |
|---|---|---|
| Нестойкий пароль | Заключается в использовании простых паролей (дата рождения, номер телефона) позволяет получить доступ к управлению сайтом путем перебора паролей или социальной инженерии, например, через выведывание | Использование автоматически сгенерированного пароля Использование сложных мнемонических паролей |
| Перехват пароля | Может быть осуществлен при передаче его от пользователя к серверу | Обязательное использованием защищенного соединения (https, ftps) при работе с сервером |

| | | |
|---|---|---|
| SQL injection | Позволяет злоумышленнику изменить запрос к базе данных, используя введенные данные. Пользуясь данной уязвимостью, можно выбрать из базы данные, не предусмотренные разработчиком (например, удалить какую либо таблицу или заменить тесты). | «Экранирование» данных при сборке запроса (удаление возможности обращения к базе данных напрямую из кода). Работа с БД организуется исключительно через специальную библиотеку, автоматически выполняющую необходимые преобразования. |
| Выполнение загружаемых файлов | Файлы, загружаемые на сервер, могут быть выполнены, позволяет злоумышленнику, имеющему доступ в административный интерфейс получить полный доступ к системе. | Разрешение записи только в определенные директории на сервере. Запрет выполнения скриптов в данной директории |
| Отказ в обслуживании (результат DDOS атаки) | Суть заключается в том, что на сервер идет поток запросов (flood), отчего заканчиваются ресурсы и сервер не может справиться с нагрузкой. | В зависимости от вида атаки (переполнение канала, sym-флуд, http-флуд) решения различны, например, расширение (резервирование) канала, фильтрация по портам, использование cookie, ограничение времени ожидания ответа и т.п.) |

Таким образом, при решении задачи обеспечения безопасности информационных ресурсов вузов МВД России необходимо учитывать все возможные уязвимости:

Организационные уязвимости – основа уязвимости – человеческий фактор. Подобные уязвимости нейтрализуются при помощи определенных правил работы с ресурсом или за счет специального программного обеспечения.

Уязвимости проектирования – уязвимость непосредственно программных продуктов. Эти уязвимости устраняются путем учета возможности атаки при разработке, большинство из них могут быть решены на уровне базового функционала, что позволяет минимизировать человеческий фактор.

Эксплуатационные уязвимости – атака может быть произведена на уровне сервера или инфраструктуры, данные проблемы решаются системными администраторами, либо администраторами информационного ресурса.

Развитие информационных ресурсов вузов МВД России является, на наш взгляд, необходимым этапом развития системы ведомственного образования. Цель этого этапа– расширить круг участников образовательного процесса, повысить его доступность для слушателей и профессорско-преподавательского состава, обеспечить требуемую безопасность образовательного процесса и адекватность современным требованиям, предъявляемым Министром внутренних дел и Департаментом государственной службы и кадров к образовательным учреждениям МВД России.

**Литература**

1. Гуде С.В., Карпика А.Г., Арбузов П.В. Место информационной образовательной среды в едином информационном пространстве вуза. //Сб. материалов II международной научно-практической конференции «Информационная среда и её особенности на современном этапе развития мировой цивилизации». Саратов, 2013.

2. Гуде С.В., Карпика А.Г., Арбузов П.В. Проблемы построения электронной образовательной платформы МВД России // Информационные технологии в решении служебно-боевых задач внутренними войсками МВД России и в образовательном процессе вузов внутренних войск МВД России: состояние, проблемы, перспективы: Сб. науч. статей межвузовской научно-практической конференции 25 октября 2013 года. Санкт-Петербург, 2013.

3. Безопасность сайта. Проблема и решение. //http://www.revisium.com/kb/ general_website_security.html.

# СОВРЕМЕННЫЕ ОСОБЕННОСТИ КОМПЬЮТЕРНОГО ТЕРРОРИЗМА

*Серебряник И.А., к.т.н., доцент, Иркутский государственный технический университет*
*Сизов В.П., Иркутский государственный технический университет, nasamolet@yandex.ru*

*Рассмотрены основные признаки современного компьютерного терроризма. Выделены его виды. Проанализированы методы террористических атак. Предложен ряд мер по борьбе с кибертерроризмом.*

Специалисты по безопасности отмечают, как может быть опасно отключение компьютерных систем. Оно способно привести к разорению 20% средних компаний уже в течение нескольких часов, еще 48% разорятся в течение нескольких дней. Около 33% банков будут разорены спустя несколько часов и 50% из банков разорятся спустя несколько суток. Отключение компьютерных систем сегодня, как правило, связано с кибератаками, кибертерроризмом. Слово «терроризм» происходит от лат. «terror» – страх, ужас. Терроризму свойственны культ насилия и отказ от диалога с оппонентами и целенаправленно организованный характер террористических актов, а также закрытый подпольный характер деятельности. Практически у всех террористических действий идеологизированная основа.

Современные террористы, в отличие от прежних завоевателей, стремятся «оккупировать» не землю (территорию), а волю, сознание людей.

Сам термин «кибертерроризм» появился предположительно в 1997 году. Специальный агент ФБР Марк Поллитт определил этот вид терроризма как «преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов».

Можно выделить два вида кибертерроризма:

1. совершение с помощью компьютеров и компьютерных сетей террористических действий (условно назовем это терроризмом в «чистом виде»);

2. использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов.

Способы использования террористами сети Интернет разнообразны:

1. Сбор с помощью Интернета подробной информации о предполагаемых целях, их местонахождении и характеристике.

2. Сбор денег для поддержки террористических движений. Так, например, сайт о Чеченской республике (amino.com) представляет номер счета банка в Калифорнии, на который можно перечислить средства для поддержки чеченских террористов.

3. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени и встрече людей, заинтересованных в поддержке террористов.

4. Вымогательство денег у финансовых институтов с тем, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.

5. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов.

6. Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма». С помощью Интернета можно посеять панику, ввести в заблуждение, привести к разрушению чего-либо. Всемирная сеть – благодатная почва для распространения различных слухов, в том числе и тревожных, и эти возможности сети также используются террористическими организациями.

Например, 19 декабря 1997 года по национальному телевидению Японии демонстрировался мультипликационный фильм, содержащий контаминацию цветовой гаммы, мигания визуальной

информации, от просмотра которого десятки людей получили психофизические расстройства различной тяжести

7. Вовлечение в террористические сети ничего не подозревающих соучастников – например, хакеров, которым неизвестно, к какой конечной цели приведут их действия. Кроме того, если раньше сеть террористов обычно представляла разветвленную структуру с сильным центром, то теперь это сети, где не просматривается четких командных пунктов – такую возможность предоставляет Интернет.

По оценкам экспертов министерства обороны, скоординированная атака 30 «хакеров», расположенных в различных точках земного шара, может привести к отключению электроэнергии по всей стране и парализации авиационно-диспетчерских линий.

Агентство информационных систем министерства обороны США в целях проверки провело 38 тысяч «атак» по собственным компьютерным сетям – только 4% персонала, отвечающего за них, поняли, что производится «атака», и лишь каждый 150-й сообщил в вышестоящую инстанцию о «вторжении».

Современные методы кибертеррористов сводятся к следующим:

1. «Логические бомбы» – программные закладные устройства. Их заранее «закладывают» в информационно-управляющие центры. Свою действие они начинают по определенному сигналу (в установленное время). Последствия таких «закладок» – уничтожение или искажение информации, закрытие доступа к тем или иным ресурсам;

2. Обычные компьютерные вирусы.

Например, вирус «666», по мнению медиков, вообще способен негативно воздействовать на психофизиологическое состояние оператора ПК, вплоть до его смерти. Принцип действия состоит в следующем: он выбирает на экране специально подобранную цветовую комбинацию, погружающую человека в гипнотический транс. Происходит резкое изменение деятельности сердечно-сосудистой системы и человек может погибнуть.

3. DoS-атаки, атаки вызывающие эффект, так называемого, отказа в обслуживании.

4. Средства радиоэлектронного подавления, не являются оружием, поражающим цели, но в условиях современной войны

именно их применение предшествует началу боевых операций. Это малогабаритные устройства, способные генерировать электромагнитный импульс высокой мощности, обеспечивающий вывод из строя радиоэлектронной аппаратуры, а также другие средства подавления информационного обмена в телекоммуникационных сетях.

Сегодня существует такой специфический вид терроризма, как «ядерный шантаж».

В начале 1999 года по электронной почте в адрес правительств более чем 20 стран (США, Великобритании, Израиля, Австрии и др.) были направлены сообщения от имени офицеров российской воинской части, расположенной в городе Козельске Калужской области и имеющей на вооружении стратегические ракеты шахтного базирования. В этих письмах информировалось, что командный состав части недоволен «унизительным положением России», и содержалась угроза «самовольно произвести пуски ракет по целям, расположенным в столицах и промышленных центрах западных стран». Кроме того, анонимы традиционно требовали выплаты крупной денежной суммы. В этой связи правительства ряда ведущих стран выразили МИД России серьезную обеспокоенность случившимся и попросили оказать содействие в розыске вымогателей. В результате проведенной ФСБ России расследования преступники были задержаны. Ими оказались два жителя Калуги, не являющиеся военнослужащими.

«Кибертерроризм», предполагает проникновение в компьютерные системы, а космический терроризм – через создание помех для искусственных спутников Земли и их уничтожение, захват космических аппаратов; пиратские нападения на морские суда и т.д.

Примером кибертерроризма может служить занесение в сентябре 2010 г. «червя» в локальную компьютерную систему атомной электростанции в Ирана в г. Бушер, передающего информацию о состоянии станции.

Первоочередными мероприятиями в борьбе с кибертерроризмом можно назвать

1. объединение усилий государств – членов международного сообщества в области обеспечения информационной безопасно-

сти, закрепление совпадающих интересов и совместное проведение мероприятий по их защите преимущественно на основе двухсторонних и многосторонних договоров;

2. создание базового понятийного аппарата – необходимо договориться о единой трактовке терминов, используемых в данной области. Необходимо стремиться к гармонизации национальных законодательств в части борьбы с информационным терроризмом. Эта проблема существенно затрагивает национальные интересы (например, в США законодательно ограничен обмен информацией между частными корпорациями о компьютерных атаках, что не позволяет использовать опыт друг друга);

3. использование потенциала хакерского сообщества, т.е. людей с ярко выраженным увлечением к познанию в области информационных технологий, выходящим за рамки познавательной и учебной деятельности, в антитеррористических целях;

4. разработка системы мер по мониторингу и контролю за распространением знаний и технологий, критичных с точки зрения информационной безопасности. Один из основных ресурсов, требующих мониторинга – это высококвалифицированные специалисты, обладающие знаниями в области высоконадежных методов защиты информации. Именно они являются объектом интереса международных террористических организаций;

5. содействие каждого пользователя (организации всех секторов экономики, образовательные учреждения, граждане – пользователи Интернет и др.) обеспечению информационной безопасности на том участке киберпространства, которым он владеет или пользуется.

**Литература**

Томчак Е. В. Из истории компьютерного терроризма // Новая и новейшая история. – 2007. – N 1. – С. 134-148

# ИДЕНТИФИКАЦИЯ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ДАННЫХ

*Федорова С.В., к.т.н., доцент, Иркутский государственный технический университет, fsta@istu.irk.ru*
*Миронова И.В., Иркутский государственный технический университет advocat_inna@mail.ru*

*Биометрия предполагает систему распознавания людей по одной или более физических или поведенческих черт. В области информационных технологий биометрические данные используются в качестве формы управления идентификаторами доступа и контроля доступа. Также биометрический анализ используется для выявления людей, которые находятся под наблюдением (широко распространено в США, а также в России — отпечатки пальцев).*

Наиболее распространенные методы идентификации пользователей (например, цифровые сертификаты и смарт-карты) предлагают использование паролей. Однако эта методика не безупречна. Надежный пароль – это тот, который трудно разгадать. С другой стороны, его нелегко и запомнить. Пароль удобен при условии, что вы пользуетесь очень небольшим количеством устройств, доступ к которым осуществляется по паролю. Однако с каждым днем становится все больше устройств, предполагающих электронную форму доступа, и в голове приходится держать около десятка паролей и PIN-кодов. Вот лишь несколько примеров: мобильный телефон, банковский счет, электронная почта, компьютер, Internet-магазины. Каждый из перечисленных видов сервиса требует ввода паролей, подтверждающих вашу личность. Чтобы решить проблему с их запоминанием, предлагается надежный метод аутентификации, основанный на биометрии.

Биометрическая идентификация – это средство автоматического опознавания личности на базе уникальных физических или поведенческих параметров. Каждому из нас присущи определенные уникальные и неизменные признаки, такие, как отпечатки пальцев, цвет и разрез глаз, или манера выполнения каких-либо

действий, в частности речь и почерк. Такие признаки достаточно сложно воспроизвести и подделать и в то же время их всегда легко «предъявить», за исключением разве что ситуаций с переломом руки, когда вы не в состоянии писать. К средствам биометрического контроля относят анализ отпечатков пальцев, сканирование сетчатки и радужной оболочки глаза, анализ почерка. Перспективными направлениями в этой области признано также распознавание по голосу и отпечаткам руки. Самой надёжной и точной методикой является сканирование сетчатки человеческого глаза. Сетчатка пронизана кровеносными сосудами, переходящими в малые вены и артерии. Их рисунок – уникальный в своём роде и с возрастом меняется незначительно. Впрочем, при тяжёлых заболеваниях и травмах, могут происходить его изменения, препятствующие распознаванию. Инфракрасный лазер отражается сосудами глазного дна. Человек должен находиться не дальше чем на расстоянии 1,5 см. от камеры и не двигаться. При этом воспринимается более 400 характерных точек. Для сравнения: при съёмке отпечатков пальцев их количество колеблется между 30 и 40. В противовес сканированию сетчатки, распознавание зрачка не требует лазерной техники. Избыточное освещение может вызвать его сужение и затруднить обследование. Поэтому часто работают с искусственным источником освещения. Распознавание базируется на значительных признаках на зрачке, типа кругов, канавок, пятен сосудиков или завитушек. И только некоторые насчитывают ровно 200 атрибутов. Самый известный биометрический способ – снятие отпечатков пальцев. Так называемый «Минутный метод» позволяет сравнивать отпечатки на основе 7 признаков, отражающих рисунок линий, их ширину и глубину, узелки и т.п. Широко распространён тепловой метод, при котором измеряется электростатическое напряжение канавок пальцев разной глубины. Компания Asustek выпустила Notebook B1000 Series с защитой на базе отпечатков пальцев. Многочисленные дискуссии ведутся вокруг распознавания лица. На сегодняшний день существуют следующие методы распознавания:

во-первых, возможна идентификация по таким характеристикам лица, как расстояние между глазами, изгиб губ и т.д. Замеряется всего 80 атрибутов и помещается в файл размером 1 Kb, потом

в соответствии с определённым алгоритмом проводится поиск по базе. Вероятность ошибки сравнительно велика.

во-вторых, за счет измерения теплоотдачи различных частей лица.

в-третьих – по методу “Eigen Face”. Человека фотографируют с разными выражениями лица в двумерном варианте, потом сопоставляют снимки и выявляют характерные признаки. Эти показатели у всех людей разные.

в-четвёртых, по характерным признакам в виде отдельных объёмных блоков скелета лица. Их всего 8, причём волосы, очки, парик не оказывают на идентификацию никакого влияния. Такая методика используется в системе “Face It” аэропорта Newham Keflavik.

Хорошие результаты дает и распознавание голоса. В этом методе отдельно анализируют язык и отдельно голос. В первом случае распознается произносимая фраза или слово, в втором сам человек. Посредством предопределённых коротких фраз выясняется тональность, скорость речи, расстановка пауз, ударения. Сильное влияние может оказывать фоновый шум. Как биометрический признак можно рассматривать и подпись. Человек подписывается при помощи графической таблетки или специальных карандашей.

Рассматриваются такие характеристики как почерк, скорость письма, сила нажима при письме. Распознавание почерка требуют крайне сложных алгоритмов и больших затрат, равно как и оборудования touch-screen. Итак, как мы видим, любой, даже самый точный из методов идентификации личности, несовершенен или требует больших финансовых затрат. Поэтому ученые стараются производить комплексный анализ по нескольким биометрическим признакам.

**Литература**

Эймор Д. Электронный бизнес. Эволюция и/или революция. – Москва-СПб-Киев, Издательский дом «Вильямс», 2001.

# ПРИМЕНЕНИЕ ГРАДИЕНТНЫХ МЕТОДОВ ВЫДЕЛЕНИЯ ГРАНИЦ ДЛЯ РАСПОЗНАВАНИЯ ЛИЦ

*Мартьянова А.В., Уральский федеральный университет, Институт радиоэлектроники и информационных технологий – РТФ, kurzinaav@gmail.com*

*Представлен сравнительный анализ градиентных методов выделения границ. Представлены результаты обработки тестового изображения данными методами.*

Методы выделения границ для распознавания лиц являются актуальным предметом исследования и находят свое применение в большом количестве систем распознавания лиц (ASID, FaceID, Trueface, Vissage Gallery, FaceIt и др.). Выделение границ для распознавания лиц требуется для идентификации персоны по лицу.

Рассматриваемые алгоритмы выделения границ могут быть применены для идентификации террористов, преступников. Также они могут быть применены для идентификации допущенных лиц на охраняемую территорию.

Существует ряд негативных факторов, затрудняющих успешное выделение границ при распознавании лиц. Во-первых, это низкое качество изображения: расфокусировка, шум, недостаточная контрастность. Во-вторых, это специфичные для решения данной задачи помехи, эмоциональные искажения, поворот головы, тени на лице, погодные условия съемки т.п. Таким образом, возникает проблема оценки качества методов выделения границ и выявления эффективных, устойчивый к условиям съемки и качеству имеющегося изображения.

## Исследования градиентных методов выделения границ

Важнейшей целью цифровой обработки изображений является распознавание присутствующих на них объектов. Возможность различать объекты заложена в высокой информативности изображения [2]. Градиентные методы основаны на выделении краевых точек и малочувствительны к шумам и контрастности изображения, но требуют применения алгоритма объединения граничных точек, что не гарантирует замкнутости контуров.

Данные методы основываются на свойстве сигнала яркости – разрывности. Эффективным способом поиска разрывов является обработка изображения с помощью скользящей маски – пространственная фильтрация.

В ходе данной фильтрации маска фильтра перемещается от пикселя к пикселю. В каждой точке *(x, y)* отклик фильтра вычисляется с использованием предварительно заданных связей. В случае линейной пространственной фильтрации маской размера 3×3 отклик *R* линейной фильтрации в точке *(x, y)* изображения составит:

$$R = w(-1,-1)f(x-1,y-1) + w(-1,0)f(x-1,y) + ... + w(0,0)f(x,y) + ... \\ + w(1,0)f(x+1,y) + w(1,1)f(x+1,y+1). \quad (1)$$

Для обнаружения перепадов яркости используются дискретные аналоги производных первого и второго порядков.

Первая и вторая производная одномерной функции[1] *f(x)* определяются как представлено в формулах 2 и 3.

$$\frac{\partial f}{\partial x} = f(x+1) - f(x). \quad (2)$$

$$\frac{\partial^2 f}{\partial x^2} = f(x+1) + f(x-1) - 2f(x). \quad (3)$$

По определению, градиент изображения *f(x, y)* в точке *(x, y)* – это вектор:

$$\nabla f = \begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \end{bmatrix}. \quad (4)$$

Рассмотренные ниже маски применяются для получения составляющих градиента $G_x$ и $G_y$. Для определения величины градиента эти составляющие необходимо использовать совместно:

$$f = \sqrt{G_x^2 + G_y^2}. \quad (5)$$

В качестве масок для определения составляющих градиента используются операторы Робертса, Превитта, Собеля и Щарра окрестностью 3×3 (рисунки 1-2).

| | | |
|---|---|---|
| z1 | z2 | z3 |
| z4 | z5 | z6 |
| z7 | z8 | z9 |

Рис. 1. Окрестность 3x3 внутри изображения

[1] Для простоты изложения рассмотрены одномерные производные.

| | | |
|---|---|---|
| 0 | 0 | 0 |
| 0 | -1 | 0 |
| 0 | 0 | 1 |

| | | |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 0 | -1 |
| 0 | 1 | 0 |

а)

| | | |
|---|---|---|
| -1 | -1 | -1 |
| 0 | 0 | 0 |
| 1 | 1 | 1 |

| | | |
|---|---|---|
| -1 | 0 | 1 |
| -1 | 0 | 1 |
| -1 | 0 | 1 |

б)

| | | |
|---|---|---|
| -1 | -2 | -1 |
| 0 | 0 | 0 |
| 1 | 2 | 1 |

| | | |
|---|---|---|
| -1 | 0 | 1 |
| -2 | 0 | 2 |
| -1 | 0 | 1 |

в)

| | | |
|---|---|---|
| -3 | -10 | -3 |
| 0 | 0 | 0 |
| 3 | 10 | 3 |

| | | |
|---|---|---|
| -3 | 0 | 3 |
| -10 | 0 | 10 |
| -3 | 0 | 3 |

г)

Рис. 2 Операторы а) Робертса, б) Превитта, в) Собеля, г) Щарра[3]

Для решения вопроса инвариантности в отношении поворота используются так называемые диагональные маски, предназначенные для обнаружения разрывов в диагональных направлениях (рис. 3–5).

| | | |
|---|---|---|
| 0 | 1 | 1 |
| -1 | 0 | 1 |
| -1 | -1 | 0 |

| | | |
|---|---|---|
| -1 | -1 | 0 |
| -1 | 0 | 1 |
| 0 | 1 | 1 |

Рис. 3 Диагональные маски Превитта

| | | |
|---|---|---|
| 0 | 1 | 2 |
| -1 | 0 | 1 |
| -2 | -1 | 0 |

| | | |
|---|---|---|
| -2 | -1 | 0 |
| -1 | 0 | 1 |
| 0 | 1 | 2 |

Рис. 4 Диагональные маски Собеля

| | | |
|---|---|---|
| 0 | 3 | 10 |
| -3 | 0 | 3 |
| -10 | -3 | 0 |

| | | |
|---|---|---|
| -10 | -3 | 0 |
| -3 | 0 | 3 |
| 0 | 3 | 10 |

Рис. 5 Диагональные маски Щарра

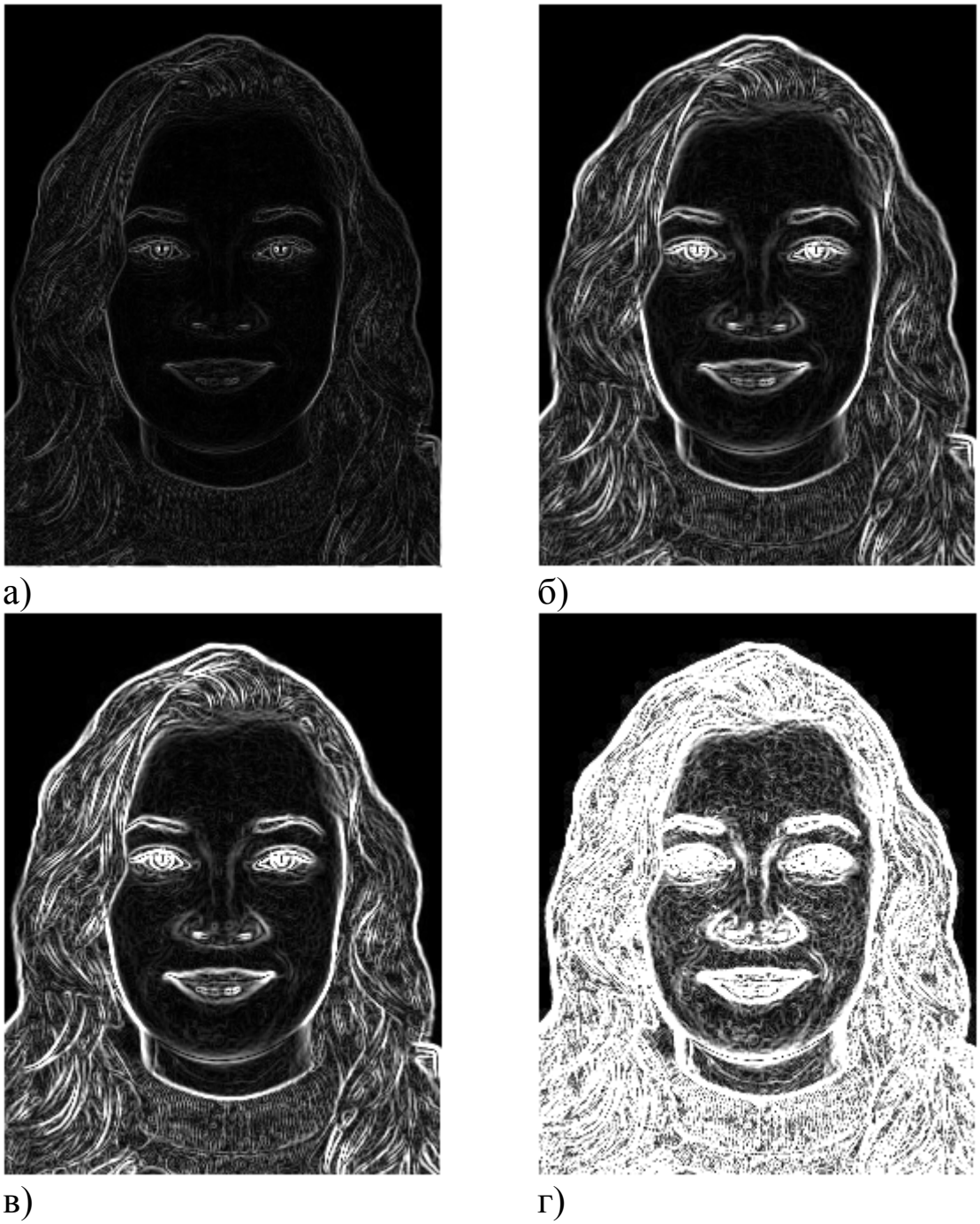
Для каждой из описанных выше масок характерны свои особенности. Результат обработки изображения (рис. 6) представлен на рис. 7. При исследованиях использовались программные реализации каждого из приведенных методов, которые показали свою надежность и правильность на протяжении большого количества времени. Тестовое изображение было выбрано случайным образом.

Рис. 6. Тестовое изображение

Применение градиентных операторов выделения границ для выявления черт лица позволяет сделать следующие выводы. Оператор Робертса (рисунок 7, а) выделяет сравнительно тонкие контурные линии, но черты лица прослеживаются, а именно глаза, брови, рот, а также волосы, но практически не оконтурен нос, подбородок и лоб. Из чего следует что данный оператор не всегда эффективен при решении поставленной задачи. Высокоядерный оператор Щарра (рисунок 7, г) выделяет излишнее количество границ, сливающихся между собой, поэтому малоэффективен в решении поставленной задачи. Операторы Превитта (рисунок 7, б) и Собеля (рисунок 7, в) наилучшим образом определяют границы лица, явно выражены глаза, брови, рот, волосы, нос, подбородок, лоб, т.е. все черты лица. Данные операторы эффективны при решении задачи выделения границ.

Рассмотренные методы применяются в различных прикладных задачах. Обработка черт лица имеет свою специфику: это и форма объектов на снимках, и повышенное внимание к замкнутости контуров, а также неизбежность влияния искажающих факторов таких, как шумы, расфокусировка и прочие артефакты изображений. Для того, чтобы максимально точно определить границы лица на изображении необходимо выбрать наиболее оптимальный для этого метод выделения границ. Также необходимо определить

оптимальные условия работы выбранного алгоритма на основе экспертной и статистической оценки.



а) б) в) г)

Рис. 7. Применение градиентных методов выделения границ

**Литература**

1. Detyniecki M., *Mathematical Aggregation Operators and their Application to Video Querying*. Universite Curie. November 2000.

2. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2005. 1072с.

# КАК СОВРЕМЕННЫЕ ТЕРРОРИСТЫ ИСПОЛЬЗУЮТ ИНТЕРНЕТ

*Васенин А.Ю., Новороссийский филиал Краснодарского университета МВД России;*
*Денисов С.Л., Новороссийский филиал Краснодарского университета МВД России*

История террористических групп в киберпространстве началась совсем недавно. В 1998 году около половины из тридцати террористических организаций, внесенных США в список «Иностранных террористических организаций» имели Web-сайты, к 2000 году практически все террористические группы обнаружили свое присутствие в сети Интернет.

Исследование глобальной сети в 2003 – 2004 г.г. обнаружило сотни сайтов, обслуживающих террористов и их сторонников. И все же, несмотря на все растущее присутствие террористов в сети Интернет, чиновники, журналисты и ученые при обсуждении комбинации терроризма и Интернета сосредоточились на переоцененной угрозе, названной кибертерроризмом или кибервойной (атаки на компьютерные сети, включая Интернет). При этом многочисленные случаи ежедневного использования сети Интернет террористами в большинстве своем игнорировались.

По своей природе Интернет во многих отношениях – идеальное поле деятельности террористических организаций. Особенно это касается предлагаемых глобальной сетью:

- свободного доступа
- небольшие регулирование, цензура и другие формы государственного контроля или вовсе их отсутствие
- потенциально огромная аудитория во всем мире
- анонимность связи
- быстрое движение информации
- невысокая стоимость создания сайта и обслуживания присутствия в сети
- мультимедийная среда: возможность комбинировать текст, графику, аудио и видео, возможность для пользователей загружать фильмы, песни, книги, постеры и т.д.

- возможность охватить также аудиторию традиционных СМИ, которые все чаще используют Интернет как источник сообщений.

Указанные преимущества не остались незамеченными террористическими организациями, независимо от их политической ориентации. На сегодняшний день почти все активные террористические организации имеют веб-сайты.

Как показывает следующий список, эти организации находятся в разных точках земного шара:

- Ближний Восток
- Европа
- Латинская Америка
- Азия: «Хамас» , ливанская «Хезболла» , бригады мучеников Аль Аксы, Фатах Танзим, Народный фронт освобождения Палестины, Палестинский исламский джихад, «Кахане чаи», «Моджахединэ Кхальк», Рабочая партия Курдистана, турецкая Революционная партия-фронт освобождения народа, «Восточный исламский фронт наступления»; Ирландская республиканская армия, Родина и свобода басков, Корсиканская армия; Тупак Амару (Перу), «Сияющий путь», колумбийская Национальная освободительная армия и Революционные вооруженные силы Колумбии; Аль-Каида, Аум Синрикё, Ансар аль Ислам в Ираке, Японская красная армия, Харакат аль – Муджахиддин.

Как правило, сайт содержит информацию об истории организации и ее действиях, детальный обзор ее социальных и политических истоков, отчет о наиболее заметных делах, биографии лидеров, основателей и героев, сведения о политических и идеологических целях, жесткую критику врагов, и текущие новости. Националистические и сепаратистские часто демонстрируют карты спорных областей. Несмотря на постоянное употребление слов «вооруженная борьба» и «сопротивление», то чего создатели сайта не делают – это детальной описание их насильственных действий. Даже если подробно разъясняется моральное и юридическое обоснование использования насилия, большинство сайтов воздерживается от описания насильственных действий террористов и их фатальных последствий. Эта немногословность вероятно обусловлена пропагандистскими и направленными на создание имиджа целями. Из этого правила есть два исключения: Хезболла и Хамас,

на сайтах которых постоянно обновляются отчеты об их действиях («ежедневные действия») и количестве «мертвых мучеников» и убитых «израильских врагов» и «сотрудников».

Террористические сайты используют лозунги и выставляют на продажу изделия, такие как значки, футболки, флаги, видеозаписи, аудиокассеты – вся эта продукция, очевидно, рассчитана на сочувствующих. Часто организация, заинтересованная в локальной поддержке в какой-либо местности, создает сайт на соответствующем языке, располагая на нем детальную информацию о действиях и внутренней политике организации, ее союзниках и врагах. На международную аудиторию, непосредственно не вовлеченную в конфликт, но в некоторой степени заинтересованную в проблеме, нацелены сайты на иных, кроме местного, языках. Большинство сайтов имеют версии на нескольких языках. Сайт баскского движения, например, содержит информацию на кастильском языке, а также немецком, французском и итальянском. Сайт организации Тупак Амару в дополнение к английской и испанской версии предлагает японскую и итальянскую, сайт Исламского движения Узбекистана использует арабский, английский и русский языки. Для удобства иностранных посетителей сайты представляют основную информацию об организации с множеством второстепенных исторических обзорных материалов . Судя по содержанию многих сайтов, в потенциальную аудиторию включены также иностранные журналисты. Для озвучивания позиции организации в традиционных СМИ используются пресс-релизы на сайтах. Детальная второстепенная информация очень полезна для международных корреспондентов. Один из сайтов Хезболла прямо обращается к журналистам, приглашая к сотрудничеству через электронную почту пресс-центра организации. Усилия по достижению аудитории «врага» (т.е. граждан государств, против которых борются террористы) не столь очевидно вытекают из содержания многих сайтов. Однако, некоторые сайты, как кажется, направляют усилия на деморализации противника, угрожая нападением и создавая чувство вины за мотивы и поведение неприятеля.

Терроризм часто называют одной из форм психологической войны, и, конечно, террористы стремятся вести такую кампанию через Интернет. Для этого у террористов есть несколько путей. Например, они могут использовать Интернет для дезинформации,

распространения угроз, направленных на то, чтобы посеять страх и ощущение беспомощности, распространять ужасающие изображения своих действий как, например, видеозапись убийства американского журналиста Дэниэла Перла лицами, захватившими его в плен, которая распространялась через несколько веб-сайтов. Террористы могут также начать психологические атаки посредством кибертерроризма, а точнее, создания опасений угрозы совершения таких действий. «Киберстрах» возникает из беспокойства об угрозе компьютерных нападений , которое усиливается настолько, что общество начинает верить, что атака случится. Интернет – среда, не подверженная цензуре, которая распространяет информацию, изображения, угрозы или сообщения независимо от их законности или потенциального воздействия – это идеально подходит даже небольшой группе лиц, чтобы усилить воздействие от передаваемой ей информации и преувеличить опасность угрозы, которую сведения несут.

Аль-Каида комбинирует мультимедиа – пропаганду и передовые технологии связи, чтобы создать сложную модель ведения психологической войны. Несмотря на постоянные преследования в последние годы подверглась эта организация: аресты и смерть многих членов, разрушение ее операционных баз и тренировочных лагерей в Афганистане – Аль-Каида способна провести кампанию по внушению паники.

Интернет значительно расширил возможности террористов по преданию гласности их деятельности. До появления Интернета надежды террористов на огласку своих действий зависели от привлечения внимания телевидения, радио или печатных СМИ. Эти традиционные СМИ имеют многоступенчатую систему редакционного отбора, в результате террористы могут не достичь своей цели. И, конечно, подобных препятствий не существует на собственных веб-сайтах террористов. То, что многие террористические организации имеют непосредственный контроль над содержанием своих сообщений, предлагает возможности для подачи информации таким образом, чтобы она воспринималась различными группами потенциальной аудитории и манипулировать своим образом и образом врага.

Как уже говорилось ранее, террористические сайты в большинстве своем не восславляют свои насильственные действия.

Вместо этого, независимо от программы террористов, мотивов и местоположения, большинство сайтов подчеркивает две проблемы: ограничения на свободу выражения своего мнения и тяжелое положение товарищей, являющихся политическими заключенными. Эти проблемы находят мощный отклик среди их сторонников и рассчитаны также на то, чтобы вызвать симпатию у западной аудитории, лелеющей свободу выражения мнения и неодобрительно относящейся к действиям, направленным на то, чтобы заставить замолчать политическую оппозицию. Аудитория противника также может быть целью этих жалоб, поскольку террористы, подчеркивая антидемократический характер предпринимаемых против них действий, пытаются создать чувство неловкости и стыда в среде противника.

Террористические сайты обычно используют три риторических конструкции для оправдания необходимости использования насилия. Первая: заявление о том, что террористы не имеют никакого выбора, кроме как обратиться к насилию. Насилие представляется потребностью, навязанной слабому как единственное средство ответа применяющему репрессии врагу. В то время как сайты забывают упомянуть о том, как террористы преследуют людей, силовые акции государства или режима, преследующего террористов, постоянно подчеркиваются и освещаются с такими характеристиками, как «кровопролитие», «убийство», геноцид». Террористическая организация изображается как постоянно преследуемая: ее лидеры подвергаются попыткам убийства, последователи избиваются, свобода выражения ограничена, последователи арестовываются. Эта тактика, изображающая организацию маленькой, слабой и преследуемой мощью сильного государства, превращает террористов в слабую сторону.

Вторая риторическая конструкция, связанная с оправданием применения насилия, – демонизация и делегитимизация врага. Члены движения или организации представляются борцами за свободу, использующими насилие против их желания, потому что безжалостный враг ущемляет права и достоинство людей. Враг движения или организации – настоящий террорист, множество сайтов настаивают: «Наше насилие ничтожно по сравнению с его агрессией». Это наиболее общий аргумент. Террористическая риторика перекладывает ответственность за насилие с террористов

на противника, который обвиняется в демонстрации зверства, жестокости и безнравственности.

Третий риторический прием – многочисленные заявления о ненасильственных действиях в противопоставление сложившемуся образу террористов. Несмотря на то, что они являются сильными организациями, многие сайты утверждают, что их группы находятся в поиске мирных решений, что их окончательной целью является дипломатическое урегулирование, достигнутое посредством переговоров и международного давления на репрессивное правительство.

Террористы используют Интернет не только для того, чтобы узнать, как создавать взрывные устройства, но и для того, чтобы планировать и координировать определенные нападения. Активисты Хамаса на Ближнем Востоке используют чат-румы для планирования действий и электронную почту для обмена информацией между активистами и координации действий между Сектором Газа, Западным берегом реки Иордан, Ливаном и Израилем. Инструкции в форме карт, фотографий, руководств, технических инструкций по использованию взрывчатых веществ маскируются посредством стенографии, сообщения скрываются внутри графических файлов. Однако иногда инструкции поступают в зашифрованном самыми простыми шифрами виде.

На брифинге в конце сентября 2001 года Рональд Дик, помощник главы ФБР, сообщил журналистам, что террористы 9/11 использовали Интернет и «использовали успешно». С тех пор террористы только совершенствуют свои навыки и увеличивают свое присутствие в глобальной сети. Сегодня террористы различных идеологических течений – исламисты, марксисты, националисты, сепаратисты, расисты получили много уроков максимального использования Интернет. Большие достоинства Интернета – легкость доступа, минимум регулирования, огромная потенциальная аудитория, быстрый поток информации и пр. – были поставлены на службу группами, использующими для достижения своих целей террористические методы.

Как должно ответить общество? Сначала необходимо стать более информированными о способах использования террористами Интернета и более приспособленными для контроля за их действиями. Как уже отмечалось в начале журналистов, ученых,

высших должностных лиц и даже правоохранительные органы больше интересовала проблема кибертерроризма, являющаяся преувеличенной угрозой, из-за чего недостаточное внимание уделялось обычному использованию террористами Интернета. Эти случаи использования многочисленны, и, с точки зрения террористов, неоценимы. Следовательно, правоохранительным органам необходимо продолжить изучение и контроль террористических действий в Интернете, а также поиск мер по ограничению использования этой среды современными террористами.

Во-вторых, в то же время не должны в процессе защиты нашего общества от терроризма, разрушать те качества и ценности нашего общества, которые мы защищаем. Интернет является почти воплощением демократических идеалов свободы слова и связи. Это рынок идей, какого раньше не было. К сожалению, как показывает практика свобода, предлагаемая Интернетом, уязвима к злоупотреблениям со стороны групп, которые, как это ни парадоксально, зачастую сами враждебны к выражениям мысли, не прошедшим цензуру. Использование передовых методов для контроля, поиска, отслеживания и анализа коммуникаций неотъемлемо несет с собой опасности. Хотя такие технологии могут оказаться очень полезными в борьбе с кибертерроризмом и использованием террористами Интернета, они вручают авторитарным режимам инструменты нарушения гражданских прав и свобод внутри страны.

## ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ В СОВРЕМЕННОМ МИРЕ

*Томашевич Е.А., Санкт-Петербургский университет МВД России, kate_karina@inbox.ru*
*Шалагинова О. Б., к.ф-.м.н., доцент, Санкт-Петербургский университет МВД России, shans331@yandex.ru*

*В наше время появилось очень много специальной техники, с помощью которой можно разными способами влиять на людей и следить за ними. Например, когда человек разговаривает по телефону, то можно услышать то, о чем он говорит, прослушивая и*

*записывая нужную информацию. В данной работе рассказ о методах защиты информации от экстремизма и терроризма в настоящее время.*

Терроризм – это криминальное явление, обусловленное внутренними, внешними противоречиями общественного развития различных стран. Терроризм представляет собой угрозу для жизненно важных интересов личности, общества и государства.

В настоящее время для террористов легко уязвимы практически все компьютерные средства обработки и хранения информации. Банковские, биржевые, архивные, исследовательские, управленческие системы, Интернет, средства коммуникации от спутников до мобильных телефонов, электронные средства массовой информации, издательские комплексы, всевозможные базы персональных данных – все это может атаковаться при соответствующей квалификации террориста с одного единственного компьютера. Мировые тенденции таковы, что информационный терроризм будет нацелен на мировую экономику. Методы информационного терроризма ориентированы не на физическое уничтожение людей и ликвидацию материальных ценностей, не на разрушение важных стратегических и экономических объектов, а на широкомасштабное нарушение работы финансовых и коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и навязывание властным структурам своей воли [1].

Деньги – капитал вчерашнего дня, информация – сегодняшнего и завтрашнего. Например, Швейцария может претендовать на финансовое господство, но информационное обслуживание 80% банков этой страны находится в США. Вследствие этого компьютер сегодня становится самым многообещающим орудием преступности. Деловые центры обработки коммерческой информации и, прежде всего, компьютеризированные банковские учреждения являются самой доступной и заманчивой целью для терроризма. Террористический информационный удар по крупному банку способен вызвать системный кризис всей финансовой системы любой развитой страны, так как лишает общество доверия к современным технологиям денежного рынка. Продуманная кампания дезинформации, сопровождающая такой террористический акт, способна спровоцировать системный кризис. Опасность информационного

терроризма неизмеримо возрастает в условиях глобализации, когда средства телекоммуникаций приобретают исключительную роль. Тревожные перспективы для развития информационного терроризма появились в связи с взрывным развитием сети Интернет, массовым и быстрым переходом банков, финансовых и торговых компаний на компьютерные операции с использованием разветвленных по всему миру электронных сетей. В поле зрения террористов оказались секретная информация, аппаратура контроля над космическими аппаратами, ядерными электростанциями, военным комплексом. Успешная атака на такие компьютеры может заменить целую армию. Очевидно, что заинтересованные структуры ведут непрерывный поиск вариантов, появляются новые средства нападения, оружие кибертеррористов постоянно модифицируется в зависимости от средств защиты, применяемых пользователями компьютерных сетей. Основой обеспечения эффективной борьбы с кибертерроризмом является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению такого рода деятельности. Для борьбы с терроризмом во всех его проявлениях работают различные антитеррористические органы. Особое внимание борьбе с терроризмом уделяют развитые страны мира, считая его едва ли не главной опасностью для общества. Но полностью обезопасить общество от террористов невозможно, можно лишь снизить угрозу превентивным контролем за «интересными» для террористов местами и борьбой с непосредственными исполнителями террористических актов. Задача состоит в том, чтобы сузить варианты действий террористов и контролировать те, что останутся. Но тотальная слежка за всеми – это нарушение прав человека. Например, правоохранительные органы России основные надежды в борьбе с компьютерными преступниками возлагают на установку подслушивающих устройств в Интернете, с помощью которых можно просматривать сообщения, присылаемые по электронной почте, и отслеживать обращения пользователей к страничкам Интернета. Создаваемая система СОРМ (полное название примерно «Система облегчения расследования материалов») предназначена в основном для выявления тех, кто уклоняется от уплаты налогов и других нарушителей, од-

нако, по мнению противников ее внедрения, она будет равносильна всеобъемлющему подслушиванию, что будет нарушать конституционные права законопослушных граждан.

Перейдем к понятию экстремизма. Экстремизм, это – приверженность к крайним взглядам, мерам. Среди таких мер можно отметить провокацию беспорядков, террористические акции, методы партизанской войны. Наиболее радикально настроенные экстремисты часто отрицают в принципе какие-либо компромиссы, переговоры, соглашения [2].

Таким образом, для борьбы с терроризмом в сетях следует выделить две стратегии национальной информационной безопасности:

- создание специальных структур, которые будут пресекать противоправные действия террористов;

- создание специальных программ, которые не будут давать возможность взламывания той или иной информации.

Среди новых инструментов борьбы с рассматриваемым явлением можно отметить появление Единого реестра Интернет-ресурсов, содержащих запрещенную информацию, который позволяет осуществлять блокирование доступа к такой информации. В тоже время, отраслевая разрозненность содержащихся в различных законах правовых средств, отсутствие их связи между собой, а также достаточно слабая регламентация аспектов борьбы с использованием Интернета в экстремистских и террористических целях в базовых законах о противодействии экстремизму и терроризму значительно ослабляет потенциал воздействия действующего законодательства. Негативным фактором остается отсутствие комплексного правового регулирования отношений, связанных с использованием сети Интернет, которое бы четко определило правовой статус их участников, включая вопросы юридической ответственности за распространение запрещенной информации [3].

**Литература**

1. http://www.bestreferat.ru/referat-406097.html
2. http://ru.wikipedia.org/wiki
3. http://sartraccc.ru/print.php?print_file=Pub/sundiev(25-07-13).htm

# ОБЗОР УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДОВ ИХ НЕЙТРАЛИЗАЦИИ

*Кузнецов А.С., Орловский Юридический институт МВД России имени В.В. Лукьянова, kuznetsov_as@bk.ru*

*Разработка и использование информационных систем требует обеспечения высокого уровня их информационной безопасности. В статье рассмотрены виды информационных угроз характерные для информационных систем построенных по технологии веб-приложений, а также способы их нейтрализации.*

Использование тонких клиентов и фактическое отсутствие клиентского программного обеспечения на рабочих местах позволяет значительно повысить уровень информационной безопасности информационных систем за счет невозможности проведения реверс-инженеринга и установления структуры запросов к основной БД. Перенос классических клиент-серверных приложений в плоскость веб-приложений с возможностями осуществлять необходимые операции по доступу и управлению массивами данных позволяет классифицировать угрозы информационной безопасности в основном, исходя из возможностей построения злоумышленником запросов к серверу с клиентской стороны.

Существуют несколько видов уязвимостей информационных систем:

1. Уязвимости в аутентификации.
2. Уязвимости в авторизации.
3. Атаки на клиентов.
4. Выполнение вредоносного кода.

*Уязвимости в аутентификации*

Атаки, отнесенные к данному разделу направлены на методы проверки идентификатора клиента сервером. Их можно разделить на несколько больших групп: подбор аутентификационных данных клиента, «недостаточная аутентификация» и небезопасный механизм восстановления паролей.

Подбор аутентификационных данных пользователя является довольно простой реализуемой на практике атакой на информационную систему. Сущность его заключается в последовательном

переборе паролей по известному логину или логина по известному паролю. Защита информационных систем от таких атак реализуется путем ведения парольной политики, то есть наложения жестких ограничений на минимальное количество знаков в пароле, обязательному присутствию строчных и прописных букв, цифр и т.д. Помимо парольной политики в системе аутентификации должен быть заложен механизм ограничения большого количества неправильных вводов пароля, фильтрации таких клиентов по ip-адресам и применении CAPTCHA для исключения автоматизированного подбора паролей с помощью специального программного обеспечения.

Группа атак, связанных с так называемой «недостаточной аутентификацией» использует просчеты администраторов ИС в вопросах назначения прав на доступ/изменение определенных данных, то есть, например, предоставление возможностей редактирования информации клиенту, имеющему права «только чтение». Данный тип уязвимостей может быть также эксплуатирован злоумышленниками при отсутствии дополнительного шага аутентификации и использовании очевидной (по умолчанию) точки входа в административный блок информационной системы, например:

/admin
/administrator
/adm

Эксплуатация небезопасного механизма восстановления паролей, на сегодняшний день, является одним из наиболее часто используемым способом несанкционированного доступа к аутентификационным данным клиента. Использование методов социальной инженерии позволяет довольно эффективно использовать данную группу уязвимостей информационных систем. Злоумышленники, на основе анализа открытых данных, полученных, например, из социальных сетей получают сведения, которые могут помочь им ответить на контрольные вопросы, задаваемые для восстановления пароля.

Очевидным методом защиты от данной группы уязвимостей является использование клиентами данных для восстановления пароля, не представленных в том или ином виде на каких-либо материальных носителях.

*Уязвимости авторизации*

Данная группа информационных атак направлена на методы определения ИС наличия прав у клиента для выполнения тех или иных действий. Их можно разделить на следующие подгруппы:

Подстановка значения идентификатора сессии.

«Недостаточная авторизация».

Отсутствие времени действия сессии.

Фиксация сессии.

Подстановка значения идентификатора сессии авторизованного клиента, возможна в том случае, когда злоумышленник может предсказать его значение, поэтому в системе безопасности ИС должна быть учтена данная возможность и генерация уникальных идентификаторов сессии должна проводится по сложному для предсказания или угадывания алгоритму.

Проблема уязвимости «недостаточной авторизации» достаточно схожа с «недостаточной аутентификацией». В данном случае злоумышленник после проведенной аутентификации может повысить свои права путем редактирования файлов сессии. Борьбу с данной уязвимостью целесообразно вести путем введения дополнительной проверки сервером соответствия роли и идентификатора клиента.

Уязвимости, основанные на отсутствие времени действия сессии и фиксация сессии относятся к тем случаям, когда клиентские компьютеры являются общедоступными и доступ к ним специальным образом не регламентирован. То есть злоумышленник может воспользоваться незавершенной «старой» сессией предыдущего пользователя для доступа к данным. Для борьбы с данным типом уязвимости необходимо ограничивать время действия сессии и предусмотреть возможность ее как ручной, так и автоматической деактивации в случае если пользователь завершил работу с ИС.

*Атаки на клиентов*

Атаки на клиентов можно разделить на следующие виды:

Подмена содержимого.

Межсайтовое выполнение сценариев.

Расщепление HTTP-запроса.

В первом случае злоумышленником генерируется страница внешним видом, напоминающая страницу ИС, с помощью которой

введенные данные для получения доступа клиентом будут направлены прямиком нарушителю. Защититься от данного вида атак довольно просто:

Обращать внимание на адрес страницы, на которой вводится авторизационные данные.

Не переходить по ссылкам из ненадежных источников.

Создать необходимые закладки в браузере для исключения неправильного набора сетевого адреса ИС и попадания на фишинговую страницу.

Второй и третий вид атак связан с выполнением вредоносного кода в браузере клиента-жертвы из-за отсутствия или неправильно настроенных правил фильтрации, передаваемых с клиентской стороны на сервер данных.

*Выполнение вредоносного кода*

Выполнение вредоносного кода на сервере дает широкие возможности злоумышленнику позволяющие осуществлять несанкционированный доступу и уничтожению информационных ресурсов ИС, а также нарушить ее работоспособность.

Классическими примерами таких атак является:

Переполнение буфера.

Атака на функции форматирования строк.

Внедрение операторов LDAP.

Выполнение команд операционной системы сервера.

Построение вредоносных SQL-запросов.

Большой спектр уязвимостей, рассмотренных в статье может быть применим практически к любому типу ИС, работающему как веб-приложение, однако, своевременное их выявление и принятие соответствующих мер позволяет снизить риск их эксплуатации злоумышленниками к минимуму.

**Литература**

1. Kim D., Solomon M. Information Systems Security/ Jones&Bartlett learning, 210 – 510 с.

2. Thomas R. Peltier Information Security Fundamentals/ CRC Press, 2013 – 438 с.

# ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

*Мищенко В.И., Инженерно-технологическая академия южного федерального университета, vovchikcool@inbox.ru*
*Шилов А.К., к.т.н., старший научный сотрудник, Инженерно-технологическая академия южного федерального университета, kms7291@mail.ru*

*Нет необходимости в очередной раз рассуждать о широком применении в деятельности современных финансовых организаций информационных и автоматизированных систем, о необходимости обеспечения конфиденциальности обрабатываемой информации. Тем не менее, несмотря на огромную зависимость от электронной информации и систем, многие продолжают сталкиваться с серьезными проблемами обеспечения информационной безопасности (ИБ).*

Информационные технологии в настоящее время активно внедряются во все сферы деятельности. Быстро развивающийся рынок электронных информационных продуктов и услуг предлагает большое количество отечественных и зарубежных экономических информационных систем (ЭИС) различного назначения. ЭИС – это не только компьютерная техника и применение новейших технологических достижений, но и совокупность внутренних и внешних потоков прямой и обратной информационной связи экономического объекта, методов, средств, специалистов, участвующих в процессе обработки информации и в выработке управленческих решений.

Важнейшим ресурсом современного предприятия, способным значительно повлиять на повышение его конкурентоспособности, инвестиционной привлекательности и капитализации, являются корпоративные информационные ресурсы и знания, которые сегодня призваны обеспечивать безопасность [1].

Понять, насколько защищена ЭИС организации, можно только по результатам оценки ИБ организации, полученной с помощью модели оценки ИБ на основании свидетельств оценки, критериев оценки и с учетом контекста оценки.

Оценка ИБ заключается в выработке оценочного суждения относительно пригодности (зрелости) процессов обеспечения ИБ, адекватности используемых защитных мер или целесообразности инвестиций для обеспечения необходимого уровня ИБ на основе измерения и оценивания критических элементов объекта оценки.

Процесс оценки ИБ включает следующие элементы проведения оценки:

- контекст оценки, который определяет входные данные: цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки и роли;
- критерии оценки;
- модель оценки;
- мероприятия процесса оценки: сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов объекта оценки;
- выходные данные оценки.

Предположим, что целью оценки ИБ является оценка процессов обеспечения всей организации или объекта организации. Для достижения такой цели оценки в качестве критерия оценки ИБ должна использоваться эталонная модель процессов обеспечения ИБ, которая описывает в зависимости от объекта оценки совокупность из одного или более процессов в терминах назначения и ожидаемых результатов. Эталонная модель процессов может содержать более подробное описание процессов с выделением атрибутов по назначению и/или ключевых атрибутов – критических элементов процессов [2].

Модель оценки процесса основывается на совокупности показателей, которые используются в качестве основы для сбора объективных данных для определения степени достижения атрибутов процессов, назначения и результатов процессов в рамках сферы модели оценки процесса. Показатели формализуют процесс оценки, дают возможность последовательно формировать суждения специалиста по оценке и повышать воспроизводимость результатов. Показатели позволяют оценить степень реализации процессов объекта оценки. Модели оценки процесса в целом обеспечивают различные степени анализа процесса на основе числа показателей оценки, предоставляемых моделью оценки процесса.

Модель оценки процесса с двадцатью показателями оценки будет считаться обеспечивающей более глубокий анализ процесса, чем модель оценки процесса с десятью показателями оценки. Однако такой анализ требует более значительных усилий во время оценки по выявлению данных, касающихся показателей оценки, а затем обработки данных.

Модель оценки процесса должна позволять отображать атрибуты процессов объекта оценки на выбранной шкале. Такой шкалой может быть количественная шкала (например, абсолютная или шкала отношений), которая указывает степень реализации процесса или достижение заданного уровня атрибута процесса, или качественная шкала (например, порядковая), которая указывает на уровень качества процесса.

Показатели, отображая назначения, результаты и атрибуты процессов, формируют таким образом эталонные профили процессов.

Отображение модели оценки процесса должно обеспечивать формальный и поддающийся проверке механизм представления результатов оценки как совокупности параметров процесса для каждого процесса, выбранного из установленной модели (моделей) процесса.

Модель оценки процесса должна обеспечивать четкое преобразование из основных элементов модели в процессы выбранной модели процессов и в соответствующие параметры процесса в структуре измерений.

Преобразование должно быть полным, четким и однозначным. Преобразование показателей в модели оценки процесса должно производиться в:

- назначения и результаты процессов в установленной модели процесса;
- параметры процесса (включая все результаты достижения, перечисленные для каждого параметра процесса) в структуре измерений.

Международный Стандарт ISO/IEC 15504 определяет, что для оценки процесса могут использоваться модель, оценивающая функционирование процесса, и модель, оценивающая возможности процесса. Измерение функционирования процесса обеспечивается эталонной моделью процесса. Измерение возможности про-

цесса состоит из структуры измерений, включающей шесть уровней возможностей процесса и соответствующие атрибуты процесса [3].

В ISO/IEC 15504 определена модель оценки зрелости, основу которой составляют идентифицированные атрибуты оцениваемых процессов, представляющие измеримые характеристики возможностей того или иного процесса, и методы их оценивания.

Стандартом определена следующая шкала рейтингов оценки процесса, определяющих степень достижения определенных значений для оцениваемого атрибута процесса:

– N — не достигнуто. Мало или нет свидетельств достижения определенным атрибутом оцениваемого процесса некоторого желаемого значения;

– P — частично достигнуто. Существуют некоторые свидетельства приближения к желаемому значению определенного атрибута оцениваемого процесса;

– L — в значительной степени достигнуто. Существуют свидетельства систематического приближения к определенному значению атрибута оцениваемого процесса. В оцениваемом процессе могут существовать некоторые слабые места, связанные с этим атрибутом;

– F — полностью достигнуто. Существуют свидетельства полного и систематического приближения к определенному значению атрибута оцениваемого процесса. Никаких слабых мест, связанных с этим атрибутом, в оцениваемом процессе не существует.

Организация инфраструктуры защиты информации бизнес-процессов должна производиться в соответствии со следующими принципами:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- простоты применения защитных мер и средств.

На основе сформулированных принципов, с учетом типовых требований к инфраструктуре защиты разработана концептуальная модель инфраструктуры защиты информации бизнес-процессов, показанная на рис.1.

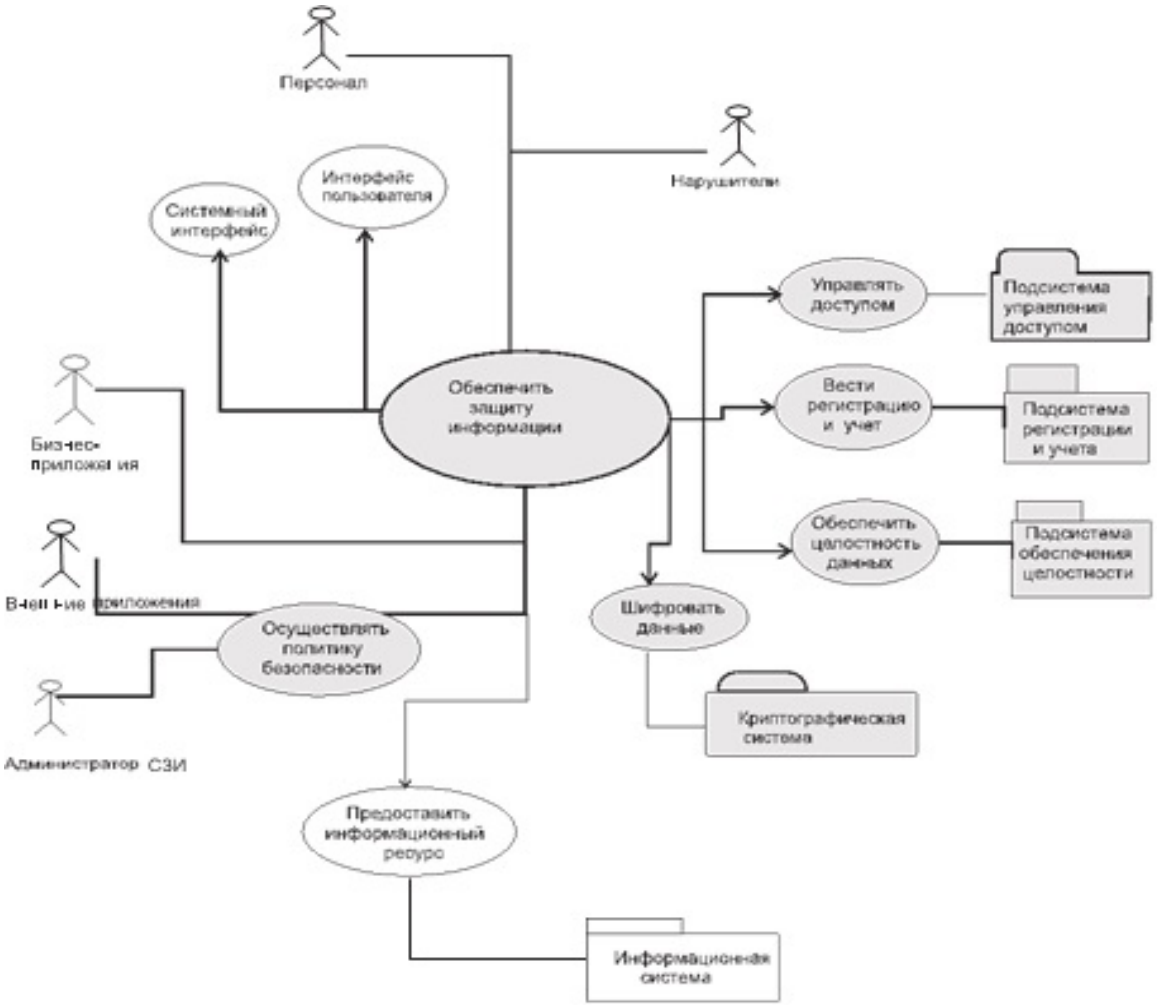



Рис. 1. Концептуальная модель инфраструктуры защиты информации бизнес-процессов

Данная модель раскрывает основные функциональные возможности инфраструктуры защиты информации с учетом внешних негативных воздействий на информационные ресурсы.

Развитие программы информационной безопасности – первый и основной шаг организации на пути построения эффективной системы информационной безопасности. Таким образом, организация должна непрерывно исследовать и оценивать риски информационной безопасности, влияющие на бизнес-процессы, установить централизованное управление информационной безопасностью, установить политики, стандарты, и средства контроля, направленные на уменьшение этих рисков, содействовать осведомленности и пониманию, описанной проблемы среди сотрудников, и оценивать соответствие и повышать эффективность.

**Литература**

1. Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике: учебное пособие. – М.: ИПКИР, 2008. – 485с.

2. Андрианов В.В., Зефиров С.Л., Голованов В.Б, Голдуев Н.А. Под общей редакцией А.П. Курило. Обеспечение информационной безопасности бизнеса. – М.: ЦИПСиР, 2011. — 373 с.

ISO/IEC 15504 Information technology — Process assessment.

# АНАЛИЗ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

*Порсев И.С., Национальный исследовательский университет «МИЭТ», person_il@mail.ru*

*В данной статье рассматривается вопросы, связанные с организацией защиты от несанкционированного доступа ресурсов корпоративной сети. Приводятся уровни, на которых необходимо использовать механизмы защиты, и технологии позволяющие выполнение требований по защите информации от несанкционированного доступа.*

Современные корпоративные компьютерные сети играют важнейшую роль в деятельности многих организаций. Большая часть из них подключена к сетям международного информационного обмена – Интернет (Internet). В связи с этим все серьезнее становится угроза внешнего вмешательства в процессы нормального функционирования корпоративных сетей, и как следствие, несанкционированного доступа (НСД) к ресурсам корпоративной сети.

В соответствии с требованиями [1] источниками угроз НСД в информационных системах (ИС) обработки информации могут быть: нарушитель, носитель вредоносной программы, аппаратная закладка.

**1. Нарушитель.** По наличию права постоянного или разового доступа в контролируемую зону (КЗ) ИС нарушители подразделяются:

- внешние нарушители – нарушители, не имеющие доступа к ИС, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена. Внешними нарушителями могут быть:

разведывательные службы государств;

криминальные структуры;

конкуренты (конкурирующие организации);

внешние субъекты (физические лица).

- внутренние нарушители – нарушители, имеющие доступ к ИС, включая пользователей ИС, реализующие угрозы непосредственно в ИС. Внешний нарушитель имеет следующие возможности:

осуществлять НСД к каналам связи, выходящим за пределы служебных помещений;

осуществлять НСД через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;

осуществлять НСД к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;

осуществлять НСД через элементы информационной инфраструктуры ИС, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны;

осуществлять НСД через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИС.

**2. Носитель вредоносной программы.** Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

отчуждаемый носитель, то есть дискета, оптический диск (CD-R, CD-RW), флэш-память, отчуждаемый винчестер и т.п.;

встроенные носители информации (винчестеры, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок, – видеоадаптера, сетевой платы, звуковой платы, модема, устройств

ввода/вывода магнитных жестких и оптических дисков, блока питания и т.п., микросхемы прямого доступа к памяти, шин передачи данных, портов ввода/вывода);

микросхемы внешних устройств (монитора, клавиатуры, принтера, модема, сканера и т.п.).

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

пакеты передаваемых по компьютерной сети сообщений;

файлы (текстовые, графические, исполняемые и т.д.).

**3. Аппаратная закладка.** Угрозы безопасности, связанные с внедрением аппаратных закладок, определяются в соответствии с нормативным документами Федеральной службы безопасности Российской Федерации в установленном ею порядке [1].

Проведя анализ вышеперечисленных источников угроз и требования, предъявляемые для защиты [2], можно выделить 6 уровней, необходимых для защиты ресурсов корпоративной сети от несанкционированного доступа, представленные на рисунке 1.


Рис. 1. Уровни защиты автоматизированной системы от НСД

Основу защиты на *уровне физического доступа* являются организационные меры, которые направлены на недопустимость

бесконтрольного проникновения (пребывания) в помещения посторонних лиц и обеспечивающие физическую сохранность защищаемых информационных ресурсов. Это достигается путем ограничения перечня лиц, допущенных в помещение и реализации требований к помещению.

Основными требованиями, предъявляемыми к помещению, являются:

– автоматические замки идентификации объекта доступа на основе систем контроля и управления доступом (СКУД) [3];

– средства сигнализации [4];

– средства видеонаблюдения [4].

В основе *уровня межсетевого сегмента* лежит наличие подключения имеющего сегмента сети или отдельной станции к другим сетям предприятия или к сетям международного информационного обмена.

Для защиты информационных ресурсов от НСД применяются

– межсетевые экраны (файервол, брандмауэр) (МЭ) – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

В качестве критериев обеспечения безопасности информации используются показатели защищенности ИС, которые представлены в [5].

Основным показателем защищенности является управление доступом (фильтрация данных и трансляция адресов), которое включает:

фильтрация на сетевом уровне;

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов.

маршрутизаторы, осуществляющие чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту (например, UDP, IPX, ICMP, IP, AppleTalk), и принимающие решения о дальнейшем маршруте следования пакета по

его сетевому адресу, включающему, как правило, номер сети и номер узла.

К сожалению, руководящие документы, регламентирующие использование данного оборудования, отсутствуют и вся функциональность маршрутизатора переносится на МЭ.

Для защиты на *уровне сетевого сегмента* могут применяться следующие методы:

– деления на уровне коммутатора на виртуальные сети (vlan);

Деление на виртуальные сети (vlan) позволяет разделить проходящий трафик и сгруппировать конечные станции, отвечающие определенным критериям. Основные критерии разделения сетей:

по порту;

по MAC-адресу рабочей станции;

по протоколу взаимодействия сети;

методом аутентификации.

К сожалению, руководящие документы, регламентирующие использование данного оборудования, отсутствуют и функциональность заложенная в коммутаторе не используется для защиты информации.

– создание защищенного сетевого соединения для обеспечения защиты данных, передаваемых по протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов.

– сетевая система обнаружения вторжений (NIDS) просматривает все (входящие/исходящие) пакеты на наличие в них подозрительных признаков, позволяя тем самым отслеживать вредоносную деятельность (DoS атаки), сканирование портов и попытки проникновения в сеть.

Основные требования, предъявляемые к системам обнаружения вторжений СОВ уровня сети, представлены в [6] и описаны в профилях защиты указанных ниже.

| Тип СОВ | Класс защиты | | |
|---|---|---|---|
| | 6 | 5 | 4 |
| СОВ уровня сети | ИТ.СОВ.С6.ПЗ | ИТ.СОВ.С5.ПЗ | ИТ.СОВ.С4.ПЗ |

Для защиты на *уровне узлового сегмента* могут применяться следующие методы:

– аутентификация – процедура проверки подлинности, путем ввода публичной информации и секретной информации.

Необходимость применения аутентификации является необходимым условием построения защиты доступа к автоматизированной системе и регламентируется [2].

Способы аутентификации:

аутентификация по многоразовым паролям, заключающаяся во вводе пользовательского идентификатора («логина») и пароля, связка, которых хранится в специальной базе данных;

аутентификация по одноразовым паролям при использовании:

- генератора псевдослучайных чисел, единого для субъекта и системы;

- временных меток вместе с системой единого времени;

- базы случайных паролей, единой для субъекта и для системы.

многофакторная аутентификация, построенная на совместном использовании нескольких факторов аутентификации.

– хостовая система обнаружения вторжений (HIDS), которая ведет наблюдение и анализ событий, происходящих внутри системы, и позволяет производить аудит нарушения безопасности непосредственно на рабочей станции.

Основные требования, предъявляемые к СОВ уровня узла, представлены в [6] и описаны в профилях защиты указанных ниже.

| Тип СОВ | Класс защиты | | |
|---|---|---|---|
| | 6 | 5 | 4 |
| СОВ уровня узла | ИТ.СОВ.У6.ПЗ | ИТ.СОВ.У5.ПЗ | ИТ.СОВ.У4.ПЗ |

Для защиты на уровне приложений должны применяться:

сертифицированное системное и прикладное программное обеспечение;

специализированные программы для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом [7].

*Информационный сегмент* заключается в защите информации на уровне контроля доступа к защищаемым информационным ресурсам [8]:

<table>
<tr><th rowspan="2">Наименование</th><th colspan="4">Класс защищенности показателя</th></tr>
<tr><th>7</th><th>6</th><th>5</th><th>4</th></tr>
<tr><td rowspan="3">Дискреционный принцип контроля доступа</td><td colspan="4">Контроль доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.)</td></tr>
<tr><td colspan="2"></td><td colspan="2">Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ</td></tr>
<tr><td colspan="3"></td><td>Должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых.</td></tr>
<tr><td>Мандатный принцип контроля доступа</td><td>-</td><td>-</td><td>-</td><td>Каждому субъекту и каждому объекту должны сопоставляться классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий.</td></tr>
</table>

Для реализации данных принципов контроля доступа используется матрица контроля доступа (access control matrix), содержащая таблицу субъектов и объектов, и информацию о том, какие действия конкретные субъекты могут делать с конкретными объектами. Права доступа назначаются с помощью:

- таблицы разрешений (capability tables) указывают права доступа определенного субъекта к определенным объектам. Таблицы разрешений являются ограничением для субъектов, а ACL –

для объектов. Разрешения соответствуют строке субъекта в матрице контроля доступа.

- списки контроля доступа (ACL – access control list) используются во многих операционных системах, приложениях и маршрутизаторах. Это списки субъектов, которым разрешен доступ к определенному объекту, с указанием уровня разрешенного доступа. Разграничение доступа может выполняться на уровне пользователей или на уровне групп.

Для реализация комплексной защиты защищаемых ресурсов, необходимо выполнение требований на каждом из уровней. В настоящее время остается не регламентированным использование таких устройств как маршрутизатор и коммутатор. В связи с этим защита на межсетевом уровне используется не рационально, а на сетевом – защита отсутствует.

Таким образом, разработка документов позволит создать дополнительную защиту и увеличить степень защищенности информационных систем.

**Литература**

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. (Выписка). Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России). Утверждено заместителем директора ФСТЭК России 15.02.2008 г.

2. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Государственная техническая комиссия при президенте Российской Федерации (Гостехкомиссия России). Утверждено приказом Председателя Гостехкомиссии России от 30 августа 2002 г. № 282- ДСП.

3. ГОСТ Р 51241-2008 Национальный стандарт РФ «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний». Утверждено приказом Федеральным агентством по техническому регулированию и метрологии от 17 декабря 2008 г. № 430-ст.

4. Руководящий документ 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». Министерство внутренних дел Российской Федерации. Утвержден Министром внутренних дел РФ от 06 ноября 2002 г.

5. Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации». Утвержден решением Председателя Гостехкомиссии России от 25.07.1997.

6. Информационное письмо ФСТЭК РФ от 01.03.2012 г. № 240 «Об утверждении требований к системам обнаружения вторжений».

7. Руководящий документ «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Утвержден решением Председателя Гостехкомиссии России от 4 июня 1999 г. N 114

8. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Государственная техническая комиссия при президенте Российской Федерации (Гостехкомиссия России). Утвержден решением председателя Государственной технической комиссии при президенте Российской Федерации от 30 марта 1992 г.

# ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ КОРУПЦИИ

*Кремнев А.М., Санкт-Петербургский университет МВД России, kremnev_a@mail.ru*
*Шалагинова О.Б., к.ф.-м.н., доцент, Санкт-Петербургский университет МВД России, shans331@yandex.ru*

*В статье рассмотрены исторические аспекты создания системы информационного обеспечения Органов внутренних дел России, а также разработка интегрированного банка данных МВД Российской Федерации в настоящее время.*

Восстановим исторические аспекты создания системы информационного обеспечения Органов внутренних дел России. Для того чтобы разобраться в понятии термина «информационное обеспечение», рассмотрим вначале такие основные элементы информационного обеспечения как информация, система информации и информационная система. Как известно, без полной, целенаправленной и достоверной информации невозможно управление.

Всякий управленческий цикл начинается со сбора, обработки информации и заканчивается получением информации, которая является исходной для нового управленческого цикла. Понятие «информация» исследовалось многими учеными, ему давались различные определения. Например, в толковом терминологическом словаре-справочнике сказано, что информация – сведения, неизвестные до их получения, являющиеся объектом хранения, передачи и обработки. Первые попытки понимания сущности информации относятся к пятидесятым годам прошлого столетия и связаны с возникновением разработанной Клодом Шеноном и Нобертом Винером «статистической» теории информации «Статистические» теории определяют информацию – передачу разнообразия; оригинальность; коммуникацию, связь, в процессе которой устраняется неопределенность. Определение информации, ставшее «классическим», выдвинул Норберт Винер в конце 50-х годов.

В этой концепции между категориями «данные» и «информация» знак тождества поставить уже нельзя, т.к. данные – это лишь фиксация результата либо хода процесса. Пока они соответствующим образом не организованы, отсутствует их влияние на управленческую деятельность. В общем виде такую информацию можно определить как знание субъекта о руководимом объекте и его среде. Для Органов внутренних дел наиболее важен функциональный подход, лишь при таком подходе к информации как знанию сотрудников о правонарушителе, его связях, среде, где могут происходить правонарушения, сотрудник может принять верное управленческое решение.

Информация, используемая в Органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. В дежурных частях, у оперативных работников, участковых инспекторов, следователей, сотрудников экспертно-криминалистических подразделений, паспортно-визовых аппаратов, других подразделений на документах первичного учета, в учетных журналах и на других носителях накапливаются массивы данных оперативно-розыскного и оперативно-справочного назначения, в которых содержатся сведения:

о правонарушителях и преступниках;

о владельцах автомототранспортных средств;

о владельцах огнестрельного оружия;

о событиях и фактах криминального характера, правонарушениях;

о похищенных и изъятых вещах, предметах антиквариата, а также другая, подлежащая хранению информация.

Службы и подразделения Органов внутренних дел характеризуются данными:

о силах и средствах, которыми располагает орган;

о результатах их деятельности.

Перечисленные выше сведения используются при организации работы подразделений и принятии практических мер по борьбе с преступностью и правонарушениями. Кроме указанных сведений широко используется научная и техническая информация, необходимая для информационного обеспечения Органов внутренних дел. Центральное место занимают учеты, которые используются для регистрации первичной информации о преступлениях и лицах, их совершивших.

Учет – это система регистрации и хранения информации о лицах, совершивших преступления, о самих преступлениях и связанных с ними фактах и предметах. Учет подведомственных МВД преступлений охватывает 95% криминальных проявлений и дает достаточно полную картину оперативной обстановки в стране и ее регионах.

Далее светим разработку интегрированного банка данных МВД Российской Федерации в настоящее время. Кроме создания собственных компьютерных учетов объектов интересующих сотрудника ОВД, сотрудник может использовать программно-технический комплекс (ПТК) «ИБД-РЕГИОН». Этот комплекс был введён в эксплуатацию в МВД по Республике Башкортостан в рамках реализации программы «Создание единой информационно-телекоммуникационной системы органов внутренних дел», рассчитанной на 2005-2008 годы, в 2006 году. Программно-технический комплекс (ПТК) «ИБД-РЕГИОН», используют универсальное прикладное математическое обеспечение (УПМО-2005) для ведения интегрированных банков данных регионального уровня. Конечной целью реализации проекта является формирование единого информационного пространства в системе МВД России, что

позволит увеличить раскрываемость и предотвращение преступлений, путём получения сотрудниками ОВД в режиме реального времени точной и достоверной оперативно-справочной, розыскной и криминалистической информации, интегрируемой на разных уровнях в системе МВД. Интегрированный банк данных регионального уровня «ИБД-Регион» представляет собой единую базу данных из совокупности имеющихся оперативно-справочных, розыскных и криминалистических учётов регионального и федерального уровней, формируемых в порядке, установленном нормативными правовыми актами МВД России. Информационное взаимодействие с ИБД осуществляется с автоматизированных рабочих мест сотрудников ОВД в режиме «ON-LINE» по существующим каналам связи. Администрирование, контроль функционирования ИБД осуществляется администраторами, назначенными распоряжением начальника ИЦ МВД. Удалённый доступ в ИБД осуществляется с использованием АРМ в «ON-LINE» режиме, что обеспечивает возможность непосредственного доступа в ИБД в диалоговом режиме в соответствии с санкционированными правами доступа. АРМ позволяет сформировать запрос, выполнить запрос, просмотреть и вывести на печать результаты исполнения. Список доступных видов учётов и запросов по ним определяется в зависимости от прав пользователя по доступу к ИБД. Руководитель подразделения назначает ответственных лиц за организацию работы АРМ в подразделении, в функции которых входит, в том числе, проверка журнала исполнения запросов, контроль обоснованности обращений в ИБД, ежемесячный доклад руководителю подразделения о результатах работы пользователей. В свою очередь пользователь АРМ несёт ответственность в соответствии с законодательством за использование информации ИБД не в служебных целях, за несанкционированную передачу третьим лицам конфиденциальных сведений, полученных при работе с ИБД, а также за передачу личного логина и пароля доступа.

В заключении можно отметить, что большинство регионов России приступили к созданию региональных информационных систем, вышли на новый уровень, вследствие чего в Органах внутренних дел России в автоматизированном режиме с помощью ЭВМ обрабатываются задачи оперативно-розыскного и справоч-

ного назначения с количеством обрабатываемых запросов примерно 10 млн. в год, а также задачи учетно-статистического, управленческого и производственно-экономического назначения. Эти перемены значительно сказываются в работе ОВД и быстродействии. Будущее полиции основано исключительно на этом.

Но помимо того, что в МВД активно внедряются информационно технические средства, базы данных, электронные картотеки и т. д., активно способствующие учету граждан и выявлению правонарушений, необходимо:

формирование механизмов защиты информационного пространства и населения Российской Федерации от пропаганды терроризма и экстремизма;

совершенствование системы информационного противодействия терроризму, предусматривающей мобилизацию органов государственной власти, общественных организаций, научных, деловых и творческих кругов для реализации антитеррористических мер;

формирование социально-политических, правовых и иных основ для эффективного противодействия идеологии терроризма и экстремизма.

При совершении террористического акта вслед за первой физической волной террористического взрыва — поражает вторая, еще более мощная — информационная, которая несет нравственный ущерб миллиардам читателей, радиослушателей и телезрителей! Российским государством и журналистским сообществом неоднократно предпринимались попытки установить морально-этические нормы для журналистов, освещающих террористические акты и контртеррористические операции. Так, 11 апреля 2003 г. в Интернете на сайте МИД России была размещена Антитеррористическая конвенция.

Борьба с терроризмом принимает новую волну и МВД должно перестраивать свои ответные действия. В обществе 21 века важную роль в борьбе с терроризмом играет, помимо новейшего информационно-технического обеспечения, защита информационного пространства и населения Российской Федерации от пропаганды терроризма и экстремизма. Это нашло себе отражения в ходе последних событий, связанных с так называемой информационной войной.

Государство должно активно продолжать вести эту политику и в дальнейшем.

# МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

*Харрасов Э.Э., Санкт-Петербургский университет МВД России, stillwatching@yandex.ru*
*Шалагинова О.Б., к.ф.-м.н., доцент, Санкт-Петербургский университет МВД России, shans331@yandex.ru*

*Террористические и экстремистские группировки в настоящее время довольно часто используют киберпространство для пропаганды, вербовки и координации действий.*

Зарубежный и отечественный опыт противодействия терроризму свидетельствуют о том, что силовые методы могут лишь на время устранить угрозу совершения террористического акта, но эта угроза будет сохраняться, пока существует система воспроизводства инфраструктуры терроризма. Ключевыми звеньями этой системы являются идеология терроризма и экстремизма, ее вдохновители и носители, а также каналы ее распространения [1].

В настоящее время Интернет является идеальным инструментом пропаганды экстремистской и террористической деятельности [2].

Основные причины осуществления данной деятельности в сети Интернет являются:

- широкий охват аудитории;
- высокая скорость распространения информации через различные блоги, социальные сети, форумы;
- возможность вести анонимную противоправную деятельность;
- злоумышленники зачастую ищут лазейки в области «информационного права» и находя их, остаются безнаказанными.

Главными факторами бесконтрольного распространения, экстремистских и террористических течений в сети Интернет является условная обезличенность и, как следствие, безнаказанность лиц, которые участвуют в Интернет – пропаганде. Все чаще международными террористическими группировками используется

Интернет-телефония, например система «Скайп», телефонные разговоры через которую трудно отследить.

В целях информационного противодействия экстремистским и террористическим действиям в сети Интернет и защите пользователей от их воздействия, можно выделить несколько основных задач:

1) выявление и блокирование Интернет – ресурсов с экстремистской и террористической пропагандой с использованием законодательства РФ;

2) распространение в сети Интернет – ресурсов антиэкстремистского и антитеррористического характера.

Для решения этих задач необходимо использовать следующие методы:

1. мониторинг Интернет – ресурсов с целью выявления пропаганды экстремистской и террористической деятельности;

2. выявление уязвимых пользователей сети Интернет. Этот метод заключается в выявлении наиболее уязвимых групп пользователей сети Интернет, на которых могут быть направлены действия пропагандистов;

(Этот метод заключается в выявлении наиболее уязвимых групп пользователей сети Интернет, на которых могут быть направлены действия пропагандистов.)

3. Информационно – просветительская деятельность.

Вся подобная деятельность разделяется в соответствии с возникающими задачами: подготовка и размещение информационных материалов; проведение разъяснительных бесед с участниками Интернет – форумов, блогов и социальных сетей.

Принятые решения о формировании принципиально новой системы противодействия терроризму во главе с Национальным антитеррористическим комитетом (НАК, Комитет) дают свои плоды [3]. Но общий фон террористической активности в России остается еще на достаточно высоком уровне и всячески поддерживается силами международного терроризма.

**Литература**

1. В.П. Журавель. Актуальные проблемы противодействия терроризму. М.: Право и безопасность. № 2 (27) 2008. С. 71-79.

2. Н.П. Патрушев. О некоторых особенностях современных вызовов и угроз национальной безопасности Российской Федерации. М.: Российское право. № 7. 2007. 18 с.

3. Федеральный закон от 6 марта 2006 № 35-ФЗ «О противодействии терроризму» // СЗ РФ. 2006. № 11. Ст. 1146; Указ Президента России от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» // СЗ РФ. 2006. № 8. Ст. 897. П. 2.

# НЕКОТОРЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

*Шевченко И.А., Ставропольский филиал Краснодарского университета МВД России, Magway1981@yandex.ru*
*Красников В.Н., Ставропольский филиал Краснодарского университета МВД России*

*В работе рассмотрен комплекс типовых мер по обеспечению защиты информационных систем от хищения и потери информации.*

Актуальность темы защиты информационных систем на современном этапе развития общества обусловлена необходимостью профилактики и предотвращения правонарушений и преступлений в области компьютерных технологий, а также утечки служебной информации ограниченного доступа.

Развитие информационных технологий и их широкое внедрение в различные сферы человеческой деятельности, вызвало в том числе и рост числа правонарушений и преступлений, объектом или орудием совершения которых являются компьютерная техника. Путем внесения изменений в компьютерную информацию, программное обеспечение, либо путем овладения различной информацией, злоумышленникам удается получать значительные суммы денег, заниматься промышленным шпионажем, уничтожать программы конкурентов, либо просто использовать «пиратское» программное обеспечение в личных целях.

К примеру стоимость лицензии к фоторедактору Adobe Photoshop достигает 18 тыс. рублей в год. Стоимость лицензионных сметных программ, используемых в строительстве составляет 30-50 тыс. рублей за одно рабочее место. Программы для работы с

графикой, Web дизайн – около 110 тыс. рублей. Программы для управления предприятием 150 тыс. рублей. Таким образом можно представить размеры ущерба, ежегодно причиняемого разработчикам программного обеспечения только путем распространения пиратского софта.

Защита информации вызывает необходимость системного подхода, т.е. здесь нельзя ограничиваться отдельными мероприятиями. Системный подход к защите информации требует, чтобы средства и действия, используемые для обеспечения информационной безопасности – организационные, технические и правовые, рассматривались как единый комплекс взаимосвязанных, взаимодополняющих и взаимодействующих мер.

Потеря компьютерной информации может произойти, например, по следующим причинам:

- сбои в работе компьютера;
- воздействие вредоносного программного обеспечения;
- ошибки пользователя;
- повреждение информационных носителей;
- перебои энергоснабжения;
- умышленная (неосторожная) деятельность других лиц. [1]

Для успешной защиты своей информации каждый пользователь должен понимать, что информация может быть не только повреждена (уничтожена), но и похищена. Так, основными путями хищения компьютерной информации являются:

- хищение носителей информации и производственных отходов,
- копирование носителей информации с преодолением мер защиты,
- маскировка под зарегистрированного пользователя,
- мистификация (маскировка под запросы системы),
- использование недостатков операционных систем и языков программирования,
- использование программных закладок и программных блоков,
- перехват электронных излучений,
- перехват акустических излучений,
- дистанционное фотографирование,
- применение подслушивающих устройств,
- злоумышленный вывод из строя механизмов защиты и т.д. [2]

Существуют различные меры по предупреждению потери информации. Условно их можно разделить на три вида: *организационные, технические и правовые.*

Организационными мерами являются: организация охраны вычислительного центра, обеспечение пропускного режима на объектах, осуществляющих обработку и хранение информации, тщательная проверка персонала при трудоустройстве, исключение случаев ведения особо важных работ только одним человеком, осуществление проверок и обслуживания вычислительных центров лицами, незаинтересованными в сокрытии нарушений режима работы центра, определение должностных лиц, которые будут обеспечивать безопасность центра, выбор места расположения центра и т.п.

К техническим мерам защиты информации можно отнести защиту от несанкционированного доступа к системе (паролирования доступа в компьютер и операционную систему), разграничение полномочий пользователей, так как утрата информации может произойти не только в результате злонамеренных действий, но и явиться следствием низкой квалификации пользователей. Разграничение уровня доступа позволяет варьировать полномочия каждого пользователя в зависимости от его квалификации и должностных обязанностей. Резервирование особо важных компьютерных подсистем, организация вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установка оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от несанкционированного проникновения в служебные помещения, хищений, саботажа, диверсий, взрывов, оснащение помещений замками, установка сигнализации, все эти мероприятия направлены на техническую защиту хранимой информации, однако при организации охраны следует придерживаться принципа «разумной достаточности», суть которого состоит в том, что ни при каких обстоятельствах не возможно добиться стопроцентной защиты, поэтому стремиться стоит не к теоретически максимально достижимому уровню защиты, а к минимально необходимому в данных конкретных условиях и при данном уровне возможной угрозы. Считается нормальным, когда 10-

15% стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания. Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства – серверы, концентраторы, мосты и т.д. – оснащены собственными дублированными системами электропитания. Для обеспечения бесперебойной работы в условиях отключения энергоснабжения необходимо предусмотреть монтаж собственных аварийных электрогенераторов или резервных линий электропитания. Эти линии подключаются к разным подстанциям, и при выходе из строя одной из них электроснабжение осуществляется с резервной подстанции.

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер. Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Основной и наиболее распространенный метод защиты информации и оборудования от различных стихийных бедствий – пожаров, землетрясений, наводнений и т.д. – состоит в хранении архивных копий информации или в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других

зданиях или, реже, даже в другом районе города или в другом городе.

К техническим средствам защиты информации так же можно отнести установку фильтров, экранов на аппаратуру, ключей для блокировки клавиатуры, устройств аутентификации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати [3] и т.д., создание электронных ключей на USB-накопителях, криптографический способ защиты информации – шифрование при вводе в компьютерную систему.

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100-150 новых штаммов ежемесячно. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Рассмотрим наиболее распространенные антивирусные программы:

**Антивирус Касперского**

Антивирус Касперского – продукт для защиты вашего ПК, чья эффективность проверена миллионами пользователей во всем мире. Программа включает в себя основные инструменты для защиты ПК.

**Eset NOD32**

ESET NOD32 обеспечивает обнаружение и блокировку вирусов, троянских программ, червей, шпионских программ, рекламного ПО, фишинг-атак, руткитов и других интернет-угроз, представляющих опасность для компаний. Несмотря на минимальную потребность в ресурсах, данное решение обеспечивает непревзойденный уровень проактивной защиты, практически не снижая производительность компьютера.

**Symantec Norton Anti-Virus**

Разработанная компанией Symantec программа Norton AntiVirus является наиболее популярным антивирусным средством в мире. Эта программа автоматически удаляет вирусы, интернет-червей и троянские компоненты, не создавая помех работе пользователя. Norton AntiVirus позволяет противостоять угрозам самых современных spyware- и adware-программ и блокирует работу таких программ еще до того момента, как пользователь перенаправляется на другой сайт.

**Dr. Web**

Антивирус Dr.Web проверит всю Windows память даже зараженного компьютера. Доктор Веб проводит полную антивирусную проверку Windows-памяти компьютера и способен остановить вирусный процесс. Важным показателем качества работы антивирусной программы является не только ее способность находить вирусы, но и лечить их, не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и возвращать их в первоначальное «здоровое» состояние.

**Trend Micro Internet Security**

Trend Micro Internet Security позволяет очень просто защитить компьютер, приватные персональные данные и онлайн-активность. Продукт обеспечивает защиту как от существующих вирусов, программ-шпионов и кражи данных, так и от будущих веб-угроз. Позволяет пользоваться электронной почтой, интернет-магазинами, онлайн-банкингом, обменивайтесь цифровыми фотографиями и не беспокоиться о безопасности приватной информации.

**Avast! Professional Edition**

Avast! Professional Edition вобрал в себя все высокопроизводительные технологии для обеспечения одной цели: предоставить наивысший уровень защиты от компьютерных вирусов. Данный продукт представляет собой идеальное решение для рабочих станций на базе Windows. Новая версия ядра антивируса avast! обеспечивает высокий уровень обнаружения вкупе с высокой эффективностью, что гарантирует 100%-ое обнаружение вирусов «In-the-Wild» и высокий уровень обнаружения троянов с минимальным числом ложных срабатываний. Механизм антивирусного ядра сертифицирован ICSA, постоянно принимает участие в тестах VirusBulletin и получает награды VB100%. Внешний вид пользовательского интерфейса отображается с помощью так называемых скинов, поэтому у пользователя есть возможность настроить внешний вид панели продуктов avast! по своему желанию.

**BitDefender Antivirus**

BitDefender Antivirus – мощная антивирусная программа с разнообразными возможностями, позволяющими оптимально защитить персональный компьютер. BitDefender Antivirus защищает от компьютерных вирусов с применением технологий ICSA Labs,

Virus Bulletin, Checkmark, CheckVir и TUV. Модуль B-HAVE подражает действительному (виртуальному) «компьютеру в компьютере». Эта BitDefender-технология представляет новый уровень безопасности, обнаруживая и обезвреживая даже редкие вирусы, или вирусный код, для которого еще не вышли новые базы записей вирусов.

### Panda Antivirus

Panda Antivirus является самым простым и интуитивно понятным в использовании решением безопасности для домашнего ПК. После установки программы пользователь может забыть о вирусах, программах-шпионах, руткитах, хакерах, онлайн-мошенниках и больше не беспокоиться о сохранности конфиденциальной информации.

Panda Antivirus имеет простые настройки, легкий и понятный интерфейс, автоматическое обновление (после установки сразу будет искать обновления), осуществляет контроль на уровне TCP/IP. Panda Antivirus является достаточно надежным антивирусом подойдет в первую очередь для домашнего пользования

### McAfee VirusScan

Продукт McAfee VirusScan осуществляет сканирование файловых серверов и рабочих станций по расписанию и по запросу пользователя, способен обнаруживать и обезвреживать вирусы-трояны и программы-черви. Кроме того, системные администраторы получают возможность присваивать программам и процессам ту или иную степень приоритетности, в соответствии с которой они и будут сканироваться антивирусом, что позволяет экономить ресурсы корпоративных сетей.

### Avira AntiVir

Популярный антивирус германской сборки. Эту программу всегда отличали качество работы и быстрая реакция на появление новых вирусов. Она включает в себя резидентный монитор, сканер и программу обновления. AntiVir может постоянно следить за файлами и архивами, которые могут быть потенциальными переносчиками вирусов. Отыскиваются также и макросы, которые внедряются в офисные документы. Программа нетребовательна к ресурсам и показывает хорошие результаты в работе по скорости и качеству поиска.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение

На практике обычно используются комбинированные способы защиты информации от несанкционированного доступа.

В целях максимального обеспечения безопасности хранимой информации, следует придерживаться нескольких простых правил:

- нельзя доверять электронной почте ничего такого, что нужно скрыть от посторонних, так как вероятность несанкционированного доступа к электронной почте, не защищенной специальными средствами (шифрование, цифровые удостоверения), весьма велика. Со многих почтовых серверов имеется возможность отправить почту от чужого имени, даже не зная пароля владельца адреса;

- подозрительные письма нужно удалять, не читая. К подозрительным относятся письма с рекламными многообещающими заголовками и сообщения с вложениями от неизвестных корреспондентов;

- нужно внимательно относиться к предупреждениям системы об опасности заражения вирусами. При появлении таких сообщений обращаться за консультацией к специалистам;

- пользоваться антивирусными программами;

-время от времени сохранять особо ценную информацию на внешних носителях.

**Литература**

1. Информационные технологии в юриспруденции : учеб. пособие для студ. учреждений высш. проф. образования / [С.Я. Казанцев, О.Э. Згадзай, И.С. Дубровин, Н.Х. Сафиуллин]; под ред. С.Я. Казанцева. – 2-е изд., перераб. – М.: Издательский центр «Академия», 2012. – 368 с.

2. Информационные технологии в юридической деятельности : учебник для бакалавров / под общ. ред. П.У. Кузнецова. – М. : Издательство Юрайт, 2012. – 422 с. – Серия : Бакалавр. Базовый курс

3. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. – М. : ФОРУМ, 2012. – 432 с.

# МЕТОДИКА ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ОРГАНОВ ВНУТРЕННИХ ДЕЛ

*Сорокина И.И., Краснодарский университет МВД России,*
*Клюев С.Г., к.т.н., Краснодарский университет МВД России*

*В статье рассматривается схема организации защищенного и юридически значимого обмена электронными документами. Кроме того, в статье описывается технология виртуальных частных сетей и условия равнозначности электронной цифровой подписи собственноручной подписи.*

В последнее время все чаще поднимается вопрос об использовании электронного документооборота в системе органов внутренних дел. В этом отношении изданы ряд нормативных правовых актов Российской Федерации и МВД России. Примерами данных нормативных правовых актов являются распоряжение Правительства Российской Федерации от 12 февраля 2011 г. № 176-р «Об утверждении плана мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности», приказ МВД России от 31 мая 2011 года № 600 «Об утверждении Перечня документов, образующихся в деятельности органов внутренних дел Российской Федерации, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов», приказ МВД России от 4 мая 2012 года № 404 «О вводе в опытную эксплуатацию единой автоматизированной информационной системы электронного документооборота и делопроизводства»

Общий порядок работы с электронными документами в системе органов внутренних дел утверждён приказом МВД России от 20 июня 2012 года № 615 «Об утверждении инструкции по делопроизводству в органах внутренних дел Российской Федерации». Согласно данному приказу, электронный документ должен быть оформлен по общим правилам делопроизводства и иметь реквизиты, установленные для аналогичного документа на бумаж-

ном носителе, за исключением оттиска печати и изображения государственного герба Российской Федерации. При этом особо отмечается, что электронные документы создаются, обрабатываются и хранятся в системах электронного документооборота.

Внедрение электронного документооборота в деятельность органов внутренних дел – очень сложная и обширная тема для исследования, поэтому в данной статье будет рассмотрена только ее часть касающаяся схемы организации юридически значимого электронного документооборота по открытым и закрытым каналам связи.

Как было указано выше Перечень документов, образующихся в деятельности органов внутренних дел Российской Федерации, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов утвержден приказом МВД России от 31 мая 2011 года № 600 и все документы из данного перечня могут быть подписаны электронной подписью. Также в данных документах электронная подпись признается равнозначной собственноручной подписи в случае выполнения всех условий определенных Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Порядок передачи и получения документов в электронном виде, подписанных электронной подписью, определяются типом документа, порядком использования таких документов, Инструкцией по делопроизводству в органах внутренних дел Российской Федерации и правилами использования систем электронного документооборота.

Как правило, передача электронных документов, должна сопровождаться регистрацией отправки и получения в соответствии с Инструкцией по делопроизводству, за исключением случаев, когда предусмотрена передача и получение электронных документов без регистрации.

Одним из вопросов при создании систем электронного документооборота в органах внутренних дел является вопрос создания доверенной среды передачи данных. Предлагается использовать в качестве такой среды локально вычислительную сеть, не имеющую подключений к сетям общего пользования и расположенную внутри органа внутренних дел.

Очень частыми бывают случаи когда структурные подразделения одного органа внутренних дел размещаются территориально в разных зданиях, улицах и даже городах. Тогда встает вопрос как в этих случаях создать доверенную среду передачи данных, так как создание локальной вычислительной сети будет стоить колоссальных затрат.

Предлагается для решения указанной проблемы стоит использовать виртуальные частные сети (VPN).

Технология VPN позволяет обеспечить одно или несколько сетевых соединений поверх другой сети (например, Интернет). Несмотря на то, что коммуникация осуществляется по сетям общего пользования, вся информация, передаваемая по виртуальной частной сети, надежно защищена от внешних злоумышленников. Это обеспечивается тем, что в технологии VPN используются средства криптографической защиты информации.

В качестве примера реализации VPN технологий в данной статье будут рассматриваться продукты из линейки «ViPNet CUSTOM» компании ОАО «ИнфоТеКС», которые позволяют создать защищенную, доверенную среду передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети с одним или несколькими структурными подразделениями органа внутренних дел находящихся на значительном удалении.

Исходя из анализа программных комплексов, входящих в линейку продуктов «ViPNet CUSTOM» особенно стоит отметить программный комплекс ViPNet Client выполняющий на рабочем месте пользователя или сервере с прикладным программным обеспечением функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

VipNet Деловая почта, входящая в программный комплекс ViPNet Client, предназначена для организации защищенной передачи электронных документов по открытым каналам связи по всему маршруту следования документа от отправителя к получателю в сети ViPNet. В почтовый защищенный сервис входят следующие услуги, предоставляемые программой:

отправка и получение писем с прикрепленными к ним вложениями;

отправка файлов (в виде вложений) из Windows Explorer адресатам ViPNet;

получение подтверждений (квитанций) о доставке и использовании документов;

шифрование писем и вложений к ним;

электронная цифровая подпись (внутренними и внешними сертификатами) писем и вложений к ним;

электронная цифровая подпись (и проверка подписи) отдельных файлов (не вложений);

предоставление информации о документе: дате и времени создания и получения документа, размере документа (в килобайтах), информации о получателях и отправителях;

ведение регистрационной нумерации документов;

экспорт и импорт писем.

ViPNet Деловая почта обеспечивает гарантированную доставку сообщений, а так же передачу их по защищенному каналу связи. Кроме того, программа предоставляет гибкие возможности по работе с электронными документами: сортировка документов, архивация документов, поиск нужного документа, автоматическая обработка файлов и входящих писем в соответствии с различными правилами, задаваемыми пользователем (автопроцессинг) и другие.

Юридическую значимость электронным документам обеспечивает электронная подпись при соблюдении условий, описанных в Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Для автоматизации деятельности удостоверяющего центра при выполнении им своих целевых функций согласно действующего законодательства Российской Федерации и для автоматизации деятельности по управлению сертификатами открытых ключей, применяемых для шифрования, аутентификации и обеспечения достоверности информации в качестве примера можно взять программно-аппаратный комплекс «Удостоверяющий Центр «КриптоПро УЦ» (ПАК «КриптоПро УЦ»).

ПАК «КриптоПро УЦ» применяется для выполнения организационно – технических мероприятий в целях:

контроля целостности электронных документов, передаваемых в информационной системе органа внутренних дел;

контроля целостности публичных информационных ресурсов;

проверки подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных при информационном взаимодействии;

создания системы юридически значимой электронной подписи в информационной системе органа внутренних дел;

создания системы управления ключами подписи субъектов информационной системы органа внутренних дел.

Для построения системы защищенного и юридически значимого электронного документооборота органа внутренних дел предлагается использовать совместно два вышеупомянутых продукта.

Предлагается подписывать электронные документы средствами электронной подписи на рабочих местах пользователей информационной системы органа внутренних дел, а затем доставлять на рабочие места с ViPNet Деловая почта и отсылать через доверенную среду передачи данных.

Предложенная система защищенного и юридически значимого обмена электронными документами не может заменить систему электронного документооборота. Но в качестве первого шага перехода к безбумажному документообороту ее можно использовать.

**Литература**

1. Приказ МВД России от 4 мая 2012 года № 404 «О вводе в опытную эксплуатацию единой автоматизированной информационной системы электронного документооборота и делопроизводства»

2. Приказ МВД России от 31 мая 2011 года № 600 «Об утверждении Перечня документов, образующихся в деятельности органов внутренних дел Российской Федерации, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов»

3. Приказ МВД России от 20 июня 2012 года № 615 «Об утверждении инструкции по делопроизводству в органах внутренних дел Российской Федерации»

4. Симаков С.В., Клюев С.Г. «Методическое обеспечение проектирования комплексов средств защиты информации автоматизированных систем с определением критериев оптимальности», Вопросы защиты информации, 2007. № 4. с. 38-41.

# ОБЕСПЕЧЕНИЕ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В ПОДРАЗДЕЛЕНИЯХ СПЕЦИАЛЬНЫХ ФОНДОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

*Чикида В.И., Краснодарский университет МВД России,*
*Клюев С.Г., к.т.н., Краснодарский университет МВД России*

*В статье рассмотрены проблемы обеспечения сохранности документов образующихся в деятельности органов внутренних дел и представленных в электронном виде. Также рассмотрены вопросы функционирования подразделений специальных фондов в части касающейся организации работы электронных архивов для хранения документов в электронном виде.*

Развитие системы электронного документооборота в органах внутренних дел Российской Федерации и ее внедрение идет с постоянным наращиванием темпов. В частности, приказом МВД России от 4 мая 2012 года № 404 «О вводе в опытную эксплуатацию единой автоматизированной информационной системы электронного документооборота и делопроизводства» [1] утверждён порядок опытной эксплуатации единой автоматизированной информационной системы электронного документооборота и делопроизводства в подразделениях центрального аппарата Министерства внутренних дел Российской Федерации и территориальных органах МВД России.

Дополнительно к этому приказом МВД России от 31 мая 2011 года № 600 утвержден Перечень документов, образующихся в деятельности органов внутренних дел Российской Федерации, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов [2].

Исходя из этого все более актуальными становятся вопросы организации и функционирования архивов документов представленных в электронной форме, которые будут способны обеспечить

долговременную данных документов и баз данных образующихся в деятельности органов внутренних дел.

Внедрение электронного документооборота в системе органов внутренних дел России осуществляется немного позже, чем в правоохранительных органах развитых западных стран, поэтому на настоящий момент не в полной мере решен вопрос сохранности электронных документов, а также требует развития методическая база по обеспечению долговременной сохранности электронных документов. Обеспечение долговременной сохранности электронных документов, образующихся в деятельности органов внутренних дел – прямая обязанность подразделений специальных фондов, так как от сохранности документа зависит его дальнейшее использование.

С целью обеспечения долговременной сохранности электронных документов, подразделениям специальных фондов необходимо обеспечить физическую сохранность электронных документов и создать условия для считывания и воспроизведения хранящейся информации.

Обеспечение физической сохранности электронных документов не представляет особой сложности и для этого в подразделениях специальных фондов уже созданы необходимые условия. Дополнительными, с учетом специфики обработки и хранения электронных документов, мерами должны быть средства создания резервных копий на внешних носителях. Резервные копии позволят уберечь электронные копии от возможных стихийных бедствий сбоев аппаратуры или программного обеспечения. Обязательным условием при хранении резервных копий должна быть территориальная разнесенность мест их хранения.

Анализ технических характеристик современных носителей информации показал [3], что выбор носителей для хранения электронных документов должен зависеть от размеров хранимых электронных документов, установленных сроков хранения, а также частоты обращения к ним.

Также из указанного анализа следует, что для краткосрочного хранения электронных документов наиболее целесообразно использование оптических лазерных дисков (CD, DVD) или USB флеш-накопителей. Эти носители способны обеспечить сохранность электронных документов на заданное время.

Для обеспечения сохранности документов на бумажных носителях в подразделениях специальных фондов реализуются необходимые условия хранения, представляющие собой совокупность установленных температурно-влажностного, светового и санитарно-гигиенического режимов и специальных средствами хранения.

В отношении условий хранения электронных документов требования к условиям достаточно просты и относятся ко всем указанным выше носителям информации. Носители размещаются в вертикальном положении и помещаются в герметичную упаковку для защиты от загрязнения, запыления и воздействия прямых лучей света. Для сохранности носителей электронных документов необходимо строгое соблюдение температурно-влажностного режима, принятого для сохранности электронных носителей информации. При соблюдении этих условиях хранения можно рассчитывать на сохранность носителей электронных документов в течение 20 лет. К примеру, если оптический лазерный диск хранить при температуре +10°С, то срок хранения информации увеличивается до 50 лет, а нормативный режим хранения такого вида дисков +25°С. Из этого примера видно, что низкая температура способствует более долгому хранению информации, но такие условия хранения некомфортны для длительной работы сотрудников специальных фондов с электронными документами, а также это должно быть сопряжено с необходимостью работы с электронными документами в специально оборудованных помещениях. Дополнительно стоит упомянуть о том, что для перемещения носителя электронных документов в обычное служебное помещение для работы носитель должен пройти процесс акклиматизации, иначе в его работе могут возникнуть проблемы со считыванием информации и физическим состоянием носителя. Время необходимое для акклиматизации носителя электронных документов от температуры хранения до температуры +23-25° составляет около 14 часов.

Необходимо остановиться еще на одной проблеме при организации хранилищ электронных документов в подразделениях специальных фондов. Это проблема обеспечения условий для считывания и воспроизведения хранимых электронных документов. Указанная проблема напрямую связана со стремительным разви-

тием средств вычислительной техники и программного обеспечения и соответственно как результат этого – быстрое устаревание носителей электронных документов. К примеру, накопители на гибких магнитных дисках, которые уже исчезли из употребления, и новые модели компьютеров не оборудуются приводами для их считывания. Исходя из этого наиболее целесообразным представляется осуществление периодического электронных документов с устаревающих носителей на более новые.

В связи с постоянным ростом количества электронных документов и отсутствием единого подхода к решению проблем обеспечения их долговременной сохранности приказом Федерального агентства по техническому регулированию и метрологии от 17 сентября 2012 г. № 325-ст утвержден национальный Стандарт Российской Федерации ГОСТ Р 54989-2012/ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов» [4]. Указанный стандарт дает возможность уяснить пользователям электронной документации концепцию и стратегии, применяемые к такому типу документов для обеспечения их долговременной доступности.

ГОСТ Р 54989-2012/ISO/TR 18492:2005 разработан на основе действующего стандарта в европейских странах ISO 11799: 2003 с учетом современных проблем работы с электронными документами. Это еще раз доказывает, что работа с электронными документами в Российской Федерации еще находится на стадии развития, поскольку это – первый официальный документ в нашей стране, регламентирующий вопросы долговременной сохранности электронных документов.

Подводя итог данной статьи необходимо отметить, что в настоящее время подразделения специальных фондов органов внутренних дел остро нуждаются в методическом обеспечении деятельности направленной на долговременное хранение электронных документов. Данное методическое обеспечение должно содержать указания и практические рекомендации по обеспечению долговременной сохранности аутентичных электронных документов и возможности доступа к ним в тех случаях, когда срок их хранения превышает расчетный срок использования технологий (оборудования и программного обеспечения), используемых для со-

здания и поддержания этих документов. Также методическое обеспечение деятельности направленной на долговременное хранение электронных документов должно быть применимо к любым видам электронных документов и информации, созданной информационными системами органов внутренних дел.

**Литература**

1. Приказ МВД России от 4 мая 2012 года № 404 «О вводе в опытную эксплуатацию единой автоматизированной информационной системы электронного документооборота и делопроизводства»

2. Приказ МВД России от 31 мая 2011 года № 600 «Об утверждении Перечня документов, образующихся в деятельности органов внутренних дел Российской Федерации, с указанием сроков хранения, создание, хранение и использование которых осуществляется в форме электронных документов»

3. Симаков С.В., Клюев С.Г. «Методическое обеспечение проектирования комплексов средств защиты информации автоматизированных систем с определением критериев оптимальности», Вопросы защиты информации, 2007. № 4. с. 38-41.

4. Национальный Стандарт Российской Федерации ГОСТ Р 54989-2012/ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов».

# БЕСПИЛОТНО-ПИЛОТИРУЕМЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

*Пономарева И.М., Краснодарский университет МВД России,*
*Александров А.Г., Краснодарский университет МВД России*

*В статье рассмотрены основные направления использования беспилотно-пилотируемых летательных аппаратов в деятельности ОВД, раскрыты задачи, выполняемые с помощью БПЛА.*

Беспилотные технологии существуют давно. Сначала они были сложными и дорогостоящими комплексами, имевшими только военное применение. Но в течение последнего десятилетия в этой области произошел настоящий прорыв. Миниатюризация вычислительных систем и развитие спутниковой навигации

(GPS/ГЛОНАСС) позволили создавать беспилотные летательные аппараты (БПЛА), у которых габариты, масса, а главное, стоимость на порядки меньше прежних. По доступности беспилотные технологии приближаются к уровню бытовых технологий. Сейчас прогресс в развитии гражданских беспилотных систем имеет высочайший темп, сформировалась новая индустрия услуг.

БПЛА считаются весьма перспективными средствами для гражданских задач, связанных с однообразной, грязной или опасной деятельностью; т.е. выполнение которых связано с монотонностью или опасностью для пилота, пилотирующего воздушное судно (ВС). Рост потребности в БПЛА в разных странах вполне закономерен. Практический опыт применения БПЛА ведущими странами выявил широкий набор гражданских задач, при решении которых беспилотники показывают высокую эффективность.

Различают беспилотные летательные аппараты:

беспилотные неуправляемые

беспилотные автоматические

беспилотные дистанционно пилотируемые летательные аппараты (ДПЛА)

Беспилотные летательные аппараты принято делить по таким взаимосвязанным параметрам, как масса, время, дальность и высота полёта. Выделяют следующие классы аппаратов:

«микро» (условное название) массой до 10 килограммов, временем полёта около 1 часа и высотой до 1 километра,

«мини» – массой до 50 килограммов, временем полёта несколько часов и высотой до 3–5 километров,

средние («миди») – до 1 000 килограммов, временем 10–12 часов и высотой до 9–10 километров,

тяжёлые – с высотой полёта до 20 километров и временем полёта 24 часа и более.

Для определения координат и земной скорости современные БПЛА как правило используют спутниковые навигационные приёмники (GPS или ГЛОНАСС). Углы ориентации и перегрузки определяются с использованием гироскопов и акселерометров. Программное обеспечение пишется обычно на языках высокого уровня, таких как Си, Си++, Модула-2, Оберон SA или Ада95. В качестве аппаратного обеспечения, как правило, используются специализированные вычислители на базе цифровых сигнальных

процессоров или компьютеры формата PC/104, MicroPC. Также могут применяться операционные системы реального времени, такие как QNX, VME, VxWorks, XOberon.

Беспилотный авиационный комплекс предназначен для решения следующих задач:

Аэрофотосъемка объектов. Это наиболее востребованный вид работ, выполняемых с воздуха. Различают плановую и панорамную (видовую) аэрофотосъемку. Плановая фотосъемка выполняется вертикально по отношению к фотографируемому объекту. Панорамная фотосъемка производится под углом к горизонту, в результате чего получается панорамный аэроснимок.

Аэровидеосъемка объектов. В связи с увеличившейся разрешающей способностью современных видеокамер и отличным качеством картинки, беспилотную аэровидесъемку применяют не реже, чем обычную фотосъемку с воздуха. В дальнейшем получившийся видеоролик при необходимости нарезают на отдельные кадры, выбирают наиболее интересные и используют их как отдельные аэроснимки. Воздушная видеосъемка нередко применяется для получения красивого видеоотчета о торжественных мероприятиях и событиях, для рекламных целей. Это возможность снять захватывающий репортаж о спортивном состязании с воздуха и запечатлеть на память красочную шоу-программу.

Контроль периметра охраняемой территории. БПЛА способен без участия человека в роботизированном режиме подняться в воздух, облететь территорию по заданному маршруту с включенной видеокамерой или фотокамерой и возвратиться на место старта. В случае обнаружения нарушителя (человека или транспортного средства), проникшего на охраняемую территорию или приближающегося к ней, беспилотник подает сигнал тревоги на станцию (НСУ). Оператор может в любое время взять управление аппаратом на себя, выполнить необходимые действия и также вернуть его к выполнению поставленной задачи.

Помощь в поисково-спасательных работах. Во время проведения поисково-спасательных работ помощь беспилотного летательного аппарата сложно переоценить. Это устройство способно оказать необходимую первоочередную информационную под-

держку службам спасения при работах на море, в пустыне, на территории непроходимых болот, в зонах стихийного бедствия или техногенной катастрофы.

Обнаружение объектов. Роботизированный комплекс авианаблюдения обеспечивает поиск, обнаружение и идентификацию объектов в режиме реального времени. Определяет их точное местоположение с помощью спутниковых систем GPS или ГЛОНАСС и передает данные на наземную станцию управления. Объектами поиска могут быть: группы людей, отдельные люди, транспорт, очаги пожаров, затоплений, объекты недвижимости, мосты, дороги и другие сооружения. Комплекс позволяет вести поиск и обнаружение объектов как в дневное, так и в ночное время суток.

Координация действий. Постоянная пожароопасная ситуация в лесах, приведшая к колоссальному материальному ущербу, катастрофы, стихийные бедствия и другие чрезвычайные ситуации требуют наличия у служб спасения и ликвидации аварий эффективных технических средств оперативной координации действий. Таким средством являются дистанционно пилотируемые летательные аппараты с установленными на них новейшими видеокамерами, тепловизорами, камерами ночного видения. Вся информация с ДПЛА поступает в режиме реального времени на наземную станцию (НСУ) и в главный центр управления, что позволит оперативно координировать действия наземных сил.

Контроль температуры на объекте. Роботизированный авиационный комплекс с установленными тепловизором и пирометром способен проводить дистанционный контроль температуры в реакторах на таких сложных объектах, как АЭС. Аппарат способен зависать над объектом и проводить, при необходимости, более тщательный анализ. В остальное время БПЛА может обследовать оборудование станции в режиме патрулирования по заданной программе.

Контроль содержания токсичных веществ. На многих опасных производствах, даже при соблюдении всех мер безопасности, не исключены аварийные ситуации с возможным выбросом в атмосферу токсичных веществ. Для раннего обнаружения и оповещения персонала об утечке отравляющих веществ уже сейчас на некоторых предприятиях применяются сверхлегкие беспилотные

летательные аппараты с установленными на них датчиками и газоанализаторами. Облет территории и контроль содержания в воздухе токсичных выбросов может осуществляться в автоматическом режиме по заданному маршруту с возможностью перехода на полуавтоматическое управление БПЛА. Все данные с химических или радиационных датчиков летательного аппарата будут постоянно передаваться на станцию управления.

Контроль состояния воздушного судна в режиме реального времени осуществляется за счет двунаправленного обмена информацией между НСУ и БПЛА по защищенному радиоканалу. Если по каким-либо причинам нарушается связь между БПЛА и станцией управления, то автоматически включается режим возврата, и беспилотный летательный аппарат летит в точку запуска для штатной посадки. При восстановлении связи во время возврата аппарата оператор может возобновить выполнение поставленной задачи. Быстрая подготовка к полету БПЛА позволяет оперативно реагировать в любых ситуациях.

Для выполнения операций видеонаблюдения оператором предварительно планируется маршрут полёта БПЛА, который зависит от поставленной задачи и характера местности. При типовом алгоритме режима воздушного наблюдения участка местности или поиска объекта, БПЛА направляется в район мониторинга и выполняет там полёт по заданной оператором программе. В процессе полёта в заданном районе БПЛА передаёт видеоизображение местности и объектов на ней на наземную станцию управления (НСУ) в реальном масштабе времени. Оператор БПЛА оценивает поступающую информацию, при необходимости корректирует маршрут полета БПЛА и управляет бортовой целевой нагрузкой (например, видеокамерой).

В дополнительное оснащение комплекса дистанционного БПЛА могут входить следующие средства мониторинга (бортовые целевые нагрузки):

видеокамеры оптического диапазона;

видеокамеры инфракрасного (ИК) диапазона (тепловизорами);

фотоаппараты оптического диапазона;

ретрансляторы телефонной и радиосвязи;

радиолокационные средства.

Передача видеоинформации с БПЛА (видеокамеры или тепловизора) производится по радиоканалу на наземную станцию управления (НСУ). Запись информации на беспилотных самолётах производится на встроенный твердотельный накопитель видеорекордер (SSD HDD или compact flash/SD card) или передается на НСУ и записывается непосредственно в память компьютера.

**Литература**

1. Беспилотные летательные аппараты. Ясин Н.В., Попури, 2003г.
2. Информационный ресурс http://www.kmechte.ru/

# ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ ПО МОТИВАМ РАСОВОЙ, НАЦИОНАЛЬНОЙ ИЛИ РЕЛИГИОЗНОЙ НЕНАВИСТИ ИЛИ ВРАЖДЫ В СЕТИ ИНТЕРНЕТ

*Бедарев К.В., Барнаульский юридический институт МВД России, bekovi@mail.ru*

В настоящее время продолжают иметь место негативные тенденции в структуре и динамике преступлений экстремистской направленности, а качественно новые условия функционирования органов внутренних дел требуют комплексного применения всех сил, средств и методов противодействия преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды.

Современный экстремизм с точки зрения управления и организации развивается не менее стремительно, чем новейшие технологии. Массовая доступность сети Интернет и средств персональной связи дают современным экстремистам огромные возможности для планирования своих мероприятий и организации связи между собой.

По словам директора ФСБ России А.В. Бортникова, сегодня Интернет превратился в универсальный инструмент для привлечения и вербовки экстремистами новых членов, их обучения, планирования и координации экстремистской деятельности. Именно там

разворачивается сейчас настоящая война за умы и сердца простых граждан, прежде всего молодежи.

Именно в виртуальном мире экстремисты получают недопустимую в реальном обществе свободу творчества и становятся не только потребителями, но и создателями экстремистских лозунгов. Интернет-пространство активно используется для ведения идеологической пропаганды и достижения преступных целей, направленных на возбуждение ненависти или вражды.

В свою очередь, массовая распространенность информационных технологий и их повсеместное использование чрезвычайно затрудняет поиск и обнаружение экстремистских групп, их активных и тайных участников.

Статистика показывает постоянный рост преступлений экстремистской направленности, совершенных в сети Интернет. Так, в 2012 году на территории Сибирского федерального округа РФ было зарегистрировано всего 94 преступления экстремистской направленности и более половины из них совершены путем размещения в сети Интернет материалов, направленных на возбуждение расовой, национальной или религиозной ненависти или вражды. В 2013 году эти показатели были достигнуты уже в сентябре, и, по итогам девяти месяцев, на территории округа было зарегистрировано 96 преступлений экстремистской направленности, из которых больше всего в Алтайском крае – 16, Кемеровской и Новосибирской областях – по 15, Забайкальском крае – 12, Иркутской области – 11. Из числа преступлений указанной категории более половины совершены с использованием сети Интернет.

По окончании 2013 года в Сибирском федеральном округе РФ было зарегистрировано 117 преступлений экстремистской направленности – это на четверть больше, чем в 2012 году или каждое седьмое в стране. Это количество примерно соответствует сумме зарегистрированных аналогичных преступлений в двух, по сути воюющих на переднем крае борьбы с экстремизмом и терроризмом регионах, таких как Северокавказский (87 или 10,0%) и Южный (52 или 6,0%). Причём показатель, например, одного только Алтайского края (21) не на много меньше, чем во всём Дальневосточном федеральном округе (22), включающем в себя девять субъектов Российской Федерации.

На современном этапе, противодействуя экстремизму в сети Интернет, оперативные подразделения органов внутренних дел сталкиваются с совершенно новыми проблемами технического оснащения и организационного реформирования, необходимого опыта решения которых еще не наработано.

Следует отметить, что именно от тактики опережения, предупреждения и оперативного пресечения криминальной ситуации сегодня многое зависит в сфере противодействия экстремизму в России.

Федеральный закон, регламентирующий рассматриваемую сферу общественных отношений, устанавливает, что противодействие экстремистской деятельности осуществляется в направлении выявления, предупреждения и пресечения экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

Правовую основу данной деятельности также составляют, в частности, ведомственные правовые акты, среди которых определяющее место занимает приказ МВД России от 31.10.2012 № 987 «Об утверждении Наставления по организации деятельности подразделений органов внутренних дел Российской Федерации и внутренних войск МВД России, осуществляющих в пределах компетенции выявление, предупреждение, пресечение и раскрытие преступлений террористического характера, преступлений и правонарушений экстремистской направленности, а также расследование преступлений террористического характера и экстремистской направленности».

Исследование правовой основы позволяет сделать вывод о том, что имеющиеся в арсенале органов внутренних дел меры противодействия преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды не учитывают специфики противоправных действий в виртуальном пространстве.

В последние годы экстремисты стали размещать множество видеороликов, аудиофайлов в социальной сети «ВКонтакте», «YouTube» и других. Операторы связи, предоставляющие телекоммуникационные услуги доступа к информационной сети Интернет, имеют техническую возможность ограничения доступа к экстремистским материалам путем фильтрации трафика и полного

блокирования доступа к IP-адресу сайта или отдельной странице сайта, на которой размещен материал (аудио, видеофайл, печатный текст).

Однако часто бывают случаю, когда необходимо незамедлительно ограничить доступ пользователей социальных сетей к контенту, содержащему призывы к экстремистским действиям. Ранее для этого требовалось дождаться окончания официальной процедуры по признанию его экстремистским, то есть решения суда и внесения страницы в единый реестр экстремистских сайтов. 01 февраля 2014 года вступил в силу Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации», который предусматривает немедленную и внесудебную блокировку сайтов, распространяющих экстремистские материалы. С этого дня в России сайты с экстремистской информацией стали блокировать в течение часа после получения предписания прокурора. Для разблокировки владельцу ресурса надо удалить противоправный контент и только после этого Роскомнадзор восстанавливает доступ к ресурсу. Отметим, что 1 февраля ведомство заблокировало сразу четыре сайта, самая старая запись датирована 2010 годом, самая свежая – 29 января 2014 года, но она никакого отношения к России не имеет, поскольку является призывом выйти на Майдан в Киеве.

Полагаем, что, несмотря на фильтрацию и блокировку сайтов, содержащих информационные материалы экстремистского характера, они должны внимательно изучаться сотрудниками оперативных подразделений для выявления источников и каналов финансирования экстремизма, изучения и составления криминологических портретов лидеров, непримиримых и активных участников международных экстремистских организаций, структуры организованных преступных формирований, способов связи и конспирации, интенсивности посещаемости этих сайтов пользователями, участия в форумах и т.д.

Рассмотрим подробнее некоторые проблемы противодействия преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды, на наш взгляд, оказывающие наибольшее негативное влияние на эффективность этой деятельности.

В первую очередь следует отметить, что в силу специфики сети Интернет установление субъекта правонарушения связано со значительными трудностями, обусловленными экстерриториальностью Интернета и анонимностью большого числа его пользователей. Анонимность пользователей сайтов, на которых размещены информационные материалы экстремистского характера, затрудняет выяснение вопросов о количестве посетивших сайт лиц, их установочных данных, местах нахождения и др. В этой связи, эффективным способом противодействия преступлениям, совершаемым по мотивам расовой, национальной или религиозной ненависти или вражды в сети Интернет выступает ликвидация анонимности пользователей данных сайтов. В настоящее время на законодательном уровне рассматривается данный вопрос, в первую очередь о необходимости блокировки доступа из российского сегмента сети Интернет к серверам «Tor» и другим анонимным сетевым центрам.

Другая проблема связана с основаниями проведения оперативно-розыскных мероприятий. Осуществляя мониторинг сети Интернет, сотрудник оперативного подразделения инициативно выявляет латентные преступления экстремистской направленности и вынужден проводить оперативно-розыскные мероприятия. Однако следует учесть, что на данном первоначальном этапе могут отсутствовать сведения, ставшие известными оперуполномоченному о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, а также иные основания для проведения оперативно-розыскных мероприятий. Учитывая изложенное, считаем необходимым внести изменения в часть 1 статьи 7 Федерального закона «Об оперативно-розыскной деятельности», дополнив ее самостоятельным основанием, предусматривающим инициативно выявлять факты преступной деятельности.

Результаты анализа современного состояния оперативных подразделений, свидетельствуют о наличии дополнительных проблем по противодействию экстремизму в сети Интернет. Большинство сотрудников оперативных подразделений органов внутренних дел оценивают свою подготовленность к работе в рассматри-

ваемом направлении не соответствующей в полном объеме предъявляемым требованиям. В то же время преступники становятся более организованы, профессиональны и данное несоответствие уровня подготовки противостоящих им оперативных сотрудников представляет серьезную проблему.

Для повышения эффективности противодействия экстремизму в сети Интернет необходимо в ближайшее время разработать специальные программы обучения сотрудников оперативных подразделений органов внутренних дел. Такие программы должны формировать комплекс профессиональных умений и навыков по выявлению и документированию экстремистских проявлений в сети Интернет.

Кроме того, остается проблемным вопросом проведение психолингвистических исследований и экспертиз. Для документирования выявленных в ходе мониторинга интернет-сайтов признаков экстремистской деятельности, необходимо точное доказывание в действиях правонарушителей умысла на совершение уголовно-наказуемого деяния. Для этого требуется проведение психолингвистических исследований и экспертиз, которые должны достоверно установить в исследуемых материалах признаки экстремистской деятельности. Однако специалисты-эксперты подобного профиля в большинстве экспертных подразделений системы МВД отсутствуют или их квалификация не отвечает требованиям, предъявляемым органами предварительного следствия и судом. В то же время, проведение подобных исследований и экспертиз в частных экспертных организациях связано со значительными материальными затратами.

В связи с этим, из-за длительного или некачественного проведения исследований, зачастую утрачиваются возможности получения доказательств экстремистской деятельности, что приводит к возникновению у определенной части населения убежденности в безнаказанности разжигания розни и дальнейшему распространению экстремистской идеологии на территории достаточно благополучных в этом отношении регионов России.

**Литература**

1. Бортников. Террористы используют Интернет для вербовки. URL: http://actualcomment.ru/news/27040/.

2. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 28 декабря 2013 N 398-ФЗ: – [Электронный ресурс] // Информационно-справочная система «Консультант Плюс». – электрон. дан. – [М.] – URL: http//www.consultant.ru., свободный. – Заглавие с экрана. – Яз. рус. – (Дата обращения: 15.05.2014).

3. О противодействии экстремистской деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ: – [Электронный ресурс] // Информационно-справочная система «Консультант Плюс». – электрон. дан. – [М.] – URL: http//www.consultant.ru., свободный. – Заглавие с экрана. – Яз. рус. – (Дата обращения: 15.05.2014).

4. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ: – [Электронный ресурс] // Информационно-справочная система «Консультант Плюс». – электрон. дан. – [М.] – URL: http//www.consultant.ru., свободный. – Заглавие с экрана. – Яз. рус. – (Дата обращения: 15.05.2014).

5. Об утверждении Наставления по организации деятельности подразделений органов внутренних дел Российской Федерации и внутренних войск МВД России, осуществляющих в пределах компетенции выявление, предупреждение, пресечение и раскрытие преступлений террористического характера, преступлений и правонарушений экстремистской направленности, а также расследование преступлений террористического характера и экстремистской направленности: Приказ МВД России от 31 октября 2012 г. № 987.

# ОБЗОР СИСТЕМ ШИРОКОПОЛОСНОГО ДОСТУПА

*Глотов А.С., Московский университет МВД России, a.s.glotov@mail.ru*
*Шуткин А.В., Московский университет МВД России*

*Рассмотрены основные современные методы построения систем высокоскоростного доступа, их достоинства и недостатки.*

Одной из важнейших проблем в нашей стране продолжает оставаться обеспечение массового доступа абонентов к современным телекоммуникационным и информационным услугам.

Вместе с распространением разнообразных технологий широко-полосного доступа, например цифровой пользовательской линии (DSL, Digital Subscriber Line), основанной на витой паре,

оптоволоконном доступе и беспроводном доступе, операторы ожидают развития большего количества услуг по радио сети, причем особое внимание уделяется видео услугам, включающим в себя трансляцию видео, видео по запросу (VoD, Video on Demand) и т.д.

Актуальность этого вопроса возрастает в первую очередь в связи с бурным развитием и внедрением в повседневную жизнь человека глобальной сети Интернет, доступ к которой требует резкого увеличения пропускной способности сетей абонентского доступа, в связи с необходимостью обеспечения всего спектра интегральных услуг. Широкополосный доступ (ШПД) – ключевой элемент современных телекоммуникаций, которые невозможно представить без наличия разнообразных услуг, основанных на передаче различныхтипов трафика – данных, голоса, видео, мультимедиа.

Под широкополосным (высокоскоростным) доступом понимается доступ в Интернет со скоростью передачи данных, превышающей максимально возможную при использовании коммутируемого доступа с использованием модема и телефонной сети общего пользования.

Каналы связи абонентских сетей современных операторов опираются на различныефизические среды проноса трафика:

традиционные медные кабели ТСОП (Телефонная сеть общего пользования) (англ. PSTN, Public Switched Telephone Network);

оптические среды – оптоволоконные кабели и беспроводные оптические линии.

радиоканалы в различных частотных диапазонах;

Систему ШПД можно разделить на две больших группы – фиксированный широкополосный доступ и мобильный широкополосный доступ.

Фиксированный ШПД строится на основе проводных соединений, в то время как мобильный ШПД включает в себя передачу данных по беспроводным соединениям.

Если традиционный (коммутируемый) доступ имеет ограничение по пропускной способности, порядка 56 кбит/с и полностью занимает телефонную линию, то широкополосные технологии обеспечивают во много раз большую скорость обмена данными и

не монополизируют телефонную линию. Кроме высокой скорости широкополосный доступ обеспечивает непрерывное подключение к Интернету (без необходимости установления коммутируемого соединения) и так называемую «двустороннюю» связь, то есть возможность как принимать («загружать»), так и передавать («выгружать») информацию на высоких скоростях.

Мобильный ШПД в настоящее время использует технологии беспроводной передачи данных, такие как Bluetooth, Wi-Fi, DECT, WCDMA/HSPA (поколение 3.5G), HSPA+ (поколение 3.75G). Также применяются технологии 4G: WiMax, LTE и др.

Беспроводные технологии, обладают рядом уникальных преимуществ и играют важную роль в развитии систем широкополосного доступа.

Эти технологии имеют различные области применения. Они предназначены для организации небольших беспроводных сетей внутри помещений и построения беспроводных мостов. В свою очередь любая информационная услуга для качественного ее предоставления, определяет свои требования к каналу передачи информации от его пропускной способности до качества такой передачи.

На территории Российской Федерации в настоящее время эксплуатируются стандарты сотовой связи второго и третьего поколения. Наиболее популярным стандартом второго поколения является стандарт GSM, использование которого началось в начале 90х годов 20 века. Данный стандарт предусматривает работу в частотных диапазонах 900, 1800, 1900 МГц. На территории Российской федерации используются частотные диапазоны 900 и 1800 МГц.

В стандарте GSM используется комбинированная TDMA (Time Division Multiple Access — множественный доступ с разделением по времени) и FDMA (Frequency Division Multiple Access – множественный доступ с разделением каналов по частоте) схема организации каналов – многостанционный доступ с временным и частотным разделением каналов. В структуре TDMA кадра содержится 8 временных окон на каждой из 124 несущих для 900 МГц и 374 несущих для 1800 МГц. Каждое окно имеет номер от 0 до 7. Нулевое окно обычно используется для передачи служебной информации, остальные окна для передачи информации абонентами

или базовой станцией абонентам. После оцифровки и сжатия речь может быть передана за гораздо меньший промежуток времени, чем она занимала в не сжатом виде. Таким образом, каждый передатчик передает сигнал только в своем временном окне, остальное время он сжимает речь. Максимальное количество каналов, организуемых в базовой станции 16-20. Длительность каждого TDMA кадра ~4.63 мс, а длительность передачи в одном окне кадра ~576.6 мкс.

Стандарт GSM в Российской Федерации предусматривает работу устройств на следующих частотах:

890-915 МГц для передатчиков подвижных станций, «от подвижной станции к базовой станции» – восходящий канал (uplink);

935-960 МГц для передатчиков базовых станций, нисходящий канал для передачи данных в режиме «от базовой станции к подвижной станции» (downlink);

1710-1785 МГц для передатчиков подвижных станций, «от подвижной станции к базовой станции» – восходящий канал (uplink);

1805-1880 МГц для передатчиков базовых станций, нисходящий канал для передачи данных в режиме «от базовой станции к подвижной станции» (downlink).

В Российской Федерации также задействован дополнительный диапазон частот E-GSM (Extended GSM), который подразумевает работу в нем устройств стандарта GSM.

880-890 МГц для передатчиков подвижных станций, «от подвижной станции к базовой станции» – восходящий канал (uplink);

925-935 МГц для передатчиков базовых станций, нисходящий канал для передачи данных в режиме «от базовой станции к подвижной станции» (downlink).

В настоящее время операторы некоторых регионов Российской Федерации используют диапазон частот E-GSM под нужды стандарта сотовой связи третьего поколения – UMTS (Universal Mobile Telecommunications System). Стандарт UMTS допускает возможность использования следующих способов разделения частотного ресурса (множественного доступа): FDD либо TDD. В России UMTS используется с FDD доступом.

Согласно спецификациям стандарта, UMTS в Российской Федерации использует следующий диапазон частот:

Для FDD доступа:

1920 МГц – 1980 МГц для передатчиков подвижных станций, «от подвижной станции к базовой станции» – восходящий канал (uplink);

2110 МГц – 2170 МГц для передатчиков базовых станций, нисходящий канал для передачи данных в режиме «от базовой станции к подвижной станции» (downlink).

Для TDD доступа выделены частотные диапазоны 1900 – 1920 МГц и 2110 – 2170 МГц.

Понятия uplink и downlink каналов для TDD нет – оба поддиапазона могут использоваться для передачи как подвижными, так и базовыми станциями. При TDD отсутствует понятие дуплексного разноса между частотами.

Технология Bluetooth предназначена для унификации возможностей ближней радиосвязи. Устройство Bluetooth – это внедрённое в микрочип радиоустройство ближнего действия. Стандарты Bluetooth разрабатываются и публикуются промышленным консорциумом Bluetooth SIG (Special Interest Group). Работая в диапазоне 2,4 ГГц (диапазон ISM – общедоступные частоты для маломощных устройств), два аппарата Bluetooth, находящиеся на расстоянии до 10 м, могут передавать данные со скоростью до 720 кбит/с, а при использовании технологии EDR (Enhanced Data Rate – повышенная скорость передачи) которая, начиная с версии 2.0, составляет до 2200 кбит/с. При применении устройства Bluetooth с дополнительным усилителем мощности, расстояние передачи может быть увеличено до 100 м. Технология Bluetooth рассчитана на работу в среде со многими пользователями, позволяя организовывать эпизодические ad-hoc сети.

Все устройства сети делятся на ведущие (master) и подчинённые (slave). Обмен информацией может осуществляться только между ведущим и подчинённым устройствами, при этом каждое устройство может быть и ведущим и подчинённым.

Основным элементом организации сетей Bluetooth является пикосеть, состоящая из одного ведущего устройства и 1-7 активных подчинённых устройств. Кроме того, в одну пикосеть может входить неограниченное количество устройств, находящихся в неактивном режиме. Подчинённое устройство может сообщаться только с ведущим, причём только тогда, когда это разрешает ведущее устройство. В каждый момент времени обмен данными может

идти только между двумя устройствами в одном направлении. Любое устройство одной пикосети может также входить в другую пикосеть в качестве как подчинённого, так и ведущего.

Технология Wi-Fi организации беспроводных сетей построена на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Первая спецификация Wi-Fi – 802.11 предусматривала передачу сигнала на выбор тремя различными способами. В двух из них использовались радиочастоты в диапазоне от 2400 МГц до 2483 МГц, в частности, один основывался на методе частотных скачков FHSS (Frequency Hopping Spread Spectrum), а другой – на методе прямой последовательности DSSS (Direct Sequence Spread Spectrum). В третьем же задействовался инфракрасный диапазон, причем между точкой доступа и клиентами не требовалось прямой видимости, так как сигнал должен был передаваться отраженным от потолка.

Однако не будем останавливаться на этом подробнее, ведь сейчас уже непросто найти сети, работающие по этому стандарту. В спецификации 802.11b от былых трех методов остался всего один – DSSS. А для стандартов 802.11a и 802.11g был избран новый метод – OFDM (Orthogonal Frequency Division Multiplexing), при этом сигнал расщепляется на множество меньших, которые пересылаются одновременно по нескольким частотам. При этом спецификация 802.11a отличается от всех остальных тем, что задействуется другой диапазон частот: 5150-5825 МГц.

Еще одной особенностью Wi-Fi является то, что весь спектр используемых частот условно разделяется на несколько каналов (узких полос частот), частично перекрывающих друг друга. Однако для нормальной работы сети необходимо, чтобы разные каналы не использовали общие частоты, поэтому одновременно в одном месте может работать не более трех каналов в сети 802.11b/g и не более восьми каналов в сети 802.11a.

Кстати, далеко не во всех странах разрешается использовать Wi-Fi на безлицензионной основе – иногда для установки Wi-Fi

точки требуется получить соответствующее разрешение, а в некоторых странах и вовсе запрещается занимать определенные частоты, поэтому для этих стран выпускается оборудование Wi-Fi с урезанным диапазоном.

Для всех Wi-Fi спецификаций 802.11 максимальное расстояние уверенного приема сигнала находится в районе 300-400 метров для открытых помещений, и 90 метров – для закрытых. Данное ограничение не является строгим, и при использовании направленных антенн в случае прямой видимости возможен прием сигнала на расстоянии порядка нескольких километров. Впрочем, не стоит рассчитывать на то, что максимальная скорость передачи данных будет обеспечиваться на любом расстоянии – при отдалении от точки доступа пропускная способность снижается пропорционально расстоянию. Кстати, электромагнитные волны в диапазоне 2.4 ГГц весьма болезненно реагируют на прохождение через различные препятствия, поэтому в сильно заставленных помещениях с большим количеством перегородок зона охвата точек доступа резко снижается. В диапазоне 5 ГГц дела обстоят заметно хуже, поэтому для покрытия того же помещения приходится или увеличивать количество точек доступа, или стараться подбирать им оптимальное размещение, например, ближе к потолку. Еще одним фактором, мешающим работе беспроводной сети Wi-Fi, может оказаться другое оборудование, работающее в том же диапазоне частот. Самым ярким примером служат микроволновые печи, которые излучают электромагнитные волны как раз с частотой порядка 2.4 ГГц – на которой и работает большинство приёмо-передатчиков Wi-Fi сетей (802.11a и 802.11b).

Технология WiMAX, в свою очередь, предназначена для организации широкополосной связи вне помещений и для организации крупномасштабных сетей. WiMAX разрабатывался как городская вычислительная сеть (MAN).

Технологической основой WiMax (World wide Interoperability for Microwave Access) является новый протокол IEEE 802.16, который позволяет обеспечить одновременно широкополосный высокоскоростной доступ в Интернет и передачу данных, а также и услуги телефонии без использования кабельных линий. В отличие от других технологий радиодоступа, WiMax позволяет работать в

условиях плотной городской застройки вне прямой видимости базовой станции. Это очень актуально для крупных мегаполисов, так как не нужно устанавливать специальные вышки, а достаточно установить базовую станцию на крышах зданий или высотных сооружений, что позволяет очень быстро развернуть такую сеть на большие расстояния.

Еще один немаловажный плюс этой технологии, в отличие от Wi-Fi, радиус покрытия которого не превышает 100 метров, – зона покрытия WiMax, при определенных условиях, может достигать 50 км. Поэтому она может быть полезна таким людям, для которых, недоступен Интернет или даже обычная телефония, например в отдаленных районах, где просто нет возможности провести кабельные сети или DSL. А таких пользователей по всей России немало, поэтому WiMax в нашей стране будет развиваться достаточно быстро и будет иметь успех не только у корпоративных клиентов и различных организаций, но и у частных пользователей, при одном, конечно, условии, что плата за оборудование будет достаточно невысокой. Эта технология позволит предприятиям с множеством филиалов (например, торговые сети) строить на базе WiMax свои фирменные беспроводные сети – один комплект оборудования позволяет получить до 8-ми телефонных номеров, с выходом в городские телефонные сети, высокоскоростной Интернет. Таким образом, например, три филиала компании, имеющих три отдельные локальные сети на основе Wi-Fi, могут быть объединены в единую с центральным офисом WiMax-сеть. Потому данная система разработана специально для решения такого рода проблем.

В заключение можно отметить, что принят Федеральный закон N 9-ФЗ «О внесении изменений в Федеральный закон «О связи» от 3 февраля 2014 г., направленный на реформирование системы универсального обслуживания. В рамках реализации этого закона все населенные пункты с количеством жителей от 250 до 500 будут подключены к услугам ШПД по современным каналам связи. В ходе решения этой задачи оптоволоконные сети построят и во всех остальных, более крупных населенных пунктах.

К 2018 году планируется достичь показателя 90-93% – современные услуги связи будут доступны во всех населенных пунктах численностью более 500 жителей. В дальнейшем связь появится в

населенных пунктах, где проживают более 250 человек, а этот критерий увеличится до 96-97%.

По итогам 2013 года уровень проникновения услуг ШПД в России составил около 55%.

**Литература**

1. «CDMA». [Электронный ресурс]: http://ru.wikipedia.org/wiki/CDMA
2. «Стандарт сотовой связи CDMA-взгляд глазами профессионалов». [Электронный ресурс]: http://www.radioscanner.ru/info/article108/
3. «DECT». [Электронный ресурс]: http://ru.wikipedia.org/wiki/DECT
4. «Безопасность стандарта DECT». [Электронный ресурс]: http://infoch.info/view_lesson.php?id=60
5. «Методы поиска электронных устройств перехвата информации с использованием сканерных приемников и программно-аппаратных комплексов контроля». [Электронный ресурс]: http://www.analitika.info/poisk.php
6. «ZigBee». [Электронный ресурс]: https://docs.google.com/document/d/1WZNJBPJn-99yP1Vp96MjuqIwklfdE-0gPoyE6sOlmkc/edit?pli=1
7. «WiFi». [Электронный ресурс]: https://docs.google.com/document/d/1nd_SYYtqkS3jcuzzzOmwwcDcy6uzNK7K0HUV6LKo3i8/edit?pli=1
8. «Bluetooth». [Электронный ресурс]: https://docs.google.com/document/d/1q_3i6xjCAKWJpKQsjAqyWC7oUlpteCthd3ZQQlt_nfs/edit?pli=1
9. «WiMax». [Электронный ресурс]: https://docs.google.com/document/d/10nJmok0MqSHN3MQIdggsVq6yXfIT2DdkBsfmZEm2iQ/edit?pli=1

# СЕТЕВАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ

*Меньших В.В., д-р физ.-мат. наук, профессор,*
*Воронежский институт МВД России*
*Толстых О.В., к.т.н., Воронежский институт МВД России*
*Толстых А.В., Воронежский институт МВД России*

В настоящее время осуществляется активное внедрение современных информационных технологий в деятельность органов внутренних дел. Однако, использование этих технологий, обеспечивая повышение эффективности решения служебных задач сотрудниками, вместе с тем существенно увеличивает риск возникновения угроз информационной безопасности (ИБ) на объектах

информатизации. В целях противодействия этим угрозам создаются системы защиты информации (СЗИ) [1]. В связи с этим актуальной является задача оценки эффективности вариантов СЗИ на объектах информатизации ОВД. В интересах решения этой задачи предлагается разработать модель на основе использования аппарата сетей Петри.

Сеть Петри $C$ является четверкой $C= (P, T, I, O)$, где $P=\{p_1, p_2,..., p_n\}$- конечное множество позиций, $T=\{t_1, t_2,..., t_n\}$- конечное множество переходов. Множество позиций и множество переходов не пересекаются, $I:T\rightarrow P^k$является входной функцией – отображением переходов в комплекты позиций,$O:T\rightarrow P^k$есть входная функция – отображение переходов в комплекты позиций [2].

Рассмотрим фрагмент сети, представленный на рис.1. Далее во избежание громоздкости будем иллюстрировать описание модели только для приведённого фрагмента. Принципиальных отличий при моделировании произвольной сети нет.

Рис. 1. Фрагмент компьютерной сети

В сетях Петри допускается возможность существования конфликтов, если из компьютера, которому соответствует позиция, угроза безопасности информации одного и того же типа может распространяться на несколько других элементов, т. е. маркирующая эту угрозу фишка удаляется из позиции. Кроме того, удаление фишки из позиции означало бы исчезновение угрозы на соответствующем компьютере, что противоречит логике решаемой задачи (рис. 2).

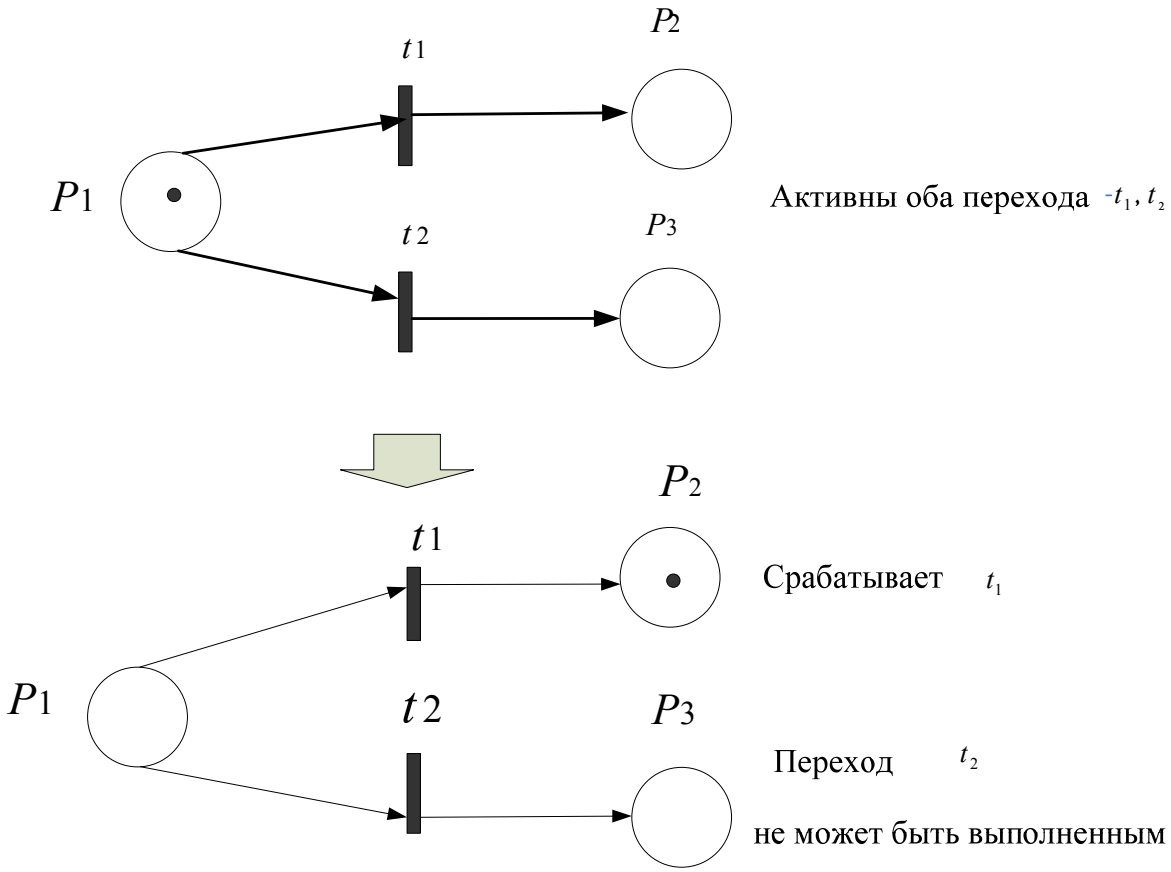



Рис. 2. Пример возникновения конфликта в сети Петри

Этого недостатка можно избежать, если каждую позицию, соответствующую компьютеру, преобразовать в так называемую «ловушку», т. е. позицию, которую не может покинуть ни одна фишка [2]. Для этого можно применить преобразование, показанное на рис. 3.


Рис. 3. Пример преобразования исключения конфликта в сети Петри

Для предотвращения реализации угроз безопасности информации на компьютерах применятся системы защиты информации (СЗИ).

Обратимся к рассмотрению вопроса моделирования действий элементов СЗИ, осуществляющих устранение угроз безопасности

информации на самих компьютерах. Такие элементы можно моделировать с помощью введения дополнительно позиций-ловушек. Их действие показано на рис. 4.

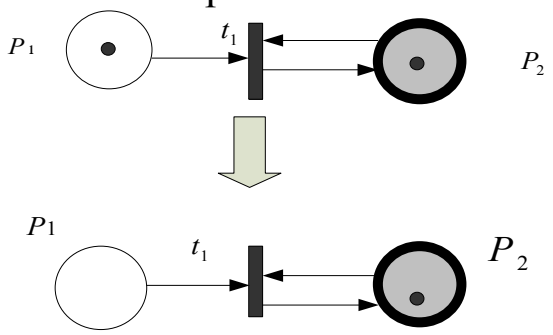



Рис. 4. Фрагмент сети Петри, содержащей позицию ловушку, соответствующую элементу СЗИ, устраняющему угрозу безопасности информации на компьютере

Поставим в соответствие компьютерам фрагмента нашей сети множество позиций *p*, линиям связи, способствующим распространению угроз, множество переходов *t*, фишки будут соответствовать угрозам [2]. Данная сеть представлена на рис 5. Маркирование позиции (появление в позиции фишки) моделирует наличие угрозы информационной безопасности. Будем считать, что количество фишек задаётся логическими переменными, принимающими значения 0 или 1. Поэтому повторное появление угрозы также маркируется одной фишкой.

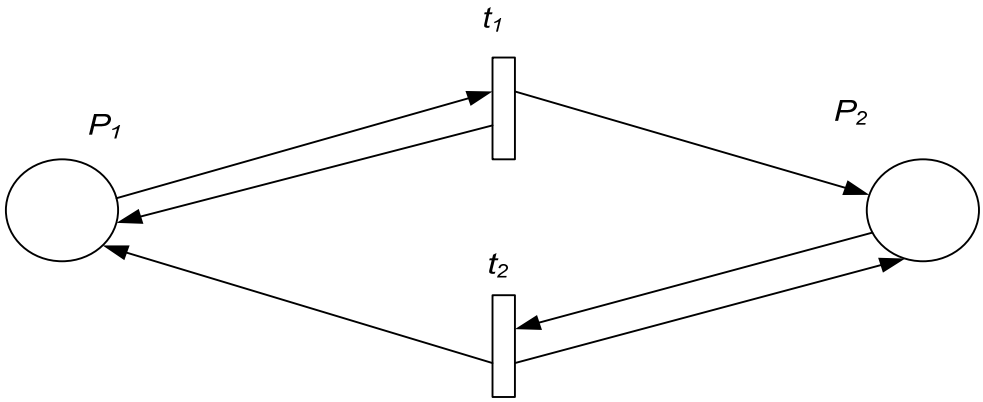



Рис. 5. Сеть Петри, соответствующая фрагменту сети

Рассмотрим компьютерную сеть с размещёнными на ней элементами СЗИ (рис.6).

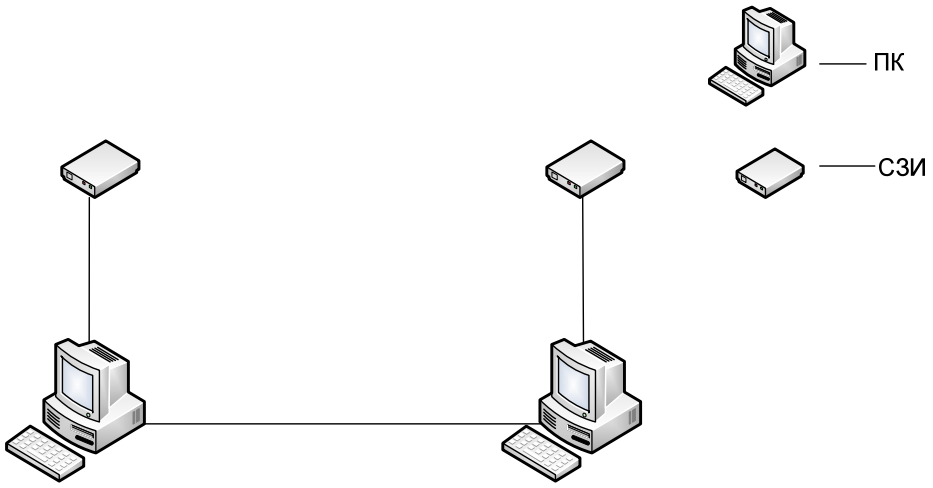



Рис. 6. Сеть, оборудованная элементами СЗИ

Сеть Петри, соответствующая данной сети, представлена на рис. 7. Выделенными позициями ($P_3$,$P_4$) обозначены элементы СЗИ.

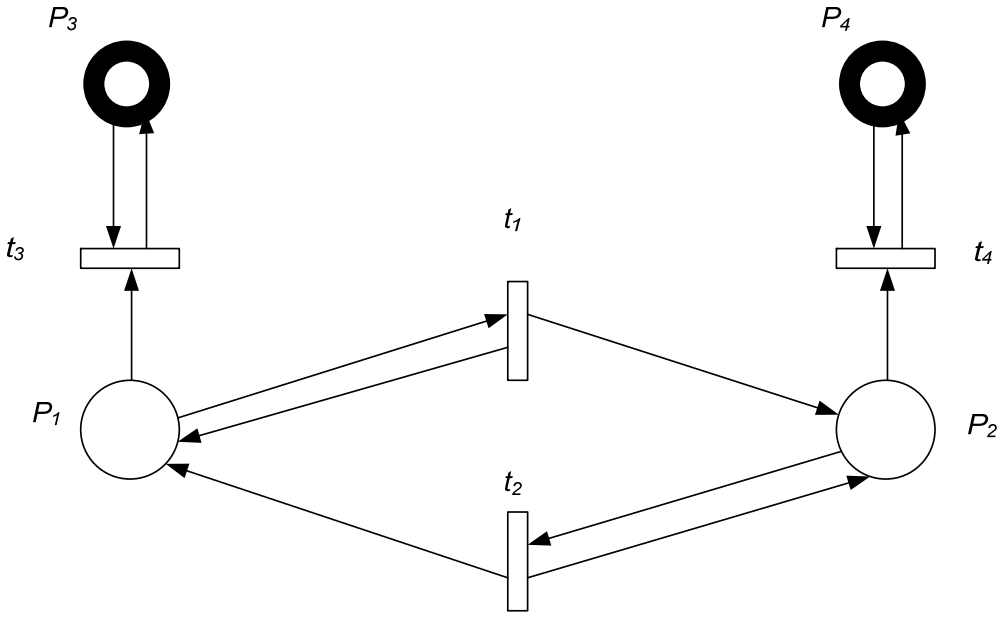



Рис. 7. Сеть Петри, содержащая элементы СЗИ

На основе предложенной сетевой модели может быть разработана имитационная модель, позволяющая оценить вероятности наличия угроз информационной безопасности на элементах компьютерной сети.

**Литература**

1. Герасименко В.А., Малюк А.А. Основы защиты информации: Учебник для высших учебных заведений Министерства общего и профессионального образования РФ / В.А. Герасименко, А.А. Малюк. – М.: МИФИ, 1997. – 538 с.

2. Питерсон Дж. Теория сетей Петри и моделирование систем/ Дж. Питерсон. – М.: Мир, 1984. – 264 с.

# ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ИМИТАЦИОННОЙ МОДЕЛИ РАСПРОСТРАНЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СЕТЕЙ ПЕТРИ

*Меньших В.В., д-р физ.-мат. наук, профессор,*
*Воронежский институт МВД России*
*Толстых А.В., Воронежский институт МВД России*

Актуальность повышения эффективности систем защиты информации для органов внутренних дел определяется широким распространением современных информационных технологий, используемых для обработки, хранения и передачи служебной информации. Одним из перспективных методов оценки эффективности систем защиты информации в компьютерных сетях различного назначения [1] является имитационное моделирование, разработка которых может быть осуществлена на основе использования аппарата сетей Петри [2]. В [3] разработана сетевая модель, которая позволяет описывать на языке сетей Петри как процесс распространения, так и процесс устранения угроз информационной безопасности в компьютерной сети. В данной работе описывается программная реализация на языке C++ имитационной модели, основанная этой сетевой модели. Программа позволяет определять вероятности нахождения элементов компьютерной сети под угрозами ИБ на основе имитационного моделирования описанных выше сетей Петри.

Для заданной начальной маркировки сети, описывающей наличие угроз на компьютерах и включение элементов СЗИ определялись вероятности нахождения компьютеров под угрозами за

достаточно большой промежуток времени *T*. При этом считались заданными вероятности распространения и устранения угроз ИБ, т. е. вероятности выполнения переходов сети.

В представленной версии были использованы следующие ограничения, которые могут быть значительно снижены: количество элементов компьютерной сети (компьютеров и элементов СЗИ) – до 100; количество каналов распространения и устранения угроз – до 100.

Введем обозначения:

*M* – начальная маркировка;

*Q*- вероятность срабатывания перехода;

*S*- вероятность нахождения компьютера компьютерной сети под угрозой или признак включения элемента СЗИ (1 – включено, 0 – не включено).

Для демонстрации работы модели используем описанный в [3] фрагмент сети, включающий два компьютера, моделируемые позициями $P_1$, $P_2$, и элементы СЗИ, моделируемые позициями $P_3$, $P_4$. Были заданы следующие вероятности срабатывания переходов Q=(0,2; 0,1; 0,5; 0,8). Рассмотрим последовательно варианты маркировки:

1. *M* = (01||00) (рис 1).Это означает, что первоначально угроза ИБ находилась только на втором компьютере, а средства СЗИ были отключены.

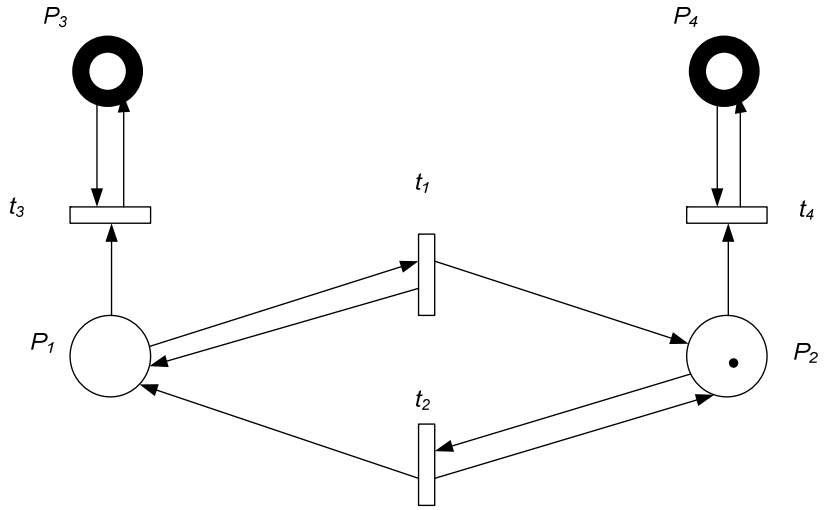



Рис 1. Сеть Петри с маркировкой в позиции $P_2$

В данном случае первоначально может сработать только переход $t_2$. После попадания фишки в позицию $P_1$ срабатывают переходы $t_1$,$t_2$. Дерево достижимости, соответствующее данной маркировке сети (рис 2). Программная реализация данной маркировки представлена на рис 3. $S$=(0,1; 1; 0; 0).

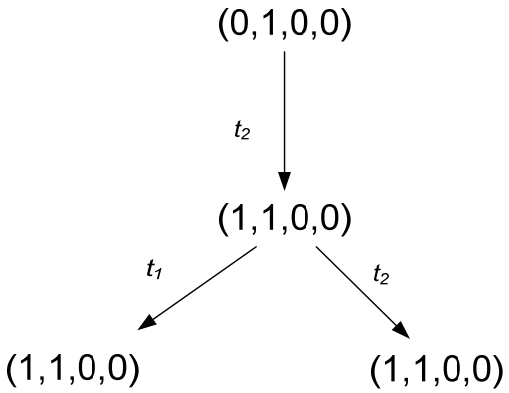



Рис 2. Дерево достижимости для сети, представленной на рис 1.

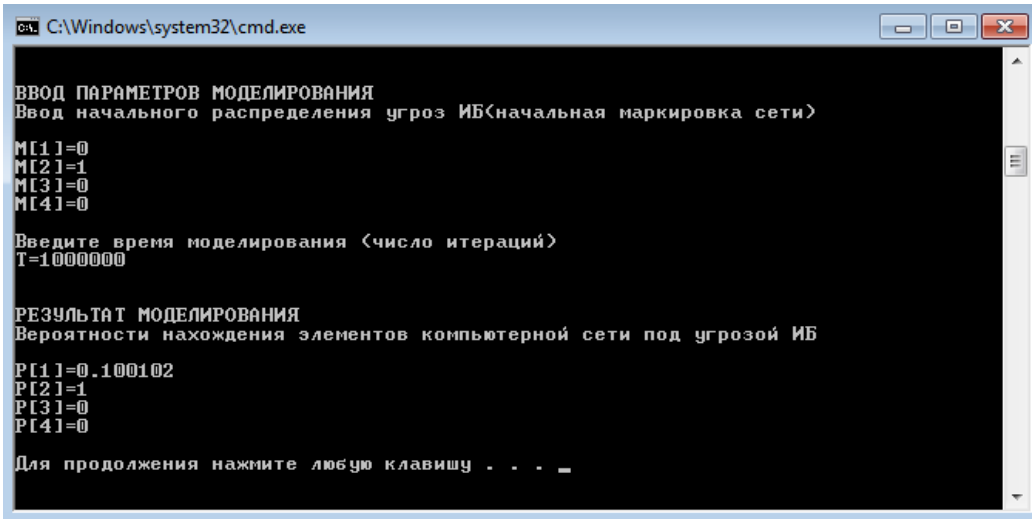



Рис 3. Окно программы для $M$=(0100)

Аналогично были получены данные для других маркировок (таблица 1).

Таблица 1

| Маркировка *M* | Вероятность нахождения компьютера под угрозой *S* |
|---|---|
| 1) 0000 | Не представляют интерес, так как попадание фишки в позиции $P_1$ и $P_2$ невозможно |
| 2) 0001 | |
| 3) 0010 | |
| 4) 0011 | |
| 5) 0100 | (0,1; 1; 0; 0) |
| 6) 0101 | (0,1; 0,2; 0; 1) |
| 7) 0110 | (0,1; 1; 1; 0) |
| 8) 0111 | (0,1; 0,2; 1; 1) |
| 9) 1000 | (1; 0,2; 0; 0) |
| 10) 1001 | (1; 0,2; 0; 1) |
| 11) 1010 | (0,499698; 0,2; 0; 1) |
| 12) 1011 | (0,499698; 0,2; 1; 1) |
| 13) 1100 | (1; 1; 0; 0) |
| 14) 1101 | (1; 0,360144; 0; 1) |
| 15) 1110 | (0,54994; 1; 1; 0) |
| 16) 1111 | (0,54994; 0.360144; 1; 1) |

Таким образом, разработана модель, позволяющая найти вероятности нахождения элементов компьютерной сети под угрозой ИБ.

Разработанная модель может быть использована в задаче проектирования систем защиты информации на объектах информатизации ОВД.

**Литература**

1. Герасименко В.А., Малюк А.А. Основы защиты информации: Учебник для высших учебных заведений Министерства общего и профессионального образования РФ / В.А. Герасименко, А.А. Малюк // — М.: МИФИ, 1997. – 538 с.

2. Питерсон Дж. Теория сетей Петри и моделирование систем/ Дж. Питерсон. – М.: Мир, 1984. – 264 с.

3. Меньших В.В., Толстых О.В., Толстых А.В. Сетевая модель распространения угроз информационной безопасности в компьютерной сети(настоящий сборник).

# ВЫБОР ОПТИМАЛЬНОГО ВАРИАНТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

*Толстых А.В., Воронежский институт МВД России*

Математическое моделирование процессов распространения и устранения угроз информационной безопасности на объектах информатизации производится в интересах обоснования выбора наиболее эффективной системы защиты информации (СЗИ) на этих объектах. Выбор вариантов осуществляться на основе некоторых показателей эффективности СЗИ. Ни одна СЗИ не может обеспечить абсолютную информационную безопасность объекта информатизации, поэтому в показателях эффективности СЗИ должен быть учтен риск использования того или иного варианта СЗИ.

В соответствии с [1] под риском понимается сочетание вероятности нанесения ущерба $v_j^{i,(t)}$ и тяжести этого ущерба.

Пусть задано множество вариантов СЗИ $\Omega = \{\omega_1, \omega_2, ..., \omega_l\}$; под $\omega_0$ будем понимать вариант, предполагающий отсутствие СЗИ.

Обозначим

$v_j^{i,(t)}(\omega_k)$ – вероятность наличия угрозы информационной безопасности на элементе объекта информатизации при использования СЗИ [2].

В свою очередь, тяжесть ущерба определяется опасностью угрозы $\delta_j^i$ и важностью элементов объекта информатизации $\gamma_j$. В таком случае абсолютное значения риска при использовании варианта СЗИ $\omega_k$ оценивается как

$$S(\omega_k) = f(v_j^{i,(t)}(\omega_k), \delta_j^i, \gamma_j),$$

где $v_j^{i,(t)}(\omega_k)$ – вероятность появления угрозы *i*-го типа на *j*-м элементе при реализации *k*-го варианта СЗИ,

$\delta_j^i$ – опасность реализации угрозы *i*-го типа,

$\gamma_j$ - важность *j*-го элемента объекта информатизации;

Относительное значения риска при использовании варианта СЗИ $\omega_k$ оценивается как $\frac{S(\omega_k)}{S(\omega_0)}$,

где $v_j^{i,(t)}(\omega_0)$ – вероятность наличия угрозы информационной безопасности на элементе объекта информатизации без использования СЗИ.

Оценки опасности угроз и важности элементов объекта информатизации могут быть получены по методу Саати [3]. Учитывая, что сумма коэффициентов, полученных по этому методу равна 1, как правило, функциональные выражения, их включающие, представляют в линейном виде.

Величину, характеризующую риск нарушения информационной безопасности на элементе $o_j$ объекта информатизации при реализации варианта $\omega_k$, учитывающая как вероятность возникновения угрозы $v_j^{i,(t)}$, так и опасность этой угрозы $\delta^i$ по формуле $\sum_{i=1}^{m} \delta^i \cdot v_j^{i,(t)}(\omega_k)$.

Тогда $S_t(\omega_k) = \sum_{j=1}^{|J|} \gamma_j \sum_{i=1}^{m} \delta^i \cdot v_j^{i,(t)}(\omega_k)$ -

величина, характеризующая абсолютное значение риска при нарушении информационной безопасности на всем объекте информатизации с учетом важности его элементов $\gamma_j$,

$$S_t = \frac{\sum_{j=1}^{|J|} \gamma_j \sum_{i=1}^{m} \delta^i \cdot v_j^{i,(t)}(\omega_k)}{\sum_{j=1}^{|J|} \gamma_j \sum_{i=1}^{m} \delta^i \cdot v_j^{i,(t)}(\omega_0)} \text{ -}$$

величина, характеризующая относительное значение риска.

Эффективной произвольной системой традиционно является величина численно находящаяся в интервале [0,1]. Значение эффективности $E_t(\omega_k) = 0$ является наименьшим и соответствует ситуации отсутствия СЗИ $(\omega_0)$. Следовательно, $(\omega_0)$ должен быть выбран таким образом, что $E_t(\omega_0) = 0$. Значение эффективности достигается в случае обеспечения «абсолютной» защиты, т.е. в ситуации, когда риск нарушения информационной безопасности $S_t(\omega_k) = 0$.

Кроме того, показатель эффективности должен монотонно зависеть от величины риска нарушения информационной безопасности: чем меньше риск нарушения информационной безопасности, тем выше эффективность СЗИ.

Всем указанным требованиям отвечает показатель эффективности *k-го* варианта СЗИ определяемый в соответствии с выражением:

$$E_t(\omega_k) = 1 - \frac{S_t(\omega_k)}{S_o(\omega_k)} \qquad (1)$$

Обычно задача выбора решается с учетом стоимости СЗИ.

Обозначим $C(\omega_k)$ – стоимость *k*-го варианта СЗИ, $\hat{C}$ – максимальная величина стоимости СЗИ.

Величина $C(\omega_k)$может быть найдена по формуле:

$$C(\omega_k) = \sum_{j=1}^{|J|} c_j(\omega_k),$$

где $c_j(\omega_k)$ – стоимость размещения и обеспечения функционирования *j*-го элемента СЗИ на объекте информатизации при выборе *k*-го варианта СЗИ.

Значение $\hat{C}$ задается пользователем исходя из возможностей финансирования обеспечения информационной безопасности объекта информатизации ОВД.

Сложность решения задачи определяется тем, что $E_t(\omega_k)$ является функцией времени, т.к. вероятности носят циклический характер и изменяются в течение суток.

Чтобы исключить параметр времени, заменим $E_t(\omega_k)$ на среднее значение $E(\omega_k) = \frac{\int_0^T E_t(\omega_k)dt}{T}$, где $T$ – достаточно большой промежуток времени, на котором осуществляется цикл изменения состояния информационной безопасности объекта информатизации, например, сутки.

Значение $E(\omega_k)$ может быть найдено с помощью методов численного интегрирования.

Промежуток времени $T$ может быть разбит на $N$ моментов времени $\tau_0, \tau_1, \tau_2, ..., \tau_N$ , где 0 – первый рассматриваемый момент на

промежутке времени $T$, а $N$ – последний рассматриваемый момент на промежутке времени $T$.

Будем считать, что по формуле

$$v_k^{i,(t+1)} = 1 - \left( \left(1 - v_k^{i,(t)} (1 - l_k^i)\right) \cdot \prod_{j=1}^{|J|} \left(1 - v_j^{i,(t)} \cdot (1 - l_j^i) p_{jk}^{i,(t)} (1 - q_{jk}^i)\right) \right)$$

найдены значения $v_{jk}^{i,(0)}, v_{jk}^{i,(\tau_1)}, v_{jk}^{i,(\tau_2)}, ..., v_{jk}^{i,(\tau_N)}$.

Это позволяет по формуле (1) найти значения $E_0(\omega_k), E_{\tau_1}(\omega_k), E_{\tau_2}(\omega_k), ..., E_{\tau_N}(\omega_k)$. Тогда по формуле трапеций

$$\int_0^T E_t(\omega_k) dt = \sum_{l=0}^{N-1} \frac{E_{l+1} + E_l}{2} \cdot |\tau_{l+1} - \tau_l|$$

Задача оптимизации выбора варианта СЗИ имеет следующий вид:

Задача 1. Найти $\omega_k^* = Arg \max E(\omega_k)$ при ограничении:

$C(\omega_k) \le \hat{C}$,

$\omega_k \in \Omega$,

где $\hat{C}$ – максимальная величина стоимости СЗИ,

$\Omega = \{\omega_1, \omega_2, ..., \omega_k\}$ – множество вариантов СЗИ.

Таким образом, оптимизация выбора варианта СЗИ сводится к решению указанной задачи.

**Литература**

1. Техническая защита информации. Основные термины и определения [Текст]: рекомендации по стандартизации Р 50.1.056 – 2005. – М.: Изд-во стандартов, 2005. – 105 с.

2. Толстых О.В. Способ получения оценки эффективности варианта системы защиты информации объекта информатизации / О.В. Толстых // Информация и безопасность. – 2012. – №2. – С. 237 – 240.

3. Саати Т. Принятие решений. Метод анализа иерархий / Перевод с английского Р. Г. Вачнадзе. – М.: Радио и связь, 1993. – 320 с.

## СОДЕРЖАНИЕ

*Научное издание*

# ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ

Материалы
I Всероссийской научно-практической конференции
(16 мая 2014 г.)

*В авторской редакции*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-0855-4


Подписано в печать 05.02.2015. Формат 60x84 1/16.
Усл. печ. л. 7,8. Тираж 500 экз. Заказ 199.

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