# НОВЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ ТРЕБУЮТ ИДТИ В НОГУ СО ВРЕМЕНЕМ

***Мошков Алексей Николаевич***, *начальник Бюро специальных технических мероприятий МВД России, генерал-майор полиции*

*В работе рассматриваются современное состояние борьбы с компьютерными преступлениями в современной России, анализируются виды преступлений, их количественный рост и изменение качественного состава преступлений. Приводится статистика и распределение высокотехнологичных преступлений с использованием информационных технологий по регионам страны. Приводятся цифры закрытых сайтов за распространение детской порнографии и показывается, что БСТМ особое внимание уделяет защите детей в сети Интернет.*

***Ключевые слова**: правонарушения в сфере информатизации, киберпреступность, безопасность Интернет, мониторинг преступности.*

# THE NEW INFORMATION THREATS REQUIRES TO KEEP UP TO TIMES

***Alexey Moshkov**, the head of the Bureau of Special Technical of Russian Interior Ministry, major general of police*

*The current state of the fight against computer crime in modern Russia is considered. The types of crimes, their quantitative growth and qualitative change in the composition of the crimes are analyzed. The statistics and distribution of high–tech crime using information technology by region of the country are given. The figures are enclosed sites for the dissemination of child pornography are shown. The special attention of BSTM to the protection of children on the Internet is displayed.*

***Keywords**: cyber offense, cybercrime, Internet security, monitoring crime.*

Функционирование современного общества во многом зависит от использования информационных технологий. За последние десятилетия они успели проникнуть практически во все сферы жизни, привнося новые возможности и значительно упрощая решение многих традиционных и повседневных задач. Но в качестве побочного эффекта инновационные процессы способствуют появлению новых угроз, для противодействия которым необходимо своевременно реагировать на все изменения окружающей нас обстановки, особенно криминальной.

Современные информационные технологии в значительной мере преобразили мир. И это свершившийся факт. Цель их применение заключается в обеспечении для личности, общества и государства позитивного использования достижений научно-технического прогресса.

За годы своего существования[1] Бюро специальных технических мероприятий МВД России (БСТМ) претер пело немало изменений, целью которых было соответствие современному уровню технического прогресса. Практически ежегодно мы наблюдаем появление новых форм преступной деятельности, равно как и совершенствование традиционных видов преступлений. Работа в таких условиях предъявляет крайне высокие требования к квалификации сотрудников и техническому оснащению подразделений.

Специалисты БСТМ, в том числе региональных подразделений, проходят подготовку и повышают свои профессиональные навыки в российских технических ВУЗах, а также учебных центрах крупнейших компаний, работающих в IT-отрасли.

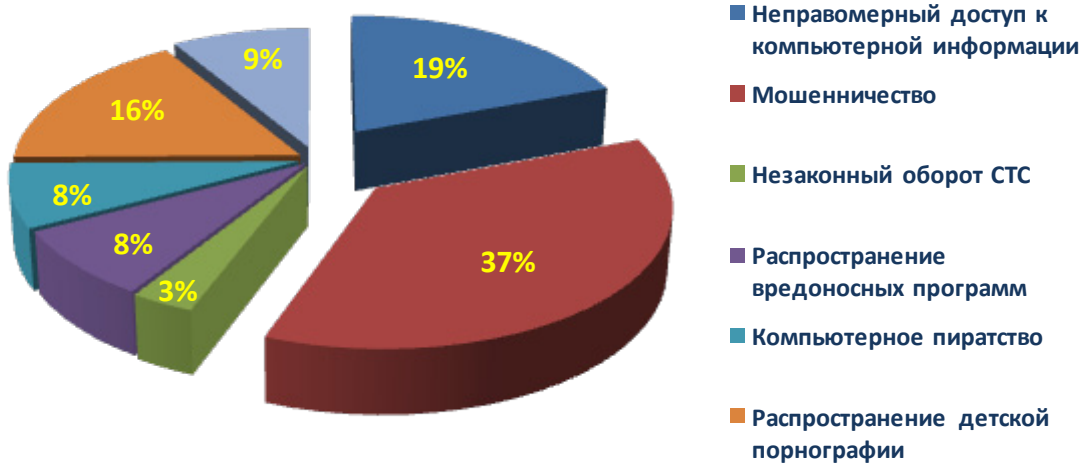
1 Образовано 19 октября 1992 года

Для сотрудников региональных подразделений ежегодно на базе Всероссийского института повышения квалификации МВД России организуются учебные занятия, включающие лекции, мастер-классы и практические занятия по расследованию инцидентов в сфере информационной безопасности.

В своей деятельности мы опираемся на передовой отечественный и зарубежный опыт и используем самые современные разработки, направленные на сбор и анализ информации. Эти меры позволяют нам заниматься расследованием самых сложных и высокотехнологичных преступлений, оставаясь в авангарде борьбы с киберпреступностью.

преступной деятельности в киберпространстве. Все больше краж и мошенничеств совершается с использованием информационных технологий. На сегодняшний день они составляют 37% от общего числа зарегистрированных преступлений в информационной сфере. Преступники все чаще используют современные технологии в качестве удобного инструмента для поиска жертв, перевода денег и сокрытия следов своей криминальной деятельности. Наибольшее количество выявленных хищений денежных средств и мошенничеств, совершенных с использованием информационных и телекоммуникационных технологий, приходится на Приволжский, наименьшее – на Северо-Кавказский федеральный округа.

## Характеристика компьютерных преступлений за 2013 год




В целом, как известно, преступность является сложным социальным явлением, зависящим от политических, экономических, демографических и иных факторов. Количественные показатели официально регистрируемой преступности, как правило, колеблются, имея тенденцию к незначительному увеличению.

Преступность в сфере телекоммуникаций и компьютерной информации не является исключением. На протяжении последних 5 лет количественные показатели данного вида преступности колебались от 8 до 17,5 тысяч преступлений.

В 2013 году было зарегистрировано 11104 подобных преступления, что на 8,6% процентов превышает показатели 2012 года.

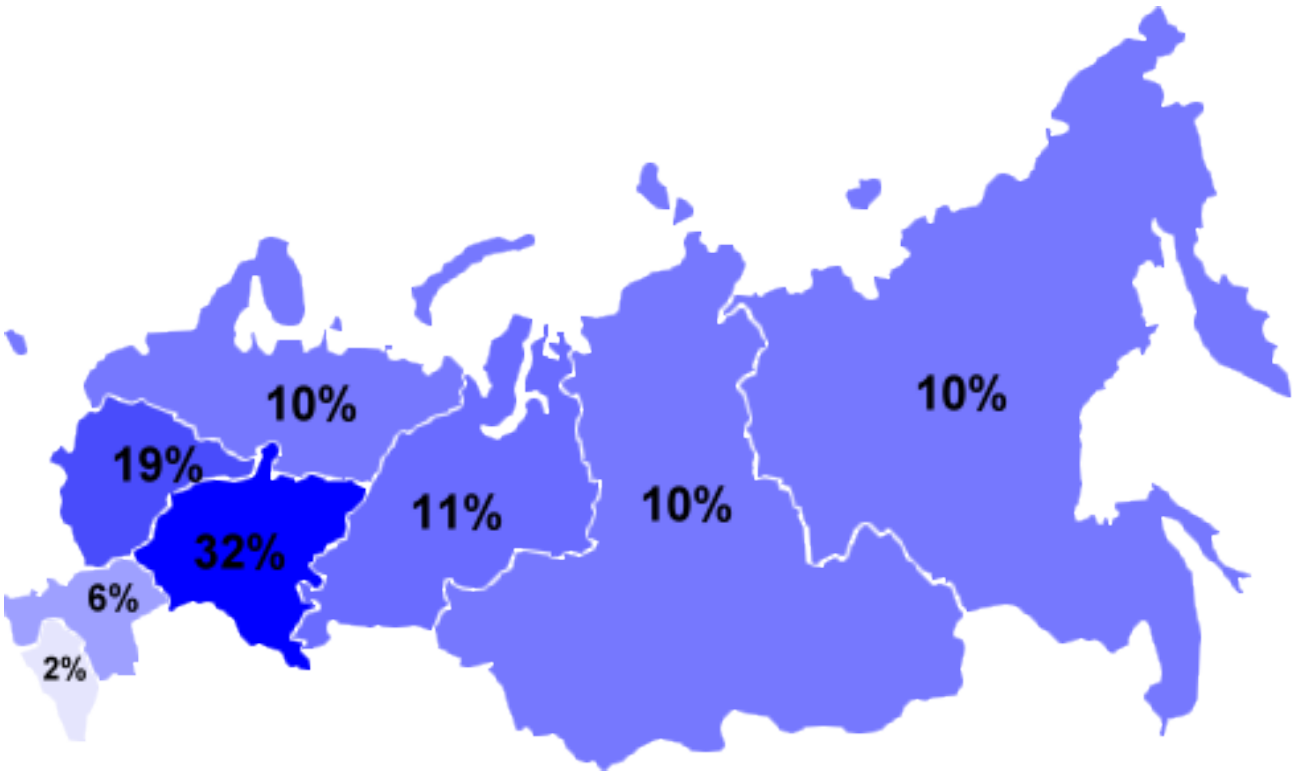
Наряду с увеличением числа преступлений меняется и их качественный состав. Так, с каждым годом возрастает миграция традиционных форм

Что же касается по-настоящему высокотехнологичных преступлений, к которым следует в первую очередь отнести неправомерный доступ к компьютерной информации, а также изготовление и распространение вредоносного программного обеспечения, то они в совокупности на сегодняшний день составляют 27% от всех зарегистрированных преступлений в IT-сфере. Количество возбужденных уголовных дел по ст. 272 УК РФ (неправомерный доступ к компьютерной информации) увеличилось на 5.8% и составило 1010.

Наибольшее количество подобных преступлений в истекшем году было выявлено на территории Дальневосточного, Уральского, Приволжского и Центрального федеральных округов.

Следует отметить, что Управление «К» специализируется на таком направлении, как борьба с лицами, занимающимися взломом программ-

**Количество выявленных преступлений в сфере телекоммуникаций и компьютерной информации в 2013 году по федеральным округам.**




ного обеспечения и изготавливающими различные вредоносные программы для этих целей. Безусловно, если эти же люди занимаются и сбытом, то они также попадают в поле зрения Управления «К».

С правовой точки зрения подобная деятельность связана с нарушением авторских и смежных прав правообладателей на программное обеспечение, и наносит им материальный ущерб, как правило, в особо крупном размере, сопровождается неправомерным доступом к охраняемой законом компьютерной информации с использованием вредоносных компьютерных программ.

Рассматривая проблему распространения «контрафакта» в Сети интернет, следует отметить, что данная проблема достаточно актуальна. Однако ее решение не может быть достигнуто исключительно репрессивными усилиями одного государства. Интернет – трансграничная среда, находящаяся под юрисдикцией различных стран. И как следствие, необходимо выработать к этой проблеме единые подходы. В частности, Российская Федерация прилагает значительные усилия по ликвидации находящихся под ее юрисдикцией технических площадок, распространяющих контрафакт. Управление «К» и МВД России в целом активно участвует в этом процессе.

Разрешение проблемы контрафакта связано, прежде всего, с формированием отношения общества к данной проблеме. Принципиально важно отметить, что государство защищает не только производителей авторского контента, но и его потребителей. Любые законодательные инициативы в этой области должны предусматривать не только механизмы запретительного характера, но и создавать возможность защиты права граждан на потребление качественного контента.

Сегодня граждане вправе рассчитывать на то, что в случае взлома их электронной почты, аккаунтов в соцсетях, размещения клеветы в Сети интернет злоумышленники будут установлены и наказаны. Любое деяние с объективной стороны, если оно образует состав преступления, предусмотренный Уголовным кодексом, подлежит обязательному расследованию.

Говоря о таких преступлениях, можно выделить две категории лиц, совершающих подобные деяния. Это лица, взламывающие электронные ресурсы индивидуально, так называемые одиночки. Вторая категория - это организованные преступные группы, часто интернационального состава, предлагающие широкий спектр криминальных «услуг» — от «взлома» ящиков электронной почты или аккаунтов в соцсетях до массированных DDoS-атак и хищения денежных средств с банковских счетов.

Так, в 2014 году сотрудниками Управления «К» была пресечена деятельность организованной преступной группы, осуществлявшей неправомерный доступ к различным электронным ресурсам социальных сетей, почтовых серверов и веб-сайтов, DDoS-атаки на сервера коммерческих компаний. Группа действовала на территории всей страны, организаторы прятались в Москве, а исполнители - в различных населенных пунктах Российской Федерации.

При расследовании взломов электронной почты и аккаунтов существуют объективные трудности, связанные с несовершенством действующего законодательства, прежде всего связанные с правообладанием. Но в настоящее время активно создаются и внедряются эффективные механизмы обеспечения защиты конституционных прав и свобод граждан и государственного суверенитета в телекоммуникационном пространстве. По завершении данной работы задача по выявлению и уголовному преследованию лиц, причастных к взлому электронных ящиков и аккаунтов в соцсетях, будет облегчена.

Что же касается размещения в Сети клеветы, то задача Управления «К» состоит в сопровождении расследований в том числе и в рамках уголовных дел, возбужденных по статье 128.1 УК РФ, и если клевета распространяется в телекоммуникационном пространстве сети интернет. Мы активно участвуем в этом процессе и предоставляем техническую информацию соответствующим службам МВД России, ведущим расследование, сотрудничаем с другими федеральными министерствам и ведомствам по этому вопросу.

Несмотря на ежегодно увеличивающуюся сложность совершаемых в IT-сфере преступлений, положительная динамика их выявления и раскрытия сохраняется. Так, в 2013 году было возбуждено 5446 уголовных дел, что на 2% превышает показатели 2012 года. Количество преступлений, уголовные дела по которым направлены в судебные органы, увеличилось на 18,7%.

В целях противодействия использованию сети Интернет в противоправных целях в 2013 году была приостановлена деятельность 1040 Интернет-ресурсов, почти половина из которых была ориентирована на распространение материалов порнографического характера с участием несовершеннолетних.

Кроме того, сотрудниками Управления «К» была пресечена деятельность крупного Интернет-форума любителей детской порнографии, а также установлен целый ряд лиц, совершавших развратные действия в отношении детей в различных городах России от Калининграда до Магадана.

По итогам 2013 года количество уголовных дел, возбужденных по признакам преступлений, предусмотренных статьями 242.1 (изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних) и 242.2 (использование несовершеннолетнего в целях изготовления порнографических материалов и предметов) Уголовного кодекса Российской Федерации, увеличилось более чем на 15%.

В рамках проведения оперативно-профилактической операции «Сорняк», направленной на выявление случаев распространения материалов, содержащих признаки детской порнографии, в российском сегменте сети Интернет было установлено и задокументировано 993 факта распространения противозаконного контента. По результатам оперативно-розыскных мероприятий возбуждено 325 уголовных дел, 161 уголовное дело уже передано в суд.

Помимо того, за время проведения операции было выявлено 3462 зарубежных пользователя (1767 из которых – в 2013 году), распространявших фотографии и видеоролики с территории 74 стран мира. Правоохранительные органы зарубежных стран проинформированы о фактах противозаконных действий их граждан.

Но меры, направленные лишь на повышение эффективности работы по раскрытию преступлений за счет совершенствования квалификации сотрудников и улучшения материально-технической базы подразделения, не помогут решить главную задачу: прекратить рост числа преступлений в сфере информационных технологий, а в дальнейшем и обратить его вспять. Ведь для снижения количества совершаемых преступлений, в первую очередь, необходимо создание условий, в которых преступная деятельность будет затруднена или экономически не выгодна.

Именно поэтому Управление «К» БСТМ МВД России совершенствует механизмы, ориентированные на профилактику преступлений. Это сложная и многоэтапная, но крайне необходимая работа, и из года в год мы получаем положительные отклики на реализуемые нами инициативы.

Несколько лет назад мы начали выпускать брошюры «Управление «К» предупреждает», в которых информировали пользователей электронных сервисов о возможных угрозах, стандартных уловках злоумышленников, а также мерах, позволяющих минимизировать риски при работе в киберпространстве. Данные памятки распространялись как в бумажном, так и в электронном виде на сайте МВД России и ряде других ресурсов. В нынешнем году мы усовершенствовали формат работы за счет анализа поступающих обращений граждан.

Анализ обращений позволяет в реальном времени учитывать все последние криминальные тенденции и корректировать направление профилактической работы. Таким образом, нам уже удалось наладить на Интернет-сайте МВД России «точечное» информирование о наиболее актуальных видах преступлений. В дальнейшем планируется размещать подобную информацию в социальных сетях и на страницах наиболее популярных Интернет-ресурсов.

Стоит упомянуть и об отдельном направлении нашей работы – защите детей в сети Интернет, поскольку дети сегодня являются довольно активной и многочисленной, и, к тому же, очень уязвимой частью Интернет-аудитории.

В рамках реализации программы «Уроки безопасности в Интернете» в прошлом году Управлением «К» был проведен онлайн-урок для учеников 5-6 классов. Встреча учащихся с киберполицейским транслировалась на все школы г. Москвы, а аудитория урока составила порядка 80 тысяч человек. И мы, конечно, не будем останавливаться на достигнутом. В наших профилактических планах проведение серии онлайн-уроков на всей территории Российской Федерации, что позволит максимально широко охватить школьную аудиторию.

Не нужно забывать, что борьба с преступностью - процесс комплексный, он требует постоянного напряжения всех имеющихся сил и средств, особенно в столь динамично развивающейся отрасли, как IT.

МВД России постоянно прилагает усилия как по предупреждению преступлений в сфере телекоммуникаций и компьютерной информации, включая повышение виктимологической устойчивости населения, так и по реализации принципа неотвратимости наказания. В настоящее время уже сформирована достаточно эффективная нормативно-правовая база, регламентирующая нормы в сфере борьбы с данными видами преступлений, во всех субъектах Российской Федерации созданы и действуют специализированные подразделения, имеющие в своем составе высококвалифицированные кадры.

На постоянной основе осуществляется взаимодействие с ведущими учебными заведениями, готовящими IT-специалистов. Благодаря взаимодействию с профильными ВУЗами и центрами компьютерного обучения в плановом режиме организовано систематическое обучение сотрудников на специальных курсах. В этих целях осуществляется взаимодействие БСТМ и с бизнес-структурами, в частности, с ЗАО «Лаборатория Касперского», на базе которой уже многие годы специалистами Лаборатории проводятся практические занятия (тренинги). На занятиях рассматриваются реальные сетевые инциденты, разъясняются различные способы выявления и нейтрализации угроз информационной безопасности.

Новые информационные угрозы требуют от Управления «К» БСТМ МВД России идти в ногу со временем, своевременно и эффективно реагировать на кибервызовы.

В заключение подчеркнем, что в нашей стране любое совершенное преступление подлежит тщательному расследованию. Права и свободы любого лица охраняются государством. Успешность же расследования преступлений в сфере телекоммуникаций и компьютерной информации зависит от многих факторов, в том числе от готовности к сотрудничеству пострадавшей (потерпевшей) стороны.