УДК 343.98

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОСУДЕБНОГО ПРОИЗВОДСТВА

И.М. КОМАРОВ

Белгородский государственный университет

e-mail: Komarov@bsu.edu.ru

В статье на основе общеметодологических подходов дается определение понятия информационной безопасности досудебного производства по уголовному делу, определяется ее структура на основе уголовно-правовых, уголовно-процессуальных, криминалистических и технических компонентов, формулируются некоторые виды угроз информационной безопасности досудебного производства и способы их нейтрализации для достижения следователем полного, объективного и всестороннего расследования преступлений.

Ключевые слова статьи: предварительное расследование, досудебное производство, информационная безопасность.

Под информационной безопасностью в Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства[1].

Свои определения информационной безопасности сформулировала и наука. Правда, в научной литературе отсутствуют однозначные подходы к определению этого понятия. Часть авторов определяет информационную безопасность на основе, в целом, технического подхода к этому понятию. Так, например, поступают в своей коллективной статье В.Ю. Статьев и В.А. Тиньков. Они пишут, что информационная безопасность есть защита информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей ее инфраструктуре[2].

Есть определения, отражающие более широкое представление об информационной безопасности. Они включают и источники информации, и информационные системы ее передачи и даже создание систем дезинформации. Об этом пишет Г.Г. Феоктистов[3].

Достаточно активно в научном обиходе используются определения информационной безопасности данные А.Д. Урсулом[4] и В.В. Крыловым[5].

Вместе с тем, в криминалистической литературе отсутствуют определения информационной безопасности конкретных стадий уголовного судопроизводства, где осуществляется процесс доказывания, в частности стадии досудебного производства, в пределах которой используются все известные способы собирания судебных доказательств. Предпримем попытку дать такое определение.

Выделяя его признаки, следует указать субъекта, осуществляющего защиту информации прикладного к возбуждению уголовного дела и предварительному расследованию характера, собственно защищаемую информацию, пределы, в которых данный вид защиты этим субъектом осуществляется, а также категорию лиц, посягающих на информацию.

---

[1] Доктрина информационной безопасности Российской Федерации // Российская газета. 2000. 28 сент.

[2] Статьев Ю.В., Тиньков В.А. Информационная безопасность распределения информационных систем // Информационное общество. 1997. №1. – с.68.

[3] Г.Г. Информационная безопасность общества // Социально-политический журнал. 1996. №5. – с.211-212.

[4] Урсул А.Д. Информационная стратегия и безопасность в концепции устойчивого развития // НТИ. Сер. 1: Организация и методика информационной работы. 1996. №1. – с.7.

[5] Крылов В.В. Расследование преступлений в сфере информации. – М., 1998. – с.59.

В соответствии с действующим Уголовно-процессуальным законодательством РФ досудебное производство вправе проводить дознаватель, следователь, а также надзирающий за ним прокурор, в пределах предоставленных ему процессуальных полномочий. Его информационная безопасность в силу должностных полномочий этих лиц должна быть обеспечена на этапах возбуждения уголовного дела и предварительного расследования.

Относительно характера защищаемой информации можно сказать, что к ней следует отнести всю доказательственную и ориентирующую информацию, добываемую в процессе досудебного производства указанными выше субъектами. Также это информация, добываемая на основе сопровождения оперативными службами этапов возбуждения уголовного дела и предварительного расследования, ее, дознаватель, следователь и прокурор, на основе принципов криминалистического взаимодействия с оперативными службами, использую в процессе расследования уголовного дела. Защита данной информации осуществляется на протяжении всего периода досудебного производства, а в исключительных случаях и в процессе судебного производства с целью обеспечения нормального слушания уголовного дела.

С учетом этих подходов, не вдаваясь в более детальный анализ приведенных признаков, информационную безопасность досудебного производства можно определить как деятельность дознавателя, следователя и прокурора (в пределах процессуальных полномочий) по созданию условий защищенности доказательственной, ориентирующей информации, а также информации добываемой на основе сопровождения уголовного дела оперативными службами на этапах его возбуждения и предварительного расследования, от негативного внутреннего и внешнего воздействия на эту информацию или ее носители со стороны заинтересованных лиц, с целью получения ими тактических выгод от результатов досудебного производства.

Данное определение дает возможность определить структуру (в целом) защиты указанной информации на стадии досудебного производства, то есть структуру информационной безопасности данной стадии.

Компонентами этой структуры, на основе процессуально-криминалистических подходов, в первую очередь можно считать уголовно-правовые, уголовно-процессуальные, криминалистические и технические средства дознавателя, следователя и прокурора (в пределах предоставленных процессуальных полномочий), которые эти участники уголовного судопроизводства вправе использовать для обеспечения информационной безопасности вверенного (поднадзорного) досудебного производства. Важным компонентом этой структуры следует считать и элемент организационных основ досудебного производства, которым является взаимодействие органов предварительного расследования и оперативных служб, сопровождающих досудебное производство.

Относительно правовых (уголовно-правовых и уголовно-процессуальных) мер обеспечения информационной безопасности досудебного производства или иными словами правовой защиты доказательственной и ориентирующей информации от негативного внутреннего и внешнего воздействия на нее со стороны заинтересованных лиц с целью получения тактических выгод от результатов досудебного производства следует отметить, что базовыми положениями их применения являются требования ст. 310 УК и 161 УПК Российской Федерации.

Определив тактику досудебного производства, лицо, осуществляющее (участвующее, надзирающее) расследование уголовного дела на основе оперативно-ситуационного прогнозирования должно определить (определять) круг лиц, участие которых в досудебном производстве требует принятия защитных мер к ним в виде предупреждения о недопустимости разглашения данных предварительного расследования. В случае нарушения предупреждения в отношении соответствующих участников уголовного судопроизводства должностными лицами, осуществляющими предварительное расследование, должны быть приняты предусмотренные правовые меры, вплоть до возбуждения уголовного дела с судебной перспективой его рассмотрения.

Арсенал криминалистических средств, разработанных для защиты информации, представляет собой комплекс из тактических приемов, криминалистических комбинаций и операций – технического, тактического и методического характера, ис-

пользование которых в досудебном производстве обеспечивает тактические преимущества процессуального субъекта, осуществляющего в соответствии с законом уголовное преследование, перед участниками уголовного судопроизводства, имеющими противоположный процессуальный интерес.

Техническую и оперативно-техническую защиту досудебного производства по поручению и под контролем дознавателя, следователя и прокурора осуществляют оперативные службы. В подавляющем большинстве случаев это службы структуры Министерства внутренних дел РФ.

Для осуществления соответствующих мероприятий разработана правовая база, в основе которой лежит Закон РФ «Об оперативно-розыскной деятельности». Использование технических и оперативно-технических средств защиты предварительного расследования регламентируется также специальными нормативными документами, например, приказами МВД России от 7.07.1995 №213 «О принятии на вооружение специальных технических средств», от 19 июля 1996 года №306 «Об утверждении инструкции об основах организации и тактики проведения оперативно-технических мероприятий» и пр.

Взаимодействие органов предварительного расследования и оперативных служб, сопровождающих досудебное производство, в качестве компонента структуры его информационной безопасности представляет собой согласованную деятельность лица, производящего расследование уголовного дела (прокурора, в пределах процессуальных полномочий) и оперативных сотрудников, совместно осуществляющих мероприятия по защите информации досудебного производства каждый своими правовыми способами и средствами, в пределах предоставленных Законом компетенций на основе определенных целей, координируемых должностным лицом в производстве (под надзором) которого находится соответствующее уголовное дело.

Однако информационную безопасность досудебного производства в современных условиях борьбы с преступностью, как структуру компонентов нельзя представить без такого компонента как методы и средства обеспечения информационной безопасности компьютерных систем, обслуживающих досудебное производство.

Положительная динамика компьютеризации органов, ведущих предварительное расследование, в последние годы достаточно активно ставит вопросы о необходимости разработки новых и совершенствовании уже имеющихся методов и средств обеспечения информационной безопасности компьютерных систем, обслуживающих этапы досудебного производства.

Дознаватель, следователь, а также прокурор, осуществляющий надзор за предварительным расследованием, либо участвующее в нем имеют в своем распоряжении персональные компьютеры. Они не только технически обеспечивают их труд, но и служат, в определенном смысле, личной базой данных, где систематизируется, накапливается и сохраняется информация доказательственного, ориентирующего и розыскного характеров, как о текущих, так и о других уголовных делах, которые в разное время были приостановлены, прекращены или направлены в суд.

Персональными компьютерами оснащены экспертные и криминалистические подразделения, обеспечивающие оперативность и объективный ход предварительного расследования преступлений. В настоящее время, на основе специальных программ осуществляется экспертно-криминалистическая деятельность по производству значительного числа судебных экспертиз. В качестве примера этому можно привести устоявшийся вид дактилоскопического исследования на основе систем «Сондо» и «Папилон». Экспертно-криминалистическая деятельность, кроме того, сопровождается определенными видами накопительной деятельности, формирующейся в банки дактилоскопических данных, данных о различных следах огнестрельных орудий, примененных на месте совершения преступлений, различных веществ, изъятых в этих местах и прочей информации.

Указанные виды деятельности следственных и экспертных подразделений обслуживаются специальными техническими подразделениями, которые не только разрабатывают программное обеспечение для них, но и готовят специальные компьютерные программы по защитам этого обеспечения. Эти подразделения в свою очередь

(наряду со следственными и экспертными подразделениями) также нуждаются в мерах по защите от несанкционированного проникновения в их деятельность со стороны заинтересованных лиц.

Мы намеренно не вдаемся в глубокий анализ содержания деятельности следственных, экспертно-криминалистических подразделений и технических подразделений, обеспечивающих их функционирование, на основе применения персональных компьютеров и их программного обеспечения на стадии досудебного производства, так как сказанным хотим лишь указать на возрастающую актуальность обеспечения информационной безопасности деятельности всех органов и должностных лиц, связанных с возбуждением уголовного дела и его предварительным расследованием.

Целью более детального исследования в этой части статьи является рассмотрение вопросов о методах и средствах обеспечения информационной безопасности компьютерных систем участников уголовного судопроизводства, осуществляющих уголовное преследование и связанных с досудебным производством.

Любая компьютерная система может состоять из нескольких компонентов, которые можно разбить на следующие группы:

– аппаратные средства – компьютер и его составные части (процессор, память, контролеры, кабели, линии связи и пр.);

– программное обеспечение – операционная система (утилиты, драйверы и пр.) и системные программы, а также прикладное программное обеспечение, в том числе периферийных устройств;

– данные – хранимые временно и постоянно на внешних носителях и печатные, архивы и базы данных, системные журналы и т.д.;

– пользователи, то есть непосредственно эксплуатирующие компьютерную систему люди (дознаватели, следователи, эксперты, программисты).

С учетом этого, в первую очередь, следует дать несколько определений понятий органически связанных с информационной безопасностью досудебного производства.

Это понятие информационная безопасность компьютерных систем досудебного производства. Оно включает в себя защищенность компьютерных систем дознавателей, следователей, прокуроров, экспертов, а также сотрудников, обеспечивающих техническое обслуживание досудебного производства от случайного или преднамеренного вмешательства противодействующих ему лиц в установленный правовой и технический порядок функционирования этих систем, а также от попыток хищения, изменения или разрушения компонентов этих систем.

Природа воздействия на них может быть разной. Однако для нас наибольший интерес представляют не события стихийного и случайного характера, а, как уже было сказано, действия преднамеренного характера, нацеленные на умышленное причинение вреда компьютерным системам для нарушения их нормального функционирования и получения этим тактических выгод в процессе досудебного производства.

Информационная безопасность компьютерных систем, обеспечивающих функционирование досудебного производства, достигается принятием должностным лицом соответствующей правоохранительной структуры мер по обеспечению конфиденциальности и целостности содержащейся в ней информации, а также доступности и целостности компонентов и ресурсов компьютерной системы, находящейся в его пользовании.

Опуская понятия доступ к информации и санкционированный доступ к информации, так как они, по нашему мнению, в данном контексте не требуют специального толкования, остановимся на понятии несанкционированного доступа к информации досудебного производства. Он, обычно, характеризуется нарушением установленных правил разграничения порядка такого доступа. Нарушителями правил разграничения доступа данного вида являются обычно лица, заинтересованные в получении соответствующей информации о ходе досудебного производства.

Данное понятие непосредственно связано с конфиденциальностью данных, которые не подлежат открытому пользованию в процессе возбуждения уголовного дела и предварительного расследования субъектам, не имеющим на них процессуального права. Конфиденциальность данных досудебного производства можно рассматривать как статус, предоставленный им и определяющий требуемую степень их защиты, то

есть это свойство данных, содержащихся в доказательственной и ориентирующей информации уголовного дела быть известными только допущенным и прошедшим проверку субъектам системы, то есть участникам уголовного судопроизводства, на которых мы указывали ранее.

По цели воздействия можно различать три вида угроз безопасности компьютерных систем обслуживающих досудебное производство. Среди них – угрозы нарушения конфиденциальности информации, нарушения ее целостности и работоспособности системы.

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или процессуальной секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступа. Эта угроза имеет место всякий раз, когда получен несанкционированный доступ к закрытой информации досудебного производства, хранящейся в компьютерной системе или передаваемой от одной системы к другой. Негативные последствия от угроз безопасности компьютерных систем данного вида могут представлять собой последствия разглашения содержания базы данных, обеспечивающих нормальное функционирование правоохранительных структур. Например, сведений о налогах, уплачиваемых физическими лицами.

Угрозы нарушения целостности информации направлены на изменение или искажение хранящейся в системе или передаваемой по сети информации, приводящее к нарушению ее качества или полному уничтожению. Данный вид угрозы может воспрепятствовать нормальному функционированию различных учетов уголовной регистрации, которые используются для решения ряда задач расследования преступлений.

Угрозы нарушения работоспособности направлены на создание таких ситуаций, когда определенные преднамеренные действия либо искажают работоспособность компьютерной системы, либо блокируют доступ к некоторым ее ресурсам. Рассматривая последствия этой угрозы можно сказать, что негативное противодействие досудебному производству на ее основе может обеспечить достаточно эффективный сбой в деятельности следователя, в случаях, когда основная процессуальная документация по уголовному делу заведена в память компьютера и распечатывается оттуда для материалов уголовного дела. Например, несанкционированный доступ к постановлению и привлечение лица в качестве обвиняемого или обвинительному заключению по уголовному делу создает возможность искажения содержания этих документов, что впоследствии может повлечь как затягивание сроков предварительного расследования, так и оправдательное решение суда по этому делу.

Нейтрализации, указанных выше угроз безопасности компьютерных систем, обслуживающих досудебное производство, способствуют различные способы и средства. Среди них достаточно эффективными являются современные криптографические системы. Разработанные на их основе средства защиты основываются, прежде всего, на теоретическом аппарате криптографии. Криптография позволяет решить основные проблемы защиты данных – целостности информации и ее конфиденциальности в процессе возбуждения уголовного дела и его предварительного расследования.

По мнению авторов монографии «Информационная безопасность: основы правовой и технической защиты информации», ее можно определить как совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника[6].

Конфиденциальность информации, т.е. ее свойство быть известной только допущенным и прошедшим проверку субъектам системы (дознавателям, следователям и пр.), достигается за счет лишения возможности лиц противодействующих досудебному производству извлечь информацию из канала связи. Целостность информации сохраняется за счет лишения этих лиц возможности изменить смысл сообщения или добавить в него информацию в своих интересах или интересах третьих лиц.

---

[6] Информационная безопасность: основы правовой и технической защиты информации: учебное пособие / В.А. Мазуров, А.В. Головин, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2005. – с.161.

С учетом того, что проблемы конфиденциальности и целостности информации тесно связаны между собой, методы решения одной из них часто применимы для решения другой и, в основном, базируются на использовании криптографических шифров и процедур шифрования и расшифрования.

Рамки настоящей статьи не позволяют нам более подробно остановиться на исследовании возможностей применения современных криптографических систем, криминалистического обеспечения информационной безопасности досудебного производства. Однако, обозначив актуальные аспекты проблемы, мы надеемся на то, что она вызовет у криминалистов интерес и послужит основой для дальнейших научно-прикладных изысканий.

Список литературы

1. Доктрина информационной безопасности Российской Федерации // Российская газета. 2000. 28 сент.

2. Статьев Ю.В., Тиньков В.А. Информационная безопасность распределения информационных систем // Информационное общество. 1997. №1.

3. Феоктистов Г.Г. Информационная безопасность общества // Социально-политический журнал. 1996. №5.

4. Урсул А.Д. Информационная стратегия и безопасность в концепции устойчивого развития // НТИ. Сер. 1: Организация и методика информационной работы. 1996. №1.

5. Крылов В.В. Расследование преступлений в сфере информации. – М., 1998.

6. Информационная безопасность: основы правовой и технической защиты информации: учебное пособие / В.А. Мазуров, А.В. Головин, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2005.

KRIMINALISTICHESKY ASPECTS OF INFORMATION SAFETY OF PRE-JUDICIAL MANUFACTURE

I.M. KOMAROV

Belgorod State University

e-mail: Komarov@bsu.edu.ru

In article on a basis общеметодологических approaches definition of concept of information safety of pre-judicial manufacture on criminal case is made, its structure on the basis of criminally-legal, criminally-remedial is defined, криминалистических and technical components, some kinds of threats of information safety of pre-judicial manufacture and ways of their neutralization for achievement by the inspector of full, objective and all-round investigation of crimes are formulated.

Key words: preliminary investigation, pre-judicial manufacture, information safety.