# Глава XIV

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## 14.1. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРАСНОЯРСКОМ КРАЕ – АНАЛИЗ УГРОЗ

На современном этапе информация становится основным ресурсом научно-технического и социально-экономического развития мирового сообщества. Информация не только приводит к ускоренному развитию науки, техники и различных отраслей народного хозяйства, но играет большую роль в процессах обеспечения безопасности государства, охраны общественного порядка, сохранности собственности, общения между людьми и в других социальных областях. В основе любого решения лежит полученная и обработанная информация. В ряде случаев она может быть использована особой категорией населения в преступных и антигуманных целях. Государство и правоохранительные органы должны опережающим образом использовать международный опыт и развивать собственные методы пресечения такой деятельности.

Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба собственникам**,** владельцам, пользователям информации и поддерживающей инфраструктуры. Среди субъектов информационных отношений выделяют три главные группы:

- органы государственной власти;
- учреждения, предприятия, рыночные структуры;
- граждане.

Спектр интересов этих субъектов можно подразделить на следующие основные категории:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления);
- обеспечение прав собственности в информационной сфере**.**

Важной компонентой региональной системы безопасности Красноярского края является система обеспечения информационной безопасности. В условиях стремительного развития информационных технологий информационная безопасность играет все большую роль в обеспечении жизненно важных интересов личности, общества и государства. Это подтверждается повышенным вниманием к данной проблеме большинства развитых стран мира, в которых защита национальной конфиденциальной информации и информации о гражданах стала одним из приоритетов государственной политики.

Информационная безопасность развивает традиционное понятие защиты информации и включает в себя три аспекта:

- безопасность информации – состояние всесторонней защищенности информации от внутренних и внешних угроз;

- защиту информации – деятельность по предотвращению утраты и утечки конфиденциальной и утраты защищаемой открытой информации;

- защиту от информации – защищенность информационных систем и субъектов информационных отношений от негативных информационных воздействий.

Необходимость развития системы обеспечения информационной безопасности обусловлена произошедшими в 90-х годах кардинальными изменениями информационной среды, в том числе на территории Красноярского края. К числу объективных факторов, характеризующих эти изменения, следует отнести:

- массовое внедрение автоматизированных систем обработки информации и активное объединение их в локальные и глобальные сети;

- интенсивное сращивание традиционных и автоматизированных технологий обработки информации;

- доступ к автоматизированным системам обработки информации и информационным ресурсам массы пользователей, не являющихся программистами и не владеющих знаниями и навыками правильного использования этих систем;

- значительное увеличение числа пользователей, имеющих доступ в Интернет и обладающих возможностью использования специального программного обеспечения для уничтожения, искажения, модификации и блокирования информационных ресурсов;

- увеличение зависимости экономической безопасности промышленных предприятий, банков, финансовых учреждений и личной безопасности граждан от степени защищенности автоматизированных информационных систем.

Анализ обстановки в области обеспечения информационной безопасности в национальных информационных сетях указывает на реальность угроз информационно-телекоммуникационным системам в Красноярском крае. Отмечается нарастание угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, объектами деятельности которых становятся органы государственной власти, политические и общественные объединения, финансово-кредитные организации, промышленные предприятия, научно-исследовательские организации и средства массовой информации. Это происходит на фоне объективной невозможности российской промышленности удовлетворить спрос на современное компьютерное оборудование, в силу чего при создании отечественных систем обработки информации приходится использовать преимущественно импортные аппаратные, аппаратно-программные и общесистемные программные средства. Организации, занимающиеся вопросами обеспечения информационной безопасности, располагают сведениями о так называемых «скрытых функциональных возможностях» программного обеспечения и других средствах и методах перехвата информации, которые могут быть заложены в системы обработки и передачи информации. Зарубежные фирмы ведут постоянную работу по продвижению на российский рынок средств защиты информации, большинство которых разработаны с учетом интересов иностранных спецслужб и фирм, являющихся конкурентами российских предприятий. При этом иностранные правительства принимают все возможные меры по пресечению экспорта используемых ими новых надежных технологий защиты информации. Серьезные проблемы возникают при вхождении отечественных информационных систем в международные компьютерные сети, в первую очередь, в Интернет. Специалисты в области защиты информации полушутя относят операционные системы семейства Windows фирмы Microsoft к программным закладкам типа «троянский конь» из-за их способности передавать при подключении к сети Интернет не контролируемые пользователем информационные пакеты.

Резкое обострение криминогенной обстановки в стране привело к пересмотру ранее существовавшей модели действий злоумышленника с учетом не только внешних, но и

внутренних угроз для безопасности информации. В стране регулярно регистрируются попытки проникновения «хакеров» в компьютерные сети органов государственной власти, факты утраты конфиденциальных сообщений, передаваемых средствами документальной электросвязи, кражи и уничтожения банковской информации и программного обеспечения систем электронных платежей, отправки фальшивых авизо с использованием кодов подтверждения достоверности межбанковских операций и возможностей локальных сетей коммерческих банков. Применение предприятиями и организациями недостаточно эффективных средств защиты при значительном увеличении числа пользователей, имеющих доступ к глобальной сети Интернет, электронной почте и обладающих возможностью использования разрабатываемого хакерами программного обеспечения может привести к катастрофическим последствиям. Правоохранительными органами Красноярского края тоже регистрируются случаи противоправных действий граждан в информационных системах, возбужден ряд уголовных дел по фактам преступлений в сфере компьютерной информации.

В целом, внешние и внутренние угрозы применительно к обеспечению безопасности информационно-телекоммуникационных систем обобщаются понятием «информационное оружие», защита от которого является новым актуальным направлением обеспечения информационной безопасности.

Важным аспектом информационной безопасности для промышленных предприятий, учреждений и организаций разных форм собственности является проблема защиты коммерческой тайны. На территории Красноярского края сосредоточен огромный экономический потенциал, эффективность деятельности которого является ключевым фактором стабильности экономики Красноярского края и России в целом. Интенсивный информационный обмен между предприятиями неизбежно затрагивает сферу коммерческой тайны и другой конфиденциальной информации. В связи с этим все более актуальной становится проблема гарантий надежности защиты такого обмена, обеспечение прав собственников информации при передаче ее другим владельцам.

По мере информатизации различных государственных, муниципальных и частных организаций, в сферу деятельности которых входит работа с гражданами, все большее внимание обращается на проблемы обеспечения прав граждан на защиту персональных данных. В соответствии с имеющейся мировой практикой основополагающим критерием здесь является принцип «информационного самоопределения», в соответствии с которым граждане сами принимают решения относительно оглашения и использования данных о них. Правила обращения с личными данными и контроль за их соблюдением должны быть определены в законодательном порядке.

С превращением информационных массивов в интеллектуальную собственность все более остро встает вопрос об обеспечении защиты авторских прав в безбумажных технологиях. В связи с подверженностью средств и субъектов информационных отношений (технических, технологических и организационных систем, людей, их коллективов и общества в целом) внешним информационным воздействиям, последствия которых могут носить тяжелый характер, значительное внимание должно обращаться на проблемы защиты от информации.

## 14.2. КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ И БОРЬБА С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ

Объективный процесс широкого внедрения электронно-вычислительной техники и современных компьютерных технологий в самых различных отраслях народного хозяйства, в частности, в финансово-банковской деятельности, сопровождается появлением новых форм

преступности, ориентирующихся на использование современных информационных технологий. Одной из причин возникновения компьютерной преступности в Красноярском крае является информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Другой причиной является возможность получения значительной экономической выгоды от противоправных деяний с использованием ЭВМ, не находясь на месте преступления.

Компьютерные преступления характеризуются следующими особенностями.

*1. Использование новых технологий, требующих специального образования и высокого интеллектуального уровня.*

2. *Высокий уровень латентности, обусловленной совершением этих преступлений в нематериальной сфере и нежеланием потерпевших предоставлять какую-либо информацию о происшедших фактах и событиях, ущербе.* В результате многие уголовные дела в ходе предварительного следствия прекращаются. В России не обобщается практика расследования таких преступлений.

*3. Высокий уровень ущерба от совершаемых компьютерных преступлений.*

*4. Сложность своевременного выявления компьютерных преступлений и установления виновных.* Не всегда компьютерные преступления влекут за собой явное физическое разрушение системы, бывает, что нападение на организацию обнаруживается слишком поздно для установления личности преступника. Немаловажное значение имеет отсутствие методик расследования, специальных лабораторий для проведения экспериментальных исследований, штатов экспертов и многое другое.

5. *Трудности собирания доказательств.* В практике правоохранительных органов России и Красноярского края не накоплен опыт судебного рассмотрения уголовных дел по компьютерным преступлениям и не разработаны документы, регламентирующие проверку, сохранение и предоставление компьютерных правонарушений на рассмотрение доказательств.

*6. Возможность совершения преступлений с использованием средств удаленного доступа, что не требует присутствия правонарушителя непосредственно на месте совершения преступления.*

7. *Интернационализация этого вида преступлений.* В настоящее время международная компьютерная сеть Интернет объединяет более 100 млн. компьютеров, из которых 3–4 млн. одновременно подключены в сеть. Каждый год в Интернете происходит около 900 млн. правонарушений.

Все эти особенности создают условия для быстрого роста компьютерной преступности.

Первое преступление в сфере компьютерной информации на территории Красноярского края было зарегистрировано в апреле 1994 г. по фактам финансовых нарушений в деятельности одного из филиалов акционерного коммерческого банка, когда был выявлен факт хищения 550 тыс. рублей, совершенного в 1993 г. с применением электронно-вычислительной техники.

В ходе расследования были выявлены и другие социально-опасные технологии, применяемые в финансово-банковской деятельности. Например, задержками в движении платежных документов создавалась возможность использования кредитных ресурсов в сферах, отличных от целевых. Иначе говоря, временное отвлечение передаваемых расчетному центру кредитных средств в нарушение целевой направленности фактически дает возможность получения дополнительных прибылей для банка за счет клиентов.

Так, целевые ресурсы, выделяемые Центробанком РФ для финансирования государственных программ, не доводились коммерческим банком через расчетный центр до своих отделений. Средства оставались на корреспондентском счете коммерческого банка,

при этом его отделениям пользоваться указанными средствами разрешалось только в пределах лимитов, которые устанавливались самим же головным коммерческим банком.

В данном неправомочном отвлечении денежных средств необходимо отметить два важных социальных момента:

а) прямое нарушение прав собственности клиентов, будь то государственные или негосударственные структуры;

б) утрата правого контроля за расходованием денежных средств в период задержки платежных документов.

В условиях отсутствия четкого правового механизма регулирования движения денежных средств и государственного контроля за их использованием возникает потенциальная опасность осуществления такого контроля со стороны криминальных структур.

Расследованием установлено, что наиболее серьезным недостатком используемых в финансово-банковской деятельности компьютерных технологий обработки данных является низкий уровень правовой и экономической безопасности. Стихийно сложившаяся практика заказа, разработки, внедрения, эксплуатации и развития банковских компьютерных систем не регламентируется сегодня никакими общими нормами, стандартами или требованиями. Используемые в большинстве банков «самодельные» компьютерные системы в ключевых операциях оказываются практически незащищенными от произвольного вмешательства многих лиц – руководства банка, сотрудников бухгалтерии, программистов и даже технического персонала – операторов банка, которые могут вмешиваться в ответственные банковские операции, часто не неся никакой ответственности за основную деятельность банка.

Действующая практика подтверждает, что социально-опасные технологии и в настоящее время применяются в финансово-банковской деятельности. Например, в 1999 г. снова выявлен факт хищения 4 млн. рублей в одном из коммерческих банков г. Красноярска, где орудием преступления являлись персональный компьютер и специальное программное обеспечение.

Наибольшую опасность для общества представляют компьютерные преступления, совершаемые в сетях передачи данных. Эти преступления могут повлечь за собой крупномасштабные техногенные и экологические катастрофы, которые грозят гибелью большого количества людей. В апреле 1999 г. Прокуратурой Красноярского края возбуждено уголовное дело по факту неправомерного доступа через телекоммуникационную сеть к охраняемой законом компьютерной информации государственных и негосударственных органов и ее копирования. В ходе расследования установлено, что в ноябре 1998 г. хакеры, воспользовавшись паролем и именем одного из отделов администрации г. Северо–Енисейска, вошли в сеть передачи данных и разослали ее абонентам письмо за подписью администратора, в котором предлагалось сообщить свои имена и пароли. Их цель, получив ответы с именами и паролями абонентов, – работать в сети под их именами, с их правами и за их счет контролировать входящую и исходящую информацию. Силами работников сети эти действия были пресечены.

В марте 1999 г. хакеры, используя пароли и права некоторых районных администраций, неоднократно осуществляли неправомерный доступ через сеть к охраняемой законом компьютерной информации более 60 государственных и негосударственных организаций. Несанкционированное копирование их имен и паролей осуществлялось программой типа «троянский конь».

Следует констатировать, что международная компьютерная сеть Интернет в настоящее время становится не только местом, но и орудием преступлений. В марте 1999 г. в сети Интернет на сайте «Коготь–2» неизвестным лицом была помещена текстовая информация о получении взяток начальником одного из краевых управлений и о нераскрытых заказных

умышленных убийствах, совершенных на территории Красноярского края. По факту распространения в сети Интернет заведомо ложных сведений, порочащих честь и достоинство, соединенных с обвинениями в совершении тяжкого преступления, Прокуратурой Красноярского края было возбуждено уголовное дело. В ходе расследования было установлено, что упомянутый сайт предположительно находился в США. Через две недели с момента появления сайт «Коготь–2» прекратил существование, что затруднило дальнейшее расследование. Опыт других стран показывает, что в дальнейшем сеть Интернет будет более активно использоваться для решения «политических заказов» и совершения преступлений в сфере компьютерной информации.

За последние полтора года на территории Красноярского края правоохранительными органами выявлены 15 преступлений с применением электронно-вычислительной техники. В основном это преступления, предусматривающие уголовную ответственность по ст. 272 УК РФ за неправомерный доступ к компьютерной информации, по ст. 273 УК РФ за создание, использование и распространение вредоносных программ, по ст. 274 УК РФ за нарушение правил эксплуатации ЭВМ, систем ЭВМ и их сетей.

В новом Уголовном кодексе РФ, вступившем в действие с 1 января 1997 г., данные составы преступлений впервые представлены в гл. 28 УК РФ и обозначены как «Преступления в сфере компьютерной информации». При этом необходимо отметить, что преступления в сфере компьютерной информации, как правило, могут совершаться в совокупности с другими преступлениями, предусматривающими уголовную ответственность по другим статьям действующего Уголовного кодекса РФ. Рассматривая вопрос о классификации компьютерных правонарушителей, необходимо отметить следующее.

На современном этапе правоохранительные органы прежде всего должны обратить внимание на людей, способных осознанно совершить противоправные действия. Учитывать повсеместную компьютерную грамотность в нашей стране еще рано, поэтому следует ограничить круг лиц, попадающих в группу риска. Человек, попадающий в группу риска, должен обладать достаточными знаниями о работе компьютера, позволяющими самостоятельно писать программы хотя бы на одном из языков программирования или командном языке операционной системы. Он должен знать состав и назначение основных частей компьютера, и обязательно должна быть увлеченность (то, что обычно называют словом «хобби»). Всех членов группы риска можно разделить на три категории.

1. Профессионалы, воспитанные во времена больших ЭВМ. В настоящее время подавляющее большинство достигло определенных результатов, их образование тесно связано с вычислительной техникой или большими объемами вычислений. Они умеют ценить немногочисленные ресурсы, имеют большой запас знаний и могут применять их в своей профессиональной деятельности, работают в больших информационных проектах; разнообразные взломы и проникновения уже давно опробованы. Вероятность совершения противоправного поступка человеком из этой категории низка по сравнению с остальными.

2. Профессионалы, воспитанные во время появления персональных компьютеров. Их обучение проходило одновременно с техническим прогрессом. Подавляющее большинство начинало работать с техникой IBM PC XT или AT, достаточно хорошо разбирается в архитектуре персонального компьютера, локальной сети, умеет ценить быстродействие программного обеспечения. Их основная работа – программисты или обслуживающий персонал в отделах автоматизации, а также сотрудники, связанные с обработкой большого количества данных. Вероятность совершения противоправного поступка человеком из данной категории достаточно высока.

3. Будущие профессионалы, проходящие в настоящий момент обучение в школах, средних специальных или высших учебных заведениях. Они воспитаны на современных операционных системах, языках программирования и ЭВМ. На формирование их профессиональных знаний большое влияние оказывает Интернет. Они работают с

мультимедийными технологиями, активно участвуют в создании компьютерных сетей в жилых домах и микрорайонах. Это самая опасная и многочисленная категория, знакомая по литературе с описанием методов и объектов взлома. Желание самоутвердиться и блеснуть знаниями толкает их на совершение противоправных поступков, без осознания губительных последствий. В большинстве случаев достаточно предупредить такого правонарушителя или провести с ним разъяснительную беседу и противоправные поступки перестанут интересовать его.

Жесткие границы между описываемыми категориями профессионалов провести невозможно. Данная классификация не измеряет уровень грамотности, а дает лишь сравнительную характеристику. Представители первой категории, учитывая накопленный опыт и знания, если и займутся каким-либо незаконным проникновением, то это будет достаточно «крупное дело» (корпоративная сеть крупной организации или предприятия, хорошо защищенная сеть банка). С большой вероятностью представитель этой категории может оказаться главой преступной группировки при совершении компьютерного преступления или консультантом при совершении экономических преступлений.

Вторая категория может принимать участие в «крупных делах» в качестве исполнителей или руководителей среднего звена при совершении компьютерного преступления или как простые исполнители в экономических преступлениях. Более вероятно совершение ими относительно мелких правонарушений, например, взлом интернет–провайдера или несанкционированный доступ к информации ради простого любопытства: «смогу или не смогу».

Третья категория в крупных делах может принимать участие только как исполнители при совершении компьютерных преступлений, а участие в экономических преступлениях является маловероятным, поскольку требует наличия опыта работы в области совершения преступления. Наиболее вероятным направлением совершения правонарушений является доступ к различным закрытым ресурсам с целью попробовать собственные силы (доступ ради доступа). В некоторых случаях они плохо понимают, что делают. Это особенно опасно для больших корпоративных сетей, где проблемы могут обнаружиться не сразу. Эта категория – самая любопытная, многочисленная и опасная. Они готовы пробовать собственными руками все, что угодно, и для них не важно, что кто-то от этого может пострадать.

В совокупности все три категории представляют собой целый класс людей, связанных общими интересами и в большинстве случаев со специфическим образом мышления и профессиональным сленгом. Они следят за новинками, связанными с вычислительной техникой, и стараются идти в ногу со временем, используя технические новинки и повышая свое профессиональное мастерство. В то же время, следует отметить, что компьютерные преступления, совершенные группой лиц по предварительному сговору, – явление очень редкое, поскольку одним из наиболее весомых факторов при совершении подобных преступлений является удовлетворение собственного самолюбия.

Профессионализм потенциальных участников компьютерных преступлений обуславливает необходимость наличия высокой профессиональной подготовки у лиц, задействованных в их расследовании. Развитие вычислительной техники происходит очень быстро, и специалисты, участвующие в расследовании, не должны отставать от научно-технического прогресса. Для поддержания профессиональной формы им необходимо следить за периодическими изданиями, постоянно изучать соответствующую литературу. Нельзя забывать об обновлении технического оснащения. Если произойдет его техническое и интеллектуальное отставание, эффективность работы упадет и выполнение задач станет затруднительным или невозможным.

Положительным моментом в деятельности правоохранительных органов следует отметить образование в структуре аппарата МВД РФ Главного управления по борьбе с

преступлениями в сфере высоких технологий, а также аналогичных управлений в субъектах Российской Федерации.

В Главном управлении внутренних дел Красноярского края в настоящее время действует Управление по борьбе с преступлениями в сфере высоких технологий, одним из направлений которого является выявление и раскрытие преступлений в сфере компьютерной информации. В следственном управлении ГУВД края создано подразделение, специализирующееся на расследовании данного вида преступлений. На базе криминалистического отдела, группы автоматизированных систем информационного обеспечения и управления Прокуратуры Красноярского края организован постоянно действующий межведомственный семинар по методике расследования преступлений в сфере компьютерной информации и тактике проведения отдельных следственных действий, в котором принимают участие следователи и оперативные работники Прокуратуры, Управления внутренних дел, ФСБ, налоговой полиции. Активную помощь в расследовании, обучении следователей и оперативных работников оказывают сотрудники вузов г. Красноярска.

## 14.3. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Резкая интенсификация информационных потоков в Красноярском крае во второй половине 90-х годов на фоне значительного территориального распределения субъектов информационных отношений и объектов информатизации остро поставила проблему создания эффективно функционирующего информационного пространства Красноярского края. Неотъемлемой частью его должна стать система обеспечения информационной безопасности, учитывающая интересы всех субъектов информационных отношений. В результате совместной работы заинтересованных сторон при координационном участии администрации Красноярского края была принята Концепция и разрабатывается целевая программа информатизации края. В них заложены, в частности, основы политики информационной безопасности Красноярского края на 2000–2005 гг.

Информационная безопасность рассматривается как необходимое условие для надежного обеспечения органов государственной власти и управления, предприятий, организаций и граждан необходимой для их деятельности полной, достоверной и своевременной информацией.

В соответствии с положениями Концепции национальной безопасности РФ, Закона об информации, информатизации и защите информации, а также других законодательных актов РФ основными целями информационной безопасности на территории Красноярского края являются:

- сохранение целостности информации в процессе ее хранения, обработки и передачи, обеспечение надежного доступа к ней пользователей в пределах их полномочий;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации и других форм незаконного вмешательства в информационные ресурсы;
- сохранение государственной тайны, конфиденциальности информации в документированном и электронном виде в соответствии с законодательством;
- сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- предотвращение незаконного использования информационных ресурсов как интеллектуальной собственности.

Развитие системы информационной безопасности Красноярского края базируется на комплексном подходе, который опирается в научно-методическом плане на современную теорию защиты информации и реализуется посредством применения научно обоснованного комплекса правовых, организационных и технических методов.

Актуальными направлениями фундаментальных и прикладных исследований являются:

- построение моделей информационной безопасности объектов информатизации Красноярского края;
- построение моделей информационной безопасности объектов информатизации Красноярского края;
- совершенствование концептуально-правовой базы информационной безопасности, в частности, в области расследования компьютерных преступлений, правового обеспечения технологии электронного документооборота, выработки критериев отнесения информации к категории ограниченного доступа;
- развитие перспективных и ориентированных на импортозамещение информационных технологий, аппаратного и программного обеспечения автоматизированных систем;
- анализ и разработка промышленных стандартов информационных технологий.

**Правовые методы** предусматривают разработку комплекса нормативно-правовых актов и положений, регламентирующих информационные отношения в крае, руководящих и нормативно-методических документов по обеспечению информационной безопасности.

**Организационные методы** обеспечивают формирование и функционирование систем защиты информации ограниченного доступа, сертификацию систем по требованиям информационной безопасности, лицензирование деятельности в сфере информационной безопасности, стандартизацию способов и средств защиты информации и информационного обмена.

**Инженерно-технические методы** направлены на следующее:

- предотвращение утечки обрабатываемой информации по техническим каналам;
- исключение или существенное затруднение несанкционированного доступа к информации, обрабатываемой и хранящейся в технических средствах;
- предотвращение специальных программно-математических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств вычислительной техники;
- физическую защиту от внешних воздействующих факторов, вызванных явлениями природы, а также преднамеренной и непреднамеренной деятельностью людей.

С целью организации межведомственного взаимодействия и координации работ на территории Красноярского края целесообразно определить подразделение в составе краевой администрации, которое может осуществлять:

- выработку единой политики информационной безопасности в регионе;
- контроль выполнения требований законодательных, нормативно-правовых, распорядительных и методических документов федерального и краевого уровней в области информационной безопасности;
- формирование пакета заказов администрации края по выполнению работ в области информационной безопасности.

## 14.4. ОРГАНИЗАЦИОННО–ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Система информационной безопасности Красноярского края является составляющей частью государственной системы информационной безопасности РФ, основы которой

заложены в Конституции РФ, Концепции национальной безопасности и регулируются соответствующими законодательными актами, постановлениями Правительства и указами Президента РФ. В Красноярском крае имеются представительства всех государственных органов Российской Федерации, обеспечивающих регулирование деятельности в области информационной безопасности: Аттестационно-лицензионный центр Государственной технической комиссии при Президенте РФ, Центр правительственной связи Федерального агентства правительственной связи и информации при Президенте РФ, Управление Федеральной службы безопасности по Красноярскому краю.

**Аттестационно-лицензионный центр Государственной технической комиссии при Президенте РФ** открыт в 1995 г. на базе подразделения по защите информации Государственного предприятия «Научно-производственное объединение прикладной механики имени академика А.Ф. Решетнева». В качестве официального звена Гостехкомиссии РФ Аттестационно-лицензионный центр ведает решением вопросов защиты информации от утечки по техническим каналам, имеет специализированную испытательную лабораторию. Центр имеет лицензию на все виды деятельности по проблемам информационной безопасности. Центр аккредитован Гостехкомиссией РФ в системе сертификации средств защиты информации по требованиям безопасности информации для проведения аттестации объектов информатизации с выдачей «Аттестата соответствия» и для проведения сертификационных испытаний средств защиты информации. Основные направления деятельности Аттестационно-лицензионного центра:

- экспертная оценка готовности организаций-лицензиатов к деятельности в области защиты информации;
- экспертиза предприятий на готовность работы с использованием сведений, составляющих государственную тайну;
- аттестация объектов информатизации на соответствие требованиям безопасности информации;
- специальные исследования технических средств обработки информации на предмет выявления каналов утечки информации по электромагнитным полям, по цепям электропитания, телефонным линиям, заземлению и т. д.; специсследования ПЭВМ (рабочих мест с ПЭВМ) на соответствие требованиям нормативных документов Гостехкомиссии РФ и последующая их аттестация;
- выявление технических устройств несанкционированного съема информации;
- инструментальные исследования возможности утечки информации по акустическому, виброакустическому каналам, кабельным линиям, по визуально-оптическому каналу на наличие средств акустического съема информации, в том числе дистанционно включаемой;
- проведение мероприятий по защите объектов, таких как монтаж систем виброакустической защиты помещений, монтаж систем активной электромагнитной защиты, монтаж приборов и устройств защиты информации, монтаж сетевых фильтров;
- проведение мероприятий по защите государственной и коммерческой тайны: категорирование и классификация объектов информатики, подготовка комплекта документации по лицензированию, разработка положений по защите коммерческой тайны, консультационные услуги по отмеченным проблемам;
- проведение аттестационных испытаний объектов информатизации с выдачей аттестата соответствия.

Специалисты Центра имеют высокий профессиональный уровень и их участие в обеспечении информационной безопасности гарантирует надежную защиту от возможной утечки информации по техническим каналам и от несанкционированного доступа к информации.

**Центр правительственной связи в Красноярском крае** (ЦПС) создан в декабре 1991г. на основе подразделения, входившего ранее в состав Управления КГБ по

Красноярскому краю. Центр является составной частью единой системы федеральных органов правительственной связи и информации и на территории края представляет Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ).

ЦПС ведает вопросами организации и обеспечения правительственной связи, иных видов специальной связи на территории Красноярского края, решает вопросы в части обеспечения краевой администрации, органов местного самоуправления, правоохранительных органов, значимых государственных структур различными видами информационных и аналитических материалов, необходимых для использования в процессе принятия управленческих решений.

В случае возникновения в крае чрезвычайных ситуаций (техногенная катастрофа, стихийное бедствие, крушение на транспорте и т. п.), Центр по решению руководящих инстанций организует правительственную связь с места происшествия.

ЦПС участвует в реализации региональных проектов развития телекоммуникационного комплекса края. Законом Красноярского края №10–682 от 27.03.2000 г. он определен основным разработчиком краевой целевой программы «Создание региональной информационно-вычислительной сети правоохранительных органов Красноярского края». В пределах предоставленных ФАПСИ полномочий Центр проводит работы по лицензированию деятельности, связанной с разработкой, производством, реализацией и эксплуатацией шифровальных технических средств.

**Региональное Управление ФСБ России по Красноярскому краю** (РУ ФСБ) также значительное внимание уделяет вопросам обеспечения информационной безопасности; при этом основной задачей является защита собственной информации ограниченного пользования, циркулирующей в служебных помещениях, а также обрабатываемой различными техническими средствами, в том числе средствами электронно-вычислительной техники, от утечки за пределы контролируемой зоны. Кроме того, на РУ ФСБ возложены задачи контроля за оборотом и использованием специальных технических средств негласного получения информации на территории Красноярского края и региона, входящего в зону ответственности Регионального Центра противодействия техническим разведкам РУ ФСБ России по Красноярскому краю. В задачи этого подразделения также входит проведение поисково-защитных мероприятий, защита основных и вспомогательных технических средств от утечки по техническим каналам, защита электронно-вычислительных средств от несанкционированного доступа, контроль за соблюдением правил использования радиоизлучающих средств вооружения и средств радиосвязи, участие в оперативно-технических мероприятиях по защите информации в оперативных отделах.

Кроме этого в РУ ФСБ существует лицензионная группа, осуществляющая контроль за деятельностью государственных структур, связанных с работой со сведениями, составляющими государственную тайну, соблюдением режима секретности. В задачи этой группы в соответствии с существующими законами входит выдача лицензий предприятиям и другим структурам на право работы со сведениями, составляющими гостайну.

Все работы по защите информации проводятся в рамках существующего законодательства, на основании ведомственных приказов и других нормативных актов, регламентирующих отдельные направления деятельности специализированных подразделений по линии противодействия техническим разведкам.

Вопросами расследования преступлений в сфере информационной безопасности занимаются специализированные отделы в правоохранительных органах.

В **Прокуратуре Красноярского края** осуществляется расследование особо важных случаев совершения компьютерных преступлений и надзор за ходом следствий, проводимых другими полномочными структурами по аналогичным делам. Важное место уделяется

организации технических экспертиз при проведении следственных действий, связанных с компьютерной информацией.

В **Главном управлении внутренних дел Красноярского края** организовано специальное Управление по борьбе с преступлениями в сфере высоких технологий (УБП СВТ). Деятельность этого подразделения охватывает возбуждение уголовных дел и проведение следственно-розыскных мероприятий по фактам совершения преступлений. Специалистами УБП СВТ проведен ряд успешных мероприятий по пресечению несанкционированного производства информационной продукции на электронных носителях. Накоплен определенный опыт борьбы с преступлениями, совершаемыми в отношении информации в электронном виде посредством удаленного доступа.

На территории Красноярского края имеется ряд негосударственных организаций, осуществляющих деятельность в области защиты информации и имеющих соответствующие государственные лицензии.

Отметим важную роль системы технических средств по обеспечению оперативно-розыскных мероприятий (СОРМ) на отечественных и импортных электронных телефонных станциях, предназначенной для оперативного контроля соединений определенных абонентов из удаленного пункта управления правоохранительных органов путем взаимодействия этого пункта с оборудованием станций. Она состоит из аппаратно-программных средств и включается в состав штатного оборудования электронных телефонных станций. Использование этой системы допускается только с санкции прокурора и действительно служит целям следствия и розыскных мероприятий. Несколько лет назад сильное возмущение провайдеров Интернета провалило попытки установить элементы СОРМ в узловых серверах Интернета. Наряду с правовой неоформленностью этой попытки, противодействие вызвано дополнительными расходами провайдеров на перепрограммирование и организацию разделения доступа. Между тем, известно о применении в США более изощренных программ-жучков, собирающих информацию не только об определенном абоненте, но и по ключевым словам и фразам.

## 14.5. НАУЧНЫЕ ИССЛЕДОВАНИЯ И ПОДГОТОВКА КАДРОВ

Вопросы обеспечения информационной безопасности могут грамотно решаться сотрудниками, имеющими специальные знания по всему комплексу проблем. Потребность в таких специалистах ежегодно возрастает. В результате сложилась ситуация, когда в отделах технической защиты или отделах по обеспечению безопасности большинства организаций работают бывшие сотрудники спецслужб. Они являются носителями знаний и традиций в области защиты информации, усвоенных до начала тотальной информатизации общества. Обычно они знают, как правильно организовать конфиденциальное делопроизводство, пропускной режим, как бороться с возможной утечкой информации за счет побочного электромагнитного излучения и по акустическим каналам. В последнее время пришли молодые сотрудники, которые владеют вычислительной техникой, но для сохранения вверенных ресурсов используют, как правило, лишь средства операционных систем. При этом необходимо каждые два-три года проводить корректировку политики безопасности и уточнение ее положений. Следует подчеркнуть, что большинство сотрудников предприятий и организаций от руководства до рядового персонала не осознает в полной мере важность решения всего комплекса задач, направленных на обеспечение информационной безопасности. Из этого следует, что задача качественной и своевременной подготовки и переподготовки специалистов и пользователей по рассматриваемым проблемам является первоочередной. Свидетельством возрастающего внимания к вопросам информационной безопасности является интенсивное расширение перечня специальностей высшего

образования в области информационной безопасности с середины 90-х годов и выделение их в 2000 г. в отдельное направление. Общее состояние и динамика этих процессов отражена в ***табл. 14.1***.

Развитие краевой вузовской системы подготовки кадров в области информационной безопасности началось с 1995 г., когда в **Красноярском государственном техническом университете (КГТУ)** на факультете информатики и вычислительной техники была открыта специальность 2206 «Организация и технология защиты информации» со специализацией по организации и защите информации в компьютерных системах. В 2000 г. осуществлен выпуск инженеров по этой специальности, прошедших полный курс обучения. Кроме того, в 1998 и 1999 гг. ряд выпускников освоили программу данной специальности по индивидуальным переходным учебным планам, имея предварительную подготовку по направлению «Информатика и вычислительная техника». Среди мест работы выпускников – институты СО РАН, Центр правительственной связи, Аттестационно-лицензионный центр Гостехкомиссии, Прокуратура Красноярского края, коммерческие банки, фирмы по разработке программного обеспечения, отделы информационной безопасности на предприятиях разных форм собственности.

С утверждением нового перечня специальностей и направлений высшего образования и их соответствия прежним названиям (приказы министра образования РФ № 686 от 2 марта 2000 г. и №1010 от 10 апреля 2000 г.) на базе специальности 2206 образованы три новые (***табл. 14.1***), и с 2000 г. в КГТУ проводится набор по специальности 075200 «Компьютерная безопасность». Данная специальность представляет область науки и техники, охватывающую совокупность проблем, связанных с построением и доказательным анализом качества защищенных компьютерных систем. Объектами профессиональной деятельности выпускника являются: защищенные компьютерные системы и средства обработки, хранения и передачи информации; службы защиты информации; математические модели процессов, возникающих при защите информации. Выпускник специальности «Компьютерная безопасность» в соответствии с требованиями Квалификационного справочника должностей руководителей, специалистов и других служащих, утвержденного постановлением Минтруда России от 21.08.1998 г. № 37, может занимать непосредственно после окончания вуза первичные должности специалиста по защите информации и инженера по защите информации.

Параллельно с развитием новой специальности стала формироваться **система переподготовки и повышения квалификации кадров в области информационной безопасности**. В 1997 г. в КГТУ были введены циклы лекций и лабораторных работ по основам информационной безопасности и защите информации в компьютерных системах в рамках курсов повышения квалификации специалистов по вычислительной технике и информационным технологиям. Для разных категорий слушателей разработаны учебные программы и накоплен опыт проведения специальных курсов по информационной безопасности с разным уровнем углубления, от обзорных до специализированных по программам, согласованным с Гостехкомиссией России. В частности, КГТУ по поручению Министерства транспорта России ведет курсы повышения квалификации по вопросам технической защиты информации для специалистов предприятий транспортного комплекса Сибири и Дальнего Востока, находящихся в ведении Минтранса РФ. В целом, можно выделить три основных направления работ, касающихся задач переподготовки специалистов и повышения общей грамотности пользователей и персонала информационных систем по вопросам информационной безопасности. Первое направление относится к возможности получения второго высшего образования лицами, имеющими высшее образование по специальностям, связанным с математикой, информатикой и вычислительной техникой. В настоящее время актуальной является проблема организации подготовки специалистов по гуманитарным аспектам информационной безопасности. Такую подготовку целесообразно

осуществлять на стыке информационных специальностей с гуманитарными (юриспруденцией, психологией, журналистикой). Второе направление относится к реализации учебных программ повышения квалификации, формируемых на основе поступающих заказов от заинтересованных организаций. Третье направление имеет целью обучение всех пользователей информационных систем элементарным правилам обеспечения информационной безопасности. Большинство таких пользователей не осознают, какое количество дестабилизирующих факторов может воздействовать на информацию в электронном виде и какие угрозы при этом могут возникнуть. Реализация образовательных программ в рамках этого направления должна осуществляться в нескольких вариантах:

- включение специальных курсов по информационной безопасности или соответствующих разделов в рамках базовых курсов по информатике для всех специальностей и направлений;
- организация краткосрочных циклов теоретических и практических занятий по актуальным проблемам компьютерной безопасности;
- изучение различных аспектов обеспечения информационной безопасности в системе общеобразовательных школ.

Научно-исследовательские работы ведутся в области математических проблем теории кодирования, распознавания образов и обработки изображений, моделирования процессов защиты информации и обмена данных в системах обработки информации. Разработки в области прикладных программных средств включают в себя информационные системы, ориентированные на работу в распределенной вычислительной среде с соблюдением необходимых требований обеспечения информационной безопасности, выполненные по заказам предприятий и организаций. К их числу относятся исследования, посвященные технологиям электронного контроля доступа, созданию автоматизированного рабочего места специалиста по информационной безопасности, проектированию систем электронного обмена данными, изучению технических и технологических аспектов доступа к информации в электронном виде как основы обеспечения права собственности на информационные ресурсы. Ведутся работы по созданию специализированного системного программного обеспечения и исследования в области обеспечения антивирусной безопасности. Деятельность в области защиты информации в КГТУ лицензирована Гостехкомиссией России. С 1997 г. при КГТУ действует научно-методический семинар «Проблемы информационной безопасности», на котором обсуждаются фундаментальные и прикладные проблемы.

В **Сибирской аэрокосмической академии (САА)** открыта специальность 220700 – «Комплексное обеспечение информационной безопасности автоматизированных систем». В 1999 г. осуществлен первый набор по дневной форме обучения в количестве 25 человек. С 2000 г. специальность получила индекс 075500 (***табл. 14.1***). Первый выпуск специалистов по защите информации в САА состоится в 2004 г.

Специальность охватывает совокупность проблем, связанных с построением, исследованием и эксплуатацией систем и технологий обеспечения информационной безопасности автоматизированных систем. Объектами профессиональной деятельности выпускника являются автоматизированные системы обработки, хранения и передачи информации определенного уровня конфиденциальности, методы и средства обеспечения информационной безопасности автоматизированных систем. Выпускник подготовлен к осуществлению проектно-конструкторской, организационно-технологической, эксплуатационной, организационно-управленческой деятельности.

Студенты имеют доступ к библиотечным фондам и базам данных, методическим пособиям и рекомендациям по всем дисциплинам, наглядным пособиям, мультимедийным и аудио-видеоматериалам. В библиотечном фонде имеются соответствующие профилю подготовки научно-технические и реферативные журналы в печатной или электронной

форме. Каждому студенту обеспечена возможность выхода в сеть Интернет и работа в ней. Компьютерные классы оснащены современной вычислительной техникой и необходимым программным обеспечением. Доля преподавателей, имеющих ученую степень, составляет около 85%. В качестве базовых предприятий и организаций для прохождения учебной, производственной и преддипломной практики предполагаются ГПО «Красмашзавод», краевые правоохранительные органы, профильные организации, учреждения и предприятия,

Выпускник этой специальности в соответствии с требованиями Квалификационного справочника должностей руководителей, специалистов и других служащих, утвержденного постановлением Минтруда России от 21.08.1998 г. № 37 может занимать непосредственно после окончания вуза первичные должности специалиста по защите информации и инженера по защите информации.

Большое внимание решению проблем информационной безопасности уделяется в **Красноярском государственном университете.** К настоящему времени Красноярский государственный университет имеет развитую телекоммуникационную структуру, которая обеспечивает деятельность различных служб университета, а также двух подразделений, основной задачей которых является развитие телекоммуникаций в Красноярском регионе: Региональный центр информатизации (РЦИ), функционирующий под эгидой Министерства образования, и Центр Интернет, созданный в рамках межправительственных соглашений России и США. В настоящее время Центр Интернет обслуживает около 9 тыс. индивидуальных пользователей и более 40 организаций г. Красноярска и региона, обеспечивая доступ к международным ресурсам сети Интернет. Он имеет хорошую базу по созданию WEB-ресурсов и предоставления услуг подключения по Dial-Up. В связи с этим проблемы информационной безопасности для Красноярского госуниверситета являются чрезвычайно важными и актуальными. Университет ведет целенаправленную подготовку специалистов в области защиты информации силами РЦИ и Центра Интернет в рамках соответствующих специализаций. В области разработки программных методов защиты информации усилия направлены не только на защиту информации от несанкционированного доступа извне, но и на защиту информации от несанкционированной передачи во внешние сети. Для этих целей в Центре Интернет разрабатываются подходы к созданию оригинальной системы по защите информации, базирующиеся на экспертных оценках различных параметров поведения пользователя в сети.

В **Сибирском государственном технологическом университете** осуществляется подготовка специалистов по информационным технологиям, неотъемлемым компонентом которой являются вопросы информационной безопасности. В ходе обучения читаются курсы по защите информации, а подготовка выпускников в этом направлении ведется в рамках соответствующей специализации.

Естественным этапом развития научной, методической и образовательной деятельности в области информационной безопасности в крае стало создание **Регионального учебно-научного центра по проблемам информационной безопасности (РУНЦ «Информационная безопасность»)** в рамках единой сети таких центров в системе высшей школы. Являясь частью общегосударственной системы обеспечения информационной безопасности единого информационного пространства России, высшая школа становится естественным центром концентрации учебно-методической базы, педагогического и научно-исследовательского кадрового потенциала в этой области. Традиционно тесная связь с академической наукой, сотрудничество со специализированными научно-исследовательскими институтами, конструкторскими бюро, другими заинтересованными организациями при поддержке федеральных и региональных органов власти создают благоприятные условия для комплексного решения актуальных задач информационной безопасности. В Красноярске РУНЦ «Информационная безопасность» создан на базе Красноярского государственного технического университета. Создание РУНЦ

«Информационная безопасность» поддержано Администрацией Красноярского края и Головным учебно-научным центром по проблемам информационной безопасности, функционирующим на базе Московского инженерно-физического института.

Основными направлениями деятельности Центра являются:

- повышение квалификации специалистов по защите информации и обучение персонала абонентов правилам работы с защищаемой информацией;
- проведение научно-исследовательских и опытно-конструкторских работ в области информационной безопасности;
- сбор и распространение сведений о предлагаемых на рынке средствах защиты, а также их тестирование и доведение результатов тестирования до потенциальных потребителей;
- оказание услуг абонентам Центра по решению ими задач, связанных с обеспечением информационной безопасности.

Главными задачами деятельности Центра являются:

- организация совместной работы и координация деятельности высших учебных заведений региона в научном, учебном и учебно-методологическом обеспечении решения проблем информационной безопасности;
- проведение фундаментальных и прикладных исследований по проблемам информатизации, обеспечения информационной безопасности, создания информационных систем, комплексных систем и средств информационной безопасности и анализа их влияния на различные аспекты национальной безопасности;
- исследование и разработка правовых основ информатизации и обеспечения информационной безопасности, борьбы с компьютерной преступностью;
- участие в разработке и реализации научно-технических и учебных программ органов государственной власти и местного самоуправления, предприятий и организаций по вопросам информационной безопасности;
- организация работ по оказанию информационно-аналитических, информационно-справочных и инженерных услуг государственным, общественным и другим организациям в области обеспечения информационной безопасности;
- создание комплексной системы регионального уровня по подготовке, повышению квалификации, переподготовке и аттестации кадров всех уровней квалификации в области информатизации и информационной безопасности;
- развитие перспективных интеллектуальных образовательных технологий;
- подготовка к изданию учебной, научной и методической литературы по вопросам информационной безопасности;
- организация и проведение методических семинаров, конференций регионального уровня, выставок достижений и результатов научных и учебно-методических исследований по проблемам информационной безопасности.

При развитии Центра используется имеющийся опыт взаимодействия с Гостехкомиссией России, региональными подразделениями ФСБ, ФАПСИ, Прокуратуры РФ и других заинтересованных ведомств Российской Федерации, органами местного самоуправления, учреждениями, предприятиями и организациями независимо от их ведомственной принадлежности и формы собственности, другими региональными и головным учебно-научными центрами по проблемам информационной безопасности.

## 14.6. ОРГАНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

На предприятиях всех форм собственности возникает необходимость защиты части информации от доступа посторонних. Угрозы сохранности конфиденциальной информации

могут быть внешними и внутренними. Внешние угрозы возникают вследствие деятельности недобросовестных конкурентов, преступных элементов, из-за неумелой постановки взаимоотношений фирмы с другими предприятиями. Внутренние угрозы инициируются персоналом предприятия.

Действия извне могут быть направлены на пассивные носители информации и выражаться в следующем:

- попытки похищения документов или снятия копий с них;
- попытки кражи дискет, магнитных лент, компакт-дисков, жестких дисков компьютеров, других средств хранения информации;
- снятие информации в процессе передачи по средствам телекоммуникации (при передаче электронной почты, работе в сети Интернет, через подключение «жучков» к телефонным кабелям, к кабельным системам вычислительных сетей);
- уничтожение информации или повреждение ее носителей;
- случайное или преднамеренное доведение до сведения конкурентов или преступных элементов документов или материалов, содержащих конфиденциальную информацию организации.

На сегодняшний день наибольшую опасность представляют внутренние угрозы. Не исключена возможность того, что отдельные сотрудники с высоким уровнем самооценки из-за неудовлетворенности уровнем зарплаты, отношениями с руководством, коллегами могут предпринимать шаги по инициативной выдаче конфиденциальной информации конкурентам, пытаться уничтожить важную информацию, заблокировать доступ к ней, внести выгодные для себя корректировки данных.

Последовательность действий по организации комплекса мер информационной безопасности зависит от формы собственности предприятия и уровня используемых информационных технологий. Рекомендуемая организационная схема включает следующие мероприятия:

1. Разработка соответствующих нормативных документов, регламентирующих деятельность всех звеньев предприятия по защите конфиденциальной информации. Прежде всего необходимо зарегистрировать право на коммерческую тайну в Уставе предприятия, поскольку в соответствии со ст. 21 Закона РСФСР «О предприятиях и предпринимательской деятельности» предприятие может осуществлять лишь те виды деятельности, которые предусмотрены в его Уставе. Примерное содержание такого дополнения в Устав может быть следующим. «Предприятие определяет состав, объем и порядок защиты сведений, составляющих коммерческую тайну, и имеет право требовать от сотрудников соблюдения установленных правил ее сохранности. Предприятие и его сотрудники обязаны обеспечить сохранность коммерческой тайны». Соответствующие изменения должны быть внесены в учредительный договор и правила внутреннего трудового распорядка предприятия.

2. Необходимо составить перечень сведений, которые должны быть защищены в соответствии с законом, а также сведений, разглашение которых может привести к нежелательным последствиям для организации и ее сотрудников. Перечней может быть несколько, например: «Перечень сведений, составляющих коммерческую тайну предприятия», «Перечень сведений, которые не должны разглашаться посторонним лицам в целях безопасности фирмы и личной безопасности сотрудников фирмы», «Перечень сведений, составляющих коммерческую информацию».

Первый документ – прямая основа для возникновения юридической ответственности в соответствии с гражданским законодательством. Два других документа нужны в связи с тем, что некоторую информацию трудно отнести к коммерческой тайне, но сохранять ее весьма важно (например, место нахождения руководителя фирмы в конкретное время, планируемые совещания, переговоры, сведения о личной жизни сотрудников и т. п.). Перечисление такой информации, которая имеет специфику в каждом конкретном случае, имеет, прежде всего,

характер дисциплинирующего воздействия на сотрудников. При этом необходимо ознакомить всех работников с соответствующими перечнями, проинструктировать о правилах обращения с документами, средствами компьютерной техники, со средствами телекоммуникации и собрать подписи о том, что люди проинструктированы и ознакомлены с перечнями конфиденциальной информации.

3. Следующим необходимым документом является «Договор-обязательство о сохранении коммерческой тайны и другой конфиденциальной информации», который необходимо подготовить и предложить подписать каждому сотруднику. Это может быть как отдельный документ, так и специальный раздел в контракте о найме на работу. Предложив сотруднику подписать договор-обязательство, руководство фирмы предупреждает сотрудника, что в дело вступает целая система мероприятий по защите информации: правовых, организационных, технических. Договор закладывает правовую основу для пресечения возможных противоправных действий.

Наличие перечисленных документов дает возможность говорить о наличии на предприятии юридически закрепленного порядка защиты коммерческой информации, что также дает возможность принимать на себя юридически обеспеченные обязательства по сохранению коммерческой тайны заказчика, относя ее к закрытой информации. При этом необходимо в договорах с заказчиком четко и однозначно указывать сведения, относящиеся к защищаемой информации.

4. Исходя из принятых перечней, необходимо обозначить защищаемую информацию соответствующими грифами на документах, на перемещаемых машиночитаемых носителях информации, организовать их учет, разграничить доступ сотрудников к информации.

5. Исходя из составленных перечней защищаемых информационных ресурсов, необходимо определить помещения, доступ в которые фактически означает доступ к конфиденциальной информации, проверить эти помещения на наличие аппаратных закладок, организовать контроль доступа в эти помещения, их физическую защиту. Как правило, к разряду таких помещений наряду с кабинетами первых руководителей, комнатами переговоров относят серверные комнаты, комнаты с коммутаторами, сетевым оборудованием, помещения, где находятся сетевые администраторы, администраторы информационной безопасности и, по возможности, комнаты пользователей компьютерной сети, которые работают с особо конфиденциальной информацией.

6. Необходимо разработать положение о защите информации на предприятии, которое бы регламентировало деятельность различных подразделений и их взаимодействие по обеспечению информационной безопасности организации. Необходимы также конкретные инструктивные материалы для различных категорий сотрудников, с которыми они должны быть ознакомлены под роспись.

7. Одним из непременных условий достижения высокого уровня информационной безопасности предприятия является постоянная работа с персоналом. Необходимо не только довести до исполнителей инструктивные материалы, но и провести обучение по материалам инструкций, проверку усвоенных знаний и консультации о действиях в различных ситуациях: при компьютерных сбоях, при подозрениях на попытки несанкционированного доступа, при возникновении чрезвычайных ситуаций, грозящих физическому уничтожению информации.

8. В целях предотвращения и выявления внесения программных закладок типа «троянский конь» в программные продукты, в организации необходимо создать архив первичных копий всех операционных систем и прикладных программ.

Полная реализации действий, направленных на обеспечение информационной безопасности предприятия возможна при наличии отдельного плана мероприятий, отражающего последовательность действий в этом направлении и привлекаемые для этой цели объемы финансирования. Для координации действий подразделений по обеспечению

информационной безопасности, разработки мероприятий и контроля их выполнения должно быть создано специальное подразделение (для небольшого предприятия может быть достаточно одного специалиста по защите информации) в непосредственном подчинении первого руководителя или его заместителя по безопасности.

Существенное повышение надежности защиты информации на средствах компьютерной техники (особенно определяемых внутренними угрозами) дает применение специальных сертифицированных программных и программно-аппаратных средств защиты информации. Но приобретение подобных систем без предварительного проведения комплекса организационных мероприятий – пустая трата средств, поскольку программно-аппаратные средства защиты информации, – это инструмент реализации и контроля выполнения принятых в учреждении правил разграничения доступа.

## 14.7. ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КРАСНОЯРСКОМ КРАЕ

Проведенный анализ состояния и проблем обеспечения информационной безопасности в Красноярском крае позволяет представить общую структуру информационного обмена и системы информационной безопасности в регионе. Отметим, что систему защиты государственной тайны в настоящее время можно считать хорошо формализованной и достаточно надежно функционирующей. Значительно хуже обстоит дело с защитой информации учреждений, предприятий и граждан.

Появление Концепции программы информатизации Красноярского края до 2005 г. дополнительно акцентировало внимание на вопросах информационной безопасности. В ней заложены некоторые мероприятия по координации действий различных организаций и учреждений в этом направлении. Этим же целям служит создание и работа Регионального учебно-научного центра по проблемам информационной безопасности. В целом, успешно развивается система подготовки вузами города Красноярска специалистов по защите информации при поддержке соответствующих краевых управлений.

Вместе с тем, не решен ряд организационно-правовых вопросов. Прежде всего, необходимо законодательно разрешить противоречие между защитой индивидуальных данных и созданием многочисленных баз данных, обобщающих разные аспекты граждан: паспортный стол, налоговая инспекция, медицинское страхование и др. В этой части большое значение имеет использование международного опыта в области защиты информации. Например, целесообразно использовать опыт ФРГ по созданию доверенных центров с целью обеспечения охраны конфиденциальной информации учреждений и предприятий, а также законодательный опыт по обеспечению прав граждан на защиту индивидуальной информации. Остро стоит вопрос о легализации такого распространенного в европейских странах и полезного средства как электронная подпись, о легитимности использования криптографических средств. Необходимо дальнейшее совершенствование деятельности по пресечению преступных действий в области компьютерных технологий, число которых в соответствии с мировой тенденцией будет нарастать.