УДК 004.056.5

Информационные ресурсы вуза и оценка их безопасности

А. О. Шемяков

Аннотация

В статье рассматриваются законодательная база, определяющая порядок отнесения сведений к государственной тайне и к конфиденциальной информации. Анализируются состав конфиденциальной информации вуза, и возможные варианты ее утечки физическими, организационными и техническими методами получения информации. Рассматриваются легальные и нелегальные методы.

Ключевые слова

информационные ресурсы, государственная тайна, конфиденциальность, несанкционированный доступ, утрата информации.

Информационными ресурсами (ИР) называются источники информации.

В соответствии с действующим Федеральным Законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ИР предприятий, организаций, и других государственных и негосударственных структур включают в себя отдельные документы и отдельные массивы документов (дела), документы и комплексы документов в ИС (библиотеках, архивах, фондах, банках данных) на любых носителях.

По принадлежности к тому или иному виду собственности ИР могут быть государственными пли негосударственными. Негосударственные ИР находятся в собственности граждан, государственных и муниципальных учреждений, организаций и предприятий, общественных объединений, предпринимательских структур.

В соответствии с интересами обеспечения национальной безопасности и степенью ценности для государства, а также правовыми, экономическими и другими требованиями ИР могут быть:

– открытыми, т.е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях и интервью;

– ограниченного доступа и использования, т.е. содержащими сведения конфиденциального характера, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению и контролю.

В соответствии с Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» (с изменениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г., 18 июля 2009 г., 15 ноября 2010 г., 18, 19 июля, 8 ноября 2011 г.) государственная тайна – это защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности. Таких сведений, распространение которых может нанести ущерб безопасности Российской Федерации. Носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Отнесение сведений к государственной тайне и их засекречивание – введение ограничений на их распространение и на доступ к их носителям в предусмотренном Законом порядке – устанавливается путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан. Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности устанавливаются Правительством Российской Федерации. Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, учебного заведения, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне регламентируется Перечнем сведений, составляющих государственную тайну, определяемым Законом РФ "О государственной тайне.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие бесконтрольного распространения этих сведений. Целесообразность засекречивания таких перечней определяется их содержанием.

Для осуществления единой государственной политики в области засекречивания сведений Межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне. В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями. Указанный Перечень утверждается Президентом Российской Федерации, подлежит открытому опубликованию и пересматривается по мере необходимости.

Министерство образования и науки РФ наделено, в ряду других ведомств РФ, полномочиями по отнесению сведений к государственной тайне. Поэтому Минобразования в соответствии с Перечнем сведений, отнесенных к государственной тайне, разрабатывает развернутый перечень сведений, подлежащих засекречиванию. В этот перечень включаются сведения, полномочиями по распоряжению которыми наделено Министерство, и устанавливается степень секретности этих сведений. В рамках целевых программ по разработке и модернизации образцов вооружения и военной техники, опытно-конструкторских и научно-исследовательских работ по решению заказчиков указанных образцов и работ могут разрабатываться отдельные перечни сведений, подлежащих засекречиванию. Такие перечни утверждаются соответствующими руководителями органов государственной власти.

Законом устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей секретных сведений: "особой важности", "совершенно секретно" и "секретно". Государственные органы, уполномоченные осуществлять охрану сведений, содержащих государственную тайну, разрабатывают подробные инструкции по порядку работы с секретными сведениями и контролируют выполнение этих инструкций учебного заведениями, наделенными полномочиями по работе с секретными сведениями.

Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, законом не допускается.

Несмотря на то, что конфиденциальность является синонимом секретности, термин «конфиденциальность» используется исключительно для обозначения ИР ограниченного

доступа, не отнесенных к государственной тайне. Конфиденциальность отражает ограничение, которое накладывает владелец ИР на доступ к информации других лиц. Т.е. собственник устанавливает режим использования принадлежащей ему конфиденциальной информации, Разумеется, руководствуясь требованиями Закона. Закон устанавливает как права, так и обязанности собственника конфиденциальной информации. Так, в соответствии с Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" к конфиденциальным документам нельзя относить учредительные документы, уставы предприятий, финансовую документацию, сведения о заработной плате персонала и другую документированную информацию, необходимую правоохранительным и налоговым государственным органам.

Под конфиденциальным (закрытым, защищаемым) документом понимается необходимым образом оформленный носитель документированной информации, содержащий сведения ограниченного доступа или использования, на которые распространяются права собственности юридического или физического лица. На конфиденциальные документы не следует ставить секретности, так как конфиденциальные и секретные документы отражают различные виды тайны.

Право на отнесение сведений к конфиденциальной информации, а также на определение перечня и состава такой информации принадлежит обладателю такой информации. А конкретно – к компетенции учебного заведения.

Общая схема классификации конфиденциальной информации представлена на рис. 1.

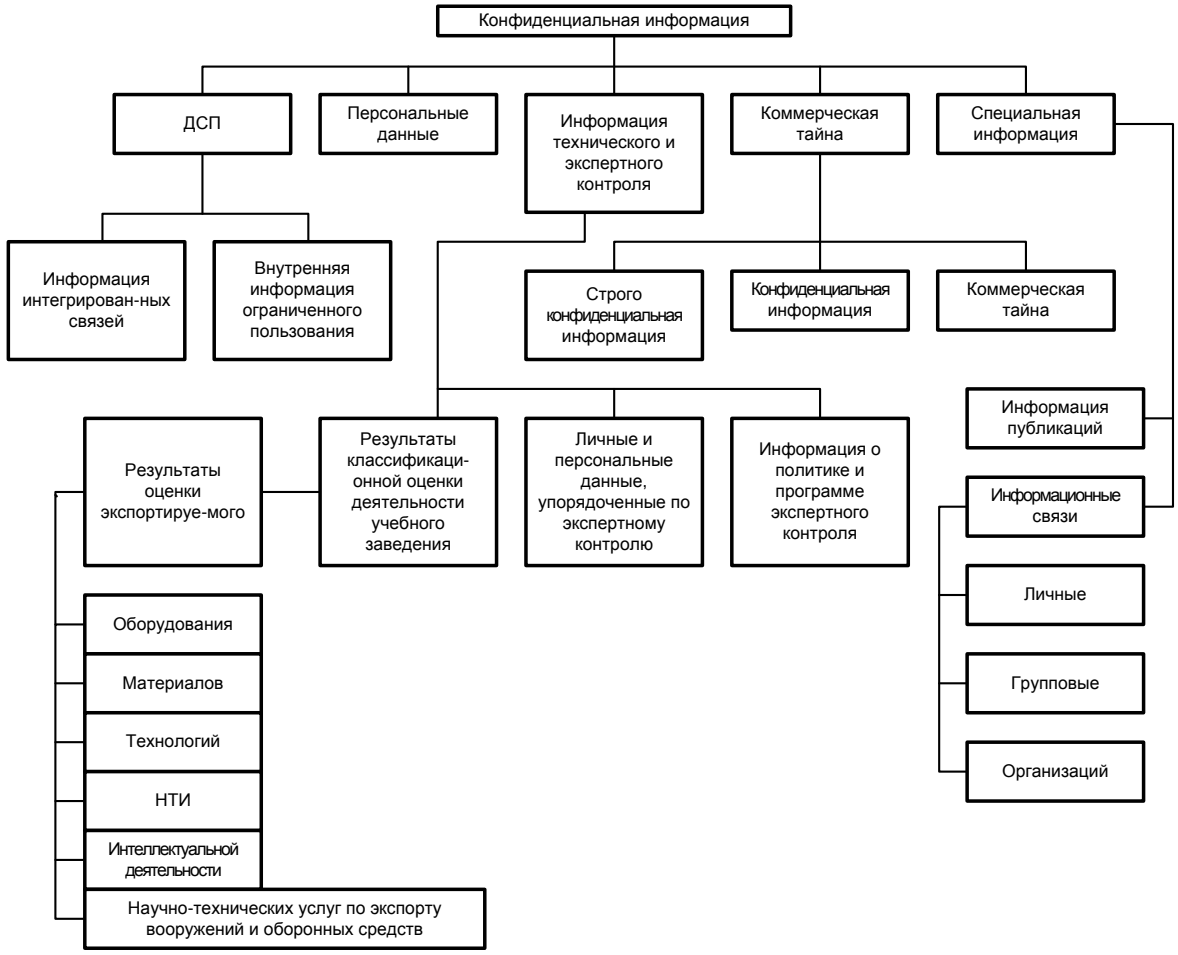

Рис. 1. Схема классификации конфиденциальной информации

Если сведения, имеющие признаки конфиденциальной информации (коммерческой тайны), получены в ходе работ по государственному контракту на выполнение научно-исследовательских, опытно-конструкторских или иных работ для федеральных государственных нужд или нужд субъекта Российской Федерации, режим конфиденциальности устанавливается контрактом.

Таким образом, документированная информация ограниченного доступа всегда принадлежит к одному из видов тайны – государственной или негосударственной. В соответствии с этим документы делятся и секретные и несекретные. Обязательным признаком (критерием) принадлежности секретного документа является наличие в нем сведений, составляющих в соответствии с законодательством государственную тайну, Несекретные конфиденциальные документы, включающие сведения, относимые к негосударственной тайне (служебной, коммерческой, банковской, профессиональной, производственной и др.), или содержащие персональные данные граждан, именуются конфиденциальными.

Конфиденциальные документы включают в себя:

– в государственных структурах – служебную информацию ограниченного распространения, именуемую в чиновничьем обиходе информацией для служебного пользования, т.е. информацией, отнесенной к служебной тайне, а также документы, имеющие рабочий характер и не подлежащие публикации в открытой печати (проекты документов, сопутствующие материалы и др.);

– в предпринимательских структурах и направлениях подобной деятельности – сведения, которые их собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне фирмы, секрету производства (know-how);

– независимо от принадлежности – любые персональные (личные) данные о гражданах, а также сведения, содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т.п.

Особенностью конфиденциального документа является то, что он представляет собой одновременно:

– массовый носитель ценной, защищаемой информации;

– основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки;

– обязательный объект защиты.

Конфиденциальность документов всегда имеет значительный разброс по срокам ограничения свободного доступа к ним персонала учебного заведения (от нескольких часов до значительного числа лет).

Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою актуальность, а, следовательно, – ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф снимается. Разумеется, снятие или снижение грифа и соответствующее изменение правил обращения с документом должно регламентироваться соответствующими утвержденными инструкциями.

Исполненные документы, сохранившие конфиденциальный характер и ценность для деятельности учебное заведение, формируются в дела в соответствии с номенклатурой дел. Период нахождения конфиденциальных документов в делах может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах

дела. Период конфиденциальности документов определяется перечнем конфиденциальных сведений и зависит от специфики деятельности.

Угрозы конфиденциальным информационным ресурсам высшего учебного заведения

Все ИР высшего учебного заведения постоянно подвергаются объективным и субъективным угрозам утраты носителя или потери ценности информации.

Под угрозой или опасностью утраты информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемые процессы переработки информации, документы и базы данных (БД).

Риск угрозы любым (открытым и ограниченного доступа) ИР создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линии связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относится: несанкционированное уничтожение документов, ускорение угасания (старения) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и другие негативные и/или деструктивные проявления.

Для ИР ограниченного доступа диапазон угроз, предполагающих утрату информации (разглашение, утечку) или утерю носителя, значительно шире, чем для документов открытых, Эта особенность обусловлена тем, что к этим документам проявляется повышенный интерес со стороны различного рода злоумышленников. В отличие от объективного распространения утрата информации влечет за собой незаконный переход конфиденциальных сведений, документов к субъекту, не имеющему права владения ими и использовании в своих целях.

Под злоумышленником понимается лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленником, и т.п.).

Основной угрозой безопасности ИР ограниченного распространения является несанкционированный доступ (НСД) злоумышленника или постороннего лица к документированной информации и как результат – овладение информацией и противоправное ее использование или совершение иных действий. Целью и результатом

НСД может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, подмена и т.п.

Обязательным условием успешного осуществления информационной атаки против ресурсов ограниченного доступа является интерес к ним со стороны конкурентов, определенных лиц, служб и организаций. При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для ознакомления с ней постороннего лица. Основным виновником осуществления НСД к ИР является, как правило, персонал, работающий с документами, информацией и БД. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а из-за невнимательности и безответственности персонала.

Утрата ресурсов ограниченного доступа может наступить:

– при наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

– при возникновении риска угрозы, организованной злоумышленником или при случайно сложившихся обстоятельствах;

– при наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией.

Эти условия могут сложиться вследствие:

– отсутствия системной аналитической и контрольной работы по выявлению и изучению угроз, каналов утечки и степени рисков;

– нарушений безопасности ИР;

– неэффективности системы защиты процессов переработки информации или отсутствие этой системы;

– непрофессионально организованной технологии обработки и хранения конфиденциальных документов;

– неупорядоченного подбора персонала и текучести кадров, сложного психологического климата в коллективе;

– отсутствия системы обучения сотрудников правилам защиты процессов переработки информации ограниченного доступа;

– отсутствия контроля со стороны руководства высшего учебного заведения за соблюдением персоналом требований нормативных документов по работе с ИР ограниченного доступа;

– бесконтрольного посещения помещений высшего учебного заведения посторонними лицами.

Факт документирования резко увеличивает риск угрозы процессам переработки информации. Великие мастера прошлого никогда не записывали секреты своего искусства, а передавали их устно сыну, ученику. Поэтому тайна изготовления многих уникальных предметов того времени так и не раскрыта до наших дней. Но возможность утраты информации – это тоже угроза. Угроза не мене опасная, чем НСД.

Угрозы сохранности, целостности и конфиденциальности ИР ограниченного доступа практически реализуются через риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов. Этот канал представляет собой совокупность незащищенных или слабо защищенных высшим учебным заведением направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Крупные высшие учебные заведения обладает практически полным набором каналов НСД к информации, что зависит от множества моментов:

- профиля деятельности, учебных занятий,
- объемов защищаемых процессов переработки информации,
- профессионального уровня персонала, местоположения здания и т.п.

Функционирование канала НСД к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

В том случае, когда речь идет об утрате информации по вине персонала или учащихся, используется термин «разглашение (огласка) информации». Термин «утечка информации», хотя и используется наиболее широко, однако в большей степени относится, к утрате информации за счет ее перехвата с помощью технических средств разведки, по техническим каналам.

Утрата информации характеризуется двумя условиями: информация переходит непосредственно к заинтересованному лицу – конкуренту, злоумышленнику или к случайному, третьему лицу. Под третьим лицом в данном случае понимается любое постороннее лицо, получившее информацию во владение в силу обстоятельств или безответственности персонала, не обладающее правом владения ею и, что очень важно, не заинтересованное в этой информации. Однако от третьего лица информация может легко перейти к злоумышленнику.

Переход информации к третьему лицу представляется достаточно частым явлением, и его можно назвать непреднамеренным, стихийным, хотя при этом факт разглашения информации, нарушения ее безопасности имеет место.

Непреднамеренный переход информации к третьему лицу возникает в результате:

– утери или неправильного уничтожения документа, пакета с документами, дела, конфиденциальных записей;

– игнорирования или умышленного невыполнения сотрудником требований по защите документированной информации;

– излишней разговорчивости сотрудников при отсутствии злоумышленника (с коллегами по работе, родственниками, друзьями, иными лицами в местах общего пользования, транспорте и т.п.);

– работы с документами ограниченного доступа при посторонних лицах, несанкционированной передачи их другому сотруднику;

– использования сведений ограниченного доступа в открытых документации, публикациях, интервью, личных записях, дневниках и т.п.;

– отсутствия маркировки (грифования) информации и документов ограниченного доступа (в том числе документов на технических носителях);

– наличия в документах излишней информации ограниченного доступа; .,

– самовольного копирования сотрудником документов в служебных или коллекционных целях.

В отличие от третьего лица злоумышленник или его сообщник целенаправленно охотятся за конкретной информацией и преднамеренно, противоправно устанавливают контакт с источником этой информации или преобразуют канал ее объективного распространения в канал ее разглашения или утечки. Такие каналы всегда являются тайной злоумышленника.

Каналы НСД могут быть двух типов: организационные и технические. Обеспечиваются они легальными и нелегальными методами. Организационные каналы разглашения информации отличаются большим разнообразием видов и основаны на установлении разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой или ее сотрудником для последующего НСД к интересующей информации.

Основными видами организационных каналов могут быть:

– поступление злоумышленника на работу в высшее учебное заведение, как правило, на техническую или вспомогательную должность (оператором ЭВМ, секретарем, дворником, охранником, шофером и т.п.);

– участие в работе подразделений высшего учебного заведения в качестве партнера, посредника, клиента, использование разнообразных обманных способов;

– поиск злоумышленником такого сообщника (инициативного помощника), работающего в высшем учебном заведении, который становится его соучастником;

– установление злоумышленником доверительных взаимоотношений с сотрудником высшего учебного заведения, учащимся или посетителем, сотрудником другого учреждения, обладающим интересующими злоумышленника сведениями;

– использование коммуникативных связей высшего учебного заведения – участие в переговорах, совещаниях, переписке и др.;

– использование ошибочных действий персонала или умышленное провоцирование злоумышленником этих действий;

– тайное или по фиктивным документам проникновение в здания и помещения высшего учебного заведения, криминальный, силовой доступ к информации, т.е. кража документов, дискет, дисков, компьютеров, шантаж и склонение к сотрудничеству отдельных сотрудников, подкуп сотрудников, создание экстремальных ситуации и т.п.;

– получение нужной информации от третьего (случайного) лица.

Организационные каналы отбираются или формируются злоумышленником индивидуально в соответствии с его профессиональным умением, конкретной ситуацией, и прогнозировать их крайне сложно. Обнаружение организационных каналов требует проведения серьезной поисковой и аналитической работы.

Широкие возможности несанкционированного получения подобных сведений создает техническое обеспечение офисных технологий. Любая управленческая деятельность всегда связана с обсуждением ценной информации в кабинетах или по линиям связи, проведением расчетов и анализа ситуаций на ЭВМ, изготовлением, размножением документов и т.п.

Технические каналы утечки информации возникают при использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом высшего учебного заведения, документами, делами и БД. Технический канал представляет собой физический путь утечки информации от источника или канала объективного распространения информации к злоумышленнику. Канал возникает при

анализе злоумышленником физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники, при перехвате информации, имеющей звуковую, зрительную или иную форму отображения. Основными техническими каналами являются:

- акустический,
- визуально-оптический,
- электромагнитный.

Это каналы прогнозируемые, носят стандартный характер и перекрываются стандартными средствами противодействия. Обычным и профессионально грамотным является творческое сочетание в действиях злоумышленника каналов обоих типов, например установление доверительных отношений с сотрудником вуза и перехват информации по техническим каналам с помощью этого сотрудника. Вариантов и сочетаний каналов может быть множество. Изобретательность грамотного злоумышленника не знает предела, поэтому риск утраты информации всегда достаточно велик. При эффективной системе защиты процессов переработки информации фирмы злоумышленник разрушает отдельные элементы защиты и формирует необходимый ему канал получения информации.

В целях практической реализации поставленных задач злоумышленник определяет не только каналы НСД к информации вуза, но и совокупность методов получения этой информации.

Легальные методы отличаются правовой безопасностью и, как правило, предопределяют возникновение интереса к вузу. В соответствии с этим может появиться необходимость использования каналов НСД к требуемой информации. В основе такого шпионажа лежит кропотливая аналитическая работа специалистов-экспертов над опубликованными и общедоступными материалами. Одновременно изучается продукция объекта шпионажа, рекламные издания, сведения, полученные в процессе официальных и неофициальных бесед и переговоров с сотрудниками, материалы пресс-конференций, презентаций и продукции, научных симпозиумов и семинаров, сведения, получаемые из информационных сетей. Легальные методы дают злоумышленнику основную массу интересующей его информации и позволяют определить состав отсутствующих сведений, которые предстоит добыть нелегальными методами.

Нелегальные методы получения ценной информации всегда носят незаконный характер и используются в целях доступа к защищаемой информации, которую невозможно получить легальными методами. В основе нелегального получения информации лежит поиск злоумышленником существующих в вузе и наиболее эффективных в конкретных условиях

незащищенных организационных и технических каналов НСД к информации, формирование таких каналов при их отсутствии и реализация плана практического комплексного использования этих каналов.

Нелегальные методы предполагают: воровство, продуманный обман подслушивание разговоров, подделку идентифицирующих документов, взяточничество, инсценирование или организацию экстремальных ситуаций, использование различных криминальных приемов и т.д. В процессе реализации нелегальных методов часто образуется агентурный канал добывания ценной информации. К нелегальным методам относятся также:

– перехват информации, объективно распространяемой по техническим каналам,

– визуальное наблюдение за помещениями, учащимися и персоналом высшего учебного заведения;

– анализ продуктов и объектов, содержащих следы защищаемой информации,

– анализ технических особенностей объектов защиты.

В результате эффективного использования каналов НСД к конфиденциальной информации и разнообразных методов ее добывания злоумышленник может получить:

– подлинник или официальную копию документа (бумажного, электронного), содержащего информацию ограниченного доступа;

– несанкционированно сделанную копию этого документа (рукописную или изготовленную с помощью копировального аппарата, фототехники, компьютера и т.п.);

– диктофонную, магнитофонную, видеокассету с записью текста документа, переговоров, совещания; письменное или устное изложение за пределами фирмы содержания документа, ознакомление с которым осуществлялось санкционированию или тайно;

– устное изложение текста документа по телефону, переговорному устройству, специальной радиосвязи и т.п.;

– аналог документа, переданного по факсимильной связи или электронной почте;

– речевую или визуальную запись текста документа, выполненную с помощью технических средств разведки (радиозакладок, встроенных микрофонов и видеокамер, микрофотоаппаратов, фотографирования с большого расстояния).

Получение ценных документов или информации ограниченного доступа может быть единичным явлением или регулярным процессом, протекающим на протяжении относительно длительного времени.

Следовательно, любые ИР вузов являются весьма уязвимой категорией и при интересе, возникшем к ним со стороны злоумышленника, опасность их утраты становится достаточно реальной.

Библиографический список

1. Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации. Издательский центр «Академия», Москва. 2007. 256 с.
2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. Издательский центр «Академия», Москва. 2009. 336 с.
3. Стрельцов А. А. Организационно-правовое обеспечение информационной безопасности. Издательский центр «Академия», Москва. 2008. 256 с.
4. Масановец В. В., Фесун А. П., Никифоров О. Г. Методы комплексного контроля безопасности на объектах телекоммуникационных систем органов государственного управления. Управление делами Президента Российской Федерации, Москва. 2009. 368 с.

Сведения об авторе

Шемяков Александр Олегович, аспирант Московского авиационного института (национального исследовательского университета).
МАИ, Волоколамское ш., 4, Москва, А-80, ГСП-3, 125993; тел.: (499) 158-40-66; e-mail: a.shemyakov@gmail.com