

Александр КОЗКА, консультант по юридическим вопросам



ТРЕБОВАНИЯ К РАБОТЕ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ УЧРЕЖДЕНИЯ

Утечка информации за пределы учреждения может нанести ей как репутационный, так и материальный вред. Данные, доступные для узкого круга лиц в связи с выполнением ими своих должностных обязанностей, из-за их небрежности, подкупа или противоправных действий третьих лиц нередко попадают в руки злоумышленников или мошенников. Что такое конфиденциальная информация, как обеспечить ее правомерное использование и защиту?

Значение термина

По данным экспертов по безопасности, на сегодня наиболее распространенным и опасным видом внутренней угрозы становится утечка информации. Нередко источником такой угрозы являются недобросовестные работники учреждения, которые в соответствии со своими служебными обязанностями имеют доступ к конфиденциальной информации и используют ее в интересах третьих лиц. Как свидетельствует судебная практика, потери предприятия в таком случае нередко бывают значительно большими, чем от мошенничества или краж.

Сам термин «конфиденциальный» происходит от английского confidence – доверие, необходимость предотвращения потери какой-либо информации. Другими словами, конфиденциальная информация должна быть известна или доверена узкому кругу лиц. Общим для всех видов конфиденциальной информации является тот факт, что свободный доступ к ней ограничен согласно предписаниям действующего законодательства или внутренних нормативных документов учреждения или органа, осуществляющего управление им.

Правовое регулирование

Общий подход к работе с конфиденциальной информацией определяет Закон от 02.10.92 г. № 2657-XII «Об информации» (далее – Закон № 2657). В соответствии со ст. 20 данного Закона по порядку доступа информация подразделяется на открытую информацию и информацию с ограниченным доступом. То есть любая информация является открытой, кроме той, которая отнесена законом к информации с ограниченным доступом. Также ст. 21 Закона № 2657 определяет, что информацией с ограниченным доступом является конфиденциальная, тайная и служебная информация.

В то же время к информации с ограниченным доступом не могут быть отнесены следующие сведения:

- о состоянии окружающей среды, качестве пищевых продуктов и предметов быта;
- об авариях, катастрофах, опасных природных явлениях и других чрезвычайных ситуациях, которые произошли или могут произойти и угрожают безопасности людей;
- о состоянии здоровья населения, его жизненном уровне, включая питание, одежду, жилье, медицинское обслуживание и социальное обеспечение, а также о социально-демографических показателях, состоянии правопорядка, образования и культуры населения;
- о фактах нарушения прав и свобод человека, включая информацию, которая содержится в архивных документах бывших советских органов государственной безопасности, связанных с политическими репрессиями, Голодомором 1932–1933 годов в Украине и другими преступлениями, совершенными представителями коммунистического и/или национал-социалистического (нацистского) тоталитарных режимов;
- о незаконных действиях органов государственной власти, органов местного самоуправления, их должностных и служебных лиц;
- относительно деятельности государственных и коммунальных унитарных предприятий, хозяйственных обществ, в уставном капитале которых более 50 % акций (долей) принадлежат государству или территориальной громаде, а также хозяйственных обществ, 50 % и более акций (долей) которых принадлежат хозяйственному обществу, доля государства или территориальной громады в котором составляет 100 %, которые подлежат обязательному обновлению в соответствии с законом;
- другие сведения, доступ к которым не может быть ограничен в соответствии с законами

и международными договорами Украины, согласие на обязательность которых дано Верховной Радой Украины.

Согласно п. 2 ст. 21 Закона № 2657 конфиденциальная информация – это информация о физическом лице (персональные данные) или юридическом лице, доступ и распространение которой возможны только с согласия ее владельцев (т. е. тех, кого эта информация непосредственно касается) и на тех условиях, которые они укажут. Конфиденциальная информация обычно содержится в виде любых документов – традиционных бумажных или электронных. Документы, которые содержат конфиденциальную информацию, принято называть конфиденциальными, а процесс изготовления таких документов и организацию работы с ними – конфиденциальным делопроизводством. Все эти источники информации могут быть объектами неправомерных посягательств, а потому подлежат соответствующей защите.

В учреждении, в зависимости от специфики его деятельности, конфиденциальная информация может содержаться в договорах, деловых письмах, отчетах, аналитических материалах, базах данных клиентов, потребителей, получателей соцпомощи и т. п. Кроме того, конфиденциальной информацией считаются и выписки из бухгалтерских, банковских счетов, схемы, графики, спецификации и другие документы. Правила работы с информацией конфиденциального характера определяются законами и детализируются в локальных нормативных актах министерств, ведомств, предприятий (учреждений, организаций) всех форм собственности.

Владелец конфиденциальной информации должен определить ее состав, соответствующие способы и средства защиты. Одновременно он должен разработать мероприятия материального и морального стимулирования работников, которые соблюдают порядок защиты конфиденциальной информации, а также их ответственности за ее разглашение.

Что подлежит защите?

Согласно абзацу второму ст. 1 Закона № 2657 **под защитой информации следует понимать совокупность правовых, административных, организационных, технических и других мероприятий, которые обеспечивают хранение, целостность информации и надлежащий порядок доступа к ней.** То есть учреждением должна быть создана система защиты конфиденциальной информации, которая бы сделала невозможным несанкционированный (незаконный) доступ к ней. Каждое учреждение, с учетом особенностей его деятельности, а соответственно, состава конфиденциаль-

ной информации, **должно разработать и утвердить перечни конкретных видов документов, содержащих такую информацию, положение о конфиденциальной информации, инструкцию по работе с документами, содержащими конфиденциальную информацию, и т. п.**

Сам перечень и объем сведений, которые относятся к конфиденциальной информации, сроки конфиденциальности, порядок защиты и доступа, а также правила ее использования определяются руководителем учреждения. Для ограничения доступа к конфиденциальной информации руководитель учреждения:

- выдает специальный приказ об утверждении «Перечня сведений, которые составляют конфиденциальную информацию учреждения»;
- предусматривает мероприятия по охране таких сведений;
- устанавливает круг лиц, которые имеют доступ к этой информации;
- устанавливает правила работы с документами, которые имеют гриф «конфиденциальная информация».

Работников учреждения следует ознакомить с приказом и приложениями к нему под подпись.

Инструменты защиты

Защита конфиденциальной информации учреждения может обеспечиваться рядом управленческих инструментов, основными из которых являются:

- установление правил отнесения информации к конфиденциальной;
- разработка и доведение до лиц, допущенных к конфиденциальной информации, соответствующих инструкций относительно соблюдения режима конфиденциальности;
- ограничение доступа к носителям информации, которые содержат конфиденциальную информацию;
- использование организационных, технических и других средств сохранения (защиты) конфиденциальной информации;
- осуществление контроля за соблюдением установленного режима сохранения (защиты) конфиденциальной информации.

В то же время защита конфиденциальной информации предусматривает:

- определение конфиденциальной информации, сроков ее защиты по категориям;
- систему допуска работников учреждения, других лиц к конфиденциальной информации;
- обязанности лиц, допущенных к конфиденциальной информации;

- определение порядка работы с бумажными и электронными документами, содержащими конфиденциальную информацию;
- обеспечение сохранения документов и дел (архивов), содержащих конфиденциальную информацию;
- механизмы организации и проведения контроля за обеспечением установленного порядка во время работы с конфиденциальной информацией;
- ответственность за разглашение конфиденциальной информации и потерю документов, содержащих конфиденциальную информацию.

Комплексность системы защиты достигается ее формированием из разных элементов – правовых, организационных и программно-технических. Соотношение элементов и их содержание обеспечивают индивидуальность системы защиты конфиденциальной информации учреждения и гарантируют ее неповторимость и сложность преодоления.

Что считается разглашением?

Под разглашением конфиденциальной информации следует понимать следующие действия работников учреждения:

- доведение конфиденциальной информации в устной, письменной, электронной или другой форме до сведения лиц, не уполномоченных руководством учреждения на владение ею и ее использование. Указанный факт может наступить в результате умысла сотрудника или по неосторожности, включая небрежное отношение к своим должностным обязанностям;
- использование конфиденциальной информации в процессе выполнения работы для другого учреждения или субъекта хозяйствования;
- использование конфиденциальной информации в научной и педагогической деятельности;
- использование конфиденциальной информации в личных целях, не связанных с выполнением должностных обязанностей;
- использование конфиденциальной информации во время публичных выступлений, интервью и т. п.;
- другие действия работников учреждения, в результате которых конфиденциальная информация стала известна не уполномоченным на это лицам.

Снижение влияния человеческого фактора

Как свидетельствует практика, невзирая на наличие в учреждении организационных мероприятий по защите конфиденциальной информации, озна-

комление значительного количества работников с ней повышает риск ее утечки. Из-за этого правильная организация работы персонала с такими документами очень важна. Основные принципы и правила управления персоналом с учетом требований информационной безопасности определены в международном стандарте ISO 17799. Суть их заключается в необходимости выполнения определенных требований во время найма и увольнения работников, обеспечении осведомленности с правилами работы и применении мер пресечения к нарушителям. Соблюдение этих мероприятий дает возможность существенно снизить влияние человеческого фактора, избежать характерных ошибок и по большей части предотвратить утечку информации и ее ненадлежащее использование.

Между тем, традиционные средства защиты от утечки конфиденциальной информации не всегда являются эффективными. Поэтому учреждение должно применять совокупность мероприятий, направленных именно на работу с персоналом. Одним из таких популярных в настоящее время мероприятий является построение так называемого «социального межсетевого экрана».

Как уже указывалось, учреждение должно разработать соответствующие инструкции относительно защиты конфиденциальной информации. Данные документы будут определять правила и критерии для разбивки информационных ресурсов на отдельные категории, исходя из степени их конфиденциальности, правила маркировки и оборота конфиденциальной информации, предоставления доступа к ней. Также разрабатываются и внедряются соответствующие процедуры и механизмы контроля. Дополнительно к ним целесообразно использовать специализированные сервисы управления правами доступа к электронным документам, позволяющие в случае распространения информации определять ограничение относительно ее использования. Например, автор документа может ограничить «время жизни» документа, а также возможность для определенных пользователей открывать, изменять, копировать в буфер обмена, печатать или пересылать документ.

Стоит заметить, что применение социального межсетевого экрана дает возможность успешно бороться с наиболее многочисленным видом угроз – неумышленным разглашением конфиденциальной информации. Однако для борьбы со злоумышленниками его явно недостаточно, а потому параллельно следует задействовать различные программно-технические механизмы защиты.

Техническая защита

Для более надежной сохранности конфиденциальной информации должна находиться преиму-

щественно в электронном виде и быть защищена электронными средствами защиты. Практика показывает, что в нынешних условиях кражи (утечки) информации происходят и по электронным каналам связи или с помощью различных носителей информации. Исходя из этого, главные усилия в борьбе с утечкой конфиденциальной информации нужно сосредоточить именно на этом направлении. В частности, в первую очередь следует наладить четкую систему контроля и аудита за использованием в работе работников тех или иных документов. Для этого используются специальные установки программного обеспечения для ограничения доступа групп пользователей к отдельным частям корпоративной сети и к документам.

Для разных работников учреждения, предприятия должны быть разные стандарты политики информационной безопасности, которые соответствуют их должностям и функциональным обязанностям.

Современные технологии делают возможным разработку и внедрение различных многоступенчатых средств контроля доступа и предотвращения утечки информации. Для ограничения доступа к информации и протоколирования фактов

осуществления несанкционированного доступа используют стандартные сервисы безопасности.

Для предотвращения несанкционированного копирования конфиденциальной информации на внешние носители используется специализированное программное обеспечение, предназначенное для контроля внешних коммуникационных портов компьютера (типа USB и т. п.). Пользователям присваиваются права доступа к контролируемым устройствам по аналогии с правами доступа к файлам.

Это лишь несколько наиболее популярных и используемых на практике систем борьбы с утратой конфиденциальной информации учреждения. В действительности их, конечно, намного больше, и выбирать нужно самому учреждению исходя из его финансовых возможностей, ценности информации и степени угрозы.

В заключение следует заметить, что ст. 27 Закона № 2657 определяет, что нарушение законодательства об информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность согласно законам Украины.