СОДЕРЖАНИЕ АДМИНИСТРАТИВНО-ПРАВОВЫХ МЕР ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ

Анфиса НАШИНЕЦ-НАУМОВА,
кандидат юридических наук, доцент кафедры правоведения
Киевского университета имени Бориса Гринченко

Summary

The article discusses the contents of legal and administrative measures to protect proprietary information. The author considers the general and special attributes to the content of the protection measures of service information. Common features are the ones that are common to all types of information with restricted access. For ladies – only those that are inherent in the main service information. Also in the study were provided by the model and the recommendation to establish a system of organized measures to protect proprietary information.

Key words: information, access information, service information, information protection.

Аннотация

В статье рассматривается содержание административно-правовых мер защиты служебной информации. К содержанию мер защиты служебной информации автор относит общие и особые признаки. Общими признаками являются те, которые свойственны всем видам информации с ограниченным доступом. К особым относятся лишь те, которые в основном присущи служебной информации. Также в процессе исследования были предоставлены модели и рекомендации по созданию системы административно-правовых мер защиты служебной информации.

Ключевые слова: информация, доступ к информации, служебная информация, защита информации.

Постановка проблемы. С распространением информационных технологий субъекты хозяйствования становятся все более зависимыми от информационных систем и услуг, а, следовательно, все более уязвимыми по отношению к угрозам безопасности. Поэтому главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, недопущение хищения финансовых средств, утечки, искажения и уничтожения служебной информации. Однако обеспечение необходимого уровня защиты информации – задача весьма сложная, требующая для своего решения создания целостной системы административно-правовых мер защиты служебной информации.

Актуальность темы исследования подтверждается степенью нераскрытости темы, поскольку в настоящее время существует вопрос определения природы понятия «служебная информация», а также определения административно-правовых мер её защиты.

Состояние исследования. Отдельные вопросы содержания административно-правовых мер защиты служебной информации исследовались в роботах Н.Т. Белухи, Ф.Ф. Бутынца, Н.И. Дороша, Е.А. Петрика, В.В. Саенко, Г.Г. Почепцова, С.П. Росторгуева, М.Я. Швеця, Б.Ф. Усача и др. Вместе с тем в научных исследованиях основное внимание уделяется анализу служебной тайны, тогда как понятие «служебная информация» надлежащим образом не исследовано, что подчеркивает важность и актуальность проблематики нашей работы.

Целью и задачей статьи является определение места и характерных особенностей содержания административно-правовых мер защиты служебной информации на основе анализа действующего законодательства.

Изложение основного материала. Анализ доктринальных источников позволяет констатировать, что определение понятия «служебная информация» не стало предметом исследования ученых, поскольку оно содержится лишь в некоторых из них. Причем в основном исследователи оперируют понятием «служебная информация» в своих исследованиях, которые были сделаны как до, так и после принятия Закона Украины «О доступе к публичной информации» [1]. Так, в словарно-энциклопедической группе предоставляется трактовка термина «служебная тайна» как обобщенное название сведений, разглашение которых запрещается действующим законодательством или обусловлено служебной необходимостью, которые стали известными и которыми пользуются в процессе и при исполнении своих служебных обязанностей должностные лица. Служебная тайна является конфиденциальной информацией, разновидностью профессиональной тайны, содержащей сведения с ограниченным доступом о деятельности государственных органов, органов местного самоуправления, предприятий, учреждений, организаций, независимо от формы собственности, а также о личности [2; 3].

Для всестороннего раскрытия понятия следует также обратиться к выделению признаков информации, составляющей служебную тайну, а именно:

1. Это конфиденциальная информация.

2. Получение, использование, распространение и хранение служебной тайны осуществляется должностными лицами, которые являются государственными и муниципальными служащими, в связи с исполнением ими служебных обязанностей в соответствии с законом.

3. Режим информации, составляющей служебную тайну, которым определяются порядок отнесения информации к служебной тайне и ее рассекречивания, порядок защиты, хранения, передачи и доступа к такой информации устанавливается специальными нормативно-правовыми актами [4, с. 776].

Анализ вышеуказанной позиции позволяет акцентировать внимание на некоторых возражениях и уточнениях. Во-первых, служебная информация может и не быть собственностью государства, так как очень часто должностные лица получают информацию,

которая является собственностью отдельных юридических или физических лиц. Например, согласно Налоговому кодексу Украины определено, что налоговая информация поступает от разных источников: налогоплательщиков и налоговых агентов, от органов исполнительной власти, органов местного самоуправления, Национального банка Украины, от банков, других финансовых учреждений, от органов власти других стран, международных организаций или нерезидентов, от подразделений налоговой службы и таможенных органов [5, с. 54].

Таким образом, налоговые органы могут получать разнообразную конфиденциальную информацию от отдельных лиц, не меняя право собственности распорядителя или владельца этой информации. Во-вторых, исследователь значительно ограничивает содержание понятия «служебная тайна», определяя, что «получение, использование, распространение и хранение служебной тайны осуществляется должностными лицами». Считаем правильным закрепление в действующем законодательстве дефиниции «служебная информация», в отличие от дефиниции «служебная тайна», как наиболее широкой категории, охватывающей любые сведения, полученные должностным лицом в связи с исполнением им служебных обязанностей, которые могут принадлежать государству или могут находиться в собственности других лиц (например, тайна завещания, тайна страхования, тайна голосования).

Как мы отмечали ранее, в действующем законодательстве отсутствует определение понятия «служебная информация». Зато в некоторых подзаконных нормативно-правовых актах дается определение служебной тайны. Например, в Постановлении правления Фонда социального страхования от несчастных случаев на производстве и профессиональных заболеваний Украины от 17 октября 2013 г. определено, что служебная тайна – это состав и объем сведений, имеющихся в распоряжении работников рабочих органов исполнительной дирекции Фонда по страхованию, необходимых для качественного проведения проверки, и которые по этой причине на определенный период не подлежат внешнему или внутреннему разглашению [6].

В проекте Закона Украины «О государственных секретах» служебная тайна рассматривается как вид информации, которая охватывает сведения в сфере внутренней и внешней политики государства, обороны, государственной безопасности и охраны правопорядка, государственного управления, экономики, финансов, банковской деятельности, науки и техники, не представляет государственную тайну, но разглашение которой может привести к негативным последствиям. Сведения, отнесенные к служебной тайне, имеют степень ограничения доступа «Для служебного пользования» [7]. Ни одно из приведенных определений не соответствует Закону Украины «О доступе к публичной информации» как по терминологии, так и для его определения. Тем более неизвестно, почему служебная тайна сводится исключительно к сведениям, которыми пользуются в процессе и в связи с выполнением своих служебных обязанностей должностные лица субъектов хозяйствования. Важной для разграничения открытой информации и служебной информации, предоставления информационного статуса служебной информации являются подготовленные Представителем Уполномоченного Верховной Рады Украины по правам человека по вопросам доступа к публичной информации и защиты персональных данных Рекомендации [8]:

1. К служебной информации в соответствии со статьей 9 Закона Украины «О доступе к публичной информации» могут быть отнесены только следующие сведения: содержащиеся в документах субъектов властных полномочий, которые составляют внутриведомственную служебную корреспонденцию, докладные записки, рекомендации, если они связаны с разработкой направления деятельности учреждения или осуществлением контрольных, надзорных функций органами государственной власти, процессом принятия решений и предшествуют публичному обсуждению и / или принятию решений; собранные в процессе оперативно-розыскной, контрразведывательной деятельности в сфере обороны страны, которая не отнесена к государственной тайне.

2. Другая информация, в том числе конфиденциальная информация о лице, не может относиться к служебной, если только она не соответствует указанным выше сведениям.

3. Если публичная информация подпадает под одно из указанных в п. 1 сведений, эта информация может быть отнесена к служебной при соблюдении совокупности следующих требований («трехсложный тест» по части второй статьи 6 Закона Украины «О доступе к публичной информации»): 1) исключительно в интересах национальной безопасности, территориальной целостности или общественного порядка с целью предотвращения беспорядков или преступлений, для охраны здоровья населения, для защиты репутации или прав других лиц, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия; 2) разглашение информации может нанести существенный вред этим интересам.

4. Публичная информация не может иметь статус служебной, если завершился процесс принятия решения по соответствующему вопросу (что подтверждается правовым актом или фактическими действиями), или проект решения вынесен на обсуждение.

5. Публичная информация, содержащаяся в правовом акте соответствующего субъекта властных полномочий, в том числе акте индивидуального действия (указ, приказ, решение, распоряжение и т.п.), может быть отнесена к служебной, только если она была собрана в процессе оперативно-розыскной, контрразведывательной деятельности, в сфере обороны страны и прошла «трехсложный тест».

6. Не может быть ограничена в доступе, в том числе путем отнесения к служебной, информация, которая была правомерно обнародована ранее распорядителем; о распоряжении бюджетными средствами, владении, пользовании или распоряжении государственным, коммунальным имуществом. В том числе копии соответствующих документов, условия получения этих средств или имущества, фамилии, имена, отчества физических лиц и наименования юридических лиц, получивших эти средства или имущество; сведения, указанные в декларации об имуществе, доходах, расходах и обязательствах финансового характера, оформленные по форме и в порядке,

которые установлены Законом Украины «О доступе к публичной информации».

7. В каждом конкретном случае при решении вопроса об отнесении публичной информации к служебной распорядитель обязательно должен обосновать следующее: 1) какому именно из интересов грозит разглашение информации (например, национальной безопасности, территориальной целостности); 2) в чем именно будет заключаться вред в случае разглашения этой информации; 3) каким образом существенный вред от обнародования такой информации превосходит общественный интерес в ее получении.

8. После определения того, что документ содержит служебную информацию, на нем проставляется гриф «Для служебного пользования», при этом должно быть определено, какая именно информация в документах является служебной – вся или только часть. Если только часть информации, содержащейся в настоящем документе, является служебной, то при запросе такого документа – несмотря на гриф «ДСП», стоящий на документе, – он предоставляется в той части, которая не является ограниченной в доступе.

9. Тот факт, что документ имеет гриф «ДСП», недостаточен для отказа в доступе к нему. В доступе к служебной информации может быть отказано только в случае прохождения «трехсложного теста» с учетом конкретной ситуации и обстоятельств дела. Письменный отказ в удовлетворении запроса со ссылкой на отнесение информации к служебной должен содержать обоснование в соответствии с применением «трехсложного теста». В случае отсутствия такого обоснования отказ следует считать неправомерным.

10. Перечень сведений, которые могут составлять служебную информацию, может состоять только из информации, упомянутой в п. 2 ч. 1 статьи 9 Закона («собранная в процессе оперативно-розыскной, контрразведывательной деятельности, в сфере обороны страны, которая не отнесена к государственной тайне»). Однако не может быть составлен исчерпывающий перечень информации, о которой говорится в п. 1 ч. 1 этой статьи («..информация, содержащаяся в документах субъектов властных полномочий, которые составляют внутриведомственную служебную корреспонденцию, докладные записки, рекомендации, если они связаны с разработкой направления деятельности учреждения или осуществлением контрольных, надзорных функций органами государственной власти, процессом принятия решений и предшествуют публичному обсуждению и / или принятию решений»). Это связано с невозможностью определить круг всех вопросов, которые могут быть подняты в служебной корреспонденции.

Принимая во внимание анализ научных позиции и нормативно-правовые акты в этой сфере, а также учитывая нормы законов Украины «Об информации» [9], «О доступе к публичной информации» и других подзаконных правовых актов, согласно которым определяется перечень сведений, составляющих служебную информацию в системе конкретного субъекта хозяйствования, считаем необходимым выделить общие и особенные признаки служебной информации. Общими признаками являются те, которые свойственны всем видам информации с ограниченным доступом, в том числе и служебной информации. Особыми – только те, что в основном присущи служебной информации [10, с. 9].

Общие признаки служебной информации – это:

– сведения, данные, которые могут быть сохранены на материальных носителях или отражены в электронном виде;

– установление ограниченного режима, предусмотренного действующим законодательством;

– особая ценность в силу неизвестности ее другим пользователям;

– за нарушение вышеуказанных мер установлена юридическая ответственность.

Особые признаки служебной информации:

– субъекты властных полномочий ее создали или получили доступ к ней исключительно на законных основаниях;

– субъекты властных полномочий ее создали или получили доступ к ней в связи с необходимостью реализации возложенных задач и функций;

– субъекты властных полномочий осуществляют в пределах своей юрисдикции необходимые меры безопасности;

– создание или получение доступа к конкретной информации ограничивается юрисдикцией конкретного субъекта властных полномочий;

– не является государственной тайной;

– диалектическая взаимосвязь с другими видами информации с ограниченным доступом и тому подобное.

Ввиду вышеизложенного защиту служебной информации можно определить как комплекс действий владельца информации, направленных на обеспечение прав на ее владение и распоряжение, а также содействие жизнедеятельности человека, общества и государства на основе создания органами управления субъектов хозяйствования безопасных условий, которые ограничивают распространение и исключают или существенно затрудняют несанкционированный, незаконный доступ к информации и ее носителям.

Административно-правовые меры защиты служебной информации – это комплекс действий и средств, направленных на создание эффективных условий для обеспечения информационной безопасности субъектов хозяйствования. В зависимости от финансовых возможностей, статуса субъекта, реализующего полномочия собственника в отношении информационных ресурсов, содержания служебной информации, этот комплекс мер может разрабатываться должностными лицами субъектов хозяйствования, которые отвечают за обеспечение информационной безопасности, или подразделениями службы информационной безопасности.

Разнообразные модели и рекомендации по созданию системы организационных мер защиты служебной информации основываются на универсальном комплексе последовательных мер:

– формирование службы информационной безопасности или назначение лица (группы лиц), ответственного за обеспечение информационной безопасности в этой структуре предприятия;

– назначение ответственных лиц в выделенных помещениях, на конкретных информационных объектах, а также в помещениях, где хранится служебная информация, в том числе на бумажных носителях;

– разработка и утверждение плана мероприятий по обеспечению ин-

формационной безопасности (годового, квартального, месячного и т.п.);

– конкретизация плана с определенной целью, задачей, местом и временем осуществления мер;

– обучение, повышение квалификации специалистов по обеспечению защиты служебной информации, контроль за уровнем их подготовки, с учётом возможности бюджетного финансирования.

Вышеуказанные планы и меры по организационному обеспечению безопасности информации, безусловно, имеют свою специфику в отношении отдельных видов информационных ресурсов и регламентируются подзаконными нормативно-правовыми актами, которые в рамках этого исследования рассматриваться не могут, ведь, как правило, имеют гриф ограниченного доступа. Однако на уровне законов установлены общие направления комплекса административно-правовых мер по обеспечению защиты служебной информации, в том числе организационных. Комплекс организационных мер обеспечения защиты служебной информации создает основу для использования технической защиты служебной информации – средств, направленных против несанкционированного доступа к этой информации, против ее искажения, блокирования, уничтожения.

Техническая защита служебной информации субъектов хозяйствования является важным фактором реализации организационно-правовых и инженерно-технических мероприятий с целью предотвращения утечки информации за счет несанкционированного доступа к ней, несанкционированных действий по воздействию на информацию, которые приводят к ее уничтожению, нарушению целостности или блокировке, а также противодействия техническим разведкам.

Следует соблюдать меры защиты во всех точках сети, при любой работе субъектов с информацией.

Правовую основу технической защиты информации в Украине составляют: Конституция Украины; законы Украины; международные договоры Украины; соглашения, обязательность выполнения которых введена Верховной Радой Украины; указы Президента Украины; постановления Кабинета Министров Украины; распоряжение администрации Государственной службы специальной связи и защиты информации Украины; другие нормативно-правовые акты по вопросам технической защиты информации. Правовую основу создания и деятельности подразделений защиты служебной информации составляют: Закон Украины «О государственной тайне»; Закон Украины «О защите информации в автоматизированных системах»; Положение о технической защите информации в Украине; Положение об обеспечении режима секретности при обработке информации, составляющей государственную тайну, в автоматизированных системах; другие нормативно-правовые акты по вопросам защиты информации; государственные и отраслевые стандарты; распорядительные и другие документы.

Подразделение защиты служебной информации осуществляет деятельность в соответствии с «Планом защиты информации», календарными, перспективными и другими планами работ, утвержденных руководством компании. Однако выполнение любых задач структурными подразделениями зависит от субъектов системы технической защиты, качества их подготовки, профессионализма, материального обеспечения и четкого взаимодействия с другими структурами компании и органами контроля.

Под субъектом в этом случае понимают пользователя системы, процесс, компьютер или программное обеспечение для обработки информации. Каждый информационный ресурс (компьютер пользователя, сервер организации или сетевое оборудование) должен быть защищен от всех возможных угроз. Государственная политика в сфере технической защиты информации формируется в соответствии с законодательством и реализуется Госспецсвязи во взаимодействии с другими субъектами системы технической защиты информации.

Целью создания подразделения защиты служебной информации является организационное обеспечение задач управления комплексной системой защиты информации (КСЗИ) на предприятии и контроль за ее функционированием. На подразделение защиты служебной информации возлагается выполнение таких работ, как определение требований по защите информации в автоматизированной информационной системе предприятия (АИС); проектирование; разработка и модернизация КСЗИ; эксплуатация; обслуживание; поддержание работоспособности КСЗИ; контроль за состоянием защищенности информации в компьютерных системах (КС).

Для проведения отдельных мероприятий защиты служебной информации в КС, связанных с направлением деятельности других подразделений компании, приказом руководства определяют перечень, сроки выполнения работ и исполнителей – подразделения или конкретных лиц. В своей работе подразделение защиты служебной информации взаимодействует с другими подразделениями компании (режимно-секретным отделом, службой безопасности, отделом деловой разведки, службы охраны и др.), а также с государственными органами, учреждениями и организациями, занимающимися вопросами защиты информации. В случае необходимости к выполнению работ могут быть привлечены внешние организации, имеющие лицензии на соответствующий вид деятельности в сфере защиты информации. В любом канале связи возникают препятствия, приводящие к искажению информации, поступающей для обработки. Для уменьшения вероятности ошибок принимаются меры по улучшению технических характеристик каналов, использованию различных видов модуляции, расширению пропускной способности и др. При этом также нужно принимать меры по защите информации от ошибок или несанкционированного доступа.

Режим защиты информации устанавливают по: сведениям, которые относятся к государственной тайне уполномоченными органами на основании действующего законодательства; конфиденциальной документированной информации владельца информационных ресурсов или уполномоченного лица на законных основаниях; персональным данным.

Основными угрозами безопасности информации являются: утечка конфиденциальной информации; компрометация информации; несанкционированное использование информационных ресурсов; ошибочное использование информационных ресурсов;

несанкционированный обмен информацией между абонентами; отказ от информации; нарушение информационного обслуживания; незаконное использование привилегий.

Утечка конфиденциальной информации – это ее бесконтрольный выход за пределы ИС через круг лиц, которым она была доверена по виду службы или стала известна в процессе работы. Эта утечка может быть следствием: разглашения конфиденциальной информации; утечки информации различными путями, преимущественно по техническим каналам; несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации, которое привело к ознакомлению с ней лиц, не допущенных к этим сведениям, можно квалифицировать как умышленные или неосторожные действия должностных лиц и пользователей, которым эти сведения были доверены в связи со служебной необходимостью. Возможна бесконтрольная утечка конфиденциальной информации визуально-оптическим, акустическим, электромагнитным и другими каналами.

Несанкционированный доступ – это противоправное умышленное овладение конфиденциальной информацией лицом, не имеющим права доступа к сведениям, которые охраняются. Наиболее распространенными направлениями несанкционированного доступа к информации являются: перехват электронных излучений; принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции; применение подслушивающих устройств (жучков); дистанционное фотографирование; перехват акустических излучений и восстановление текста принтера; считывание остаточной информации в памяти системы после выполнения санкционированных запросов; копирование носителей информации с преодолением мер защиты; маскировка под зарегистрированного пользователя; маскировка под запросы системы; использование программных ловушек; использование недостатков языков программирования и операционных систем; незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации; злонамеренный вывод из строя механизмов защиты; расшифровки специальными программами зашифрованной информации; информационные инфекции.

Перечисленные направления несанкционированного доступа требуют значительных технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Причиной возникновения каналов утечки является конструктивное и технологическое несовершенство схематических решений. Все это позволяет взломщику делать преобразования, которые действуют по определенным физическими принципами и имеют присущий этим принципам канал передачи информации – канал утечки.

Выводы. Итак, административно-правовые меры защиты служебной информации – это комплекс действий и средств, направленных на создание эффективных условий для обеспечения информационной безопасности субъектов хозяйствования. В зависимости от финансовых возможностей, статуса субъекта, реализующего полномочия собственника в отношении информационных ресурсов, содержания служебной информации этот комплекс мер может разрабатываться должностными лицами субъектов хозяйствования, которые отвечают за обеспечение информационной безопасности, или подразделениями службы информационной безопасности.

Перспективой дальнейших исследований этой проблематики является исследование государственных институтов в системе обеспечения безопасности информации на предприятиях.

Список использованной литературы:

1. Про доступ до публічної інформації : Закон України // Відомості Верховної Ради України від 13.01.2011. – № 2939-VI.

2. Юридична енциклопедія: в 6 т. / [редкол.: Ю.С. Шемшушенко (гол.ред.) та ін.]. – К. : Укр. енцикл., 1998. – Т. 5. : П-С. – 2003. – 733 с.

3. Юридичний словник-довідник / за ред. Ю.С. Шемшушенко. – К. : Феміна, 1996. –696 с.

4. Великий енциклопедичний юридичний словник / за ред. акад. НАН України Ю.С. Шемшушенко. – К.: Юридична думка, 2007. – 992 с.

5. Папаїка О.О. Податковий менеджмент : [навчальний посібник для студентів ВНЗ] / [О.О. Папаїка, В.О. Орлова, О.В. Грицак та ін.]. – Донецьк, 2012. – 361 с.

6. Про затвердження Порядку здійснення контролю за правильністю нарахування, своєчасністю і повнотою сплати страхувальниками страхових внесків на загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві, та професійного захворювання, які спричинили втрату працездатності, інших платежів до Фонду та цільовим використанням коштів № 68 від 17 жовтня 2003 р. : Постанова Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України від 17 жовтня 2003 р. № 68. [Електронний ресурс]. – Режим доступу : http://www.social.org.ua/laws/resolutions-of-fond?rstart=15.

7. Про державні секрети : Проект Закону України [Електронний ресурс]. – Режим доступу : http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=83571.

8. Роз'яснення Уповноваженого Верховної Ради України з прав людини щодо віднесення публічної інформації до службової згідно із Законом України «Про доступ до публічної інформації» [Електронний ресурс]. – Режим доступу : http://www1.ombudsman.gov.ua/index.php?option.

9. Про інформацію : Закон України // Відомості Верховної Ради України від 02.10.1992. – № 2657-XII.

10. Жмур Н.В. Правове забезпечення службової інформації в Україні : автореф. дис. … канд. юрид. наук : спец. 12.00.07 / Н.В. Жмур. – К. : НАУ. – 2015. – 20 с.