

Сергей Сергеевич ТУРБЫЛЕВ

*студент специальности «Экономическая безопасность»
Тюменского государственного университета, г. Тюмень, turbo1401@icloud.com*

Анна Алексеевна НОВОСЕЛЬЦЕВА

*студентка специальности «Экономическая безопасность»
Тюменского государственного университета, г. Тюмень, anna13102000@gmail.com*

Юлия Сергеевна САХНО

*кандидат экономических наук, доцент, доцент кафедры экономической безопасности,
системного анализа и контроля Тюменского государственного университета,
г. Тюмень, y.s.sakhno@utmn.ru*

РОЛЬ КОММЕРЧЕСКОЙ ТАЙНЫ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Аннотация. Конфиденциальные сведения, которыми владеет та или иная организация, лежат в основе коммерческой деятельности предприятия. В настоящей статье идет речь о коммерческой тайне организации, ее роли в системе экономической безопасности. Рассмотрено законодательство в сфере коммерческой тайны организации и какие меры необходимы для защиты конфиденциальной информации. Также представлен примерный перечень сведений, составляющих коммерческую тайну. В статье рассмотрены исследования о каналах утечки информации, а также сведений, которые были подвержены утечке.

Ключевые слова: коммерческая тайна, конфиденциальная информация, информационная безопасность, организация, утечка информации, экономическая безопасность.

Sergey Sergeevich TURBYLEV

*Student of the specialty "Economic Security" at the Tyumen State University,
Tyumen, turbo1401@icloud.com*

Anna Alekseevna NOVOSELTSEVA

*Student of the specialty "Economic Security" at the Tyumen State University,
Tyumen, anna13102000@gmail.com*

Yulia Sergeevna SAKHNO

*Candidate of Economic Sciences, Associate Professor of the Department of Economic Security,
System Analysis and Control, Tyumen State University, Tyumen, y.s.sakhno@utmn.ru*

TAKING MEASURES TO PREVENT DEFORMATION OF THE STRUCTURE OF THE RUSSIAN ECONOMY

Abstract. Confidential information owned by this or that organization forms the basis of the business of the enterprise. This article deals with the trade secret of the organization, its role in the system of economic security. The legislation in the field of commercial secrets of the organization and what measures are necessary to protect confidential information were considered. An approximate list of information constituting a trade secret is also presented. The article examines research on the channels of information leakage, as well as information that has been leaked.

Keywords: trade secrets, confidential information, information security, organization, information leakage, economic security.

Деятельность любой организации непосредственно связана с добычей и использованием различной информации. В современных условиях информация выступает в роли товара, имеющего высокую ценность, а также является объектом правовых отношений.

Информация может быть, как общедоступной, так и с ограниченным доступом. Для руководителей компаний некоторая информация, которая используется для достижения определенных целей, будет основным источником для получения прибыли. Утечка ценной информации угрожает как стратегическим целям, так и безопасности всей организации в целом, а именно она может нанести непоправимый ущерб деловой репутации, подорвать финансовое положение, вызвать конфликты с государственными органами. Из этого следует, что одной из важнейших экономических проблем организации является всестороннее обеспечение защиты информационных ресурсов. В аспекте экономической безопасности информационная безопасность представляет собой состояние защищенности деятельности организации и ее информационной среды от преднамеренного или случайного вмешательства, нанесшее ущерб владельцу информации [1].

При найме работников, сотрудники службы экономической безопасности совместно с сотрудниками информационной безопасности должны зафиксировать в договоре формы и размеры его личной ответственности за сохранность коммерческой тайны, указать на его конкретные обязательства по защите коммерческой тайны, запретить ее использование в ущерб предприятию, определить условия расторжения договора, если какие-либо требования конфиденциальности не соблюдены.

Коммерческой тайной может выступать различная информация: производственная, техническая, экономическая, организационная и так далее [2]. Также ей могут являться результаты интеллектуальной деятельности в научно-технической сфере или информация о способах осуществления профессиональной деятельности, которые имеют актуальное значение, или потенциальную коммерческую ценность, в связи с неизвестностью данной информации третьим лицам, и к которой они не имеют свободного доступа на законных основаниях. В отношении такой информации, владелец вводит режим коммерческой тайны.

Согласно Федеральному закону № 98-ФЗ «О коммерческой тайне», обладатель коммерческой тайны — это лицо, владеющее теми сведениями, которые составляют коммерческую тайну. Доступ к таким сведениям ограничен на законных основаниях, а также в отношении этих сведений установлен режим коммерческой тайны [2]. Законодательством упорядочены меры для охраны конфиденциальности информации, то есть режим коммерческой тайны считается установленным после принятия специальных мер, предусмотренных статьей 10 Федерального закона № 98-ФЗ «О коммерческой тайне».

Путем установления в организации режима коммерческой тайны осуществляется правовая защита информации. Данный режим подразумевает собой правовые средства, которые характеризуют систему запретов, разрешений, рекомендаций, определенных обязательств и санкций, а также иные организационные, технические и другие меры, принимаемые для обеспечения защиты такой информации.

Определенного перечня объектов, подлежащих защите коммерческой тайной, в действующем законодательстве не существует, его определение невозможно по причине того, что субъекты данных правоотношений многообразны и далеко не универсальны.

Каждая организация обладает определенным перечнем информации, который является конфиденциальным, то есть не подлежит разглашению. Состав такого перечня информации определяется руководством, а именно руководителем организации. Варианты такого перечня информации зависят от различных аспектов деятельности компании.

Далее рассмотрена информация, которая может являться коммерческой тайной организации:

- данные о производстве, которые характеризуются сведениями о структуре и масштабах производства, размещением оборудования, производственными мощностями, запасами сырья/материалов/комплектующих/готовой продукции (например, структура кадров и производства, условия производства, сведения о типе и размещении оборудования и т. д.);

- данные о применяемых оригинальных способах управления организацией, сведениями о подготовке, принятии и исполнении отдельных решений руководства предприятия по коммерческим и другим вопросам;

- данные о планах расширения или свертывания производства различных видов продукции (работ, услуг), сведения о планах инвестиций, закупок и продаж;

- данные о финансовой составляющей, а именно об оборачиваемости средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредитов организации (например, сведения о бюджете, оборотах, банковских операциях и т. д.);

- данные, которые включают в себя сведения о результатах сегментации рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры, об эффективности служебной или коммерческой деятельности фирмы (например, результаты маркетинговых исследований, рыночная стратегия предприятий, коммерческие замыслы организации и т. д.);

- данные о контрагентах и других партнерах (например, списки клиентуры, негласные компаньоны товарищества, коммерческие связи, места закупки товаров и т. д.);

- данные об условиях контрактов организации с контрагентами (например, условия по совершенным сделкам или соглашениям, условия договоров, включающие цены, скидки, отсрочки платежей и т. п.);

- данные о применяемых и перспективных технологиях, технологических процессах, приемах и оборудовании;

- данные о безопасности организации, а именно о порядке защиты конфиденциальной информации, коммерческой тайны, системы сигнализации, а также пропускном режиме.

Согласно проведенным исследованиям в 2020 г., основными каналами утечки информации являются: почта (47%), устройства хранения и мобильные (43%), мессенджеры (32%), облачные хранения (15%), документы, отправляемые на печать (19%), другое (11%) [3].

На рисунке 1 представлено наглядное процентное распределение основных каналов утечки конфиденциальной информации в организации в 2020 г.

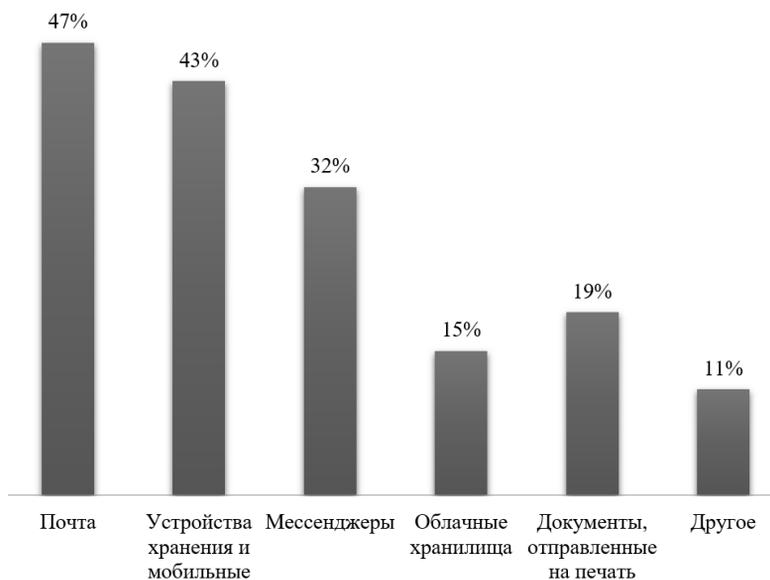


Рис. 1. Основные каналы утечек конфиденциальной информации в 2020 г.

Источник: [3, с. 11].

Почта и устройства хранения являются наиболее вероятными каналами утечки данных. Организации стараются контролировать с помощью технических средств. Обычно этого достаточно, но в условиях дистанционной работы в связи с эпидемией Covid-19 сильно изменила ситуацию. Стало гораздо проще выносить информацию «за периметр», тем более в условиях удаленной работы она уже за его пределами. В этой связи сейчас возрастает актуальность защиты облачных хранилищ через такие инструменты как, например, TeamViewer, AnyDesk или TightVNC.

Утечка конфиденциальной информации зависит от нескольких факторов, которые оказывают наиболее сильное влияние.

Во-первых, это ошибки персонала организации, которые могут быть вызваны непониманием необходимости выполнения мер по предотвращению утечки конфиденциальных сведений, а также несоблюдением пунктов договора о соблюдении режима коммерческой тайны.

Во-вторых, возможны обстоятельства, при которых утечка коммерческой тайны происходит в результате сознательных действий персонала (например, мотивированные взяткой и др.).

В исследованиях за 2020 г. была выявлена информация, которая повержена утечке. На рисунке 2 также представлена информация о процентном распределении информации, подверженной утечке, которую удалось зафиксировать организациями.

В 2020 г. впервые выяснили, как компании обнаруживают инциденты. Из графика видно, что большинство инцидентов выявляется техническими автоматизированными средствами, а также технически вручную. На рисунке 3 в процентном соотношении наглядно показаны способы выявления утечки информации в организациях в 2020 г.

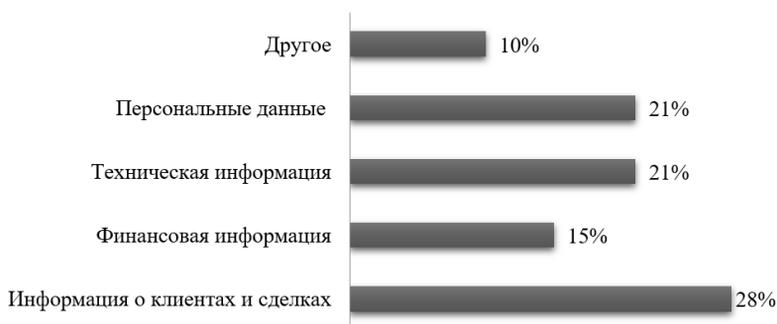


Рис. 2. Информация, которая была подвержена утечке в 2020 г.

Источник: [3, с. 11].



Рис. 3. Способы выявления утечки информации организации в 2020 г.

Источник: [3, с. 12].

Технические меры по защите конфиденциальной информации позволяют в полной мере защитить от утечки информации и несанкционированной передачи данных. В общем оснащенность персональных компьютеров организации остается средней и в достаточной мере отличается по отраслям.

Надлежащая защита конфиденциальной информации влияет на результаты деятельности всей системы экономической безопасности организации. Стабильность производственного цикла, прибыльность коммерческой деятельности, а также эффективное управление персоналом — это является результатами обеспечения экономической безопасности. Основными звеньями являются персонал, материальные и информационные ресурсы. Из этого следует, что обеспечение экономической безопасности включает в себя следующие функциональные направления:

- защиту материальных ценностей организации;
- защиту интеллектуальной собственности организации;
- эффективное управление сотрудниками организации;
- защиту информации.

Необходимость всеобъемлющего поддержания режима коммерческой тайны обусловлено его высокой ролью в системе обеспечения экономической безопасности всей организации, так как рассекречивание конфиденциальной информации в последствии наносит непоправимый ущерб, и приводит к серьезным экономическим последствиям.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гомалеев А.О. Информационная безопасность как составляющая экономической безопасности организации // Научно-практический электронный журнал Аллея Науки. Калуга. 2018. №10 (26). URL: https://alley-science.ru/informacionnye_i_kommunikativnye_tehnologii__10__26__2018/ (дата обращения: 25.10.2021).
2. О коммерческой тайне: Федеральный закон от 29.07.2004 № 98-ФЗ // Консультант-Плюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 25.10.2021).
3. Исследование уровня информационной безопасности в компаниях России и СНГ за 2020 г. // ООО «СёрчИнформ». 2021. 42 с.