**УДК 334.722.1**

**ОРГАНИЗАЦИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ**

**Иванник А.С.**

Студент (магистрант)

Сургутский государственный университет,

Россия, г. Сургут

Аннотация: в статье рассматривается важность защиты на предприятии информации, носящей конфиденциальный характер, а также персональных данных сотрудников. Актуальность выбранной темы обусловлена тем, что разглашение коммерческой тайны является прямой угрозой финансовому состоянию и имиджу предприятия. В связи с этим, автором рассмотрены способы разрешения данной проблемы, основным из которых является введение режима коммерческой тайны на предприятии.

Ключевые слова: информация, коммерческая тайна, персональные данные, экономическая безопасность, информационная безопасность.

Annotation: the article discusses the importance of protecting confidential information at the enterprise, as well as personal data of employees. The relevance of the chosen topic is due to the fact that the disclosure of trade secrets is a direct threat to the financial condition and image of the enterprise. In this regard, the author considers ways to solve this problem, the main of which is the introduction of a trade secret regime in the enterprise.

Keywords: information, trade secrets, personal data, economic security, information security.

В современном мире немалая часть успеха производственно-хозяйственной деятельности зависит от умения правильно распоряжаться таким ценнейшим ресурсом, как информация, и выгодно использовать лишь ту информацию, которая требуется рынку, но неизвестна ему. Именно поэтому в условиях жесткой конкуренции успех компании, гарантия прибыльности в большей степени зависят от сохранения тайн производства, которые опираются на конкретный интеллектуальный потенциал и определенную технологию. В связи с этим, на руководство предприятия возложена задача по обеспечению защиты информации на всех уровнях управления.

Нормативно-правовую базу по защите информации предприятия составляет ряд документов: Конституция РФ, Гражданский кодекс РФ федеральные конституционные законы, ФЗ «О коммерческой тайне», ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ «О рынке ценных бумаг», ФЗ «О связи» и другие.

Стоит отметить, что защите подлежит только та информация, которая представляет ценность для предпринимателя. Ценность определяется такими критериями, как полезность, своевременность и достоверность поступивших сведений. Наибольшую ценность составляют коммерческая тайна и персональные данные, так как чаще всего конкурирующих фирм интересуют данные о клиентах и сделках, бизнес-план, персональные данные сотрудников, секретные разработки и технологии, а также информация о нарушениях.

В соответствии с ФЗ «О коммерческой тайне», термин «коммерческая тайна» трактуется как режим конфиденциальности информации, который позволяет ее обладателю при определенных обстоятельствах получить коммерческую выгоду [1]. Сведения, составляющие коммерческую тайну, проиллюстрированы на рисунке 1.



Рисунок 1. Сведения, составляющие коммерческую тайну

В соответствии с ФЗ «О персональных данных», под «персональными данными» следует понимать любую информацию, которая прямо или косвенно относится к субъекту персональных данных (определенному или определяемому физическому лицу) [2]. К ней относятся следующие сведения:

* фамилия, имя, отчество;
* год, месяц, дата и место рождения;
* адрес места регистрации и проживания;
* семейное, социальное, имущественное положение;
* образование, профессия, доходы;
* паспортные данные;
* и т.п..

Следует отметить, что в России к осени 2020 года зафиксировано 302 утечки информации ограниченного доступа, что на 5,6% больше, чем в период с января по сентябрь 2019 года. Количество «утекших» записей персональных данных и платёжной информации при этом сократилось на 29,2%. На данную статистику оказала большое влияние пандемия COVID-19. В результате быстрой перестройки бизнес-процессов и перевода существенной доли сотрудников на удаленную работу контроль над информационными активами во многих фирмах мог быть снижен, а доля зафиксированных инцидентов сократилась.

Угрозы сохранности важной информации могут быть внешними и внутренними. Наиболее распространенные виды атак проиллюстрированы на рисунке 2.



Рисунок 2. Виды атак

Таким образом, существует множество способов получения конфиденциальной информации дистанционно. Помимо перечисленных способов получения информации, действия преступников по захвату информации могут осуществляться «извне», то есть направленны на пассивные носители важной информации, например, попытки похищения документов или снятия копий с документов, съемных носителей, уничтожение или повреждение носителей информации; случайная или преднамеренная передача данных конкурентам, содержащих коммерческую тайну. [5] А также действия преступников по захвату информации, направленные на персонал организации, например, подкуп сотрудника, предъявление угроз, шантажа, выведывания информации, составляющей коммерческую тайну, или переманивание ведущих специалистов на конкурирующую фирму и другое.

Из этого следует, в целях обеспечения и поддержания высокого уровня экономической безопасности предприятия в целом, его руководству необходимо принять ряд определенных мер, регулирующих информационную безопасность. Одной из основных мер является введение режима коммерческой тайны на предприятии, выраженной в разработке и утверждении внутреннего Положения организации «О защите коммерческой тайны». [3] В данном документе должны быть закреплены следующие сведения:

* общие положения;
* сущность понятий, используемых в документе;
* полномочия руководства фирмы в части обеспечения сохранности коммерческой тайны;
* перечень сведений, составляющих коммерческую тайну;
* порядок отнесения той или иной информации к коммерческой тайне;
* перечень обязанностей сотрудников по обеспечению сохранности коммерческой тайны;
* порядок доступа тех или иных лиц к коммерческой тайне;
* механизмы защиты коммерческой тайны, действующие на предприятии;
* механизмы ответственности сотрудников за нарушение обязательств, предусмотренных положением.

Помимо вышеперечисленного, следует ввести правила хранения важных сведений. Так, к примеру, информацию конфиденциального характера, содержащуюся на материальных носителях, необходимо хранить в сейфе; также у каждого сотрудника должен быть свой логин и пароль для индивидуального пользования персональным компьютером и локальной сетью [4].

Мы выделили следующие этапы организации эффективной защиты конфиденциальной информации на предприятии:

I этап: предварительный (период, предшествующий приему сотрудника на работу)

На данном этапе разрабатывается ряд требований к кандидату на предполагаемую должность. Если поиск кандидата не осуществлялся одним из надежных способов, например, обращением в службы занятости, рассмотрением кандидатов среди студентов или по рекомендациям фирм-партнеров и доверенных сотрудников фирмы, тогда необходимо при подборе кандидата сделать запрос на предыдущее место работы в целях получения характеристики сотрудника. Когда сведения о кандидате изучены, с ним проводит собеседование кадровая служба организации. Если кандидат успешно прошел вышеперечисленные этапы, организация с ним заключает трудовой договор, содержащий пункт об обязанности сотрудника не разглашать конфиденциальную информацию и соблюдать меры безопасности, а также договор о неразглашении коммерческой тайны.

II этап: текущий (в период работы сотрудника)

На данном этапе необходимо определить персональную ответственность сотрудника, которая заключается в том, что работник должен нести ответственность за сохранность доверенных ему документов и за свои действия в информационных системах; разграничить порядок доступа сотрудника к данным автоматизированных систем различного уровня и назначения; ограничить доступ персонала в зоны предприятия, где проводятся работы конфиденциального характера.

III этап: заключительный (при расторжении трудового договора с сотрудником)

При расторжении трудового договора с работником, который был допущен к секретной информации, изначально нужно провести ее ревизию. При возможности необходимо сменить коды и пароли доступа, ключи к хранилищам конфиденциальной информации. Также в обязательном порядке убедиться, что сотрудник сдал все источники, которые находили у него, носящие коммерческую тайну, это могут быть в первую очередь документы, компьютерные программы, чертежи и другое. [6]

 Также в период увольнения сотрудника необходимо его предупредить о последствиях распространения им важной информации, получить от него расписку с ознакомлением со статьей 1470 Гражданского кодекса РФ «Служебный секрет производства». В соответствии с данной статьей работник, которому известна конфиденциальная информация, обязан не разглашать ее, пока конфиденциальность не будет снята (ограничений по срокам закон не устанавливает). В случае, если работник отказывается какие-либо документы при увольнении, в силу статьи 1470 Гражданского кодекса он обязан соблюдать режим коммерческой тайны.

Данные меры позволят обезопасить организацию от утечки информации конфиденциального характера, а также дадут возможность взыскать убытки, которые могут возникнуть в результате разглашения информации в судебном порядке.

В заключении вспомним всеми известную фразу «кто владеет информацией, тот владеет миром», если же организация разработает комплексный подход к защите конфиденциальной информации, который предотвратит владение секретными сведениями посторонними лицами, то будет достигнут необходимый уровень информационной безопасности и экономической безопасности предприятия в целом, способствующий успешному развитию фирмы.

Список литературы

1. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» // «Российская газета» от 5 августа 2004 г.

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» // «Российская газета» от 29 июля 2006 г.

3. Абросимова А.В. Коммерческая тайна как особая разновидность интеллектуальной собственности // Российское правоведение: Трибуна молодого ученого: Сборник статей. - Томск: Изд-во Томск. гос. ун-та, 2014, Вып. 9. - 64-65 с.

4. Варламова А.Н. Северин В.А. Коммерческая тайна в России. - М.: ЗЕРЦАЛО-М, 2014. - 615 с. // Вестник Московского университета. - М.: Изд-во Моск. ун-та, 2014, № 3. - 118-120 с.

5. Пресняков М. Социально-трудовые гарантии работника в связи с допуском к сведениям, составляющим коммерческую тайну // Право и экономика. - М.: Юрид. Дом "Юстицинформ", 2012, № 1. - 69-73 с.

6. Ханкевич А.Г. Особенности формирования и использования режима коммерческой тайны // Информационное право. - М.: Юрист, 2014, № 1 (16). -26-31 с.