Доклад

Защита государственной и коммерческой тайны.

Сунгурова Мариян Мухсиновна

Содержание

1 Введение **5**

2 Коммерческая тайна **6**
2.1 Меры по обеспечению защиты коммерческой тайны 6
2.1.1 Внутренние меры 7
2.1.2 Внешние меры 7
2.1.3 Правовые меры 8
2.1.4 Организационные меры 8
2.1.5 Технические меры 8
2.1.6 Психологические меры 10

3 Государственная тайна **11**
3.1 Организация защиты государственной тайны 11

4 Заключение **15**

Список литературы **16**

Список иллюстраций

Список таблиц

1 Введение

Государственная безопасность - система гарантий государства от угроз извне и основам конституционного строя внутри страны. Для реализации этих гарантий в стране создана и функционирует система защищаемых законом тайн. Тайна - это, прежде всего, сведения, информация. Признаки тайны:

- сведения должны быть известны или доверены узкому кругу лиц;
- сведения не подлежат разглашению (огласке);
- разглашение сведений (информации) может повлечь наступление негативных последствий (материальный или моральный ущерб ее собственнику, владельцу, пользователю или иному лицу);
- на лицах, которым доверена информация, не подлежащая оглашению, лежит правовая обязанность ее хранить;
- за разглашение этих сведений устанавливается законом юридическая ответственность.

2 Коммерческая тайна

В настоящее время сущность и правовая природа понятия коммерческая тайна определяются федеральным законом РФ «О коммерческой тайне» № 98-ФЗ, который был принят 29.07.2004 (последняя редакция 18.04.2018). В нем разграничиваются такие понятия, как «коммерческая тайна» и «информация, составляющая коммерческую тайну».

В п.2 ст.3 он определяет «информацию, составляющую коммерческую тайну», как «сведения любого характера, в т.ч. о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны»

В п.1 ст.3 «коммерческая тайна» определяется как «режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду». [1]

2.1 Меры по обеспечению защиты коммерческой тайны

Меры по обеспечению защиты коммерческой тайны условно можно разделить на внешние и внутренние. Среди них можно выделить правовые, организацион-

ные, технические и психологические[2]

2.1.1 Внутренние меры

Действие внутренних мер по обеспечению конфиденциальности в основном направлено на рабочий персонал предприятия. Работники, имеющие доступ к сведениям, составляющим коммерческую тайну, обязуются:

- сохранять КТ, которая известна по работе, и не разглашать ее без разрешения, при условии, что сведения КТ, не были известны им ранее и не были получены ими от третьего лица без обязательства соблюдать конфиденциальность;
- выполнять требования инструкций, положений, приказов по обеспечению сохранности КТ;
- сохранять КТ деловых партнеров;
- не использовать КТ для занятия деятельностью, которая в качестве конкурентных действий может нанести ущерб предприятию/работодателю;
- в случае увольнения передать все носители информации, составляющей КТ

2.1.2 Внешние меры

Внешние меры по обеспечению сохранности коммерческой тайны необходимы при осуществлении торгово-экономических, научно-технических, валютно-финансовых и иных деловых связей с партнерами. Для этого в договоре специально должны быть оговорены характер и состав сведений, составляющих КТ, а также взаимные обязательства по обеспечению её сохранности в соответствии с действующим законодательством.

2.1.3 Правовые меры

Правовые меры обеспечения сохранности КТ являются первоочередными (первичными), т.к. призваны обеспечить эффективное функционирование остальных мер.

Первый шаг по реализации правовых мер – принятие Положения по обеспечению сохранности КТ, в котором определяются:

- состав и объем сведений КТ;
- порядок присвоения грифа «Секрет предприятия» и порядок его снятия;
- процедура допуска сотрудников;
- порядок применения предусмотренных законодательством мер дисциплинарного и материального воздействия на работников, разгласивших КТ;
- возложение ответственности за обеспечение сохранности КТ на должностное лицо предприятия.

2.1.4 Организационные меры

Организационные меры защиты КТ включают в себя:

- создание специальных подразделений (например, службы безопасности)
- организация конфиденциального делопроизводства
- разработка системы допуска к информации
- назначение ответственного за обеспечение конфиденциальности

2.1.5 Технические меры

Технические меры по обеспечению защиты коммерческой тайны

- выявление возможных источников утечки информации
- приобретение и монтаж специализированной аппаратуры и назначение ПП для защиты информации (ПП — это внутренние сотрудники и сторонние специалисты, которые имеют расширенные полномочия для работы с корпоративными ресурсами и приложениями, в частности для их установки, настройки, аудита и обслуживания.)
- проведение регулярных оперативных мероприятий по технической защите и поиску каналов утечки информации

Техническая защита коммерческой тайны строится на основе таких принципов:

- Ограничение доступа к системе (только определенным сотрудникам).
- Назначение ролей (доступ специалистов только к необходимой для работы информации).
- Обеспечение каждого пользовательского аккаунта уникальным логином и паролем с высокой надежностью.

Также способы защиты коммерческой тайны включают доступ к системе только с определенных IP-адресов. Это дополнительная мера безопасности, которая дополняет уже установленные права пользователей, пароли и, при необходимости, двухфакторную аутентификацию.

Дополнительную защиту коммерческой тайны на предприятии может обеспечить внедрение DLP-системы (Data Loss Prevention)(например Solar Dozor.) Эти программные комплексы обеспечивают мониторинг, анализ событий и, при необходимости, блокировку пользователей в случае нарушения политики безопасности. DLP-системы решают несколько важных задач в контексте защиты конфиденциальных данных:

- полный контроль информации на 3 ключевых стадиях: пользование, передача, хранение.

- мониторинг коммуникаций сотрудников на рабочих устройствах, включая электронную почту, мессенджеры, социальные сети и внешние ресурсы.
- фильтрация и анализ трафика для выявления ценной информации, предотвращения ее утечки и раннего обнаружения угроз.
- захват трафика с помощью снифферов (это программы, способные перехватывать и анализировать сетевой трафик) на шлюзе или рабочем компьютере.
- мониторинг корпоративной сети, чтобы выявить новые узлы и сервисы.
- контроль действий персонала в рабочее время: контроль копирования, передачи информации, а также печати документов.

2.1.6 Психологические меры

Психологические меры защиты КТ

- проведение разъяснительной работы с персоналом
- создание благоприятной атмосферы в коллективе
- проведение регулярных проверок (гласных и негласных)

3 Государственная тайна

Государственная тайна — это информация, разглашение или несанкционированный доступ к которой может причинить ущерб государству. Однако, информация, которая может причинить ущерб безопасности другого государства, не является информацией, составляющей государственную тайну.

Государство защищает данные в таких областях как: военная, внешнеполитическая, экономическая, разведывательная, контрразведывательная и оперативно-розыскная. Полный список того, какие данные можно засекретить указаны в специальном перечне сведений, которые относятся к государственной тайне. Помимо привычных носителей информации, вроде бумажных документов и виртуальных файлов, носителем признается и человек, обладающий секретными данными.

3.1 Организация защиты государственной тайны

Согласно ст. 20 Закона “О государственной тайне” органы государственной власти, предприятия, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции.

Организация работ по защите государственной тайны на предприятиях осуществляется их руководителями. В зависимости от объема работ руководителем предприятия создается структурное подразделение по защите государственной тайны либо назначаются штатные специалисты по этим вопросам.

Общие требования по организации и проведению работ по защите государственной тайны устанавливаются в Инструкции, утверждаемой Правительством РФ.

Для защиты информации государственной тайны обычно применяются комбинированные способы защиты, которые включают технические средства, программные средства, организационные мероприятия и криптографию.

К организационным мероприятиям можно отнести пропускной режим, хранение устройств и носителей в сейфе, ограничение доступа посторонних лиц в компьютерные помещения и другие методы защиты информации государственной тайны.

Технические средства по защите информации государственной тайны включают в себя множество аппаратных способов защиты:

- экраны на аппаратуру;
- фильтры;
- ключи для блокировки клавиатуры;
- установка устройств аутентификации – для чтения форм руки, отпечатков пальцев, радужной оболочки глаз;
- электронные ключи на микросхемах.

К программным средствам защиты информации государственной относятся такие средства, которые создаются в результате разработки специального программного обеспечения, что не позволяет посторонним лицам получать информацию из системы. К программным средствам относятся:

- блокировка клавиатуры и экрана;
- парольный доступ-задание;
- применение средств парольной защиты BIOS на персональный компьютер.

Криптографическими средствами защиты информации государственной тайны является применение шифрования при вводе в компьютерную систему.

Противостоять угрозам информационной безопасности можно на основе формирования и внедрения эффективных систем защиты информации государственной тайны. Особое место занимают правовые меры.

В статье 8 Закона Российской Федерации «О государственной тайне» говорится о трех степенях секретности сведений, которые находятся в режиме государственной тайны, а также соответствующих грифах секретности – секретно, совершенно секретно, особой важности. Присвоение грифа секретности регламентировано Правилами отнесения сведений, которые составляют государственную тайну, утвержденные Постановлением № 870 Правительства РФ.

Допуск граждан РФ и должностных лиц к государственной тайне реализуется в добровольном порядке. Данный допуск предусматривает:

- принятие обязательств на себя перед государством по нераспространению тех сведений, что составляют государственную тайну и что доверены им;
- согласие на временные, частичные ограничения их прав в соответствии с Федеральным законом РФ «О государственной тайне»;
- письменное согласие граждан и должностных лиц на проведение проверочных мероприятий уполномоченными органами;
- определение размеров, видов и порядка предоставления социальных гарантий, которые предусмотрены ФЗ «О государственной тайне»;
- ознакомление с законодательными нормами РФ, которые предусматривают ответственность за его нарушения в сфере государственной тайны;
- принятие решения руководителем предприятия, органа государственной власти, организации или учреждения о допуске оформляемого гражданина к тем сведениям, которые составляют государственную тайну.

Согласно статье 13.13 Кодекса РФ об административных правонарушениях занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществ-

лением мероприятий или оказанием услуг по защите информации, составляющей государственную тайну, без лицензии - должностное лицо получит штраф в размере от 4 тыс. до 5 тыс. рублей, юридическое лицо — от 30 тыс. до 40 тыс. рублей. Также у нарушителей конфискуют средства защиты информации при их наличии.

Закон «О государственной тайне» предусматривает и уголовную ответственность, прописанную в четырех статьях УК РФ:

- Статья 275. Государственная измена. За разглашение иностранному государству либо организации государственной тайны, а также за оказание финансовой, материально-технической, консультационной помощи подсудимый получит наказание в виде лишения свободы от 12 до 20 лет и штраф в размере 500 тыс. рублей.
- Статья 276. Шпионаж. Сбор, передача, кража или хранение гостайны в целях ее передачи иностранному государству или организации, а также передача и сбор информации по заданию иностранной разведки карается законом лишением свободы на срок от 10 до 20 лет.
- Статья 283. Разглашение государственной тайны. За разглашение сведений, составляющих государственную тайну, гражданин может быть арестован на срок от 4 месяцев до 4 лет. Если содеянное привело к тяжким последствиям, наказание может составить от 3 до 7 лет лишения свободы.
- Статья 284. Утрата документов, содержащих государственную тайну. Это нарушение может грозить нарушителю арестом от 4 до 6 месяцев, либо лишением свободы до 3 лет с лишением права заниматься определенным видом деятельности.

4 Заключение

Были исследованы вопросы защиты государственной и коммерческой тайны. Основные выводы:

- предприятия могут хранить коммерческие тайны и привлекать к ответственности виновных в их разглашении, при условии наличия документально утвержденного режима коммерческой тайны: что к ней относится, кому она доступна, как передавать документы с тайной.
- Государственая тайна РФ имеет повышенную важность, ее разглашение недопустимо и карается по всей строгости закона. Подавляющая часть сведений имеет засекреченную форму и жестко ограниченный доступ. Тем не менее утечки такого рода информации вероятны, и поэтому должен проводиться регулярный мониторинг доступа и обращения с ней для пресечения любых попыток ее утечки.

Список литературы

1. Н. С. Кармановский С.Л.С.-Н. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ОХРАНЫ СЛУЖЕБНОЙ ТАЙНЫ НА ПРЕДПРИЯТИИ. Университет ИТМО, 2018. 69 с.
2. КРУТИН Ю.В. ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ КОНСПЕКТ ЛЕКЦИЙ. 2020. 30 с.