

**МЕХАНИЗМ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ КАК
ОДНОЙ ИЗ СОСТАВЛЯЮЩИХ ЭКОНОМИЧЕСКОЙ
БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**Андреева А.Ю., студентка 1 курса магистратуры факультета
Программной инженерии и компьютерной техники
Карягина В.С., студентка 5 курса специалитета Института Экономики
Научный руководитель – Зелинская Г.А., доцент кафедры
«Экономическая безопасность» ФГБОУ ВО «АГТУ»
ФГАОУ ВО «НИУ ИТМО», ФГБОУ ВО «АГТУ»**

Ключевые слова: экономическая безопасность, коммерческая тайна, информационные технологии, DLP-системы, SIEM-системы.

В данной работе исследуется обеспечение экономической безопасности организации путем внедрения в ее деятельность информационных технологий. Особое внимание будет уделено коммерческой тайне как одной из важнейших составляющих экономической безопасности. Данное исследование проводится в рамках разработки механизма обеспечения экономической безопасности организации и его практического применения.

На протяжении последних десятилетий одним из самых дорогих активов не только для организаций, но и в целом для человека, является приобретающая все большую значимость информация. Обладающий информацией человек способен грамотно принимать решения, уменьшается вероятность ошибки. В современном мире для эффективного обеспечения экономической безопасности каждой организации необходим грамотно разработанный механизм обеспечения экономической безопасности, который был бы способен предусматривать все текущие изменения в сфере информационных технологий, так как за последние несколько лет все активнее развивается цифровая экономика. В связи с этим необходимо изучение

экономической безопасности в непосредственной зависимости от информационных технологий.

Рассматривая определение безопасности через понятие «угроза», можно сделать вывод, что это понятие охватывает комплекс определенных действий, условий и факторов, опасных для какого-либо объекта в заданный промежуток времени [1].

Одной из главных угроз экономической безопасности, непосредственно связанных с применением информационных технологий, является сохранение не только коммерческих, но и государственных тайн.

В условиях цифровизации большинство жизненных процессов всех организаций и сфер деятельности в определенный период времени связано с коммерческой тайной, в этой связи в данном исследовании ей уделено особое внимание.

Федеральный закон «О коммерческой тайне» [2] определяет коммерческую тайну как «конфиденциальную информацию, позволяющую ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

Так как на текущий момент большая часть всех организаций существует в прямой зависимости от информационных технологий, необходимо обеспечение защиты и сохранности данных, проведение мероприятий для экономической безопасности.

Использование программ, которые во всех аспектах позволяют в полной мере защитить информацию от несанкционированного копирования, утечек или передачи данных составляет одну из главных технических мер защиты коммерческой тайны. К такому программному обеспечению относятся DLP-системы и SIEM-системы.

DLP (Data Leak Prevention) система является программным обеспечением, созданным для отслеживания и блокировки попыток неразрешенной администратором передачи данных из корпоративной сети. С помощью данной системы можно отследить практически все действия пользователя: сообщения в чатах, соцсетях, почтовые отправления, произвести их запись и анализ. В каждой организации существует своя

политика конфиденциальности. Так вот, защите этой политики и служат DLP-системы.

Используют DLP-системы настоящее время в основном те организации, в которых утечка информации может нанести непоправимый репутационный или финансовый ущерб, а также предприятия, где приоритетом является лояльность сотрудников [3]. DLP-системы обеспечивают защиту такой конфиденциальной информации, как например, заказы на услуги и решения, номера пластиковых карт, условия тендеров, сведения о счетах клиентов, финансовые данные, персональные данные сотрудников, клиентов и т.д.

SIEM (Security Information and Event Management) системы – программное обеспечение, которое предназначено для управления событиями, полученными из различных источников и эффективного управления информационной безопасностью в целом. В режиме реального времени SIEM-системы анализируют события, поступающие от сетевых приложений и устройств различного типа.

Основными задачами SIEM-систем являются [4]:

1. Объединение и защита от внешних проникновений в журналы событий из различных источников (приложений, сетевых устройств, средств защиты, журналов операционных систем).
2. Возможность проведения исследования и анализа событий администратором.
3. Предоставление инструментов и оповещений при работе с чрезвычайными ситуациями для управления ими.
4. Проведение корреляции и обработка данных в соответствии с политикой деятельности и правилами, заданными администратором.

Благодаря SIEM системе организациям предоставляется возможность автоматического выявления различных угроз. Эффективное внедрение данной системы обеспечивает вывод информационной безопасности на совершенно иной уровень организации своей деятельности. SIEM система акцентируется только на важных и критических угрозах, взаимодействует с последствиями, а не с событиями, выявляет риски и помехи, способствует предотвращению финансовых потерь и повышает безопасность управления деятельностью организации в целом [4].

Среди дополнительных мер по защите от несанкционированного доступа и сохранению коммерческой тайны в организациях можно рассмотреть создание каналов связи с дополнительной степенью защиты от внешних угроз, при этом сотрудники, имеющие доступ к персональной или конфиденциальной информации, должны пользоваться только такими каналами для передачи информации.

Еще одной дополнительной мерой является создание корпоративного сервера с выделением индивидуального корпоративного адреса электронной почты для каждого сотрудника, и использование в работе только данного почтового адреса.

Таким образом, проблемы финансовой и информационной защищенности организаций очень актуальны в настоящее время. Сохранение конфиденциальности – забота предприятий всех уровней организации экономики. И для того, чтобы предотвратить, минимизировать или полностью снять потери от внешних угроз, необходимо использовать современные информационные технологии, так как экономическая безопасность во многом зависит от информационной безопасности.

Библиографический список:

1.Криворотов, В.В. Экономическая безопасность государства и регионов: учеб. пособие/ А.В. Калина, Н.Д. Эриашвили. - М.:ЮНИТИ-ДАНА, 2015. - 351 с.

2.Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 05.04.2021)

3.Гречанная А.Ю., Тастенов А.Д. DLP-системы и их роль в защите от утечек конфиденциальной информации // Научный журнал Наука и техника Казахстана. - Павлодарский государственный университет имени С. Торайгырова, 2015. - С. 23-27

4.Быков А.А. Siem система - универсальный инструмент службы информационной безопасности // Научно-практический журнал Современные инновации. - Олимп, 2017. №6 (2) - С. 46-48

THE MECHANISM OF PROTECTION OF COMMERCIAL SECRETS AS ONE OF THE COMPONENTS OF ECONOMIC SECURITY THROUGH THE USE OF INFORMATION TECHNOLOGIES

Andreeva A.U., Karyagina V.S.

Key words: *economic security, trade secrets, information technology, DLP systems, SIEM systems.*

This paper examines ensuring the economic security of an organization by introducing information technologies into its activities. Particular attention will be paid to trade secrets as one of the most important components of economic security. This study is carried out as part of the development of a mechanism for ensuring the economic security of an organization and its practical application.