УДК 657

# К ВОПРОСУ О СОЗДАНИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Афанасьева С.Г., студент гр.ЭУб-161, IV курс
Научный руководитель: Тюленева Т.А., к.э.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Информация на протяжении последних десятилетий является важным активом предприятий. Рост информатизации и компьютеризации производственных и управленческих процессов, усиление международного сотрудничества еще больше повысили ее ценность. Каждый хозяйствующий в конкурентной среде субъект для поддержания своей конкурентоспособности должен обеспечивать защиту важной информации в отношении собственной производственной или хозяйственной деятельности [1; 2]. Усиливает значение защиты информации хозяйствующих субъектов и повышение открытости информационного пространства жизнедеятельности общества, связанного с развитием глобализации. Предпринимательские структуры и их стейкхолдеры в своей деятельности все больше полагаются на использование информационных и коммуникационных технологий, что способствует быстрому прогрессу во взаимодействии организаций и потребителей продукции и услуг через Интернет. В государственном секторе информационные и коммуникационные технологии используются для предоставления услуг, хранения и обработки информации, а также для обеспечения связи с дальнейшей необходимостью защищать конфиденциальность, безопасность и целостность информации, которая хранится в системах управления.

Менеджмент предприятий ЕС в основном принципиально определился о целесообразности применения в собственной хозяйственной деятельности систем защиты собственной информации. Они официально используют политику информационной безопасности, причем крупные предприятия в большей степени признают целесообразность защиты собственной информации. Такое соотношение может быть свидетельством еще и того, что крупные предприятия имеют больше возможностей (финансовых, организационных и т.п.) ее реализации [3].

Хотя защита информации является важным атрибутом существования предприятия, ее организация не сможет решить все его проблемы. Необходимо помнить о том, что наиболее значимым направлением деятельности большинства предприятий является их основная деятельность, направленная на создание конкретного продукта, а защита информации лишь создает предпосылки для успешной деятельности предприятия в условиях конкурентной

среды. Именно поэтому основной целью системы защиты является обеспечение условий для осуществления эффективной деятельности предприятия и всех его подразделений.

Для сохранения информации на предприятиях могут быть использованы определенные защитные методы, причем система защиты информации должна быть адаптирована к специфике внешней среды предприятия и его внутренних возможностей, а в каждом отдельном предприятии методы защиты информации могут быть различны по масштабам внедрения и форме.

Количественный и качественный состав способов и приемов защиты информации зависит [4]:

– от специфики производственной деятельности (больше всего нуждаются в защите информации предприятия, которые функционируют в условиях интенсивной конкуренции, деятельность которых напрямую зависит от качества информации);

– от производственных, финансовых и других возможностей предприятия;

– от количества конфиденциальных сведений, используемых конкретным предприятием и нуждающихся в защите, а также полезности (ценности) информации.

Во время обеспечения защиты информации на предприятиях необходимо придерживаться определенных организационно-экономических принципов, основными из которых являются экономическая целесообразность, активность, уверенность, безпрерывность, разнообразие, комплексность (целостность) защиты информации.

С точки зрения целесообразности защиты всю информацию предприятия можно разделить на открытую (общедоступную), конфиденциальную (с ограниченным доступом) и тайную (доступна только узкому кругу работников предприятия, не доступна внешним пользователям). Для того чтобы обеспечить экономическую целесообразность защиты информации, необходимо, чтобы возможные потери от утечки информации были больше затрат на ее защиту. Оптимизация достигается при минимизации расходов на защиту информации , то есть чем ниже уровень этих расходов, тем экономически целесообразнее система защиты информации. Экономическая целесообразность защиты информации будет повышаться за счет сокращения затрат на защиту информации за одновременного повышения (поддержания) общего уровня качества системы ее защиты, поэтому установление возможных потерь от утечки определенной информации является задачей более экономичным, чем организационным. Ведь от рассчитанной величины возможных потерь от утечки информации будет зависеть величина средств, которые могут будут потрачены на ее защиту, а следовательно, и количественный и качественный содержание составляющих системы защиты информации на предприятии. Эта закономерность может быть использована также и для проверки соответствия уже действующей системы защиты информации на предприятии требованию экономической целесообразности. При этом стоимостное значение расходов

определяется на основе сметы как сумма расходов на проведение всех защитных мероприятий.

Потери от утечки информации могут быть вызваны такими обстоятельствами, как потеря приоритета в освоенных областях научно-технического прогресса, рост расходов на переориентацию деятельности исследовательских подразделений; потеря доверия потребителя к качеству продукции; возникновения или создания конкурентами трудностей с закупкой сырья, технологий, оборудования и других компонентов, необходимых для осуществления нормальной производственной деятельности; усложнение отношений с партнерами, срыв выгодных контрактов; рост расходов на создание новой рыночной стратегии, изменение плана проведения маркетинговых исследований и тому подобное.

Вероятность потерь от утечки информации будет зависеть от вероятности возникновения угроз информационной безопасности предприятий. Учитывая природу угроз, присущих их различным группам, можно выделить [5]:

– преднамеренные угрозы (вероятность их возникновения зависит от мотивации, знаний, компетенции и ресурсов, доступных потенциальному преступнику, а также от привлекательности активов для реализации атак);

– случайные угрозы (оцениваются с использованием статистики и опыта, а их вероятность может зависеть от близости организации к источникам опасности);

– инциденты, возникавшие в прошлом (характеризующие проблемы в защитных системах, используемых предприятием);

– новые разработки и тенденции (включают в себя отчеты, новости и тенденции, полученные из Интернета и других источников информации).

Таким образом, проблеме защиты информации в современных условиях любое предприятие должно уделять достаточное внимание, поскольку это является одним из важных аспектов, обеспечивающих его эффективную работу в условиях свободного конкурентного рынка. Проблема защиты информации в большинстве развитых государств мира приоритетна и рассматривается на государственном уровне. Создание надежной системы защиты информации обеспечит сохранение и развитие конкурентных преимуществ предприятия на основе использования его информационных ресурсов.

## Список литературы:

1. Raiding as a treat to economic security of Kuzbass coal mining enterprises / Tyuleneva T.A. // В сборнике: E3S Web of Conferences Electronic edition. 2018.

2. Improvement of measures to counteract raider acquisition of Kuzbass coal mining enterprises / Tyuleneva T.A. // В сборнике: E3S Web of Conferences Electronic edition. 2018.

3. Enterprises having a formally defined ICT security policy, by size class, EU-28, 2015 (% enterprises). Eurostat Statistics. URL:

http://ec.europa.eu/eurostat/statistics-explained/index.php/ (Дата обращения: 09.03.2020)

4. Дейнега А.В. Информационная безопасность предприятий в условиях глобализации 4.0. // Экономика и общество, № 20, 2019. С. 199-208.

5. Астахов А.М. Искусство управления информационными рисками. Москва: ДМКПресс, 2010. 312 с.