УДК 004.056
ГРНТИ 81.93.29
DOI: 10.23947/interagro.2020.1.336-337

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИЯХ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Айдинян А.Р., Цветкова О.Л.

Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Аннотация. Предприятия агропромышленного комплекса заинтересованы в предотвращении утечки информации. Обнаружение и перекрытие каналов утечки информации возможно только при использовании комплекса мер, включающих в себя технические, организационные и правовые меры. Рассмотрены вопросы, связанные с организацией защиты конфиденциальной информации от утечки на предприятиях агропромышленного комплекса.

Ключевые слова. Защита информации, информационная безопасность, каналы утечки информации, методы предотвращения утечки информации, информационная безопасность предприятия агропромышленного комплекса.

THE METHODS OF INFORMATION PROTECTION AT AGRICULTURAL ENTERPRISES

Aidinyan A.R., Tsvetkova O.L.

Don State Technical University, Rostov-on-Don, Russian Federation

Abstract. Agricultural enterprises are interested in preventing information leakage. Detection and blocking of information leakage channels are possible only when using a set of measures that include technical, organizational, and legal ones. The article deals with issues related to the protection of confidential company information leakage in the enterprises of the agro-industrial complex.

Keywords. Information protection, information security, information leakage channels, methods for preventing information leakage, information security of enterprises in the agro-industrial complex.

Реализация на современных предприятиях различных электронных средств общения приводит к необходимости усилить контроль за потоками информации. Предприятия, в том числе и предприятия сельскохозяйственного комплекса, заинтересованы в том, чтобы защитить свою конфиденциальную информацию с целью недопуска ее распространение. В настоящее время предприятия проводят меры, направленные на обеспечение информационной безопасности [1]. Однако, при этом необходимо решить актуальную задачу, суть которой заключается в правильном выборе совокупности мер, позволяющей при минимально возможных затратах обеспечить требуемый уровень уровня защиты.

На предприятиях агропромышленного комплекса можно выделить относительно много потенциально возможных каналов утечки информации. При этом особое внимание должно быть уделено возможной недисциплинированности и неосведомленности сотрудников предприятия о правилах работы с конфиденциальной информацией, что может привести к неумышленному нарушению конфиденциальности, целостности и/или доступности информации.

Также важно предотвратить целенаправленную преднамеренную передачу информации нелояльными сотрудниками предприятия агропромышленного комплекса, например с целью получения незаконной материальной выгоды. Также важно защитить информацию от утечки уволенными сотрудниками к конкурирующим предприятиям.

Важно рассмотреть, проанализировать информационную инфраструктуру предприятия, выявить уязвимые места системы защиты и все каналы утечки информации. Как правило, каналы утечки информации разделяют на следующие группы [2]: электромагнитные, акустические, визуально-оптические, материально-вещественные.

Ясно, что требуется комплексный подход к защите информации. И даже, используя комплексный подход, необходимо выбрать оптимальное соотношение между ценой и качеством проводимых работ по обеспечению информационной безопасности. При этом важно не допустить такой ситуации, при которой внедрение большого количества мер информационной безопасности приведет к усложнению и снижению продуктивности работников при выполнении своих непосредственных обязанностей.

Система предотвращения утечки конфиденциальных данных строится на базе следующих принципов:

– работа с персоналом. Правила работы с персоналом с целью минимизации влияния человеческого фактора на утечку информации определены в международном стандарте ISO/IEC 17799:2000. При этом одним из основных правил является обязательное заключение с сотрудниками договора о неразглашении конфиденциальной информации;

– использование сервисов безопасности для ограничения доступа к информации, протоколирования фактов доступа и контроля потоков информации. К этим средствам относятся DLP-системы [3];

– использование разработанной политики безопасности, что позволяет обеспечить обнаружение, предупреждение, предотвращение и реагирование на факты, связанные с утечкой информации. К сервисам безопасности относятся: сервисы аутентификации, шифрования, аудита безопасности и управления доступом.

Каждый руководитель предприятия заинтересован в минимизации и полном исключении утечки конфиденциальной информации. К способам предотвращения утечки конфиденциальной информации относятся следующие меры.

1. Технические меры, которые используют различные электромеханические, механические, электронные и другие устройства и системы для защиты. Они являются сертифицированными и дорогостоящими и, несмотря на это, не гарантируют полную защиту.

При выборе технических средств защиты, в связи с их дороговизной и необходимостью грамотного их применения, предприятие должно исходить из своих финансовых и кадровых возможностей. Использование технических средств защиты невозможно при отсутствии грамотных специалистов в области информационной безопасности на предприятии. К техническим средствам первостепенной важности относятся датчики охранной сигнализации, средства защиты носителей информации, средства защиты информации от похищения, средства контроля и проверки средств защиты, средства, предотвращающие прослушивание и перехват информации [2].

2. Организационные меры, к которым в первую очередь относятся организация работы с документами и сотрудниками, техническими средствами хранения информации [4], выработка мер по обеспечению защиты информации [5, 6], организация работы по эффективному планированию перемещений и транспортировки ценных и конфиденциальных информационных ресурсов предприятия [7].

3. Правовые меры, к которым относятся нормы действующего законодательства. Для полного использования правовых мер защиты информации необходимо включать в заключаемые договора вопросы обеспечения конфиденциальности.

Обнаружение и перекрытие каналов утечки информации необходимо решать комплексно с учетом финансовых и кадровых возможностей предприятия, предварительно выбрав оптимальный уровень защиты и планируемых финансовых затрат. При этом необходимо использовать комплекс мер, включающих в себя сочетание организационного, правового и технического. Рекомендуется также использовать аналитические способы выбора средств защиты для сокращения затрат [3] и обязательно проводить оценку достигнутого уровня защищенности предприятия [6].

Список использованных источников

1. Волокитин А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. – М.: НТЦ «ФИОРД – ИНФО», 2002. – 272 с.

2. Максимов Ю.Н., Сонников В.Г. и др. Шпионские штучки. Технические методы и средства защиты информации. – СПб: Полигон, 2000. – 320 с.

3. Айдинян А.Р., Цветкова О.Л., Черняков П.В., Сокол Д.С. Методики интеллектуального выбора и оценки DLP-систем для решения задач информационной безопасности // Молодой исследователь Дона. – Ростов н/Д: Издательский центр ДГТУ, 2018. – №1. – С. 2-5.

4. Айдинян А.Р., Цветкова О.Л. Информационные технологии: учебное пособие. – Ростов н/Д: Издательский центр ДГТУ, 2011. – 132 с.

5. Цветкова О.Л., Айдинян А.Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз // Вестник компьютерных и информационных технологий. – 2014. – №8(122). – С. 48–53.

6. Куринных Д.Ю., Айдинян А.Р., Цветкова О.Л. Подход к кластеризации угроз информационной безопасности предприятий // Инженерный вестник Дона. – 2018. – № 1 (48). – С. 91.

7. Цветкова О.Л., Айдинян А.Р., Долженкова Ю.Ю. Постановка задачи планирования маршрутов доставки грузов с учетом безопасности транспортировки // Инженерный вестник Дона. – 2018. – № 1 (48). – С. 41.

Работа выполнена в рамках инициативной НИР.