УДК 004.056.5

ИНФОРМАЦИЯ, ПОДЛЕЖАЩАЯ ЗАЩИТЕ ОТ УТЕЧЕК СРЕДСТВАМИ DLP-СИСТЕМ

Е.С. Захарова

Институт информационных технологий БГУИР, г. Минск, Республика Беларусь

Аннотация. Информационная безопасность предприятия невозможна без построения надежной системы защиты информации. В настоящее время набирает популярность включение в систему защиты информации DLP-решений. Однако в Республике Беларусь отсутствуют научные исследования правового обеспечения внедрения и использования систем предотвращения утечки информации. Неизученным остается и вопрос о категории информации, которую целесообразно защищать от утечек с использованием DLP-систем. Динамика развития информационной сферы, законодательства о персональных данных, о коммерческой, банковской и иной тайне, появление новых вызовов и угроз информационной безопасности, включая угрозы утечки информации, позволяет сделать вывод, что эта работа должна продолжаться на высоком научном уровне.

Ключевые слова: информационная безопасность; риск; утечка информации; защита информации; общедоступная информация; информация, распространение и (или) предоставление которой ограничено; информационная система; проектирование системы защиты; система предотвращения утечки информации; DLP-система.

INFORMATION SUBJECT TO PROTECTION AGAINST LEAKS BY MEANS OF DLP SYSTEMS

H. Zakharova
Institute of Information Technologies BSUIR, Minsk city, Republic of Belarus

Abstract. Information security of an enterprise is impossible without building a reliable information security system. Currently, the inclusion of DLP solutions in the information security system is gaining popularity. However, in the Republic of Belarus there is no scientific research into the legal support for the implementation and use of information leakage prevention systems. The question of the category of information that is advisable to protect from leaks using DLP systems also remains unexplored. The dynamics of development of the information sphere, legislation on personal data, on commercial, banking and other secrets, the emergence of new challenges and threats to information security, including threats of information leakage, allows us to conclude that this work must continue at a high scientific level.
Keywords: information security; risk; information leak; information protection; public information; information, the distribution and (or) provision of which is limited; information system; design of a protection system; information leakage prevention system; DLP system.

Введение

Объемы информации, обрабатываемые и хранимые предприятиями и организациями в своих информационных ресурсах, зачастую не позволяют адекватным образом ее контролировать и защищать. При этом многие руководители оказываются не готовыми к внутренним угрозам, возникающим из-за утечки информации, вызванной действиями работников. Поэтому вопросы предотвращения утечек информации стоят сейчас особенно остро.

Одним из самых надежных способов защиты информации от внутренних угроз является установка систем предотвращения утечки информации (DLP – Data Leak Prevention – в дословном переводе «предотвращение утечки данных» [1, с. 37]).

Следует отметить, что в настоящее время отсутствуют нормативные правовые акты, закрепляющие требования к порядку и условиям внедрения и использования на предприятиях и в организациях Республики Беларусь систем предотвращения утечки информации. Законодательно не определена категория информации, для защиты которой могут быть использованы рассматриваемые системы. Не определены гарантии соблюдения прав работников предприятий, организаций, использующих в своей работе системы предотвращения утечки информации. Несмотря на это DLP-системы широко применяются на практике банками, предприятиями оборонного комплекса, предприятиями, имеющими коммерческие секреты [2, с. 57].

На основании изложенного представляется необходимым четко определить категорию информации, для защиты которой действующее законодательство предусматривает возможность применения систем предотвращения утечки информации.

Основная часть

В различных источниках авторы подчеркивают высокий уровень защиты DLP-системами от утечек «конфиденциальной информации» [1, с. 37; 3, с. 59, 61; 4, с. 4]. Отдельные авторы используют понятие «корпоративная информация» [5, с. 57].

Однако в Государственном стандарте Республики Беларусь «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования. СТБ 34.101.76-2017» используется термин «защищаемая информация», к которой

относится «информация, распространение и (или) предоставление которой ограничено Законом Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» и иными законодательными актами Республики Беларусь, а также неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу» (п. 3.6).

Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (далее - Закон) в статье 15 в зависимости от категории доступа выделяет:

1. Общедоступную информацию;

2. Информацию, распространение и (или) предоставление которой ограничено.

Общедоступной является информация, доступ к которой, распространение и (или) предоставление которой не ограничены (ч. 1 ст. 16 Закона).

Распространение общедоступной информации не предполагает активных действий по доведению информации до как можно большего числа получателей. Достаточно обеспечить возможность любым лицам получить к ней доступ. Это можно сделать, например, разложив печатные материалы в общедоступном, публичном месте или предоставив информацию на интернет-сайте с возможностью для любого абонента найти ее в сети через поисковую систему [6, с. 177].

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней (ч. 2 ст. 28 Закона). Таким образом, действующее законодательство не предусматривает защиту общедоступной информации от утечек. Следовательно, применение систем предотвращения утечки информации при использовании в работе предприятий и организаций Республики Беларусь общедоступной информации, не требуется.

Ко второй категории – информации, распространение и (или) предоставление которой ограничено, Закон относит:

– информацию о частной жизни физического лица и персональные данные;

– сведения, составляющие государственные секреты;

– служебную информацию ограниченного распространения;

– информацию, составляющую коммерческую, профессиональную, банковскую и иную охраняемую законом тайну;

– информацию, содержащуюся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

– иную информацию, доступ к которой ограничен законодательными актами (ч. 1 ст. 17 Закона).

Требования по защите информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, определяются законодательством (ч. 3 ст. 28 Закона).

Положение о порядке государственной регистрации информационных ресурсов и ведения Государственного регистра информационных ресурсов, утвержденное Постановлением Совета Министров Республики Беларусь от 26.05.2009 № 673, предписывает при использовании государственных информационных систем реализовывать меры по защите информации в соответствии с законодательством о защите информации (абз. 8 п. 6).

Так, Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки

информации, распространение и (или) предоставление которой ограничено, утвержденным Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – Положение), предусмотрено на этапе проектирования системы защиты информации составление технического задания, которое должно содержать требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем (п. 8, абз. 3 ч. 2 п. 10 Положения).

Информационные системы, в которых обрабатывается информация, распространение и (или) предоставление которой ограничено, могут быть отнесены к классам:

– 3-ин – если в них обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.

– 3-спец – если в них обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных.

– 3-юл – если в них обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые подключены к открытым каналам передачи данных (п.п. 6, 7, 9 Приложение 1 «Классы типовых информационных систем» к Положению).

Согласно п. 7.15. Приложения 3 к Положению, использование системы обнаружения утечек информации из информационных систем, отнесенных к классам 3-ин, 3-спец и 3-юл, является рекомендуемым, то есть не обязательным.

И только в отношении информационных систем, содержащих служебную информацию ограниченного распространения и которые подключены к открытым каналам передачи данных, отнесенных к классу 3-дсп (п. 10 Приложения 1 «Классы типовых информационных систем» к Положению) должны использоваться системы обнаружения утечек информации.

Заключение

В результате проведенного исследования действующего законодательства в сфере защиты информации можно сделать следующие выводы:

1. Многообразие дефиниций информации, зашишаемой DLP-системами, слабая определенность используемого в различных научных и научно-популярных источниках понятийного аппарата, использование терминов «конфиденциальная информация», «корпоративная информация» для целей конкретной научной работы является актуальной проблемой на протяжении многих лет. Все это может привести к неправомерному использованию систем обнаружения утечек информации в отношении общедоступной информации.

2. Использование DLP-систем допускается в государственных информационных системах и информационных системах, в которых обрабатывается информация, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения).

3. Использование систем обнаружения утечек информации является обязательным для защиты служебной информации ограниченного распространения.

Список использованных источников

1. Станкевич, В. DLP: белорусский опыт / В. Станкевич // IT Бел : технологии автоматизации бизнеса : научно-практический журнал / учредитель частное производственное унитарное предприятие «Редакция журнала «IT Бел». – 2011. – № 1/2. – С. 37-39.

2. Никифоров, С.Н. Проблематика внедрения DLP систем в Республике Беларусь / С. Н. Никифоров // Технологии безопасности. – 2012. – № 3. – С. 57.

3. Барановский, А.В. Обзор систем противодействия утечкам информации. DLP системы в Беларуси / А.В. Барановский // Технологии безопасности. – 2012. – № 3. – С. 58-63.

4. Система противодействия утечке данных «Контур информационной безопасности Searchinform» : пособие / Т.В. Бороботько [и др.]. – Минск : БГУИР, 2021. – 284 с.

5. Акимов, А.И. DLP в Беларуси: пять вопросов, требующих ответов / А.И. Акимов // Технологии безопасности. – 2012. – № 3. – С. 56-57.

6. Саперов, С.А. Информация как объект правоотношений: монография / С.А. Саперов. – М.: Юстицинформ, 2023. – 704 с.

References

1. Stankevich, V. DLP: Belarusian experience / V. Stankevich // IT Bel: business automation technologies: scientific and practical journal / founder of the private production unitary enterprise "Editing Office of the magazine "IT Bel". – 2011. – № 1/2. – С. 37-39.

2. Nikiforov, S.N. Problems of implementing DLP systems in the Republic of Belarus / S.N. Nikiforov // Security technologies. – 2012. – № 3. – С. 57.

3. Baranovsky, A.V. Review of systems to combat information leaks. DLP systems in Belarus / A. V. Baranovsky // Security Technologies. – 2012. – № 3. – С. 58-63.

4. System for combating data leakage "Searchinform Information Security Circuit": manual / T. V. Borobotko [and others]. – Minsk: BSUIR, 2021. – 284 с.

5. Akimov, A.I. DLP in Belarus: five questions that require answers / A.I. Akimov // Security technologies. – 2012. – № 3. – С. 56-57

6. Saperov, S.A. Information as an object of legal relations: monograph / S.A. Saperov. – M.: Justitsinform. 2023. – 704 с.

Сведения об авторе

Захарова Е.С., слушатель Института информационных технологий БГУИР, zaharova@info-center.by.

Information about the author

Zakharova H., student of the Institute of Information Technologies BSUIR, zaharova@info-center.by.