УДК 004.056

Исмагулова Жулдыз Сауелхановна – к.т.н., доцент (г. Алматы, Казахская академия транспорта и коммуникаций им. М. Тынышпаева)

Нагаев Руслан Дамирович – магистрант (г. Алматы, Казахская академия транспорта и коммуникаций им. М. Тынышпаева)

РАЗРАБОТКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Надежная защита вычислительной и сетевой корпоративной инфраструктуры является базовой задачей в области информационной безопасности для любой компании. С ростом бизнеса предприятия и перехода к территориально-распределенной организации она начинает выходить за рамки отдельного здания. Эффективная защита IT-инфраструктуры и прикладных корпоративных систем сегодня невозможна без внедрения современных технологий контроля сетевого доступа. Участившиеся случаи кражи носителей, содержащих ценную информацию делового характера, все больше заставляют принимать организационные меры [1].

Перечень угроз информационной безопасности, нарушений, преступлений настолько обширный, что требует научной систематизации и специального изучения с целью оценки связанных с ними рисков и разработки мероприятий по их предупреждению. Исследования свидетельствуют о том, что основной причиной проблем компаний в области защиты информации является отсутствие продуманной и утвержденной политики обеспечения информационной безопасности, базирующейся на организационных, технических, экономических решениях с последующим контролем их реализации и оценкой эффективности. Все это предопределяет необходимость разработки научно обоснованных методов обеспечения информационной безопасности предприятий, учитывающих практический опыт казахстанских и зарубежных предприятий в этой области [1].

Проблемы информационной безопасности предприятий рассматривались в работах многих отечественных исследователей и специалистов. Вместе с тем проведенные исследования касаются лишь отдельных аспектов обеспечения информационной безопасности, в то время как комплексность этой проблемы предполагает разработку для ее решения более современных и адекватных методов. Все это и предопределило цели и задачи магистерской работы. Информационная защита данных должна происходить таким образом, чтобы не мешать сотрудникам компании заниматься повседневными задачами.

Для обеспечения информационной безопасности и управляемости сети в компании необходимо использовать следующие приемы. Системный администратор сети обязан иметь возможность добавлять, менять и уничтожать параметры учетных записей пользователей для самых разных платформ, операционных систем и приложений. Такой подход, называется «единой точкой регистрации».

Управление информационной безопасностью системы из единой точки позволяет объединить в единую базу данных контроля доступа к ресурсам. Хороший защитный сервер компании обеспечит прозрачное представление информации обо всех доступных пользователю ресурсах [2].

Система информационной безопасности выявляет подозрительные действия со стороны как внутренних, так и внешних пользователей. Для этого надо использовать программу специального назначения. DLP-системы (*Data Leak Prevention)*. Данная система защиты от утечек данных призвана обеспечивать контроль над распространением конфиденциальной информации за пределы предприятия по доступным каналам передачи

информации. DLP – решение предотвращает несанкционированные операции с конфиденциальной информацией (копирование, изменение и т.д.) и ее перемещение (пересылку, передачу за пределы организации и т.д.). Функционал DLP направлен в первую очередь на защиту от случайных утечек. Основная задача DLP-системы заключается в том, чтобы обезопасить общество от нежелательных элементов и их пропагандистских заявлений. Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации [3]. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются. В DLP - системах должен быть развит контроль (рисунок 1) системы защиты информационной безопасности.

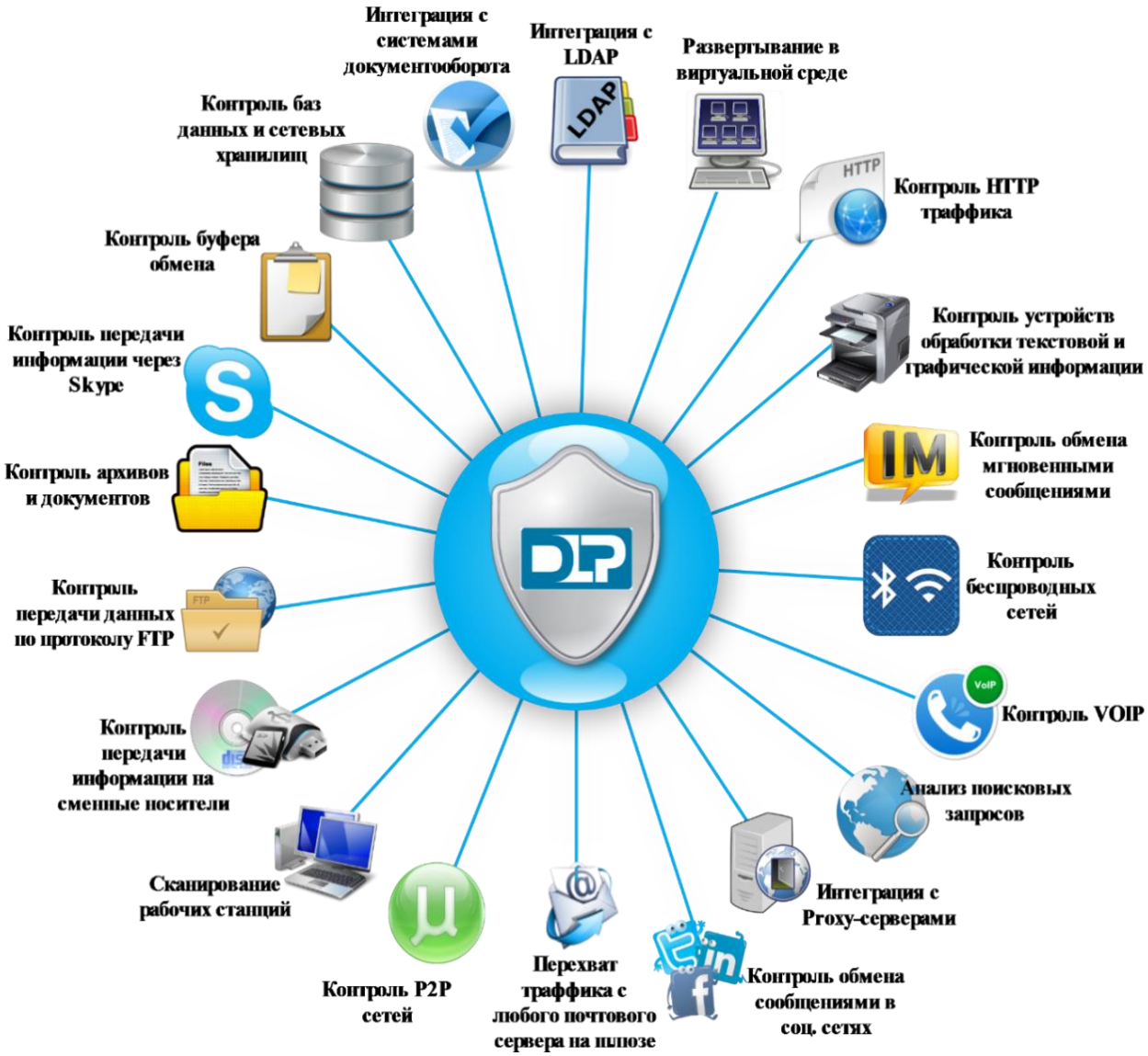

Рисунок 1 – Работа DLP – системы

Выбор способов защиты информации в информационной системе - сложная оптимизационная задача, при решении которой требуется учитывать вероятности различных угроз информации, стоимость реализации различных способов защиты и наличие различных заинтересованных сторон. Эффективность информационной безопасности означает, что затраты на ее осуществление не должны быть больше возможных потерь от реализации информационных угроз. Планирование безопасности информации осуществляется путем разработки каждой службой детальных планов защиты информации. Поэтому для защиты информации компании были изучены различные системы обеспечения информационной безопасности и разработана система DLP, система защиты от утечек данных, призвана обеспечивать контроль над распространением конфиденциальной информации за пределы предприятия по доступным каналам передачи информации.

Выводы. В статье представлено описание, достоинства и основные особенности системы обеспечения информационной безопасности.

Данная система предотвращает утечки конфиденциальной информации за пределы корпоративной сети. Строится эта система на анализе потоков данных, выходящих за пределы корпоративной сети. В случае сработки определенной сигнатуры и детекта передачи конфиденциальной информации система либо блокирует такую передачу, либо посылает уведомления системному администратору.

ЛИТЕРАТУРА

1. Мельников В.П. Информационная безопасность и защита информации [Текст] / Учебное пособие для вузов - М.: Академия, 2008. — 336 с.

2 Мельников, Д.А. Информационная безопасность открытых систем [Текст] / учебник - Д.А. Мельников. - М.: Флинта, 2013. - 448 с.

3. Ячейка комплектного распределительного устройства [Электронный ресурс] https://research-journal.org/technical/razrabotka-sistemy-informacionnoj-bezopasnosti-dlya-stroitelnoj-kompanii/