2. Andreas Opelt, Boris Gloger, and Wolfgang Pfarl Agile Contracts. – Creating and Managing Successful Projects with Scrum. – Published by John Willey&Sons, 2013 – 26 c.

3. Scrummasters [Электронный ресурс] – Режим доступа: https://scrummasters.com.ua

4. Project Management Journal [Электронный ресурс] – Режим доступа: https://pmjournal.ru/articles/biznes-stati/otchet-ob-issledovanii-agile-v-rossii-2018/

ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ВНЕДРЕНИЯ DLP-СИСТЕМ

Богдевич П.С., Холупко И.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ермакова Е.В. – к.э.н.,доцент

Все современные операционные системы оснащены встроенными модулями защиты данных на программном уровне, однако для создания эффективной работы с конфиденциальной информацией важно использовать дополнительные модули защиты, которые создают защищенный цифровой «периметр» вокруг организации, анализируя всю исходящую, а в ряде случаев и входящую информацию.

Научно-технический прогресс превратил информацию в продукт, который можно купить, продать, обменять. Качество коммерческой информации обеспечивает необходимый экономический эффект для компании, поэтому важно охранять критически важные данные от неправомерных действий.

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц.

Конфиденциальные данные – это информация, доступ к которой ограничен в соответствии с законами государства и нормами, которые компании устанавливаются самостоятельно (личные, служебные, судебные, коммерческие, профессиональные).

Угроза – это возможные или действительные попытки завладеть защищаемыми информационными ресурсами. Источниками угрозы сохранности конфиденциальных данных являются компании-конкуренты, злоумышленники, органы управления. Угрозы бывают внутренними или внешними.

Под DLP-системами принято понимать программные продукты, защищающие организации от утечек конфиденциальной информации. Сама аббревиатура DLP расшифровывается как Data Leak Prevention, то есть, предотвращение утечек данных. DLP-системы также хорошо подходят для решения ряда других задач, связанных с контролем действий персонала (контроль использования рабочего времени; мониторинг общения; контроль правомерности действий; выявление сотрудников, рассылающих резюме).

Главной тенденцией, как полагают эксперты, является переход от «заплаточных» систем, состоящих из компонентов от различных производителей, решающих каждый свою задачу, к единым интегрированным программным комплексам. Ещё одной важной тенденцией в сфере DLP является постепенный переход к модульной структуре, когда заказчик может самостоятельно выбрать те компоненты системы, которые ему необходимы.

Сегодня наиболее распространены два способа определения степени конфиденциальности документа: путём анализа специальных маркеров документа и путём анализа содержимого документа. Чаще применяется второй вариант, поскольку он устойчив перед модификациями, вносимыми в документ перед его отправкой, а также позволяет легко расширять число конфиденциальных документов, с которыми может работать система.

Все DLP-системы можно разделить по ряду признаков на несколько основных классов:

По способности блокирования информации (активные, пассивные)

По сетевой архитектуре (шлюзовые, хостовые)

DLP-системы используют, когда необходимо обеспечить защиту конфиденциальных данных от внутренних угроз. DLP-система должна уметь отличать конфиденциальную информацию от неконфиденциальной. Функциональность DLP-системы строится вокруг «ядра» – программного алгоритма, который отвечает за обнаружение и категоризацию информации, нуждающейся в защите от утечек. В ядре большинства DLP-решений заложены две технологии: лингвистического анализа и технология, основанная на статистических методах. Также в ядре могут использоваться менее распространенные техники, например, применение меток или формальные методы анализа.

Лингвистический метод анализа работает напрямую с содержанием файла и документа (морфологический анализ, семантический анализ).

При статистическом методе анализа документ (текст) делится на фрагменты приемлемой величины, с фрагментов снимается хеш (в DLP-системах встречается как термин Digital Fingerprint – «цифровой отпечаток»), затем хеш сравнивается с хешем эталонного фрагмента.

Выбор подходящей DLP-системы начинается с составления грамотного технического задания. Критерии выбора, которые следует учитывать при составлении документа, включают:

Количество контролируемых каналов

Надежность и скорость работы системы

Аналитические возможности

Наличие, качество и быстрота реакции техподдержки

Важный критерий, который сузит круг подходящих решений на этапе формирования требований к DLP-системе, – цена продукта. Цена DLP-системы прямо пропорциональна наличию расширенного инструментария, включая механизм распознавания текста в изображении, модули лингвистического анализа, технологии самообучения и другие функции. Затраты на DLP-систему включают не только стоимость самого продукта.

Инвестиции в DLP = Единовременные затраты (обследование, проектирование, закупка ПО и оборудования, внедрение, обучение, консалтинг, разработка ОРД, приемочные испытания) + Постоянные затраты (техническая поддержка, продление подписок, администрирование и эксплуатация).

Коэффициент возврата инвестиций (ROI) – основной экономический показать эффективности ИБ, он определяется как отношение сокращения ожидаемых среднегодовых потерь (ALE) к стоимости реализации контрмер (TCO). Простая формула ROI = ALE / TCO может дать ответы на все экономические вопросы ИБ. ROI > 10 – хорошо, ROI < 10 – плохо, ROI < 0 – отвратительно.

Риск утечки информации, который количественно определяется величиной (ALE) и рассчитывается по формуле:

Величина риска = Вероятность угрозы * Величина Уязвимости * Размер ущерба, где Вероятность угрозы – среднее количество инцидентов ИБ в год, Величина уязвимости - процент успешных инцидентов от общего количества инцидентов, Размер ущерба – совокупная стоимость скомпрометированных информационных активов (потери организации от успешных инцидентов).

Помимо всего прочего, функционирование DLP-системы должно поддерживаться комплексом организационных и юридических мер, документирование которых осуществляется в ходе разработки комплекта организационно-распорядительных документов (ОРД).

Для инцидентов, связанных с утечкой информации, возможны три вида последствий:

Утрата конкурентных преимуществ, недополученная прибыль (например, в результате утечки ноу-хау или клиентской базы).

Ущерб репутации (например, в результате утечки персональных данных клиентов, банковской тайны или внутренней финансовой отчетности).

Прямой финансовый ущерб: судебные издержки, штрафы со стороны регуляторов, компенсации пострадавшим, затраты на ликвидацию последствий инцидента (например, в результате утечки данных третьих лиц, клиентов, партнеров или контрагентов).

В наше время DLP-системы получают все более широкое распространение, несмотря на их дороговизну с одной стороны и отсутствие четких представлений об их экономической эффективности с другой. Применение DLP-систем сопряжено с рядом «побочных эффектов», таких как ухудшение морального климата в коллективе, а также непростые отношения с законодательством, защищающим право граждан на личную жизнь.

Список использованных источников:

1. Информационная безопасность | Обеспечение информационной безопасности – SearchInform [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/. – Дата доступа: 01.03.2019.

2. DLP-системы | DLP-системы – что это такое и как это работает – SearchInform [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/. – Дата доступа: 01.03.2019.

3. Принцип работы DLP-системы | DLP-системы – что это такое? – SearchInform [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/printsip-raboty-dlp-sistemy/. – Дата доступа: 01.03.2019.

4. Как выбрать DLP-систему | Выбираем DLP-систему для организации – SearchInform [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/kak-vybrat-dlp-sistemu/. – Дата доступа: 01.03.2019.

5. Стоимость DLP-систем | Сколько стоит DLP? – SearchInform [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/stoimost-dlp-sistem/. – Дата доступа: 01.03.2019.