УДК 004.056.5 Вестник УрФО № 3(25) / 2017, с. 5–11

Шабуров А. С., Журилова Е. Е.

ОБ ОСОБЕННОСТЯХ ИНТЕГРАЦИИ DLP-РЕШЕНИЙ В КОРПОРАТИВНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

В статье рассматриваются проблемы внедрения комплексных систем защиты информации, обусловленные интеграцией различных подсистем безопасности. Анализируется опыт внедрения и эффективность DLP-решений. Приводится модель реализации вариантов решений по внедрению СЗИ. Ставится задача выбора конкретного решения на основе особенностей информационных систем. Приводятся требования, предъявляемые к данным системам, на основе принципов их организации. Сопоставляются особенности корпоративных систем и функциональные возможности DLP-решений. Представлена типовая модель взаимодействия подсистем защиты информации в корпоративной информационной системе. Приводятся аналитические выражения для оценки эффективности внедрения DLP - решений в корпоративные информационные системы.

Ключевые слова: *система защиты информации, DLP-система, синергичность, канал утечки информации, безопасность корпоративных систем, эффективность защиты информации.*

Shaburov A. S., Zhurilova E. E.

ABOUT FEATURES OF INTEGRATION DLP-SOLUTIONS IN CORPORATE INFORMATION SYSTEMS

In this article consider the problems of implementing complex information security systems, due to the integration of various security subsystems. It is analyzed the experience of implementation and efficiency of DLP-solutions. Also, it's given a model of realizing solutions for implementing in ISS. The task is to choose a specific solution based on characteristics of information systems. The requirements for these systems are presented on the basis of the principles of their organization. The features of corporate systems and the functionality of DLP solutions are compared. It is presented a typical model of interaction of information protection subsystems in the corporate information system. Also, there are presented the analytical expressions for evaluat-

ing the effectiveness of implementing DLP-solutions in corporate information systems.

Keywords: *information security system, DLP-system, synergism, data leak channel, security of corporate systems, efficiency of information security.*

В условиях совершенствования информационных технологий, внедрения перспективных проектов, обеспечивающих переход на цифровую экономику, приобретает особое значение проблема информационной безопасности корпоративных систем (КС). Современное обеспечение безопасности информации основано на внедрении эффективных комплексных системных решений. Как правило, комплексная система защиты информации представляет собой множество разнородных компонентов взаимосвязанных и взаимодействующих между собой, обладающих свойствами целостности, синергичности и иерархичности. Это не противоречит традиционному толкованию термина «система защиты информации» (СЗИ), которое предполагает комплексное внедрение совокупности органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованной и функционирующей по правилам и нормам, установленным соответствующими документами в области защиты информации[1]. С другой стороны, традиционное понимание системы защиты не должно противоречить современным инновационным решениям в области обеспечения информационной безопасности, во многом зависящим от интеграции в архитектуру конкретной информационной системы.

Как правило, произвольная информационная система включает множество подсистем, в том числе и СЗИ, в свою очередь, также детализируемую на множество интегрированных и взаимосвязанных компонентов. Традиционно, комплексное функционирование СЗИ обеспечивается подсистемами технических средств охраны (ТСО) управления доступом, антивирусной защиты, криптографической защиты информации и рядом других подсистем. В последние годы также получили распространение SIEM-системы, DLP-системы, а так же аналогичные, достаточно дорогостоящие, но эффективные инструменты защиты. Подобное совершенствование систем безопасности, в первую очередь, ориентировано на противодействие актуальным угрозам безопасности информации, связанным, как с кибернетическими атаками, так и с утечкой информации ограниченного доступа из КС.

Опыт внедрения систем предотвращения утечек информации, основанных на DLP-решениях, демонстрирует их достаточную высокую эффективность. В то же время, внедрение подобных систем в корпоративных сетях, без интеграции с другими подсистемами системы защиты информации, не является панацеей[2].

В первое время, после появления DLP-систем на рынке средств защиты информации, по мнению некоторых специалистов, предполагалось, что такие системы смогут решить все проблемы утечек информации по техническим каналам связи. Практическое же использование доказало, что это не всегда так. Согласно статистике, в первое время DLP-системы внедрялись по принципу «от конца к началу», т.е. сначала осуществлялось внедрение, а потом выявлялись каналы утечки информации, недостатки политики информационной безопасности. Прежде всего, эти недостатки проявлялись в отсутствии четкого разделения корпоративных данных на открытые данные и данные ограниченного доступа[3]. Такой способ внедрения DLP-системы, как правило, был длительным, поскольку приходилось начинать с исследования уязвимостей информационных систем и построения системы информационной безопасности с самого начала. Кроме того, возникало значительное количество проблем внедрения DLP-систем, прежде всего, заключающихся в необходимости комплексного объединения множества компонентов, на основе DLP-решения. Настройка же правильного взаимодействий внутри СЗИ между средствами и подсистемами защиты позволила бы обеспечить эффект синергичности, а так же обойтись оптимальным набором средств, для достижения требуемого уровня защищенности информации.

КС предприятий и организаций имеют свои отличительные особенности, требования к внедрению, правила внедрения и область действия. Кроме того, особенности КС проявляются в преимуществах и недостатках, влияющих на эффект от внедрения того или иного решения, специальных требований по доступности информации, необходимой для обеспечения бизнес-процессов.

Согласно проведенным исследованиям,

эффективность работы DLP-решений проявляется лучше в системах с количеством сотрудников свыше пяти тысяч человек, поэтому рассмотрение комплексного подхода к внедрению предполагается на примере подобной КС.

Опыт внедрения DLP-решений, с учетом особенностей информационных систем, как правило, позволяет получить максимальный эффект от реализации функций защиты, при оптимальном количестве, используемых программных продуктов. С другой стороны, подобные особенности и обуславливают основные проблемы интеграции DLP-решений в корпоративной сети.

Рассмотрим модель ситуации, когда предполагается внедрение трех программных продуктов A, B, C (рис. 1) для обеспечения информационной безопасности КС. Конкретная система предполагает существование ранжированного перечня угроз безопасности информации. При этом, результат внедрения может быть оценен по различным критериям.

Решение «А» обеспечивает защиту от угроз с максимальным и средним риском, но перекрывает не весь список угроз. Решение «В» обеспечивает защиту от угроз с максимальным риском, но является дорогостоящим. Решение «С» обеспечивает защиту от угроз со средним и минимальным риском.

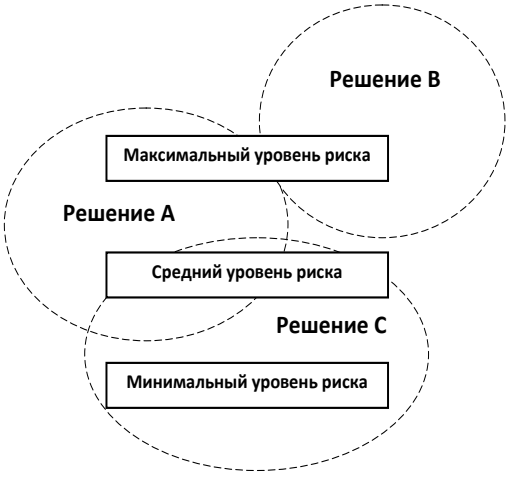

Рис. 1. Модель реализации вариантов решений по внедрению СЗИ

Даная модель предполагает, что различные комбинации перечисленных средств защиты информации предотвращают различный набор угроз безопасности информации. В данном случае возникает задача выбора такого набора решений, что бы была обеспечена требуемая эффективность при оптимальных затратах. При этом, учет особенностей системы, в которую будет проводиться внедрение, является ключевым фактором, поскольку помогает осуществить корректный выбор.

Основной особенностью КС является строгая организованность административной и производственной деятельности, что порождает территориальную и функциональную распределенность подразделений, большие объемы обрабатываемых данных, высокий уровень регламентации событий в системе[4].

В общем случае корпоративные системы строятся на 6 базовых принципах:

1) системности;
2) совместимости;
3) эффективности;
4) открытости;
5) унификации;
6) единого руководства.

Базовые принципы построения КС порождают требования к системам защиты, внедряемым в такие системы, к основным из которых относятся:

1. Интегрируемости (изменение показателей бизнес-процессов одной части системы должно повлечь за собой изменение связанных с ними характеристик).

2. Автоматизации процессов.

3. Обеспечения дружественного интерфейса по отношению к пользователю, с учетом не предоставлять возможности выполнять больше разрешенного.

4. Логирование (возможность контроля действий пользователей в определенные моменты времени).

В общем случае корпоративная система состоит из следующих компонентов[5]:

1. Ядра системы, содержащего полный набор функциональных модулей для автоматизации задач управления.

2. Автоматизированной системы электронного документооборота.

3. Системы обработки информации.

4. Системы информационной безопасности.

5. Средств и систем обеспечения взаимодействия с пользователем .

6. Сети, локальной и/или внешней.

7. Офисных программных решений.

8. Систем специального назначения, для реализации функций предприятия.

Исходя из выделенных особенностей корпоративных систем, можно провести ана-

лиз и выяснить, по каким причинам внедрение только DLP-решений не может обеспечить качественную защиту информации от утечек.

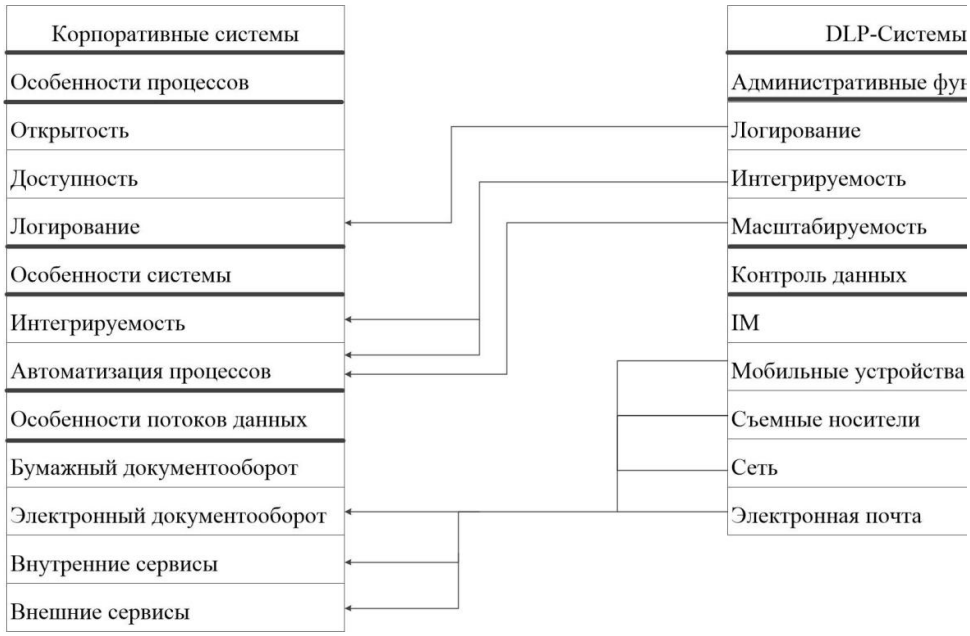

Рис. 2. Сопоставление особенностей КС и возможностей DLP-решений

На рис. 2 отображены взаимозависимости функций DLP систем и КС, позволяющие сформировать подмножества реализуемых функций. При этом, очевидно, что нереализованные функции по ЗИ должны быть обеспечены иным подмножеством компонентов СЗИ.

Данные предположения обосновывают вывод о необходимости нахождения сбалансированной и эффективной архитектуры КС на основе внедрения комплексной системы защиты. Традиционно, данная система должна включать в себя средства и системы контроля и управления доступом, межсетевого экранирования, средств резервного копирования, средства предотвращения вирусных атак, и ряд других. С другой стороны, возможна интеграция требуемого решения непосредственно в систему защиты информации. При этом, блокирование выявленных каналов утечки, не должно существенно затруднить работу пользователей и не спровоцировать новые возможности для реализации угроз безопасности информации.

Особенности же интеграции DLP-систем в КС, как правило, связаны с возникновением проблемы доступности информационных ресурсов. Внедрение всех необходимых средств защиты информации существенно затрудняет работу сотрудников организации, может повлечь за собой нарушение бизнес-процессов. Кроме того, возможны значительные расходы, связанные со стоимостью внедрения и эксплуатации оборудования для построения подобной системы защиты. Нахождение оптимальных вариантов архитектуры СЗИ, с учетом взаимодействия ее компонентов, предполагает разработку набора модельных представлений.

На рисунке 3 представлена модель взаимодействия подсистем защиты информации в информационной системе КС[6]. Модель сгенерирована для корпоративной организации с количеством сотрудников более 5 000 человек, поскольку при меньших объемах внедрение некоторых подсистем является нерациональным.

В данном случае система защиты представлена совокупностью подсистем СКУД, видеонаблюдения, DLP и SIEM, и межсетевых экранов. Поскольку SIEM системы предназначены для анализа событий, как в реальном времени, так и архивированных, то данные со всех подсистем передаются именно на входы SIEM-систем. Система осуществляет анализ данных на соответствие заданным критериям безопасности, доводит результаты анализа администратору безопасности[7,8]. В частных случаях предполагаются совмещения некоторых функций администрирования системы и

ее безопасности, однако в крупных корпоративных системах, на которые ориентирована рассматриваемая модель, данные функции разделены.

процентном соотношении предполагается на основе зависимостей:

$$E = \xi_n + \xi_v + \xi_s \quad (1)$$

где

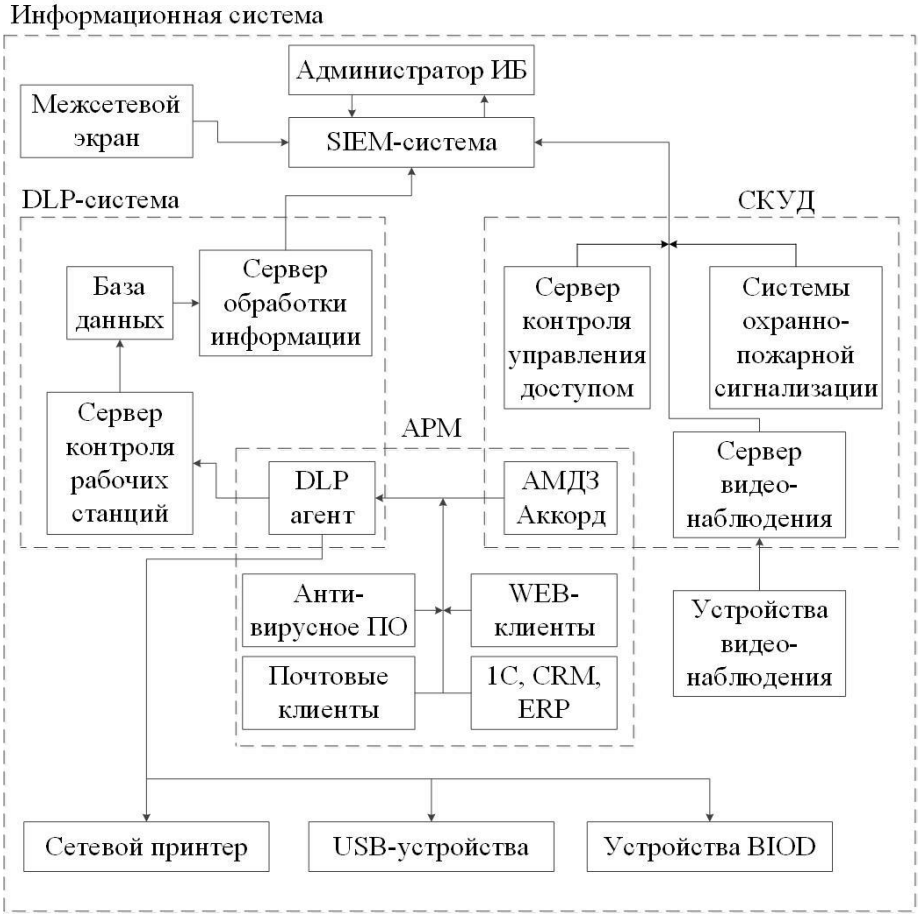

Рис. 3. Схема взаимодействий подсистем внутри системы защиты информации в КС

Предполагается, что представленный на схеме набор подсистем перекрывает все возможные каналы утечки информации, в том числе и те каналы, которые не выявляются посредством DLP-решения. Например, согласно исследованиям, вероятность реализации технических каналов утечки не исключает возможности утечки традиционных документов и утраты оборудования[8]. То есть, подобные угрозы должны быть ликвидированы за счет других, традиционных решений, например, системы контроля и управления доступом и видеонаблюдения.

Поиск оптимальной архитектуры СЗИ, основанной на внедрении DLP-решения, включает необходимую оценку их эффективности, с точки зрения нахождения требуемых решений по защите информации. Оценить эффективность E, для представленной модели в

$$\xi_n = \left(\frac{(k-x)\cdot sz + p\cdot sz}{sz\cdot y^2} \right) \cdot n \cdot 100\% \quad (2)$$

$$\xi_v = \left(\frac{(k-x)\cdot sz + p\cdot sz}{sz\cdot y^2} \right) \cdot v \cdot 100\% \quad (3)$$

$$\xi_s = \left(\frac{(k-x)\cdot \boldsymbol{s} + p\cdot \boldsymbol{s}}{\boldsymbol{s}\cdot y^2} \right) \cdot s \cdot 100\% \quad (4)$$

Формулы 2,3,4 определяют эффективность данной системы защиты для каждой категории рисков: формула 2 – для низкого риска, формула 3 – для высокого риска, и формула 3 – для среднего риска.

При этом:

k – количество каналов утечки в системе;

sz – количество систем защиты информации;

p – количество каналов утечки перекры-

ваемых несколькими средствами защиты информации;

n – количество каналов утечки с минимальным риском реализации;

s – количество каналов утечки со средним риском реализации;

v – количество каналов утечки с высоким риском реализации;

x – количество каналов не перекрываемых средствами защиты;

y – процентная оценка затруднения реализации пользователями своих функций после внедрения средств защиты.

Таким образом, нахождение оптимальных решений по разработке комплексных СЗИ, на основе внедрения DLP-систем, предполагает их интеграцию с другими подсистемами информационной безопасности, а также учет особенностей и свойств самой корпоративной системы. Поиск оптимальной архитектуры СЗИ требует учета всех функциональных возможностей DLP-систем, с учетом иных подсистем информационной безопасности. Эффективность системы защиты информации определяется набором критериев ее оценки, с учетом необходимости сохранения свойств иерархичности, синергичности и разнородности, используемых компонентов.

Примечания

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

2. Емельянников М.DLP-решения – это не панацея!//Информзащита Системный интегратор: [электр. ресурс]URL: http://www.infosec.ru/news/experts/2527 (дата обращения: 25.10.2017).

3. Безмалый В.Ф. Внедряем DLP?// ITBand: [электр. ресурс] URL: http://itband.ru/2009/08/%D0%B2%D0%BD%D0%B5%D0%B4%D1%80%D1%8F%D0%B5%D0%BC-dlp/ (дата обращения:26.10.2017).

4. Корпоративные информационные системы//Конспект лекций: [электр. ресурс] URL: http://sergeeva-i.narod.ru/inform/page501.htm (дата обращения: 27.10.2017).

5. Игнатова Ю.А. Классификация корпоративных информационных систем: реферат по информационному менеджменту. Университет ИТМО. – СПб, 2015. URL: http://iablov.narod.ru/igupit/kislec.htm (дата обращения: 27.10.2017).

6. Шабуров А.С., Журилова Е.Е., Лужнов В.С. Технические аспекты внедрения DLP-системы на основе Falcongaze Secure Tower // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2015. – № 4(16). – С. 57-67.

7. Борисов В.И., Шабуров А.С. О применении SIEM-систем для обеспечения безопасности корпоративных сетей // Инновационные технологии: теория, инструменты, практика. – Пермь, 2015. – С. 249-254.

8. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпортаивной сети на основе внелрения SIEM-системы // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2016. – №19. – С. 111-124.

9. Шабуров А.С., Журилова Е.Е. Модель выявления каналов утечки информации в автоматизированных системах на основе симплекс-метода // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – Пермь, 2017. – № 4(24).

References

1. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i opredeleniya.

2. Emel'yannikov M.DLP-resheniya – ehto ne panaceya![DLP-solutions is not a panacea] Informzashchita Sistemnyj integrator [Informsecurity System's itnegrator].

3. Bezmalyj V.F. Vnedryaem DLP? [Will we introduce DLP?] ITBand.

4. Korporativnye informacionnye sistemy [Corporate information systems] Konspekt lekcij [Abstract of lectures].

5. Ignatova YU.A. Klassifikaciya korporativnyh informacionnyh system [Classical corporate information system] Referat po informacionnomu menedzhmentu. Universitet ITMO [Essay of information menegment. ITMO University].

6. Shaburov A.S., Zhurilova E.E., Luzhnov V.S. Tekhnicheskie aspekty vnedreniya DLP-sistemy na osnove Falcongaze Secure Tower [Technical aspects of implementation of DLP-systems, based on falcongaze secure tower] Vestnik PNIPU. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [Vestnik PNIPU. Electrotechnics, information technologies, control systems]. №16. 2015. P. 57-67.

7. Borisov V.I., Shaburov A.S. O primenenii SIEM-sistem dlya obespecheniya bezopasnosti korporativnyh setej [About application of the SIEM-systems for ensuring safety of corporate networks] Innovacionnye

tekhnologii: teoriya, instrumenty, praktika [Innovation technologies: theory, instruments, practice]. P. 249-254.

8. Shaburov A.S., Borisov V.I. Razrabotka modeli zashchity informacii korportaivnoj seti na osnove vnelreniya SIEM-sistemy [Developing model information protection corporate network based on the implementation of SIEM-system] Vestnik PNIPU. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [Vestnik PNIPU. Electrotechnics, information technologies, control systems].№19. 2016. P.111-124.

9. Shaburov A.S., Zhurilova E.E. Model' vyyavleniya kanalov utechki informacii v avtomatizirovannyh sistemah na osnove simpleks-metoda [Model of identification of information leaks channels in automated systems based on the symplex method] Vestnik PNIPU. Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya [Vestnik PNIPU. Electrotechnics, information technologies, control systems].№ 24 2017.

ЖУРИЛОВА Елена Евгеньевна, студент, кафедры автоматики и телемеханики, Пермский национальный исследовательский политехнический университет. Адрес: 614990, Пермь, Комсомольский пр.,29. E-mail:ele11485995@yandex.ru

ШАБУРОВ Андрей Сергеевич, кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета. Адрес: 614990, Пермь, Комсомольский пр.,29. E-mail: shans@at.pstu.ru

ZHURILOVA Elena, student, Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail:ele11485995@yandex.ru

SHABUROV Andrey, Ph.D. of Technical Science at the Department of Automation and Telemechanics, Perm National Research Polytechnic University. 614990, Perm, 29, Komsomolsky pr. E-mail: shans@at.pstu.ru