УДК 004.056.5

ИСПОЛЬЗОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕСА

Е. А. Стрябкова, А.Н. Плохих
г. Белгород, Россия
Белгородский государственный
национальный исследовательский университет

Аннотация. Данная статья посвящена важности использования комплексных систем для обеспечения информационной безопасности бизнеса. Рассмотрены основные угрозы и риски, с которыми сталкиваются компании на современном этапе, и раскрыта необходимость внедрения программ для предотвращения утечки конфиденциальной информации. Проведена сравнительная характеристика DLP-систем и сделан вывод о целесообразности их применения в зависимости от размера бизнеса.

Ключевые слова: *комплексные системы, информационная безопасность, бизнес, угрозы, DLP-системы, программные продукты.*

THE USE OF INTEGRATED SYSTEMS TO ENSURE BUSINESS INFORMATION SECURITY

E.A. Stryabkova, A.N. Plokhikh
Belgorod, Russia
Belgorod State
National Research University

Annotation. This article is devoted to the importance of using integrated systems to ensure business information security. The main threats and risks faced by companies at the present stage are considered, and the need to implement programs to prevent the leakage of confidential information is disclosed. A comparative characteristic of DLP systems is carried out and a conclusion is made about the expediency of their use depending on the size of the business.

Keywords: *complex systems, information security, business, threats, DLP-systems, software products.*

Развитие экономики свидетельствует о развитии ее составляющей – бизнеса. С древних времен представители бизнеса (купцы и мануфактурщики) заботились о безопасности своего дела, в современном мире этому вопросу также уделяется большое внимание, но произошло изменение объекта защиты. Если раньше основной задачей было обеспечение физической сохранности имущества, то сейчас на первое место выходит экономическая составляющая. Бизнес вынужден для своего существования и развития использовать все корпоративные ресурсы для стабильного функционирования организации, предотвращения внешних и внутренних угроз, обеспечив тем самым экономическую безопасность.

Одной из основных составляющих экономической безопасности предприятия является информационная безопасность. В нашу жизнь стремительно вошли информационные технологии. На данном этапе развития невозможно представить хотя бы одну отрасль экономики, которую бы не коснулась цифровизация. Это повлекло за собой создание и использование программ, процедур и инструментов, позволяющих обеспечивать всестороннюю защиту от взлома компьютерных систем, несанкционированного доступа, раскрытия, изменения и уничтожения конфиденциальной информации.

Ускорил внедрение цифровых технологий карантин, введенный в результате распространения коронавирусной инфекции Covid-19. В период пандемии началось широкое использование формата видеоконференций для проведения совещаний и переговоров. Это, в свою очередь, обусловило создание специализированных платформ и защищенных каналов связи. Переход экономических процессов, которые предполагают обмен конфиденциальной информацией в онлайн-режиме поставил вопрос о ее защите. Созданные платформы, на которых проводятся торги, покупаются и продаются товары, заключаются миллионные сделки, обладают колоссальными секретными данными и не могли не заинтересовать людей, желающих завладеть незаконно этой информацией. Так, например, предприниматели, находившиеся на большом расстоянии от банков или друг от друга, получили возможность подписывать документ электронно. На данный момент в каждой организации любой предприниматель имеет электронный сертификат подписи, позволяющий удаленно подписать документ, который будет иметь юридическую силу, обладать такими же полномочиями, как и документ, подписанный собственноручно. Соответственно, незаконное обладание данной подписью может помочь незаконному обогащению, следовательно, возникает потребность в защите данных. Эта функция очень упростила и ускорила экономические процессы, но и создала дополнительные риски.

Преступники также стали активно пользоваться для совершения противоправных действий информационными системами. Учеными из Великобритании и Австралии было проведено исследование, посвященное изучению географии киберпреступности, по итогам которого был представлен первый в истории Мировой индекс киберпреступности, где Российская Федерация находится на первом месте (рис.1) [1]. Основными категориями киберпреступлений являются технологические продукты/услуги, атаки и вымогательства.

Rank	Country	I	P	TS	WCI Score	Tech	Attacks	Data	Scams	Cash
1	Russia	8.96	8.81	8.73	**58.39**	82.17	81.34	65.18	21.70	41.56
2	Ukraine	8.37	8.29	8.24	**36.44**	52.97	50.76	36.01	11.20	31.27
3	China	8.22	7.70	7.81	**27.86**	40.22	24.24	34.89	15.83	24.13
4	United States	7.99	7.21	7.21	**25.01**	27.64	17.68	30.36	22.72	26.63
5	Nigeria	8.25	6.49	5.80	**21.28**	7.93	8.41	23.04	52.17	14.86
6	Romania	7.12	7.04	7.15	**14.83**	17.83	9.17	22.50	13.15	11.49
7	North Korea	7.91	7.23	7.38	**10.61**	8.66	25.33	13.01	2.17	3.88
8	United Kingdom	7.86	7.21	6.75	**9.01**	5.04	4.75	5.80	7.86	21.63
9	Brazil	6.90	6.35	6.32	**8.93**	13.70	8.77	10.29	7.28	4.64
10	India	7.90	6.60	6.65	**6.13**	4.46	3.62	6.81	12.75	3.01
11	Iran	6.88	6.45	6.64	**4.78**	8.62	10.00	3.59	0.94	0.72
12	Belarus	6.84	7.20	7.32	**3.87**	11.92	5.58	1.85	--	--
13	Ghana	8.57	6.83	6.09	**3.58**	1.23	0.76	2.97	10.36	2.57
14	South Africa	6.95	5.35	5.50	**2.58**	1.20	0.65	0.58	7.17	3.30
15	Moldova	7.38	7.19	7.56	**2.57**	6.70	0.98	2.43	0.83	1.88

I = Impact; P = Professionalism; TS = Technical skill, Technical = *Technical products/services*, Attacks = *Attacks and extortion*, Data = *Data/identity theft*, Cash = *Cashing out and money laundering*. I, P, and TS are scored out of 10. 'WCI Score', and all columns following, are scored out of 100. Each country's top score across all cybercrime types is shaded in grey.

Рисунок 1 – Общий мировой индекс киберпреступности

Стоит отметить, что возросло также и количество угроз внутри фирмы. Связано это прежде всего с кадрами, так как сейчас большое количество работников предприятий имеют доступ к конфиденциальной информации и ее хранение производится не на отдельных компьютерах, а на общих серверах. Вместе с этим появились новые риски и угрозы, встали новые задачи по обеспечению защиты информации и контролю ее получения непосредственно работниками организации.

Основные угрозы, с которыми сталкиваются компании и учреждения на современном этапе:

- кибератаки;
- утечка данных;

- промышленный шпионаж;
- инсайдерское мошенничество;
- социальная инженерия.

Экспертно-Аналитическим центром InfoWatch вместе с ассоциацией BISA в сентябре 2023 года было проведено исследование путем анонимного опроса среди представителей компании, в результате которого было выявлено, что минимум 75% утечек конфиденциальной информации произошло по вине инсайдеров (сотрудников компании) и только 13% по вине внешних злоумышленников (рис. 2). При этом 54% случаев несанкционированного распространения информации было следствием умышленных действий персонала. В основном происходят утечки персональных данных (59%), коммерческой тайны (31%) и служебной тайны (23%) [5].

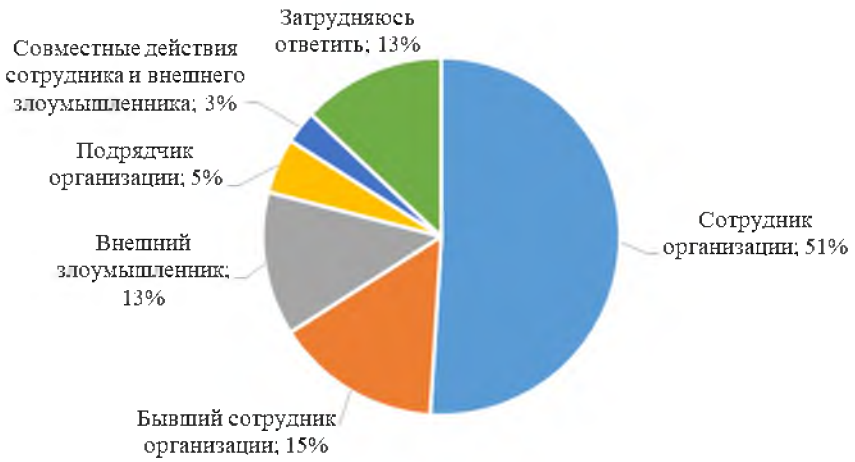

Рисунок 2 – Ответы респондентов на вопрос о виновнике инцидента

В крупных предприятиях появляются отделы, занимающиеся противодействием возникшим угрозам и защите информации организации от несанкционированного ознакомления, скачивания и внедрения в системы вредоносных программ. А для упрощения отслеживания, профилактики и расследования применяются комплексные системы. DLP-системы (Data Leak/Loss Prevention) – программные продукты, позволяющие обеспечивать комплексную защиту конфиденциальной информации от утечки. Внедрение данных систем способно повысить уровень информационной безопасности, снизить риск потери данных, соблюдать действующее законодательство и избежать штрафов, а также повысить конкурентоспособность и эффективность деятельности компании.

На рынке представлено множество DLP-систем, имеющих свои преимущества и недостатки. Они обладают схожим функционалом:

- выявляют и предотвращают утечки конфиденциальной информации, киберугроз, корпоративного мошенничества;
- мониторят как действия сотрудников, так и каналы передачи данных;
- ведут учет рабочего времени персонала и его продуктивность, благодаря которому возможен контроль прогулов и опозданий сотрудников;
- поддерживают контроль удаленных сотрудников;
- составляют поведенческий портрет персонала;
- уведомляют администраторов о подозрительных действиях пользователей;
- контролируют использование внешних устройств;
- блокируют несанкционированные действия;
- помогают в расследовании и предупреждении инцидентов;
- способствуют установлению компрометирующих связей;

- подготавливают отчеты в виде графика активности для руководителя компании.

Выбор комплексной системы должен основываться на потребностях конкретной компании, исходя из ее размеров и бюджета. Сравнительная характеристика популярных DLP-систем представлена в таблице 1 [2,3,4,6].

Таблица 1 – Сравнительная характеристика DLP-систем

Характеристика	DLP-системы			
	Solar Dozor	Falcongaze SecureTower	Стахановец	LanAgent
Потребители	Государственные учреждения и крупные компании	Государственные учреждения, крупные и средние компании	Государственные и негосударственные учреждения, крупные, средние и малые компании	Средние и малые компании
Преимущества	- единый интерфейс - созданы столы как для аналитиков, так и для руководителей; - встроен модуль поведенческого анализа с 20 паттернами поведения и расчетом индекса уязвимости сотрудников; - доступен контроль аномалий коммуникаций; - возможна запись видео с экрана рабочей станции	- предоставляет помощь в установке, настройке системы и обучении сотрудников; - позволяет назначить категории инцидентам; - производит анализ не только документов и текста, но также и изображений, цифровых отпечатков, голосовых сообщений и звонков; - доступен автоматический анализ поведения сотрудников	- имеет функционал на основе машинного обучения; - доступна скрытая установка клиентской части; - производит распознавание биометрических характеристик сотрудников; - позволяет осуществлять запись в видео-, аудиоформате и с помощью скриншотов веб-камер и микрофона; - возможно прогнозирование рисков	- имеет бюджетную стоимость; - доступна бессрочная лицензия; - возможна индивидуальная настройка в зависимости от рода деятельности сотрудников; - производит контроль печати на принтерах - позволяет осуществлять защиту от хакеров
Недостатки	- не рассчитан на малые и средние по размеру компании; - блокировка отправки данных возможна не во всех мессенджерах; - необходимы дополнительные виджеты для активации всех возможностей	- невозможна блокировка принтеров и сетевых каналов; - слабая интеграция со сторонними системами; - нацелена больше на мониторинг, чем на перехват утечек	- высокая стоимость; - оповещает работников о работе системы - нефункциональный интерфейс	- устаревший интерфейс; - отсутствие мобильной версии; - возможны проблемы при интеграции с другими системами безопасности
Поддержка операционных систем	Windows, Linux, macOS	Windows	Windows	Windows, macOS, Linux
Пробный период	3 недели	30 дней	30 дней	15 дней
Срок внедрения	От 1 месяца	От пары часов	От нескольких часов	От 15 минут до нескольких дней
Стоимость	От 600 000 руб. на 300 сотрудников	70 000 руб. лицензия	От 215 руб./чел.	79,9 руб./чел. единоразово

Из проведенного сравнительного анализа можно сделать вывод, что для крупных компаний наиболее целесообразно внедрение Solar Dozor, несмотря на высокую стоимость, данная DLP-система выполняет все необходимые функции для обеспечения информационной безопасности бизнеса. Среднем по размеру компаниям подходит Falcongaze SecureTower, так как он обладает широким функционалом и легко интегрируется с другими системами безопасности. LanAgent удобен для применения в малых компаниях, в связи с минимальными затратами на внедрение и обслуживание, также он обладает простым интерфейсом. Государственные и негосударственные учреждения могут использовать Стахановец для контроля за рабочим временем сотрудников и мониторингом их действий на рабочих станциях, что позволит обеспечить безопасность данных.

Таким образом, в сложившейся ситуации информационная безопасность хозяйствующих субъектов является важнейшей задачей для нормального функционирования бизнеса. Существующие киберугрозы и появляющиеся новые диктуют предприятиям необходимость использования комплексных систем, позволяющих пресекать сразу ряд угроз. Такие программы затратоемкие, так как требуют не только установку, но и обслуживание. Крупные представители бизнеса, имеющие отделы по экономической безопасности, используют системы с расширенными возможностями, для среднего и малого бизнеса можно подобрать программные продукты по более низкой цене, но со схожим функционалом. Комплексные системы, помимо основных функций по защите и контролю, используются также для мониторинга эффективности использования рабочего времени и учета нагрузки персонала. Внедрение комплексных систем позволяет работать предприятию более эффективно и защищать информационные системы от несанкционированного входа и передачи информации, вредоносных программ, способных нанести системам компании урон.

ЛИТЕРАТУРА

1. Bruce M., Lusthaus J., Kashyap R., Phair N., Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index. 2024. [Электронный ресурс]. – Режим доступа: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312#references (Дата обращения: 12.04.2024)

2. Falcongaze SecureTower [Электронный ресурс]. – Режим доступа: https://falcongaze.com/ru/russian-dlp-system.html (Дата обращения: 18.04.2024).

3. LanAgent [Электронный ресурс]. – Режим доступа: https://lanagent.ru/dlp-systemi-stoimost.html#6 (Дата обращения: 18.04.2024).

4. Solar Dozor [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/products/solar_dozor/ (Дата обращения: 18.04.2024).

5. Осведомленность сотрудников организаций об утечках информации [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/analitika/osvedomlennost-sotrudnikov-organizatsiy-ob-utechkakh-informatsii (Дата обращения: 17.04.2024).

6. Стахановец [Электронный ресурс]. – Режим доступа: https://stakhanovets.ru/dlp/ (Дата обращения: 18.04.2024).

7. 26 лучших программ для контроля рабочего времени сотрудников 2024: преимущества, недостатки, сравнительный анализ [Электронный ресурс]. – Режим доступа: https://martsoft.ru/articles/26_programm_dlya_kontrolya_rabochego_vremeni_sotrudnikov/#h2-9 (Дата обращения: 19.04.2024).