ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИЕ МЕРЫ ПО ЗАЩИТЕ ПРЕДПРИЯТИЯ ОТ ПРОМЫШЛЕННОГО ШПИОНАЖА И ФИШИНГОВЫХ АТАК

В.В. Филатов, В.В. Кудрявцев, Е.Е. Родина, С.М. Пащук
Московский государственный университет технологий и управления им. К.Г. Разумовского, г. Москва

В последние годы решению проблем информационной безопасности посвящены работы школ ряда научных направлений – по разработке информационных технологий, программных продуктов, в том числе и защитного плана, по разработке компьютерного оборудования, по обоснованию правовых основ, а также по реализации организационно-управленческих систем, имеющих целью – обеспечение информационной безопасности бизнеса (для любой организации по масштабам, подчиненности, расположению).

Известны работы Клейменова С.А. и Мельникова В.П.[1], Степанова Е.А., Балдина К.В., Уткина В.Б.[2], Гафнер В.В.[3], Исаева Г.Н.[4] , Тарасова А.В.[5], Петрова С.В., Слиньковой И.П. [6], Шаньгина В.Ф.[7], Кострова А.В.[8], Рудаковой О.С., Родиной Ю.В.[9], Абрамова М.А.[10] и других ученых. Следует отметить, что значительное число разработок имеет техническую направленность и вследствие этого реализуются специальным персоналом по информационному сопровождению бизнеса. Кроме того, несмотря на растущее внимание к исследованиям в области информационной безопасности, вопросы управления процессом обеспечения информационной безопасности предприятий и организаций не получили всестороннего исследования.

На сегодняшний день рынок IT заполонен невообразимым количеством технологий, каждая из которой направлена на улучшение какого-либо аспекта работы с информационными ресурсами, будь то хранение, обработка, передача или что-то другое. Обладая рядом серьезных преимуществ, данные тенденции влекут за собой еще больший объем угроз и уязвимостей[11].

Ежегодно данные отчётов ведущих компаний об утечках информации и их последствиях: частичное или полное приостановление деятельности предприятий, огромные финансовые потери, говорят о необходимости не только обеспечения ИБ, восстановлении информации после сбоя работы систем, но и об обеспечении комплексного управления информационной безопасностью (ИБ). Отчёт компании InfoWatch, опубликованный на официальном сайте в прошлом году (рис.1), говорит о росте числа утечек защищаемой информации.

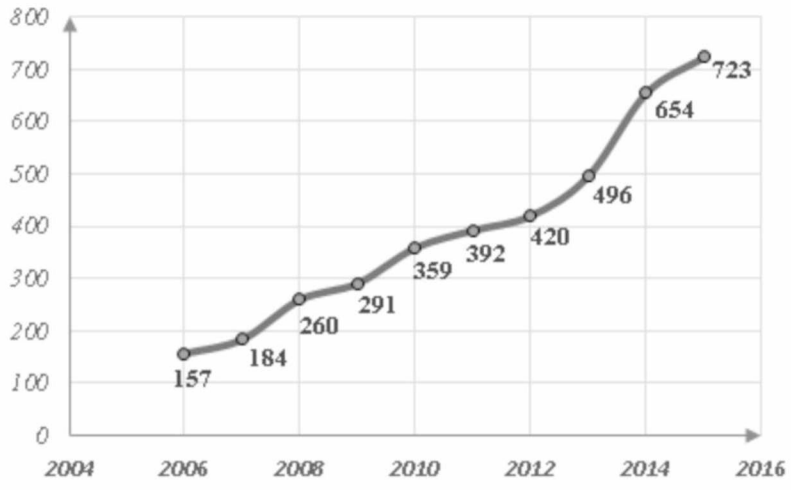

Рисунок 1 - Результаты исследования утечек информации компанией InfoWatch[12]

Атаки с использованием вредоносного ПО — это самый опасный инструмент, обладающий высокой эффективностью. Его применение практически в половине случаев приводит к утечке информации. При применении промышленного шпионажа пятая часть случаев заканчивается потерей конфиденциальной информации, а в случае с фишинговыми атаками — в 14% случаев. Основным последствием любой атаки в случае ее успешного осуществления становится утрата предприятием конфиденциальной информации. В целом по Российской Федерации эффективность внешних атак выросла на 5 п. п., и четверть предприятий за истекший год утратили важную информацию. При всем многообразии внешних угроз они далеко не исчерпывают перечень проблем информационной безопасности[13]. Не менее опасны внутренние угро-зы предприятий. Основной внутренней угрозой на предприятиях остается уязвимость в ПО, далее случайные утечки по вине сотрудников, вызванные в основном незнанием утвержденных на предприятиях правил и на третьем месте, утечки информации, вызванные преднамеренным действием сотрудников.

Наиболее распространенный инструмент обеспечения информационной безопасности на предприятиях по всему миру — это антивирусная защита. 60% респондентов сообщили, что на рабочих станциях предприятий за исследуемый период установлено защитное ПО. Однако эта мера внедряется очень активно, поэтому ее актуальность с течением времени серьезно уменьшались. Снизилась и популярность такой меры, как управление обновлением ПО, включающей регулярную установку обновлений ПО, хотя она про должает оставаться на втором месте в данном рейтинге. Вырос интерес к контролю приложений, что привело к тому, что он вошел в тройку лидеров. Потеряло свои позиции шифрование информации на рабочих станциях сотрудников компании. Все эти тенденции связаны с высоким уровнем распространения указанных мер информационной безопасности в практике защиты на предприятиях. Так, антивирусное ПО, обновление программ, шифрование данных входит в стандартный перечень средств информационной безопасности, который применяется на российских предприятиях. Именно поэтому респонденты все чаще не включают их в список важных инструментов. При этом появились и новые актуальные инструменты, такие как внедрение систем для защиты финансовых транзакций, технологий защиты мобильных устройств, а также средств поддержания работоспособности вебсервисов и защиты от DDoS-атак[14].

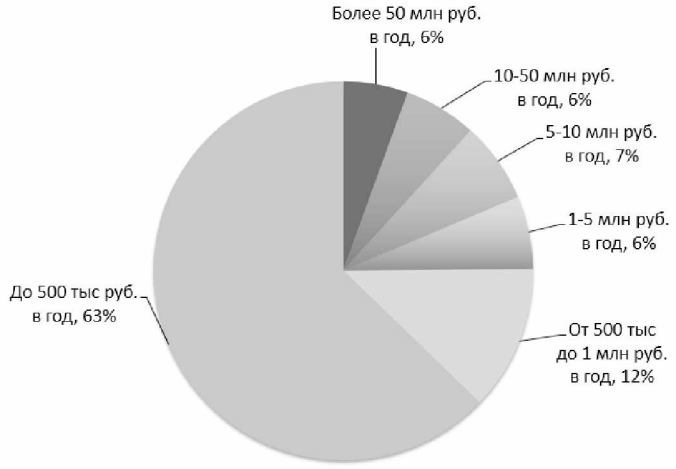

Рисунок 2 - Размер бюджета на информационную безопасность в год[16].

Бюджеты на информационную безопасностью. Наиболее интересной оказалась статистика по размерам бюджетов, выделяемых на информационную безопасность в опрошенных российских организациях. В 63% компаний на ИБ выделяется минимальный бюджет — до 500 тыс. руб. в год, см. рис.2. Еще 12% опрошенных имеют годовой бюджет от 500 тыс. до 1 млн. руб. в год. Только 12% респондентов

могут похвастаться бюджетом на ИБ более 10 млн. руб. в год. Из них лишь 6% крупных компаний имеет бюджет на ИБ более 50 млн. руб. в год. 7% опрошенных располагают бюджетом от 5 до 10 млн. руб. в год, и еще 6% — бюджетом от 1 до 5 млн.руб. в год [15]. Как видно, у подавляющего числа российских компаний на информационную безопасность выделяются минимальные бюджеты, которых может хватить лишь на базовые средства защиты (такие как антивирусы или межсетевые экраны).

В результате приоритетных направлений развития ИБ оказалось несколько, см. рис.3. В равной мере для опрошенных организаций оказались актуальны задачи защиты от внутренних угроз (включая утечки информации), автоматизации процесса управления ИБ, защиты периметра и создания SOC (центров оперативного мониторинга, анализа и реагирования на инциденты).

Рисунок 3 - Приоритетные направления развития информационной безопасности[16].

Подводя итог, можно отметить, что даже увеличение внимания к решению проблем информационной безопасности, внедрение точечного и прагматичного подхода не привело к снижению инцидентов информационной безопасности и количество успешных сценариев реализации информационных угроз продолжает увеличиваться. Безусловно, предприятия стали особенно глубоко вникать в суть существующих рисков, что доказывает увеличение внимания к защите данных от таргетированных атак.

Библиографический список

1. Мельников В.П., Клейменов С.А., Петраков А.М. Под ред. С.А. Клейменова. Информационная безопасность и защита информации // М.: Издательство «Академия». – 2008. – 336 с.
2. Балдин, К.В., Уткин. В.Б. Информационные системы в экономике: Учебник // М.: Издательско-торговая корпорация «Дашков и Ко». – 2006. – 395 с.
3. Гафнер В.В., Информационная безопасность: Учебное пособие // Ростов н/Д: Феникс. – 2010. – 324 с.
4. Исаев Г.Н. Информационные системы вэкономике: Учебник для студентов вузов,обучающихся по специальностям «Финансы и кредит», «Бухгалт. учет, анализ и аудит». – 6-е изд. // М.: Издательство "Омега-Л". – 2013. – 462 с.
5. Тарасов, А.В. Управление промышленным предприятием на основе формирования эффективной системы информационной безопасности // автореф. дис... канд. эконом, наук. Орел: ОГТУ. – 2006. –24с.

6. Петров С.В., Слинькова И.П., Гафнер В.В. Информационная безопасность:Учебное пособие // М.: АРТА. – 2012. – 296 с.
7. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие // М.: ИД ФОРУМ, НИЦ ИНФРА-М. – 2013. – 416 с.
8. Костров А.В. Основы информационного менеджмента // Финансы и статистика. 2001. – 336 с.
9. Рудакова О.С., Родина Ю.В. Анализ угроз информационной безопасности кредитных организаций // Национальные интересы: приоритеты и безопасность. –2009. – №23(56). – С. 61-67.
10. Филатов В.В., Борисова Т.А., Медведев В.М., Шестов А.В., Фадеев А.С. Прогнозы и ключевые тенденции глобального рынка IT // Интернет-журнал Науковедение. – 2015. – Т. 7. – № 1 (26). – С. 48.
11. Козунова С.С. Система управления информационной безопасностью предприятия // Евразийский Союз Ученых (ЕСУ). – №7 (28). – 2016. – С. 22-24.
12. Филатов В.В., Дадугин М.В. Региональные аспекты управления информационно-экономическим развитием современных инновационных предприятий на основе внедрения системы контроллинга // Вестник Университета (Государственный университет управления). – 2012. – № 14-1. – С. 141-149.
13. Балановская А. Анализ современного состояния угроз информационной безопасности предприятий // Информационная безопасность регионов. – 2015. № 3(20). – С.9-16.
14. Родина Е.Е., Петрякова Ю.И. Бюджетирование в системе контроллинга. // Московский экономический журнал. – 2017. – № 4. – С. 77.
15. Шабанов И. Анализ рынка информационной безопасности в России. Часть 1 [Электронный ресурс] // URL: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1
16. Шабанов И. Анализ рынка информационной безопасности в России [Электронный ресурс] // URL: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-3