УДК 334.02:65.011.56

© Р. А. Сейткереев, *2016*
Институт инновационных и телекоммуникационных систем, г. Уральск, Республика Казахстан
E-mail: rubek74@mail.ru

СОСТОЯНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В СОВРЕМЕННЫХ УСЛОВИЯХ

Анализируются внешние и внутренние угрозы информационной безопасности, которые наиболее сильно влияют на деятельность предприятий РФ. Как следствие реализации данных угроз, автором выделяются приоритеты специалистов в сфере информационных технологий и безопасности, а также приводятся наиболее распространенные инструменты и средства защиты, обеспечивающие на предприятиях информационную безопасность. Автор приводит ряд рекомендаций по повышению эффективности управления информационными угрозами на предприятии.

Ключевые слова: информационная безопасность, информационные угрозы, утечка, атака, защита.

Вопрос информационной безопасности предприятий в настоящее время является максимально актуальным. Это связано с очень серьезным уровнем информатизации хозяйственной деятельности и общества в целом, в том числе и в глобальном аспекте, повсеместным внедрением во все сферы человеческой деятельности информационных ресурсов, которые зачастую выдавливают другие виды ресурсов. В эпоху становления и развития глобальной информационной экономики противодействие различным угрозам и вызовам, рожденным этой эпохой, становится серьезной проблемой, которая затрагивает вопросы обеспечения всестороннего устойчивого функционирования и развития как современного мира, так и отдельно взятых объектов в текущей и стратегической перспективах [5, с. 94].

На сегодняшний день IT-рынок 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 [6, с. 1]. Обладая рядом серьезных преимуществ, данные тенденции влекут за собой еще больший объем угроз и уязвимостей. Выход каждой последующей усовершенствованной новой версии продукта влечет за собой определенные уязвимости, которые могли уже предостав-

ляться с первоначальной версией, а часто появляются еще и дополнительные уязвимости. Это только способствует все большему проникновению в корпоративные сети, краже информации и другим негативным моментам. Существующее огромное количество информационных источников, легко доступных вспомогательных программных средств способствуют процветанию интереса к чужой информации, серверам, станциям, компьютерам. И зачастую может быть вызвано обыкновенным любопытством. Даже в этом случае предприятиям наносится ущерб. И, безусловно, ущерб будет совершенно не соизмерим в случае, если атака носит таргетированный характер.

Такое развитие информационных угроз в современном мире повлекло за собой необходимость проведения различных систематических исследований, направленных на выявление новых тенденций, изучение наиболее эффективных методов борьбы и предотвращения, трансляцию накопленного опыта в вопросах управления информационной безопасностью предприятий. Международные и российские аналитические центры и аудиторско-консалтинговые компании, такие как InfoWatch, PwC, «Лаборатория Касперского», проводят подобные исследования. Так, в исследовании, проводимом в 2012 году «Лабораторией Касперского», 44% российских специалистов в сфере информационных технологий и безопасности включили информационные угрозы в тройку наиболее значимых угроз для предприятий, и в итоге они заняли вторую строчку в общем рейтинге [4, с. 3]. При этом около трети всех респондентов указали, что в течение последнего года наблюдается значительное увеличение их количества и, по их мнению, актуальность этой проблемы с течением времени будет только неуклонно расти. Что, безусловно, подтверждается сегодняшними реалиями и обосновывается постоянно выявляющимся количеством новых видов вредоносного программного обеспечения (ПО) и новых видов атак. Так, если в 2013 году количество ежедневно появляющихся новых образцов вредоносного ПО оценивалось на уровне 200 тыс. [5, с. 5], то в 2014 году это показатель достиг 315 тыс. образцов ежедневно [3, с. 7]. При этом следует отметить, что только 4% опрошенных имеют объективное представление о масштабах угроз, тогда как больше 95% эти угрозы очень серьезно недооценивают.

Хотя ежегодно возрастает уровень осознания проблемы обеспечения информационной безопасности, многие предприятия в настоящий момент не готовы к эффективной борьбе с киберпреступностью в силу ряда причин.

Кроме того, единой оптимальной структуры защиты информации не существует, так как каждая организация — участник информационных процессов имеет свой собственный, отличающийся от других, набор требований, проблем и приоритетов, продиктованных объективными экономическими, производственными, социальными условиями функционирования данного предприятия [1, с. 115].

Безусловно, всем придется учиться жить в условиях, когда предприятиям любого размера в любой стране мира регулярно придется сталкиваться с инцидентами информационной безопасности. Так, в РФ этот показатель имеет неуклонную тенденцию к увеличению и, более того, уже приближается к 100%. 98% российских предприятий за истекший год столкнулись с инцидентом информационной безопасности, который был вызван действием внешнего фактора. Также за этот период выросло количество предприятий, подвергшихся внешним атакам, на 3 п. п. Не менее важно учитывать и внутренние угрозы информационной безопасности.

Такое распределение угроз по типам становится основой для построения системы информационной безопасности для конкретного предприятия, а на его основе осуществляется организационная защита. В настоящее время в теории информационной безопасности существует ряд классификаций рисков и угроз защиты информации, наиболее часто используемых в практике. В нашем исследовании интерес представляет разделение угроз на внешние и внутренние. Эта классификация предполагает разделение по локализации злоумышленника (или группы). Так, получая доступ к конфиденциальной информации предприятия, он действует удаленно, либо же посредством доступа к внутренним ресурсам и соответствующей инфраструктуре объекта атаки.

В случае с внешними атаками осуществляется поиск уязвимости в информационной структуре для доступа к основным узлам, хранилищам, персональным компьютерам сотрудников, организационной сети и т. д. Инструментами выступают вирусы, черви, трояны, которые принято называть вредоносным ПО. Его используют для нанесения вреда объектам, копирования, видоизменения, шпионажа, отключения систем защиты, уничтожения и т. д.

Для реализации внутренних угроз требуется один или несколько сотрудников предприятия, действия которых в случае необходимости, по умыслу или непреднамеренно, могут повлечь утечку конфиденциальной или ценной информации.

На протяжении нескольких лет самой значимой угрозой специалисты называют вредоносное ПО, практически не отстает от него спам, который часто является носителем вредоносного ПО. Увеличилась доля тех, кто столкнулся с фишинговыми атаками. Наблюдается и серьезный рост количества отказов в обслуживании, выросла и доля корпоративного шпионажа. Корпоративный шпионаж в основном касается крупных предприятий. По всем остальным пунктам внешние угрозы также демонстрируют тенденцию к росту.

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. Не менее опасны внутренние угрозы 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.

Однако следует отметить, что основные показатели имеют тенденции к сокращению. Это объясняется более активным внедрением в практику процессов обновления ПО в связи с осознанием опасности реализации данной угрозы.

В результате все эти угрозы также приводят к потере конфиденциальной информации. Так, около четверти предприятий, подвергшихся воздействию внутренних угроз, утратили важную информацию.

Хотя для целей кражи любого типа сведений наиболее опасными являются уязвимость в ПО и случайные утечки информации, к наихудшим последствия приводят преднамеренные действия сотрудников с целью передачи информации. Так практически в 10% похищается критически важная для предприятий информация. Для

остальных инцидентов показатель критичности имеет существенно более низкие значения.

Изучение внешних и внутренних угроз, с которыми столкнулись предприятия в последнее время, говорит о необходимости внедрения комплексных решений в сфере обеспечения информационной безопасности. Наличие инцидентов реализации угроз говорит о том, что инфраструктура по обеспечению информационной безопасности развита недостаточно хорошо и защита неэффективна.

Для выяснения причин сложившихся тенденций интерес представляет изучение приоритетов специалистов в области информационных технологий и информационной безопасности в деле обеспечения организационной защиты.

Достаточно долго в данном списке лидировал вопрос защиты данных, который в этом году переместился на вторую строчку, уступив место защите данных (данных о клиентах, финансовой информации и др.) от таргетированных атак. А третью строчку заняла задача обеспечения бесперебойной работы критически важных систем. Такое изменение в тройке лидеров может быть вызвано упоминанием за истекший период в различных источниках о ряде громких целевых атак, как в нашей стране, так и за ее пределами, которые увенчались успехом, и в руки нарушителей попала информация о миллионах клиентов и партнеров. Конечно, для крупного бизнеса, а в особенности для промышленных предприятий, эта проблема имеет серьезное значение. Рос интереса к обеспечению бесперебойности работы также может быть вызван рядом событий в отношении нескольких российских банков. Следует отметить, что «Лаборатория Касперского» зафиксировала новый скачок мощности DDoS-атак в Рунете. Средняя мощность атаки составляла 70–80 Гб/с, а в пиковые моменты превышала 100 Гб/с. Такие показатели стали новым рекордом для российского сегмента Глобальной сети. В 2013 году самая мощная DDoS-атака в Рунете не превышала порога в 60 Гб/с [2, с. 5].

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 веб-сервисов и защиты от DDoS-атак. Кроме того, почти четверть респондентов отметили в качестве новой меры безопасности применение систем для защиты от утечек данных. Однако, несмотря на это, предприятий, где признают важность применения дополнительных средств защиты, пока недостаточно. С одной стороны, это вызвано недооценкой лицами, принимающими решения, важности обеспечения информационной безопасности, с другой стороны, перечень угроз ежегодно меняется и очень сложно успевать за ним, обеспечивая системам информационной защиты максимально актуальное состояние. Практически на всех предприятиях присутствует принцип реагирования уже по факту свершившихся угроз. Однако, это не всегда оправданно, так как зачастую последствия реализации информационных угроз для предприятий могут носить критичный и даже летальный характер.

В большинстве случаев инцидент информационной безопасности приводит к нарушению бизнес-процессов на предприятии. Серьезный ущерб наносится и репутации предприятия. Очень часто инциденты парализуют работу предприятия, т. к. наступает утрата доступа к важной информации, которая хоть и носит временный характер, но доставляет массу неудобств и приводит к более серьезным последствиям. В результате предприятию грозят расторгнутые договоры, упущенные возможности в развитии хозяйственной деятельности, незапланированные траты и т. д.

Подводя итог, можно отметить, что даже увеличение внимания к решению проблем информационной безопасности, внедрение точечного и прагматичного подхода не привело к снижению инци-

дентов 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. Однако, как известно, их количество постоянно растет в связи с ростом спроса на них, и более того, они уникальны и готовятся адресно, с учетом специфики, поэтому противостоять им крайне сложно.

В заключение отметим, что существующее разнообразие информационных угроз и динамика их изменения не позволяют предприятиям найти единственное решение, которое избавило бы от всех проблем обеспечения информационной безопасности. Внедрение современных и эффективных решений защиты IT-инфраструктуры предприятия и управление ею позволит существенно повысить уровень безопасности предприятия в целом. Однако следует постоянно мониторить все информационные угрозы, следить за актуальными тенденциями развития угроз и средств защиты, планомерно и обдуманно выбирать и внедрять необходимое обеспечение, сохранять высокий уровень знания сотрудниками (связанных и не связанных с IT-технологиями) сферы информационной безопасности. В результате комплексное применение вышеуказанных мер позволит существенно снизить влияние угроз и обеспечить высокий уровень защиты предприятия.

Литература

1. Волкодаева А. В. Проектирование эффективной системы информационной безопасности // Вестник Самарского муниципального института управления. 2015. № 2. С. 115–124.

2. Информационная безопасность бизнеса // Результаты исследования. «Лаборатория Касперского». 2014. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf.

3. Информационная безопасность бизнеса // Результаты исследования. «Лаборатория Касперского». 2013. URL: http:// http://media.kaspersky.com/pdf/IT_risk_report_Russia_2013.pdf.

4. Информационная безопасность бизнеса // Результаты исследования. «Лаборатория Касперского». 2012. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2012.pdf.

5. Сейткереев Р. А. Перспективы управления глобальными экономическими процессами в условиях воздействия информационных угроз // Вестник Самарского муниципального института управления. 2015. № 2. С. 94–101.

6. Филенко Е. С. Угрозы информационной безопасности и возможные пути решения // Концепт: электронный журнал. 2013. Современные научные исследования. Выпуск 1. URL: http://e-koncept.ru/2013/53521.htm.

Статья поступила в редакцию 20.01.16 г.
Рекомендуется к опубликованию членом Экспертного совета д-ром экон. наук, доцентом О. А. Булавко