Отдельные аспекты информационной безопасности на предприятии

Гладких Евгений Леонидович

Магистрант MEHG-162 РГЭУ (РИНХ) г. Ростов-на-Дону

E-mail: ros.lom.vd@gmail.com

Соавтор ***Неделько Станислав Иванович***

Магистрант ЭKGZ-551 РГЭУ (РИНХ) г. Ростов-на-Дону

E-mail:stas630023@mail.ru

Аннотация

В данной статье рассмотрена проблема информационной безопасности компаний. Проанализированы основные факторы, способствующие увеличению уязвимости конфиденциальных данных. Выявлена и обоснована необходимость защиты информации на предприятии от кибератак, приведены статистичексие данные финансовых потерь от атак за предыдущий год. На основе проведенного исследования автором предлагается произвести комплексный подход к защите информации.

Ключевые слова: информация, информационная безопасность, информационные угрозы, кибератака, вирус, финансовые потери, кибербезопасность, киберугроза, стратегия, информационная защита

Keywords: data, data security, data threats, cyber attack, virus, financial losses, cyber security, cyber threat, strategy, data protection

В современном мире, быстрое развитие производства тесным образом находится в зависимости от информатизации управления. Информация занимает важнейшую часть при производстве товаров и услуг как ресурс и как товар. Все процессы, происходящие на производстве так или иначе связаны с информацией, которая необходима чтобы снизить риск при принятии решений. Информация является стратегическим ресурсом, от которого зависят конкурентоспособности организаций.

Информация – это ресурс, который, как и другие важные бизнес-ресурсы, имеет определенную ценность для организации, а это значит, что она нуждается в соответствующей защите. Таким образом обеспечение информационной безопасности является необходимым условием функционирования любой компании, а создание политики безопасности – одно из первых требований к организации информационной безопасности предприятия.

Компьютеры обслуживают промышленные, торговые, строительные предприятия, банки, распределяют энергию, следят за расписанием поездов и т.п. Компьютерные системы хранят информацию, обрабатывают её и предоставляют потребителям. При развитии вычислительной техники и информационных технологий увеличивалась сложность систем защиты компьютерной информации. Конкуренция между предприятиями ставит на первый план вопрос информационной безопасности.

Вице-президент корпорации SymantecSecurity, Артур Вонг, являющаяся мировым лидером в сфере информационной безопасности, говорит, что «злоумышленники предпринимают все более изощренные атаки, пытаясь нарушить целостность корпоративных и личных данных» . В связи с

развитием и усложнением средств и методов автоматизации процессов информационной обработки, увеличивается её уязвимость. Основными факторами, которые способствуют увеличению уязвимости, являются:

- рост объема информации, которая накапливается, хранится и обрабатывается с помощью ЭВМ и других автоматизированных средств;
- единые базы данных информации разного характера и принадлежностей;
- расширение круга пользователей, которые имеют непосредственный доступ к ресурсам вычислительной системы и находящимся в ней данных;
- сложность режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, режимов разделения времени и режима реального времени;
- автоматизация межмашинного обмена информацией.

Источники информационных угроз могут быть как внутренними, так и внешними. Чаще всего такое деление происходит по территориальному признаку и по признаку принадлежности к объекту информационной защиты (таблица 1).

Таблица 1

Источники информационных угроз

Источники внешней опасности	Источники внутренней опасности
разведка	сотрудники
конкуренты	-с корыстными целями
политические противники	-с преступными целями
преступники	"любители"
лица с нарушенной психикой	безответственные
стихийные бедствия	

Соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать так:

- -82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;
- -17% угроз совершается извне — внешние угрозы;
- -1% угроз совершается случайными лицами.

Информационные угрозы имеют векторный характер, т.е. всегда преследуют определенные цели и направлены на конкретные объекты.

Источниками конфиденциальной информации являются люди, документы, публикации, технические носители информации, технические средства обеспечения производственной и трудовой деятельности, продукция и отходы производства.

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих

правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Каждая компания часто сталкивается с проблемами информационной безопасности. В Российской Федерации данная проблема с каждым годом увеличивается. В результате опроса, было выявлено, что за год около 98% компаний в России сталкиваются с инцидентами безопасности информации, которые вызваны факторами извне. За 12 месяцев на 3 п.п. растет количество организаций, подвергнутых кибератакам.

Самая значимая из внешних угроз, около 77%, это вредоносное программное обеспечение. 74% составляют нежелательные электронные письма, хотя спам очень часто содержит в себе вирус или ссылку на фишинговый сайт. К тому же, фишинговые сайты в 2014г. составляли также одну из самых значимых внешних угроз – 28%.

Количество DDoS-атак увеличилось за год с 13% до 18% - в октябре 2013 года группа хакеров провела атаку на несколько ключевых российских банков, а весной 2014 года хакерскими организациями, такими как Anonymous Caucasus, была совершена серия мощных DDoS-атак на СМИ, различные государственные и окологосударственные сервисы.

В 2014 году значительно выросла доля корпоративного шпионажа – в основном за счет сильного роста количества таких инцидентов в крупных организациях (почти треть компаний, 32%). В СМБ-сегменте этот показатель существенно ниже – 19%. По всем остальным пунктам внешние угрозы также демонстрируют тенденцию к росту (рис.1).

Рис.1 Статистика атак

Кибератаки несут значительные финансовые потери для компаний. Опрос респондентов по поводу прямых финансовых убытков при кибератаках, о дополнительных расходах, показал, что

убытки от инцидента складываются из расходов на профессиональные сервисы (внешние специалисты по информационной безопасности, юристы, специалисты по связям с общественностью и т.д.), упущенных бизнес-возможностей (испорченная репутация, срыв контрактов из-за инцидента и т.п.), а также ущерба от вынужденного простоя IT-инфраструктуры компании и приостановки бизнес-процессов.

Результат показал, что в среднем от одного инцидента информационной безопасности крупные компании потеряли около 20 млн. рублей, а компании сегмента СМБ – около 780 тыс. рублей.

За 2014 год сумма средних потерь для небольших компаний выросла более чем на 100 тыс. рублей, в то время как для крупных компаний она снизилась (рис.2).

Рис.2 Потери от кибератак

Значительная часть суммы потерь компаний в результате серьезного инцидента информационной безопасности - это дополнительные расходы на устранение последствий инцидента и предотвращение подобных происшествий в будущем.

Общая оценка дополнительных затрат складывается из расходов на подбор дополнительного персонала, проведение тренингов по информационной безопасности для сотрудников и приобретение программного обеспечения и аппаратуры для защиты информационных систем компании от внешних и внутренних инцидентов в будущем. Для средних и малых компаний эти расходы составляют около 324 тыс. рублей, для крупных – около 2,2 млн. рублей (рис.3).

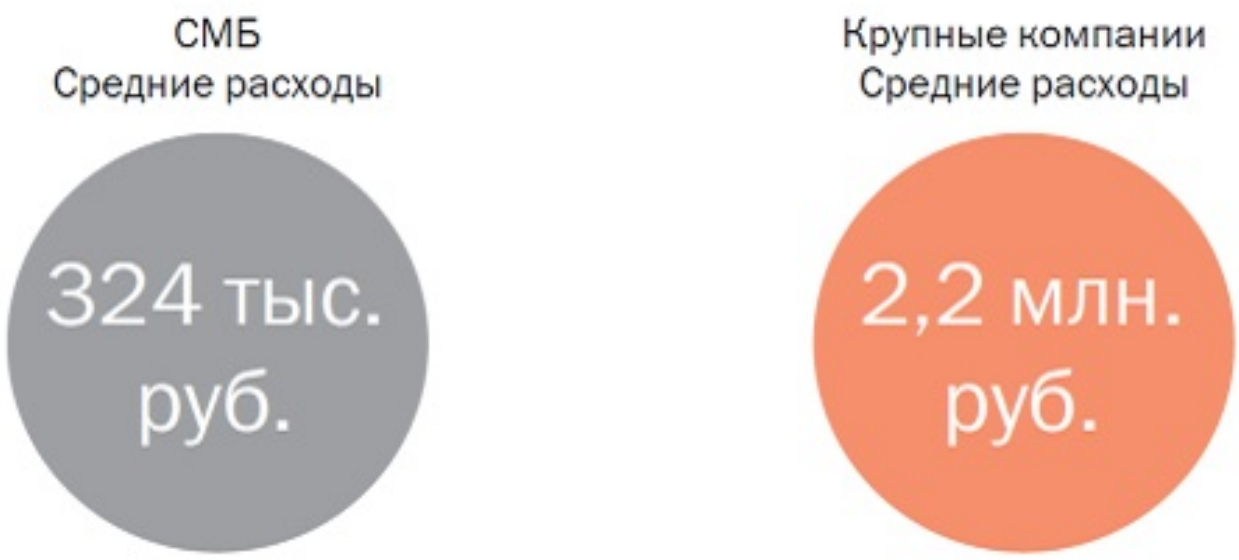

Рис.3 Дополнительные расходы компаний

Помимо финансовых потерь, инцидент информационной безопасности приводит к репутационному ущербу. Так, за исследуемый период 59% компаний были вынуждены публично признать произошедшее и раскрыть конфиденциальную информацию. В 33% случаев компания уведомляла клиентов, которые могли пострадать в результате инцидента, в 28% случаев – партнеров, и в 27% – поставщиков. Крупные корпорации в большинстве случаев обязаны сообщить об инциденте регулятору, клиентам и прессе, что наносит серьезный удар по деловой репутации таких компаний (рис.4)

Рис.4 Репутационный ущерб

Главный вывод, который можно сделать на основании результатов опроса, заключается в том, что несмотря на более прагматичный и точечный подход российских компаний к обеспечению информационной безопасности своей IT-инфраструктуры, количество успешных атак на бизнес продолжает расти.

Чтобы защитить информацию, одной антивирусной программы недостаточно. Сейчас при росте целевых атак, которые направленны на похищение конфиденциальной информации, а также денег, актуальность информационной безопасности выросла. Необходим комплексный подход к защите данных.

Защита не будет эффективной без обучения сотрудников и внедрения политик безопасности. Как показали результаты опроса, значительная часть инцидентов информационной безопасности, приводивших к утечке конфиденциальных данных, происходила по вине сотрудников компании, случайно или намеренно провоцировавших потерю ценной информации. Для того чтобы избежать случайных утечек, компаниям следует повышать уровень образованности сотрудников в области информационной безопасности. Особенно это касается обращения с корпоративной информацией, хранящейся на мобильных устройствах.

Политики безопасности, определяющие ответственность сотрудника за распространение конфиденциальной информации, – еще одна мера, которая может существенно повысить уровень защищенности корпоративных данных.

Вопрос об информационной безопасности в России давно назрел, и его следует решать комплексно. Необходимо отметить, что руководство России понимает серьезность существующих проблем, и на уровне ведущих ведомств разрабатываются различные меры по исправлению ситуации и предупреждению возможных негативных последствий. Так, Совет Федерации Федерального Собрания РФ в 2012 году разработал «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации».

В настоящее время на публичное обсуждение представлена вторая редакция проекта Федерального Закона «О безопасности критической информационной инфраструктуры российской федерации». ФСТЭК разрабатывает технические рекомендации по информационной защите АСУ ТП критически важных объектах.

Помимо законодательной базы, конечно, должны быть разработаны и типовые отраслевые методики построения защищенной инфраструктуры КВО; выработаны критерии оценки защищенности инфраструктуры, которые в необходимых случаях могут оперативно дорабатываться и адаптироваться под изменения ландшафта угроз; разработаны также методы стимулирования и юридической поддержки критически важных объектах; подготовлены и реализовываться образовательные программы для работников и управляющих. Ведь надежную защиту способно обеспечить только реальное сотрудничество государства, владельцев компаний и других участников рынка.

Библиографический список

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2012. - 324 с.
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2013. - 384 с.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.