Петросян Ани Артуровна
студентка
Крюкова Ксения Игоревна
студентка
Золотарюк Анатолий Васильевич
канд. техн. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПАНИИ: ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ

Аннотация: *в статье описываются проблемы защиты информационных систем организаций от внутренних нарушителей. Определяются критически значимые для ведения бизнеса внутренние угрозы. Приводятся оценки угроз. Предлагаются меры, способы и средства обеспечения информационной безопасности корпоративных информационных систем.*

Ключевые слова: *информационная безопасность, внутренние угрозы, утечки информации, внутренние нарушители, методы защиты, обеспечение безопасности информации.*

Менеджмент любой компании нацелен на поддержание и развитие уровня операционной эффективности бизнеса в любых, реально складывающихся экономических условиях. В то же время необходимо соответсвовать законодательно-нормативным требованиям регулирующих органов, заботиться об увеличении акционерной привлекательности компании, выдерживать жесткое противодействие конкурентов, внедряя в производственные и управленческие процессы инновационные средства и технологии, в том числе направленные на соблюдение в должной мере информационной безопасности, разграничение доступа и защиту интеллектуальной собственности и важных конфиденциальных сведений, критически значимых для ведения бизнеса.

Безусловно, реализация указанных положений возможна только при комплексном подходе к вопросам безопасности, тесно и всесторонне увязанным с целями и задачами бизнеса, включая материальную, финансово-экономическую, технологическую, юридическую и иные виды безопасности. В данной статье, однако, мы остановимся только на проблемах информационной безопасности, прежде всего, вопросах противодействия внутренним угрозам, в частности, утечкам информации.

Как показывают аналитические отчеты отечественных и зарубежных центров, основанные на глобальном рассмотрении проблемы, на протяжении последних лет от 60 до 80 процентов нарушений информационной безопасности компаний связаны с внутренними угрозами, вызванными ошибочными или неправомерными действиями, приводящими к нарушениям доступности, целостности, конфиденциальности и достоверности информации [2; 4; 8]. В некоторой степени, – помимо упущений в подборе персонала компаний, привитии сотрудникам норм корпоративной этики и предоставлении им возможностей карьерного роста, – это объясняется проблемами образовательного процесса, глобализацией бизнеса, разветвленностью корпоративных информационных систем (КИС), широким применением инновационных сетевых технологий, облачных сред и ресурсов [3; 5; 6; 7].

Анализируя данные по утечкам информации в 2015 г., было установлено, что в 51,2% случаев нарушителями были настоящие (48,9%) или бывшие (2,3%) сотрудники. 1% случаев связан с нарушениями руководящего звена компаний (топ-менеджеры, руководители отделов и департаментов). Значительными (7,6%) являются нарушения со стороны подрядчиков с легитимным доступом к режимной информации [8].

Оценка опасности внутренних угроз показывает, что наиболее деструктивной является утечка данных (55%); далее следует угроза искажения корпоративной, финансово-экономичексой информации [8].

Предлагается применение следующих способов, средств, мер и приемов защиты от внутренних нарушителей, что позволит организациям

минимизировать риск утечки информации и уменьшение возможных бизнес-потерь [1; 2; 4].

1. Регулярно проводить аудит рисков информационной безопасности для установление баланса между доверием к своим сотрудникам и контролем за их действиями и ограждения себя от внутренних нарушителей.

2. Внедрять современные процедуры и средства защиты информации от от воздействия от реальных и потенциально возможных неправомерных действий.

3. Проводить обучение сотрудников компании основам информационной безопасности.

4. Разграничивать привилегии сотрудников по доступу к данным в соответсвие с их должностными обязанностями.

5. Установить строгую политику управления учетными записями, системой задания и смены паролей.

6. Усложнить процедуры аутентификации и авторизации пользователей в сетях.

7. Оперативно декактивировать несуществующих пользователей.

8. Проводить мониторинг и анализ сетевых действий сотрудников в режиме on-line.

Помимо этого, следует также использовать другие меры защиты.

1. Проводить активную защиту от вредоносного кода надежными антивирусными программами.

2. Использовать резервное копирование критически важных данных и процедуры восстановления.

3. Фильтровать исходящий сетевой трафик на предмет утечек (e-mail, сообщения ICQ, web-почту, постинги на форумах, блоги, другую Internet-активность).

4. Ввести политику учета работы с периферийными, сменными и мобильными устройствами во избежание записей на них и выноса за пределы компании конфиденциальных документов: FDD, CD/DVD, RW, Cart Reader,

Flash-накопителями, присоединяемых по различным шинам (USB и PCMCIA). Обеспечить контроль беспроводных сетей (IrDA, Bluetooth, WiFi).

5. Обеспечить контроль учета распечатанных документов и их фрагментов.

6. Фильтровать все запросы к базам данных, не допускать выполнение запросов, извлекающих секретные сведения, без реализации особой процедуры контроля.

7. При использовании мобильных устройств и планшетов обеспечивать шифрование критической информации.

8. Использовать DLP-системы (Data Leak Prevention – технологии предотвращения утечек конфиденциальной информации).

Таким образрм, для построения эффективной системы информационной безопасности компании, решающей в том числе защиту от внутренних угроз, необходимо выполнение сложной задачи, начиная с проектирования КИС и ее разработки [9]. Это трудный и непрерывный процесс, от внимания к которому зависит жизнеспособность бизнеса. Для построения такой системы необходимо использовать современные информационно-технологические средства, привлекать к участию топ-менеджмент компании, ИТ-специалистов, консультантов. Следует помнить, что «обеспечение безопасности информации достигается путем комплексного применения технических и программных средств, криптографических методов и организационно-правовых норм и мероприятий» во всех структурных элементах КИС, во всех режимах ее функционирования, на всех этапах ее использования для решения стоящих перед компанией бизнес-задач [2].

Список литературы

1. Гайдар Е.В. BI-технологии предотвращают мошенничество в банковской сфере / Е.В. Гайдар, А.В. Золотарюк, Е.С. Худеньких // Валютное регулирование и валютный контроль. – 2015. – №5. – С. 63–66.

2. Гобарева Я.Л. Автоматизация деятельности кредитной организации на платформе «1С: Предприятие 8» / Я.Л. Гобарева, А.В. Золотарюк, Е.Р. Кочанова [и др.]; под общ. ред. проф. Д.В. Чистова. – М.: 1С-Паблишинг, 2012.

3. Гобарева Я.Л. Проблемы образовательного процесса и их решение с применением облачных технологий / Я.Л. Гобарева, А.В. Золотарюк, Е.Р. Кочанова // Новые информационные технологии в образовании: Сборник научных трудов Пятнадцатой Международной научно-практической конференции «Применение технологий «1С» для формирования инновационной среды образования и бизнеса» 3 – 4 февраля 2015 г. / Под общ. ред. проф. Д.В. Чистова. Ч. 1. – М.: 1С-Паблишинг, 2015. – С. 210–213.

4. Журин С.И. Основы противодействия инсайдерским угрозам. – М.: НИЯУ МИФИ, 2013.

5. Золотарюк А.В. Облачные технологии как фактор разрешения проблем глобализации образования // Информационные технологии в финансово-экономической сфере: прошлое, настоящее, будущее: Материалы международной научной конференции (17 декабря 2013 г.) / Под ред. О.В. Голосова, Д.В. Чистова. – М.:1С-Паблишинг, 2013. – С. 68–73.

6. Золотарюк А.В. Проблемы образовательного процесса и их разрешение // Новые информационные технологии в образовании (НИТО-Байкал): Материалы международной научно-практической конференции (12–14 июля 2010 г.). – Улан-Удэ: Изд-во БГСА, 2010. – С. 58–59.

7. Золотарюк А.В. Роль облачных сервисов в формировании профессиональных информационно-технологических компетенций студентов / А.В. Золотарюк, Т.Л. Фомичева, А.И. Кижнер // Известия Института инженерной физики. – 2015. – №2 (36). – С. 96–100.

8. Исследование утечек конфиденциальной информации в 2015 году [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/report2015 (дата обращения: 30.10.2016).

9. Чистов Д.В. Проектирование информационных систем: Учебник и практикум / Д.В. Чистов, П.П. Мельников, А.В. Золотарюк, Н.Б. Ничепорук; под ред. проф. Д.В. Чистова. – М.: Юрайт, 2015.