экспериментальные группы для различных предложений с помощью a/b тестирования. После оценки итогов анализа, были сформированы наиболее эффективные предложения.

Третий этап – это тонкий анализ поведения клиентов – анализировались смежные и похожие покупки с целью предложить клиенту попробовать новинки.

В ходе всего эксперимента все данные проверялись сверкой со сводными таблицами за предыдущие периоды, объективность выборки и полученных результатов оценивалась приглашенным экспертом.

Плановый результат подтвердился фактическим – после формирования точечных предложений в результате анализа групп, был получен возврат порядка 12% от числа клиентов, которые не покупали, но начали снова покупать после предложения. В результате проведенного анализа были получены новые знания о том, что рассылка клиентам со специальным предложением в их День Рождения увеличивает средний чек на 86 %, а купит по специальному предложению каждый второй участник программы лояльности. В результате рассылок с предложениями о покупках из зон смежных предпочтений прирост продаж составил 200% [6].

Таким образом, с распространением новых алгоритмов анализа данных и автоматизации этих процессов важно понимать, насколько корректные результаты мы получаем, тем самым определяя степень доверия к этой информации. Ошибки могут повлечь за собой потери для компании как в трудозатратах – на расчеты, так и в денежном выражении. Достоверная же информация позволяет принимать операционные и стратегические решения на качественно новом уровне.

Источники литературы*

1. Свободная энциклопедия Википедия [Электронный ресурс] . – Режим доступа: https://ru.wikipedia.org/wiki/Большие_данные. Дата доступа: 06.12.2016.
2. Свободная энциклопедия Википедия [Электронный ресурс] . – Режим доступа: https://ru.wikipedia.org/wiki/Data_mining. Дата доступа: 06.12.2016.
3. Профессиональный информационно-аналитический ресурс [Электронный ресурс]. – Режим доступа: http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение. Дата доступа: 06.12.2016.
4. Профессиональный информационно-аналитический ресурс [Электронный ресурс] . – Режим доступа: http://www.machinelearning.ru/wiki/index.php?title=Регрессия. Дата доступа: 17.11.2016.
5. Официальный сайт Coursera [Электронный ресурс]. – Режим доступа: https://www.coursera.org/learn/real-life-data-science. Дата доступа: 17.11.2016.
6. Официальный сайт А2 Консалтинг [Электронный ресурс]. – Режим доступа: http://a2c.by/press-tsentr/738-kupilka.html. Дата доступа: 10.12.2016.

**Статья опирается на свободную энциклопедию Википедия и Профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных, т.к. по выбранной теме актуальные материалы можно найти только в источниках на оригинальных языках или в переводе энтузиастов на подобных ресурсах.*

Русакова Марина Михайловна
Белорусский государственный экономический университет

Аудит информационной безопасности предприятия

Данная тема актуальна в связи с тем, что сегодня информационные системы играют ключевую роль в обеспечении эффективности работы коммерческих и государственных предприятий. Повсеместное использование информационных систем для хранения, обработки и передачи информации делает актуальными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. Для эффективной защиты от атак

компаниям необходима объективная оценка уровня безопасности информационной системы, и именно для этих целей применяется аудит безопасности.

Аудит информационной безопасности — независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций. Основными целями же аудита могут быть:

- Оценка текущего уровня защищенности ИС для принятия решения о ее модернизации
- Локализация узких мест в системе защиты ИС
- Определение соответствия системы управления информационной безопасностью задачам и целям предприятия
- Оценка эффективности инвестиций и планирование затрат на обеспечение защиты информации
- Оценка соответствия и полноты выполнения требований, предъявляемых к предприятию со стороны законодательства, стандартов ИБ, нормативных документов, политики безопасности или требований, предусмотренных контрактом

Одной из стратегических задач, решаемых при проведении аудита информационной безопасности и получении соответствующего сертификата, является демонстрация надежности предприятия, его способности выступать в качестве устойчивого партнера, способного обеспечить комплексную защиту информационных ресурсов, что может быть особенно важно при осуществлении сделок, предполагающих обмен конфиденциальной информацией, имеющей большую стоимость

Существует множество случаев, когда целесообразно проводить аудит безопасности. Это делается, в частности, при подготовке технического задания на проектирование и разработку системы защиты информации и после внедрения системы безопасности для оценки уровня ее эффективности. Возможен аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства. Аудит может также предназначаться для систематизации и упорядочения существующих мер защиты информации или для расследования произошедшего инцидента, связанного с нарушением информационной безопасности.

Как правило, для проведения аудита привлекаются внешние компании, которые предоставляют консалтинговые услуги в области информационной безопасности. Инициатором процедуры аудита может стать руководство предприятия, служба автоматизации или служба информационной безопасности. В ряде случаев аудит также проводится по требованию страховых компаний или регулирующих органов. Аудит безопасности выполняется группой экспертов, численность и состав которой зависит от целей и задач обследования, а также от сложности объекта оценки.

Можно выделить следующие основные виды аудита информационной безопасности:

- экспертный аудит безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования;
- оценка соответствия рекомендациям международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии);
- инструментальный анализ защищенности ИС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;
- комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Любой из перечисленных видов аудита может проводиться по отдельности или в комплексе, в зависимости от тех задач, которые решает предприятие. В качестве объекта аудита может выступать как ИС компании в целом, так и ее отдельные сегменты, в которых обрабатывается информация, подлежащая защите.

Процесс аудита информационной безопасности является многогранным и должен учитывать множество параметров. Аудит объединяет несколько форм работ, основанных на единых принципах и методологии, но различающихся по содержанию конечной цели и объемам проводимых испытаний. Можно выделить следующие этапы, представленные на рисунке 1:

1. Планирование работ;
2. Обследование информационной системы (ИС);
3. Анализ и оценка уровня защищенности ИС;
4. Модернизация и оптимизация системы информационной безопасности.

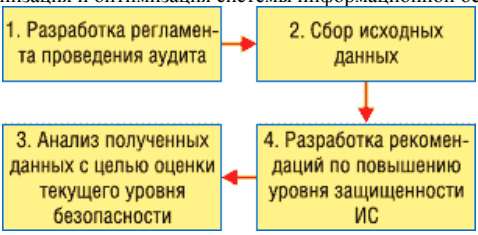

Рисунок 1 - Основные этапы работ при проведении аудита безопасности

На первом этапе совместно с заказчиком разрабатывается регламент, устанавливающий состав и порядок проведения работ. Основная задача регламента – определить границы, в рамках которых будет проводиться обследование. Регламент позволяет избежать взаимных претензий по завершении аудита, поскольку четко определяет обязанности сторон.

На втором этапе, в соответствии с согласованным регламентом, собирается исходная информация. Методы сбора информации включают интервьюирование сотрудников заказчика, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации, использование специализированных инструментальных средств.

Третий этап работ предполагает анализ собранной информации с целью оценки текущего уровня защищенности ИС предприятия.

По результатам проведенного анализа на четвертом этапе разрабатываются рекомендации по повышению уровня защищенности ИС от угроз информационной безопасности.

Аудит информационной безопасности – один из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Кроме того, результаты аудита дают основу для формирования стратегии развития системы обеспечения информационной безопасности организации. Однако необходимо понимать, что аудит безопасности – не разовая процедура, он должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности компании.

Источники литературы

1. Бармен, С.. Разработка правил информационной безопасности. - М.: Вильямс, 2002. — 208 с.

2. Семененко, В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2004 – 215 с.

3. Ярочкин, В. И. Информационная безопасность: Учебник для студентов — М.: Академический Проект; Гаудеамус, 2-е изд., — 2004. — 544 с.

4. Анализ состояния защиты данных в информационных системах: Учебно-методическое пособие. – М.: НГТУ. – 2012. - 52 с.