# АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ

А.Н. Лазуткин, магистрант
Научный руководитель – А.И. Демиденко, к.т.н., доцент.
ФГБОУ ВПО «Брянский государственный технический университет», г.Брянск
E-mail: lazutkin93@mail.ru

Активное развитие банковского сектора влечет за собой увеличение клиентских баз, в связи с чем особую актуальность приобретают вопросы защиты информации о клиентах банка.

Сегодня уже известны ряд случаев, когда информационные системы крупнейших российских банков подвергались внешнему проникновению злоумышленников для получения несанкционированного доступа к сетевым ресурсам банка, либо для нарушения нормального режима работы сетевых сервисов.

Проникновение в финансовую систему банка, а также на сервера баз данных может повлечь за собой исчезновение крупных сумм со счетов, разглашение тайны клиента о состоянии его счета, а взлом серверов баз данных чреват распространением сведений о клиенте. [1]

На сегодняшних день во всех существующих сетевых операционных системах имеется много уязвимых мест с точки зрения защиты информации. Поэтому необходимо проводить проактивные мероприятия борьбы с взломами и проникновениями в банковские системы.

Одной из таких мер является проведение аудита систем обеспечения информационной безопасности, который позволяет на начальном этапе выявить уязвимые места и предпринять дальнейшие шаги для их устранения.

Для того, чтобы в будущем избежать нежелательных проникновений и атак, а также для формирования стратегии развития бизнеса и сопутствующей модернизации корпоративной информационной системы и системы защиты информации было необходимо:

- получить объективную информацию об актуальном состоянии компонентов системы для обеспечения информационной безопасности;
- выявить «узкие» места системы информационной безопасности для принятия проактивных мер предотвращения атак;
- оценить стоимость развития системы обеспечения информационной безопасности;
- оценить зрелость ИТ-инфраструктуры и системы информационной безопасности банка в соответствии с требованиями стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2006).

Основными целями мониторинга и контроля защитных мер в Банке являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели. Такими целями анализа могут быть:

- контроль за реализацией положений внутренних документов Банка по обеспечению ИБ;
- выявление нештатных, в том числе злоумышленных, действий в КИС Банка;
- выявление инцидентов ИБ.

Мониторинг и контроль защитных мер проводится персоналом Банка, ответственным за ИБ.

Целью программы аудита является оценка соответствия ИБ Банка критериям аудита. [2]

В качестве проверяющих организаций рекомендуется привлекать организации, имеющие квалификацию и опыт проведения оценки соответствия ИБ требованиям стандарта Банка России СТО БР ИББС-1.0.

Внедрение программы аудита должно включать в себя:

- доведение программы аудита до участвующих в ее реализации сторон;
- планирование аудитов;
- определение привлекаемых аудиторских организаций и предоставляемых ресурсов для проведения аудитов;
- проведение аудитов в соответствии с программой аудита;
- анализ и утверждение отчетов по результатам аудитов;
- определение действий по результатам аудитов.
- В Банке должны проводиться контроль внедрения программы аудита, анализ достижения целей программы аудита и определение возможностей для ее совершенствования. О результатах анализа должно информироваться руководство Банка. [3]
- Контроль и анализ программы аудита должны включать в себя:
- проверку возможностей аудиторских групп, служб или лиц по реализации аудита (подтверждением возможности по реализации аудита могут являться информация об образовании и опыте работы членов аудиторской группы, сертификаты, подтверждающие квалификацию членов аудиторской группы);
- анализ достижения целей аудита и программы аудита в целом;
- анализ отчетов и заключений по результатам аудита.
- По итогам аудита банк получает комплект документов, содержащий отчет о текущем состоянии системы защиты информации, рекомендации по устранению обнаруженных уязвимостей и концепцию развития информационной безопасности с учетом требований законодательства Российской Федерации в области защиты и информации и требований.

Список литературы:

1. Пискунов И. Особенности обеспечения информационной безопасности в банковской системе // Anti-Malvare.ru – Независимый информационно-аналитический центр. – 2014. – [Электронный ресурс]. URL: http://www.anti-malware.ru/analytics/Technology_Analysis/Features_information_security_in_the_banking_system (дата обращения: 27.09.2015).

2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд., 2011. - 544 с.

3. Курило А.П., Зефиров С.Л., Голованов В.Б и др. Аудит информационной безопасности. - М.: Издательская группа «БДЦ-пресс», 2013. - 304 с.