ООО «RAQAMLI BIZNES AGREGATOR»

«УТВЕРЖДАЮ»

10 января 2023 год

Директор Толаганов А.А.

Сведения о системах безопасности, механизмах и системах контроля

ООО «RAQAMLI BIZNES AGREGATOR»

Ташкент 2023

Защита информации в платежных системах

1. Оценка соответствия платежной системы требованиям по безопасности информации и разработка плана мероприятий по обеспечению соответствия:

- сбор и анализ свидетельств аудита;
- анализ документации организации и бизнес-процессов, в части функционирования платежной системы;
- интервьюирование представителей организации;
- анализ полноты и эффективности реализуемых мер по защите информации;
- вычисление обобщающих показателей соответствия и итогового показателя соответствия;
- документирование результатов оценки соответствия;
- разработка плана организационно-технических мероприятий по обеспечению соответствия платежной системы требованиям по безопасности информации.

2. Анализ защищенности платежной системы

- идентификация и анализ организационных уязвимостей ИБ платежной системы;
- идентификация и анализ технических уязвимостей ИБ платежной системы для внешнего периметра корпоративной сети и внутренний ИТ-инфраструктуры;
- анализ защищенности программных модулей и сервисов платежной системы;
- оценка уровня защищенности платежной системы;
- разработка рекомендаций по повышению уровня защищенности платежной системы и совершенствованию механизмов защиты.

3. Оценка и обработка рисков информационной безопасности платежной системы

- инвентаризация активов платежной системы;
- разработка моделей угроз и нарушителей информационной безопасности платежной системы;
- оценка информационных активов, угроз, уязвимостей и механизмов контроля ИБ платежной системы;
- формирование реестра информационных рисков платежной системы;
- определение допустимого уровня остаточных рисков;
- подготовка и согласование решений по обработки рисков платежной системы;
- разработка и согласование плана обработки рисков платежной системы.

4. Разработка комплекса организационно-распорядительных документов для обеспечения соответствия платежной системы организации требованиям по безопасности информации

- определение требований к процессам обеспечения информационной безопасности в платежной системе;
- определение ролей и ответственности персонала;
- определение порядка взаимодействия между подразделениями для реализации мер по защите информации в платежной системе;
- разработка и согласование проектов организационно-распорядительных документов по обеспечению информационной безопасности платежной системы.

5. Разработка и внедрение технических решений по комплексу программно-технических средств защиты информации в платежной системе

- проектирование архитектуры обеспечения ИБ платежной системы;
- выбор основных технических решений по защите информации в платежной системе;
- определение состава сертифицированных СЗИ по каждой подсистеме защиты и анализ их технической совместимости;
- разработка проектной документации, описание процессов и механизмов функционирования СЗИ;
- поставка и внедрение СЗИ;
- проведение приемо-сдаточных испытаний подсистемы информационной безопасности платежной системы;
- проведение аттестационных испытаний платежной системы по требованиям безопасности информации (опционально).

Информационные системы стали основой функционирования большинства компаний, от их работоспособности зависят непрерывность и качество течения бизнес-процессов. Выбор механизма защиты зависит от категории информационных ресурсов.

Информация и необходимость ее защиты

Информация представляет собой сведения, передающиеся в любой форме – устной речи, бумажного документа, файла. Она имеет ценность не только для ее владельца, но и для третьих лиц, способных использовать чужие конфиденциальные данные для получения конкурентного преимущества или личного обогащения.

Информационные массивы подразделяются на три группы:

- данные, для которых отсутствует необходимость защиты от утечек, или общедоступные, раскрытие которых обусловлено нормами законов;

- защищаемые в качестве коммерческой тайны при условии введения режима коммерческой тайны и составления перечня сведений, относимых к ней;
- те, которые необходимо охранять исходя из требований законодательства – банковская или государственная тайны, персональные данные.

В зависимости от категории данных компании выбирают необходимые средства из арсенала защиты. Они делятся на группы:

- административные и организационные, выстраивающие систему управления в компании таким образом, чтобы исключить несанкционированный допуск к данным;
- технические, аппаратными средствами блокирующие НСД (токены, при помощи которых происходит аутентификация, заглушки на USB-входы в компьютер);
- программные, равно защищающие от несанкционированного доступа инсайдеров и от внешних атак.

Безопасность электронных платежных систем

Современную практику банковских операций, торговых сделок и взаимных платежей невозможно представить без расчетов с применением пластиковых карт.

Система безналичных расчетов с помощью пластиковых карт называется ***электронной платежной системой***.

Для обеспечения нормальной работы электронная платежная система должна быть надежно защищена.

С точки зрения информационной безопасности в системах электронных платежей существуют следующие уязвимые места:

- пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом;
- обработка информации внутри организации отправителя и получателя сообщений;
- доступ клиентов к средствам, аккумулированными на счетах.

Пересылка платежных и других сообщений связана с такими особенностями:

- внутренние системы организаций отправителя и получателя должны обеспечивать необходимую защиту при обработке электронных документов (защита оконечных систем);

- взаимодействие отправителя и получателя электронного документа осуществляется опосредовано - через канал связи.

Эти особенности порождают следующие проблемы:

- взаимное опознание абонентов (проблема установления взаимной подлинности при установлении соединения);
- защита электронных документов, передаваемых по каналам связи (проблема обеспечения конфиденциальности и целостности документов);
- защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);
- обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости).

Для обеспечения функций защиты информации на отдельных узлах системы электронных платежей должны быть реализованы следующие механизмы защиты:

- управление доступом на оконечных системах;
- контроль целостности сообщения;
- обеспечение конфиденциальности сообщения;
- взаимная аутентификация абонентов;
- невозможность отказа от авторства сообщения;
- гарантии доставки сообщения;
- невозможность отказа от принятия мер по сообщения;
- регистрация последовательности сообщений;
- контроль целостности последовательности сообщений.

Корпоративная информационная безопасность

Для решения общих задач информационной безопасности, не связанных исключительно с персональными данными или государственной тайной, компании разрабатывают собственные системы защиты с опорой на комплексные решения, например, на SIEM- и DLP-системы. Выбор программных и технических решений опирается на модель угроз, зависящую от типа обрабатываемой информации и вида бизнеса организации. Также итоговые программные решения зависят от типов корпоративных систем, использования АСУ, CRM-систем, программ автоматизированного электронного документооборота.

Построение единого механизма обеспечения безопасности информационных систем строится по алгоритму:

- проведение аудита существующей сети, элементов инфраструктуры, программного обеспечения, выявление узких мест и определение направлений модернизации;
- разработка и утверждение политики безопасности, определяющей ключевые моменты ее обеспечения – от правил работы со съемными носителями до принципов использования Интернета и личных ящиков электронной почты в профессиональной деятельности;
- создание системы аутентификации пользователей требуемого уровня, при необходимости с использованием двухфакторного механизма, исключающего возможность несанкционированного доступа к защищенным данным;
- реализация одной из моделей дифференцированного доступа, при котором в зависимости от ранга пользователя ему предоставляется возможность совершать необходимые операции с файлами;
- создание системы мониторинга работоспособности ИС при помощи сканеров, выявляющих уязвимости, разработка правил стандартной реакции на них, создание базы данных инцидентов с целью последующего анализа статистики;
- создание защиты каналов связи, по которым связываются пользователи на удаленном доступе, от несанкционированных подключений, использование защищенных протоколов, VPN-туннелей;
- использование криптографических средств защиты информации, обеспечивающих безопасность баз данных и трафика;
- создание системы управления конфигурацией, поддержание функций среды ИС в соответствии с требованиями.

Для реализации стратегии необходимо или привлечение профессиональных организаций на условиях аутсорсинга, или создание собственного дееспособного ИТ-подразделения, которое может оперативно и эффективно реагировать на инциденты информационной безопасности. Модель управления рисками при выстраивании механизма обеспечения информационной безопасности может опираться на национальные стандарты, ГОСТы или на зарубежные методики. Это зависит от уровня угроз и того, от кого необходимо в большей степени защищать информацию – от внешних или внутренних нарушителей. Построение механизма всегда опирается на принцип целесообразности: принимаемые меры безопасности не должны быть избыточными и мешать эффективному функционированию бизнеса. Модель доступа к информационным ресурсам должна обеспечивать их постоянную вовлеченность в бизнес-процессы компании.

В резервном сервере работаю программный файрволл.