Александр Каминский,
Республика Молдова

ФОРМИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Formation of the security policy of information systems

Политика безопасности (информации в организации) (*Organizational security policy*) – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

В современной практике термин «политика безопасности» может употребляться как в широком, так и в узком смысле слова. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению безопасности организации. В узком смысле под политикой безопасности обычно понимают локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения безопасности. Примерами таких документов могут служить:

- Правила работы пользователей в корпоративной сети;
- Политика обеспечения безопасности удаленного доступа к ресурсам корпоративной сети;
- Политика обеспечения безопасности при взаимодействии с сетью Интернет;
- Антивирусная политика, инструкция по защите от компьютерных вирусов;
- Политика выбора и использования паролей;
- Правила предоставления доступа к ресурсам корпоративной сети;
- Политика установки обновлений программного обеспечения;
- Политика и регламент резервного копирования и восстановления данных;
- Соглашение о соблюдении режима информационной безопасности, заключаемое со сторонними организациями.

Разработка политик безопасности собственными силами – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания нормативной базы в области информационной безопасности. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы

защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких как: *ISO 17799*, *ISO 9001*, *ISO 15408*, *BSI*, *COBIT*, *ITIL* и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

Основными нормативными документами в области информационной безопасности выступают:

- «Общие критерии оценки безопасности информационных технологий» (*ISO 15408*), которые определяют функциональные требования безопасности и требования адекватности реализации функций безопасности;
- «Практические правила управления информационной безопасностью» (*ISO 17799*). Данный стандарт содержит систему практических правил по управлению информационной безопасностью и используется в качестве критериев оценки эффективности механизмов безопасности на организационном уровне, включая административные, процедурные и физические меры защиты.

Содержание политики безопасности.

Обеспечение информационной безопасности предполагает подчиненное единому замыслу, эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности. Главная цель принимаемых мер зашиты информации состоит в том, чтобы гарантировать **целостность**, **достоверность**, **доступность** и **конфиденциальность** информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах независимо от типа носителей этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности жизнедеятельности организации, не жертвуя при этом основными принципами информационной безопасности.

При этом основной посылкой для разработки политики безопасности, являются следующие причины, которые можно разделить на внутренние и внешние.

Внутренние:

- требования руководства;
- обеспечение конкурентоспособности;
- демонстрация заинтересованности руководства в обеспечении информационной безопасности;
- вовлечение сотрудников в процесс обеспечения информационной безопасности;

- уменьшение стоимости страхования;
- экономическая целесообразность;

Внешние:

- требования законодательства и стандартов:
- требования клиентов и партнеров;
- необходимость сертификации по стандартам;
- требования аудиторов;

Политика информационной безопасности является планом высокого уровня, в котором описываются цели и задачи мероприятий в сфере безопасности.

Для построения политики информационной безопасности рекомендуется отдельно рассматривать следующие направления защиты информационной системы:

- Защита объектов информационной системы;
- Защита процессов, процедур и программ обработки информации;
- Защита каналов связи;
- Подавление побочных электромагнитных излучений;
- Управление системой защиты.

При этом по каждому из перечисленных выше направлений Политика информационной безопасности должна описывать следующие этапы создания средств защиты информации:

1. Определение информационных и технических ресурсов, подлежащих защите;
2. Выявление полного множества потенциально возможных угроз и каналов утечки информации;
3. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
4. Определение требований к системе защиты;
5. Осуществление выбора средств защиты информации и их характеристик;
6. Внедрение и организация использования выбранных мер, способов и средств защиты;
7. Осуществление контроля целостности и управление системой защиты.

Политика безопасности – это организационно-правовой и технический документ одновременно. При его составлении надо всегда опираться на принцип разумной достаточности и не терять здравого смысла. Этот принцип означает, что затраты на обеспечение безопасности информации должны быть не больше, чем величина потенциального ущерба от ее утраты. Анализ рисков, проведенный на этапе аудита, позволяет ранжировать их по величине и защищать в первую очередь не только наиболее уязвимые, но и обрабатывающие наиболее ценную информацию участки.

Адекватный уровень информационной безопасности в организации может быть обеспечен только при комплексном подходе, включающем как программно-технические, так и организационные меры защиты. Причем организационные меры играют более важную роль и в среднем должны составлять более 60% усилий в этом направлении. Эффективность любых сложных и дорогостоящих

программно-технических механизмов защиты может быть сведена к нулю в случае, если пользователи информационных систем игнорируют элементарные правила парольной политики. Установка межсетевого экрана может даже понизить защищенность сети в случае отсутствия политики управления доступом, которую он должен реализовывать. В основе организационных мер защиты информации лежат политики безопасности организации, от эффективности которых в наибольшей степени зависит успешность мероприятий по обеспечению ИБ.

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия.

Литература:

1. *Разработка политики информационной безопасности предприятия*. Сергей Петренко, Владимир Курбатов, компания АйТи.
2. *Разработка правил информационной безопасности*. Скотт Бармен.
3. *Практические аспекты разработки политики информационной безопасности*. Сергей А. Охрименко, Константин Ф. Склифос.
4. *Формирование политики безопасности для информационной системы*. Сергей А. Охрименко, Геннадий А. Черней.
5. *Политика безопасности: разработка и реализация*. В.Г. Грибунин.
6. Основные положения международного стандарта безопасности ISO/IEC 17799.

Анна Милованова,
«IT&IS Management»

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На сегодняшний день корпоративные сети даже небольших компаний представляют собой достаточно сложные и многофункциональные объекты, позволяющие решать различные задачи. Нынешняя тенденция к усложнению функциональности, администрирования информационных систем ведет к появлению возрастающего числа ошибок, связанных с безопасностью системы, а иногда к недостаточности опыта и знаний для безопасного администрирования системы.

В связи с этим общепринятой практикой является проведение сторонней, доверенной, специализированной компанией всестороннего аудита информационной безопасности (ИБ) всех автоматизированных ресурсов и бизнес-процессов компании.