УДК 65.012.8

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ НА ОСНОВЕ СТАНДАРТА ISO27001

Григорьева Виктория Андреевна, Мешков Вадим Игоревич
Государственный ВУЗ «Национальный горный университет», vikylya_1992@mail.ru

В работе рассмотрен стандарт ISO 27001, основные его требования к информационной безопасности на предприятии. Расмотрены основные подходы к построению системы безопасности с помощью стандарта.

Ключевые слова – стандарт ISO 27001, предприятие, управление.

ВВЕДЕНИЕ

Международный стандарт ISO/IEC 27001:2005 «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования» разработан Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) на основе британского стандарта BS 7799.

ОСОБЕННОСТИ ДОКУМЕНТА

Стандарт ISO 27001 определяет информационную безопасность как: «сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность». ISO/IEC 27001:2005 представляет собой перечень требований к системе менеджмента информационной безопасности, обязательных для сертификации. Стандарт ISO 27001 определяет процессы, представляющие возможность бизнесу устанавливать, применять, пересматривать, контролировать и поддерживать эффективную систему менеджмента информационной безопасности; устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной системы менеджмента информационной безопасности в контексте существующих бизнес рисков организации.

Система управления информационной безопасностью на основе стандарта ISO 27001 позволяет:

- сделать большинство информационных активов наиболее понятными для менеджмента компании;
- выявлять основные угрозы безопасности для существующих бизнес-процессов;
- рассчитывать риски и принимать решения на основе бизнес-целей компании;
- обеспечить эффективное управление системой в критичных ситуациях;
- проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности);
- четко определить личную ответственность;
- достигнуть снижения и оптимизации стоимости поддержки системы безопасности;
- облегчить интеграцию подсистемы безопасности в бизнес-процессы и интеграцию с ISO 9001:2000;
- продемонстрировать клиентам, партнерам, владельцам бизнеса свою приверженность к информационной безопасности;
- получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках;
- подчеркнуть прозрачность и чистоту бизнеса перед законом благодаря соответствию стандарту.

Наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом, обеспечению непрерывности производственного процесса, юридическим требованиям.

Корректное построение системы менеджмента информационной безопасности (СМИБ) в организации — основа для дальнейшей деятельности организации. Построение СМИБ организации подразумевает прохождение следующих основных этапов:

- предварительный аудит;
- определение области действия и границ СМИБ;
- назначение сотрудников, ответственных за СМИБ (создание структуры, которая будет внедрять и обеспечивать работоспособность СМИБ организации, к примеру, отдел внутренней безопасности);
- инвентаризация активов организации и определение их важности;
- оценка защищённости активов организации (анализ существующих угроз и уязвимостей, а также вероятностей их реализации);
- определение подхода организации к оценке рисков (стандарт не устанавливает обязательного метода к определенному методу оценки рисков – наоборот, организация может предложить свой метод оценки рисков, и чем проще будет этот метод, тем лучше);
- подсчёт рисков в организации, как в качественных, так и в количественных показателях;
- анализ рисков и принятие решений по обработке рисков (принять риск, уменьшить риск до допустимого уровня, передать третьей стороне, избежать риска);
- выбор целей управления и средств обработки рисков;

- анализ существующих контрмер (организационные мероприятия и программно-технические средства, направленные на защиту определённого актива организации);
- анализ процессной документации организации (создаётся список организационных документов, требующих внедрения).

Предоставление Заявления о применимости (обязательный документ, который содержит все рекомендации Приложения А стандарта ISO/IEC 27001:2005 с описанием, выполняется ли данное требование в организации).

Но, если в организации уже существует своя система информационной безопасности необходимо проведение внутреннего аудита. На основе результатов такого анализа можно откорректировать действующую систему, разработать недостающие процессные документы, улучшить подход к оценке рисков в организации и т. д.

ВЫВОД

В результате проанализировав стандарт можно сделать вывод: для существующей системы безопасности необходимо проводить аудит с помощью которого определяем недостатки системы и в дальнейшем устраняем ошибки. Если на предприятии не существует системы безопасности, то благодаря стандарту были пошагово рассмотрены пункты построения необходимой системы.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ISO 27001:2005 «Информационные технологии - Методы обеспечения безопасности - Системы управления информационной безопасностью - Требования»