УДК 65.012.8

ЗАДАЧИ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Смирнов Арсений Евгеньевич[1], Начовный Иван Ильич[2]
ГВУЗ «Национальный горный университет», www.nmu.org.ua,
smirnov.a.e.work@gmail.com[1], Gnomus_tiger@yahoo.com[2]

В данной статье рассматриваются основные задачи, решаемые при создании, внедрении и дальнейшем использовании Системы управления информационной безопасностью. Перечислены главные цели системы, состав рабочей группы, ответственной за её функционирование и задачи, стоящие перед членами этой группы. Методика работы системы создана на основе международных стандартов.

Ключевые слова – Системы управления информационной безопасностью (СУИБ); анализ рисков; информационный актив; информационная безопасность.

ВСТУПЛЕНИЕ

В современных условиях перед предприятиями особо остро встает задача сохранения информационных активов, в том числе сведений, составляющих коммерческую или государственную тайну. Конфиденциальность, целостность и доступность информации могут быть существенными аспектами для поддержания конкурентоспособности, денежного оборота, доходности, юридической гибкости и коммерческого имиджа. Одним из основных инструментов обеспечения защищенности информации и поддерживающих её процессов, является Система управления информационной безопасностью.

ОСНОВНЫЕ ЗАДАЧИ ПРИ СОЗДАНИИ И ВНЕДРЕНИИ СУИБ

Система управления информационной безопасностью (СУИБ) обеспечивает объединение всех применяемых на предприятии защитных и организационных мер в единый адекватный реальным угрозам и управляемый комплекс, позволяющий достигать корпоративных целей информационной безопасности на уровне всего предприятия. Построение СУИБ позволяет четко определить, как взаимосвязаны процессы и подсистемы информационной безопасности, кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования, и т.д.

Цели СУИБ:

- Постановка управления информационной безопасности для достижения целей бизнеса;
- Управление рисками компании;
- Оптимизация затрат на информационную безопасность;
- Управление ресурсами, выделенными на обеспечение информационной безопасности;
- Централизация всех функций обеспечения информационной безопасности в компании;
- Измерения производительности информационной безопасности. [2]

Для создания, внедрения и дальнейшего функционирования СУИБ в организации необходимо создать рабочую группу, ответственную за внедрение СУИБ. В ее состав должны войти:

- представители высшего руководства организации;
- представители бизнес-подразделений, охватываемых СУИБ;
- специалисты подразделений, обеспечивающих информационную безопасность в компании, имеющие соответствующее образование или подготовку, знающие основные принципы и лучшие практики в области информационной безопасности. [3]

В процессе внедрения СУИБ перед специалистами по информационной безопасности стоят следующие задачи:

1. Выбор области деятельности организации, которая будет охвачена СУИБ

При выборе области деятельности, в которой будут внедряться механизмы СУИБ, необходимо учесть следующие факторы:

- деятельность и услуги, предоставляемые организацией своим партнерам и клиентам;
- целевая информация, безопасность которой должна быть обеспечена;
- бизнес-процессы, обеспечивающие обработку целевой информации;
- подразделения и сотрудники организации, задействованные в данных бизнес-процессах;
- программно-технические средства, обеспечивающие функционирование данных бизнес-процессов;
- территориальные площадки компании, в рамках которых происходят сбор, обработка и передача целевой информации.

Результатом является согласованная с высшим руководством область деятельности организации, в рамках которой планируется создание СУИБ. [2]

2. Выявление несоответствий

Для уточнения объема работ и необходимых затрат на создание и последующую сертификацию СУИБ сотрудники, отвечающие за информационную безопасность проводят работы по выявлению и

анализу несоответствий существующих в организации мер защиты требованиям стандартов СУИБ.

Результатом этих работ должен стать перечень несоответствий требованиям стандартов и план работ по созданию СУИБ организации. [2]

3. Идентификация и определение ценности активов

Специалисты по информационной безопасности должны рассмотреть все бизнес-процессы, определить ценность этих активов, которая выражается в величине ущерба для организации, если нарушается какое-либо из следующих свойств актива: конфиденциальность, целостность, доступность. Информация о ценности актива может быть получена от его владельца или же от лица, которому владелец делегировал все полномочия по данному активу, включая обеспечение его безопасности.

Результатом данных работ является отчет об идентификации и оценке ценности активов. [2]

4. Анализ рисков

Анализ рисков — это основной движущий процесс СУИБ. Он выполняется не только при создании СУИБ, но и периодически при изменении бизнес-процессов организации и требований по безопасности.

Необходимо подобрать такую методику анализа рисков, которую можно было бы использовать с минимальными изменениями на постоянной основе.

В процессе анализа рисков для каждого из активов или группы активов производится идентификация возможных угроз и уязвимостей, оценивается вероятность реализации каждой из угроз и, с учетом величины возможного ущерба для актива, определяется величина риска, отражающего критичность той или иной угрозы. [3]

5. Реализация плана обработки рисков

Принятие плана обработки рисков и контроль над его выполнением осуществляет высшее руководство организации. Выполнение ключевых мероприятий плана является критерием, позволяющим принять решение о вводе СУИБ в эксплуатацию.

6. Разработка политик и процедур СУИБ

Разработка организационно-нормативной базы, необходимой для функционирования СУИБ, может проводиться параллельно с реализацией мероприятий плана обработки рисков. [2]

7. Внедрение СУИБ в эксплуатацию

Датой ввода СУИБ в эксплуатацию является дата утверждения высшим руководством компании положения о применимости средств управления. Данный документ является публичным и декларирует цели и средства, выбранные организацией для управления рисками. [2]

ЗАКЛЮЧЕНИЕ

Выполнение вышеуказанных действий, а также постоянный контроль, анализ, поддержание в рабочем состоянии и улучшение СУИБ являются общепризнанными методами работы в области информационной безопасности, позволяющими добиться защиты информации от широкого диапазона угроз, гарантировать непрерывность бизнеса, снижать риски и максимизировать возврат инвестиций.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 27001 Первое издание 2005-10-15 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования

2. ГСТУ СУИБ 2.0/ISO/IEC 27002: Информационные технологи. Методы защиты. Свод правил для управления информационной безопасностью.

3. Информационная технология. Практические правила управления информационной безопасностью. МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 17799:2000