

МОДЕЛЬ ПОЛИТИКИ УПРАВЛЕНИЯ ОСВЕДОМЛЕННОСТЬЮ СОТРУДНИКОВ ОРГАНИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.В. Астахова, Н.Л. Ульянов

На основе международных стандартов по управлению информационной безопасностью в статье определено понятие осведомленности сотрудников в области информационной безопасности, а также обоснована модель Политики управления осведомленностью сотрудников в области информационной безопасности.

Ключевые слова: осведомленность, информационная безопасность, управление, политика, модель.

Типовая Политика осведомленности в области ИБ сотрудников организации – это ключевой документ, определяющий основополагающие принципы и порядок создания и изменения программы повышения осведомленности персонала. В то время как программа осведомленности может изменяться довольно часто в зависимости от влияния внешних условий, на политику большинство изменений внешних условий не должно оказывать влияния. Политика должна включать основные аспекты программы повышения осведомленности, поэтому ее оптимальная структура выглядит следующим образом:

1. Термины и определения.
2. Общие положения.
3. Осведомительные материалы.
4. Потребность в обучении и подготовке персонала.
5. Планирование процесса обучения.
6. Организация процесса обучения.
7. Контроль.
8. Совершенствование.
9. Ответственность.

В разделе 1 дается определение понятия осведомленность в области информационной безопасности сотрудников организации. К сожалению, ни в одном документе нет четкого определения данного понятия. Анализ стандартов ISO/IEC 27002:2013 [1], NIST SP800-50 [2], СТО БР ИББС 1.0-2014 [3] показал, что в них закреплены следующие принципы осведомленности:

- понимание сотрудником своих ролей и должностных обязанностей [2];
- понимание сотрудником требований и процедур информационной безопасности, принятые в организации [1] [2] [3];
- понимание сотрудником общих вопросов использования ИТ-ресурсов и обеспечения информационной безопасности [2];
- понимание сотрудником значимости и важности деятельности работников для обеспечения ИБ организации [1] [3];
- понимание сотрудником своей персональной ответственности за свои действия и бездействие по отношению к безопасности конфиденциальной информации [1].

Опираясь на названные принципы, мы сформулировали следующее определение:

Осведомленность сотрудника в области информационной безопасности – это наличие у сотрудника знаний об общих вопросах обеспечения информационной безопасности и понимание им своих ролей и обязанностей, как должностных, так и по обеспечению информационной безопасности, и средств выполнения этих обязанностей, а также осознание им важности соблюдения режима информационной безопасности и персональной ответственности за его несоблюдение.

Раздел 2 должен быть построен с учетом того, что:

- политика разработана для повышения уровня информационной безопасности предприятия;
- в организации должна быть создана и поддерживаться программа повышения осведомленности в области информационной безопасности;
- целью программы повышения осведомленности является ознакомление сотрудников с их обязанностями, касающихся вопросов информационной безопасности, и средствами выполнения этих обязанностей;

– программа повышения осведомленности должна быть установлена в соответствии с существующими политиками организациями и средствами обеспечения информационной безопасности, а так же учитывать особенности деятельности организации, а также должна планироваться с учетом роли сотрудников в организации.

В разделе 3 должны содержаться сведения о том, какие осведомительные материалы должны быть внедрены (будут это постеры, ручки или всплывающие сообщения на мониторе и т.д.), кто будет создавать осведомительные материалы, как часто следует их обновлять.

В разделе 4 необходимо описать условия, наличие которых определяет необходимость прохождения сотрудником обучения. Такими условиями являются: получение новой роли и обязанностей, важные изменения локальных, нормативных или иных актов, наступление срока переобучения, негативный результат проверки сотрудника. В этом же разделе нужно распределить обязанности по контролю.

В разделе 5 необходимо описать аспекты, которые стоит учитывать при планировании программы обучения [3, п. 3.3]:

- распределение ролей и обязанностей по разработке программ обучения;
- распределение ролей и обязанностей по проведению обучения;
- распределение сотрудников по группам;
- источники материалов для программы обучения;
- определение перечня тематик для каждой группы;
- методы обучения (аудиторные, дистанционные, самостоятельные);
- перечень необходимой документации для регистрации событий прохождения обучения и оценки результатов обучения.

В Раздел 6 должна быть включена информация о порядке регистрации событий прохождения обучения, фиксации результатов прохождения обучения работников [2, п. 8.9]; определен порядок распределения ролей и обязанностей для выполнения этих функций; должен быть описан порядок обработки случаев пропуска сотрудниками занятий, неудовлетворительных результатов прохождения обучения.

В разделе 7 определяется порядок контроля уровня осведомленности персонала и соблюдения политики осведомленности: распределены роли и обязанности по контролю соблюдения политики осведомленности, описаны методы контроля уровня осведомленности персонала. Так, методами контроля могут быть:

- явные проверки (опросы, тесты, интервью, внешний или внутренний аудит) [3, п. 6.2];
- неявные проверки (телефонные звонки и электронные письма провокационного характера с использованием приемов социальной инженерии) [2, п. 7.2.6];

– сбор и анализ статистики инцидентов информационной безопасности в организации [1, п. 7.2.2].

В разделе 8 должны быть описаны условия, при которых необходимо производить совершенствование программы повышения осведомленности. Такими условиями могут быть отсутствие положительной динамики изменения количества инцидентов информационной безопасности в течение длительного периода после внедрения программы повышения осведомленности; существенное изменение законодательства, локальных или иных актов, требующее немедленного пересмотра программы и другие.

В разделе 9 определяется ответственность. Ответственность должна быть назначена как за несоблюдение требований информационной безопасности, так и за невыполнение обязанностей по разработке программы обучения, регистрации событий прохождения обучения и др.

Таким образом, сформулированное нами понятие осведомленности сотрудников в области информационной безопасности позволило смоделировать Типовую политику управления осведомленностью сотрудников в области информационной безопасности. Она может быть использована для повышения уровня информационной безопасности в организации любой формы собственности и отраслевой принадлежности.

Библиографический список

1. ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.
2. СТОБРИББС-1.0-2014. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М., 2014.
3. NIST SP 800-50. Building an Information Technology Security Awareness and Training Program.

[К содержанию](#)