Казыханов А.А., Казыханова Д.Р., Киреева А.И.

Разработка типовых рекомендаций для предприятий по защите информации

Башкирский государственный университет
(Россия, Уфа)

doi:10.18411/lj-11-2018-150

idsp: ljournal-11-2018-150

Аннотация

В данной статье рассматривается разработка типовых рекомендаций. В процессе написания статьи будут сформулированы рекомендации по различным направлениям защиты информации на типовом предприятии

Ключевые слова: рекомендации, защита информации, направления защиты, технические аспекты

Abstract

This article discusses the development of standard recommendations. In the process of writing this article, recommendations will be formulated on various areas of information protection in a typical enterprise.

Keywords: recommendations, protection of information, directions of protection, technical aspects

В первую очередь, необходимо учитывать важность обрабатываемой информации. Отметим, система защиты информации должна быть тщательно продумана, основана на нормативно-правовых актах, а также должна эффективно и бесперебойно работать. В качестве типовых примеров рекомендации были сформулированы по двум основным направлениям:

- организационные аспекты защиты информации;
- технические аспекты защиты информации.

Под организационными аспектами защиты информации подразумевается регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. В качестве рекомендации по данному направлению отметим следующее:

- необходимо своевременное обновление локальных нормативно-правовых актов, регулирующих защиту информации. Так как обычно такие акты либо устарели, либо нуждаются в доработке. Из-за этого система защиты информации предприятия имеет некоторые уязвимости с точки зрения организационной защиты. Безусловно, создание и разработка локальных нормативно-правовых актов требует большого количества времени и материальных средств, однако, благодаря данному шагу общий уровень системы защиты информации на предприятии повышается. Также, необходимо отметить, что для эффективной работы системы защиты информации локальные акты не только должны быть разработаны, но и внедрены;
- необходимо проводить семинары и лекции по основам информационной безопасности, данный шаг поможет поднять общий уровень знаний персонала в области ИБ, именно это поможет предотвратить инциденты информационной безопасности. Такие курсы помогут избавиться от информационных инцидентов по вине некомпетентности сотрудника в данной области. Стоимость таких курсов варьируется от количества часов и от уровня специалистов, проводящих лекции. Для общего обучения

персонала достаточно будет кратковременных курсов, которые помогут сотрудникам, которые никогда не касались области информационной безопасности, получить необходимые знания о роли защиты информации, а также о способах и методах защиты информации. Данные курсы, как правило, часто проводятся системными интеграторами в области защиты конфиденциальной информации;

- необходимо ввести поощрения и штрафы за соблюдение или не соблюдение элементарных правил информационной безопасности. Например, вешать стикер со своим логином и паролем от учетной записи на монитор персонального компьютера. Метод поощрения и штрафов за соблюдение или не соблюдение правил информационной безопасности поможет повысить общий уровень защищенности, а также избежать неприятных инцидентов информационной безопасности. При этом, элементарные правила информационной безопасности следует описать в документе, после чего с этим документом ознакомить всех сотрудников. О поощрениях или штрафах за соблюдение или не соблюдение правил информационной безопасности стоит написать в трудовом договоре.

Касаемо рекомендаций в области технической защиты информации, отметим:

- необходимо обеспечить все ПК пользователей двухфакторной аутентификацией;
- необходимо установить самое свежее антивирусное программное обеспечение;
- необходимо своевременно обновлять парк машин.

1. Нестеров, С.А. Информационная безопасность: Учебник и практикум для академического бакалавриата / С.А. Нестеров - М.: Юрайт, 2017. - 322 с. ISBN 978-5-534-00258-4
2. Милославская, Н.Г., Сенаторов, М.Ю., Толстой, А.И. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М.: Гор. линия-Телеком, 2013. - 214 с. - ISBN 978-5-9912-0274-9

Казыханов А.А., Казыханова Д.Р., Киреева А.И.

Актуальность проведения аудита

*Башкирский государственный университет
(Россия, Уфа)*

doi:10.18411/lj-11-2018-151

idsp: ljjournal-11-2018-151

Аннотация

В данной статье будет рассмотрено понятие аудит. В процессе изучения данной темы будет объяснена актуальность аудита информационной безопасности, а также сформулирован перечень рекомендаций, которые напрямую взаимосвязаны с аудитом

Ключевые слова: аудит, информационная безопасность, угрозы, уязвимости

Abstract

This article will consider the concept of auditing. In the process of studying this topic, the relevance of the information security audit will be explained, and a list of recommendations that are directly related to the audit will be formulated

Keywords: audit, information security, threats, vulnerabilities

Актуальность проведения аудита обуславливается различными факторами. Одна из причин – современный рынок, который насыщен аппаратно-программным