УДК 004.9

Чаденкова А.А.,
студентка
2 курс, факультет «Информационные системы и технологии»
ФГБОУ ВО «Поволжский государственный университет
телекоммуникаций и информатики»,
г. Самара, Российская Федерация
Научный руководитель: Бедняк С.Г.,
К.п.н., доцент, преподаватель
кафедры «Информационные системы и технологии»
ФГБОУ ВО «Поволжский государственный университет
телекоммуникаций и информатики»,
г. Самара, Российская Федерация

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ НАДЕЖНОСТИ РАБОЧЕЙ СТАНЦИИ И ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: *В работе рассматриваются основные организационные принципы по обеспечению информационной безопасности в организациях. Основное внимание уделяется человеческому фактору в данном вопросе, выделены основные пункты для составления политики безопасности компании.*

Ключевые слова: *информационная безопасность, кибербезопасность, политика безопасности, администратор безопасности, конфиденциальная информация.*

ORGANIZATIONAL AND TECHNICAL ACTIONS TO ENSURE THE RELIABILITY OF THE WORKING STATION AND PROTECTION OF INFORMATION

Abstract: *The paper discusses the basic organizational principles for ensuring information security in organizations. The focus is on the human factor in this matter, highlighted the main points for drawing up the company's security policy.*

Keywords: *information security cyber security, security policy, security administrator, confidential information.*

Организационное обеспечение – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основ таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий.

При рассмотрении угроз кибербезопасности человеческая ошибка является фактором, который часто упускается из виду. Однако, согласно статистике IBM, треть от числа всех атак совершена сотрудниками компаний непреднамеренно, игнорируя политику безопасности компании.

Основной шаг в снижении роли человеческих ошибок в вопросе защиты информации является установление политики кибербезопасности, а именно определение организационных и технических мер по обеспечению надежности ПК и защиты корпоративной информации.

В данную политику следует включить следующие пункты:

1) Важность кибербезопасности

На первом шаге необходимо определить почему важна компьютерная безопасность и каковы потенциальные риски. Если данные клиента или сотрудника будут утеряны или украдены, это может серьезно повлиять на вовлеченных лиц, а также серьезно поставить под угрозу компанию. Если

системы компании заражены вредоносным ПО, это может серьезно снизить эффективность компании.

2) Эффективное управление паролями

Парольная защита является важным элементов в системе кибербезопасности компании. Именно поэтому на втором шаге необходимо разработать требования к паролям, их хранению, передаче (обмену между сотрудниками), обновлению (сроки).

3) Основные виды угроз компьютерной безопасности

Для составления правильного плана по информационной безопасности необходимо знать основные виды угроз.

4) Обновления

Обязательным условием для поддержания компьютерной безопасности является регулярное обновление антивирусных программ, веб-браузеров и других настольных приложений. Так же выполнение полного сканирования на наличие вредоносных программ не реже одного раза в неделю.

5) Защита конфиденциальной информации

К конфиденциальным данным компании относятся: данные кредитных карт, имена, адреса электронных почт и другие персональные данные клиентов. Для отправки за пределы организации данного вида информации должна быть использована система безопасной передачи данных, которая шифрует информацию и позволяет только авторизованным пользователям получить к ней доступ.

6) Блокировка компьютеров и устройств

Для предотвращения несанкционированного доступа к техническим средствам сотрудников компании, они должны быть по окончанию работы заблокированы и/или должен быть осуществлен выход из системы.

7) Безопасные портативные носители

При использовании портативных устройств, таких как мобильные телефоны и ноутбуки, пароли должны быть установлены для ограничения доступа. При подключении портативных носителей, таких как USB-накопители

и DVD-диски, важно сканировать их на наличие вредоносных программ при подключении к сети.

8) Фиксирование потерянных или украденных устройств

Похищенные устройства могут быть отправной точкой для злоумышленника, чтобы получить доступ к конфиденциальным данным, поэтому сотрудникам организации стоит немедленно сообщать о потерянных или украденных устройствах. Ранее обнаружение может помочь удаленно заблокировать устройство.

9) Активное участие

Все сотрудники организации должны принимать активное участие в обеспечении информационной безопасности. О подозрительной активности, ошибках в системе и других неисправностях сотрудникам необходимо своевременно сообщать ИТ-специалистам, чтобы можно было избежать ущерба или хотя бы минимизировать.

Политика кибербезопасности должна быть включена в трудовое соглашение, а так же должен быть составлен план регулярного обучения информационной безопасности, чтобы сотрудники понимали руководящие принципы.

Ответственным за составление политики безопасности в компании является администратор безопасности, к обязанностям которого так же относятся:

- мониторинг и управление компьютерами и устройствами;
- разработка и поддержка организационных стандартов безопасности, лучших практик, профилактических мер и планов аварийного восстановления;
- проведение тестов на проникновение (симуляция кибератак, чтобы заранее обнаружить уязвимости);
- сообщение о нарушениях безопасности пользователям по мере необходимости и высшему руководству;
- внедрение и обновление программного обеспечения для защиты информации;

– ознакомление с последними тенденциями и информацией в области информационной безопасности.

Задача обеспечения информационной безопасности актуальна для среднего и малого бизнеса. Особенно сегодня, когда бизнес-процессы активно переходят в виртуальное пространство: оплата товаров и услуг через Интернет, электронная почта, IP-телефония, облачные хранилища, виртуальные сервера — все это стало типично для современных фирм средней руки, как и атаки хакеров, утечка конфиденциальных данных, в том числе финансовых и так далее.

СПИСОК ИСТОЧНИКОВ ИНФОРМАЦИИ

1. Бабаш, А.В. Информационная безопасность. История защиты информации в России [Текст]: учеб. пособие для вузов / А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. – КДУ: 2015. – 736с.
2. Максимов, Н.В. Современные информационные технологии[Текст]: учеб. пособие для вузов / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. – Москва: Форум, 2013. - 512 с
3. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности [Текст]: учеб. пособие для вузов / Ю. А. Родичев. – СПб: Питер, 2017. – 256с.
4. Шаньгин, В.Ф. Информационная безопасность и защита информации [Текст]: учеб. пособие для вузов / В.Ф. Шаньгин. – Москва: ДМК Пресс, 2014. – 702с.
5. Информационные технологии в профессиональной деятельности [Элек-тронный ресурс]: учебное пособие/ Клочко И.А.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2014.— 236 с. – Режим доступа: http://www.bibliocomplectator.ru/book/?&id=20424.
6. www.intuit.ru [Электронный ресурс]/ Национальный Открытый Университет «ИНТУИТ» ─ Электрон. дан. – www.intuit.ru, 2016.–Режим доступа: http://www.intuit.ru/, свободный.