

УДК: 004.056(072) + 81`272 + 003-048.85

**ПРИМЕНЕНИЕ ПРАВИЛ ЯСНОГО ЯЗЫКА ПРИ ОБУЧЕНИИ РАБОТНИКОВ
ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ**

Захарова Е.С.

*Институт информационных технологий БГУИР, г. Минск, Республика Беларусь,
zaharova@info-center.by*

Для обеспечения защиты информации в организациях разрабатываются политики информационной безопасности. Доведение требований сложного для прочтения и понимания текста

политики должно осуществляться простым и понятным для работников языком. Адаптацию текста политики информационной безопасности рекомендуется осуществлять по правилам ясного языка.

Ключевые слова: обучение работников, информационная безопасность, защита информации, ясный язык, стиль изложения

Сегодня сложно представить государственный орган, учреждение, организацию или предприятие, в которых не используются информационные системы. Одним из наиболее важных элементов информационной системы является база данных, под которой понимается «совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях» (абз. 2 ст. 1 Закона Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (далее – Закон об информатизации). Закон об информатизации обязывает всех субъектов информационных отношений осуществлять защиту информации, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу (ч. 1 ст. 28 Закона об информатизации). Даже общедоступная информация подлежит защите от уничтожения, модификации, блокирования правомерного доступа к ней (ч. 2 ст. 28 Закона об информатизации).

Порядок защиты информации определен в Положении о технической и криптографической защите информации, утвержденном Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации», а также в Положении о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденном Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – Положение). В процессе эксплуатации информационной системы лицо, ответственное за обеспечение защиты информации обязано на регулярной основе, но не реже одного раза в год проводить инструктажи, иные мероприятия, направленные на повышение уровня знаний и навыков работников по вопросам применения системы защиты информации в части, их касающейся (п. 19 Положения).

Оперативно-аналитическим центром при Президенте Республики Беларусь разработаны Рекомендации по обеспечению защиты общедоступной информации в информационных системах [1], в которых отдельный раздел посвящен вопросам информирования и обучения персонала. В частности, рекомендуется определить политики и процедуры информирования и обучения работников, не реже одного раза в квартал информировать работников об угрозах информационной безопасности, правилах безопасной работы с объектами информационной системы, а также не реже одного раза в полугодие проводить с работниками практические занятия по правилам безопасной работы с объектами информационной системы.

Таким образом, представляется актуальным рассмотрение особенностей обучения работников основам защиты информации, обрабатываемой в информационных системах.

В настоящее время в научной литературе проблеме обучения работников основам информационной безопасности уделяется большое внимание, поскольку «никто не может нанести большего ущерба организации, чем ее работник, допущенный практически ко всем средствам и секретам предприятия» [2, с. 205].

Применительно к теме настоящего исследования всех работников можно условно разделить на:

1. работников подразделения защиты информации. Они имеют высшее образование в области защиты информации либо высшее, или среднее специальное, или профессионально-техническое образование и прошли переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством (п. 9 Положения). Данная категория работников имеют необходимый уровень знаний и компетенций в сфере защиты информации.

2. иных работников, которые имеют иное, не связанное с защитой информации, образование. Уровень знаний в сфере информационной безопасности у данной категории работников будет различаться в зависимости от возраста, сферы профессиональной деятельности, цифровых навыков, в том числе умения работать с информацией, хранить ее и защищать. И именно с этих категорий работников необходимо систематически проводить обучение, направленное на повышение уровня осведомленности в сфере информационной безопасности.

Следует отметить, что в настоящее время работа по повышению грамотности работников в сфере информационной безопасности и защиты информации не носит системный, плановый характер. Зачастую оно осуществляется формально, без «привязки» к должностным обязанностям конкретного работника, а также без учета его возможностей по восприятию, запоминанию и исполнению установленных в организации правил работы в информационных системах.

С нашей точки зрения, при обучении работников основам информационной безопасности и защиты информации при работе в информационных системах особое внимание следует уделять стилю подачи информации [3, с. 96].

Так, основные положения, определяющие принципы защиты информации, общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, обрабатываемой в информационной системе, закрепляются в политике информационной безопасности (далее – политика ИБ) (п. 10 Положения). Как локальный правовой акт политика ИБ должна быть написана с соблюдением норм официально-делового стиля литературного языка и с использованием терминов и определений, предусмотренных нормативными правовыми актами, техническими нормативными правовыми актами, в том числе государственными стандартами Республики Беларусь, и терминологическими словарями (п. 63, 66 Инструкции по делопроизводству в государственных органах, иных организациях, утвержденная Постановлением Министерства юстиции Республики Беларусь от 29.08.2025 № 65). На практике политика ИБ – набор формальных правил, которые регламентируют порядок обеспечения информационной безопасности с использованием слов и терминов официально-деловой сферы. Такой официальный стиль подачи информации затрудняет ее восприятие, ухудшает понимание о возможности применения полученных знаний в практической деятельности работника на своем рабочем месте, и в конечном итоге может демотивировать исполнение установленных правил информационной безопасности. Ситуация может осложняться еще и тем, что работники, не имеющие технического или юридического образования, наверняка не будут знакомы с терминами и определениями, предусмотренными в нормативных правовых актах, технических нормативных правовых актах, а также в государственных стандартах. Ситуация усложняется, если работник является иностранным гражданином и испытывает трудности в чтении и(или) понимании текста на русском языке.

Для облегчения понимания положений, закрепленных в политике ИБ, ускорения процесса запоминания установленных в ней правил и требований информацию рекомендуем адаптировать с учетом уровня целевой аудитории по правилам ясного языка. При подготовке материалов по информационной безопасности на ясном языке целесообразно придерживаться положений, установленных Государственным стандартом Республики Беларусь «Ясный язык. Основные положения» СТБ 2595-2021[4] (далее - СТБ 2595-2021).

Так, СТБ 2595-2021 в качестве критерия сложности изложения информации на ясном языке указывает развитие речи целевой аудитории:

A1 – люди, которые плохо читают и пишут;

A2 – люди, которые читают и пишут с ошибками;

B1 – люди, которые читают и пишут с ошибками, но хорошо разбираются в некоторых темах и знают основные термины (подп. 4.3. п. 4).

Информация на ясном языке уровня A1 должна содержать:

- небольшой текст с 1-3 короткими предложениями на странице (слайде);

- большие понятные изображения: пиктограммы, рисунки, в редких случаях фото;

- призыв к действию, запрет, короткие инструкции.

Информация на ясном языке уровня А2 должна содержать:

- более 3 предложений;
- различные виды графических изображений;
- в предложении не более 18 слов;
- текст на странице формата А4 объемом не более 900 знаков (без учета пробелов).

Информация на ясном языке уровня В1 должна содержать: предложения, состоящие максимум из 18-20 слов; термины, понятные целевой аудитории, без сложных синтаксических конструкций; большой объем информации по знакомой теме; текст на странице формата А4 объемом не более 1800 знаков (без учета пробелов) (Приложение А к СТБ 2595-2021).

С нашей точки зрения, при проведении обучения по вопросам информационной безопасности целесообразно всех работников распределить на соответствующие группы с учетом не только уровня развития речи, но и уровня образования, возраста, должностных обязанностей. В литературе можно встретить иные предложения по группировке работников, например, по признаку желаемого темпа обучения [5, с. 29].

Предположим, в организации работают архивариус с нарушением слуха, делопроизводитель с общим средним образованием, секретарь приемной, инженер по охране труда и специалисты по работе с клиентами со средним специальным образованием, главный бухгалтер, маркетолог, юрисконсульт и специалист по кадрам с высшим образованием. Все перечисленные работники ежедневно пользуются информационными системами (ресурсами): общаются друг с другом посредством корпоративного портала, получают и отправляют электронные письма, работают с системой электронного документооборота, CRM-системой и др., следовательно, с ними необходимо проводить мероприятия, направленные на повышение уровня их знаний и навыков в сфере защиты информации.

При проведении обучающих мероприятий с архивариусом материал по вопросам защиты информации следует переработать и изложить максимально просто, без употребления профессиональных терминов, используя разговорный стиль, придерживаясь правил ясного языка уровня А1. Например, вместо фразы «Работник обязан обеспечить конфиденциальность своего пароля. Запрещается передавать третьим лицам пароль для входа в учетную запись» можно использовать выражение «Никому не сообщайте пароль для входа в ваш компьютер».

В ходе обучения делопроизводителя, секретаря приемной, инженера по охране труда, а также специалистов по работе с клиентами установленные в локальных правовых актах правила защиты информации при работе в информационной системе необходимо отредактировать. Для этого подобрать к словам или фразам, которые могут быть непонятны, синонимы или разъяснения. Если подобрать простой и ясный синоним невозможно, а разъяснение слишком загромождает текст, фразу необходимо перестроить таким образом, чтобы, с одной стороны, избежать употребления сложного термина или фразы, а с другой, максимально сохранить первоначальный смысл. Например, фразу «Пароль должен соответствовать следующим требованиям: состоит не менее чем из восьми символов; содержит символы трех категорий из числа следующих: буквы верхнего регистра английского или русского алфавита; буквы нижнего регистра английского или русского алфавита; цифры, специальные символы» заменить на «Оптимальная длина пароля 8-10 символов. Используйте заглавные и строчные буквы, символы, цифры, знаки препинания».

Информация для работников с высшим образованием (главный бухгалтер, маркетолог, юрисконсульт, специалист по кадрам) можно упростить путем замены сложных технических терминов, аббревиатур и иностранных слов на простые и понятные слова и формулировки. Например, вместо фразы «До начала инсталляции необходимого ПО обязательно выполнение антивирусной проверки файлов дистрибутивов» использовать выражение «Перед установкой необходимого программного обеспечения выполните его антивирусную проверку».

Написанные по правилам ясного языка тексты для различных групп работников можно разбить на взаимосвязанные тематические модули, загрузить их на платформу для электронного обучения и определить срок, в течение которого работники должны пройти

обучение. Добавляем на платформу работников, присваиваем им роль ученика и разбиваем на группы по описанным выше правилам. Пройдя последовательно, в свободном режиме обучение по всем модулям курса, обучаемый получает знания и умения [6, с. 187] в соответствии со своими возможностями восприятия и понимания информации.

Таким образом, можно сделать следующий вывод. Использование правил ясного языка при обучении основам безопасной работы в информационных системах позволит работникам с различным образованием, возрастом, уровнем развития речи и иными особенностями, в доступной для себя форме усвоить правила защиты информации и успешно применять их на практике.

Литература

1. Рекомендации по обеспечению защиты общедоступной информации в информационных системах - URL: <https://www.oac.gov.by/recommendations-for-government-agencies>
2. Викторovich, А. Н. Обеспечение кадровой безопасности инфраструктуры информационных ресурсов / А. Н. Викторovich // Управление информационными ресурсами: материалы XVII Международной научно-практической конференции (Минск, 12 марта 2021 г.) / [редкол.: А. С. Лаптенко и др.]. – Минск: Академия управления при Президенте Республики Беларусь, 2021. - С. 204-206
3. Лямин, Д. П. Некоторые аспекты информационного воздействия на население в условиях глобальной цифровизации общества / Д. П. Лямин // Управление информационными ресурсами: матер. XVII Международной научно-практической конференции (Минск, 12 марта 2021 г.) / [редкол.: А. С. Лаптенко и др.]. – Минск: Академия управления при Президенте Республики Беларусь, 2021. - С. 95-96.
4. Государственным стандартом Республики Беларусь Ясный язык. Основные положения = Зразумелая мова. Асноўныя палажэнні: ГОСТ СТБ 2595-2021; введ. впервые 01.07.2021. – Минск: Госстандарт: Белорус. гос. ин-т стандартизации и сертификации, 2021. - 19 с.
5. Обухова, Г. Н. Цифровой работник: опыт Российской Федерации / Г. Н. Обухова // Проблемы трудового и социального права в условиях трансформации общества: сб. науч. тр. / редкол. К. Л. Томашевский (отв. ред.) [и др.]. – Минск: Междунар. ун-т «МИТСО», 2023. – 308 с. С. 25-32
6. Стацук, И. П. Применение LMS для организации непрерывного образования управленческих кадров / И. П. Стацук // Управление информационными ресурсами: матер. XVI Международной научно-практической конференции (Минск, 26 февр. 2020 г.) / [редкол. : Н. Л. Бондаренко, А. И. Ящук, Б. В. Новыш]. – Минск: Академия управления при Президенте Республики Беларусь, 2020. - С. 186-188

APPLYING CLEAR LANGUAGE RULES TO TRAIN EMPLOYEES IN THE BASICS OF INFORMATION SECURITY AND INFORMATION PROTECTION

Zakharova E.S.

Institute of Information Technologies of Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus, student

Organizations develop information security policies to ensure information security. The requirements of a policy text that is difficult to read and understand must be communicated in simple and understandable language for employees. It is recommended that the text of the information security policy be adapted according to the rules of clear language.

Keywords: employee training, information security, information protection, clear language, writing style.