Роль персонала в системе информационной безопасности: правовые инструменты или корпоративная культура?

Максим Кобрин

1. Кафедра социальной информатики,
Харьковский национальный университет радиоэлектроники,
УКРАИНА, г. Харків, пр. Науки, 14,
Юридическая компания «Кобрин и партнеры»
E-mail: kobrin.law@gmail.com

Коротка анотація – In this paper, issues of enhancing information security through the use of such personnel management tools as the formation of a corporate culture and strengthening the motivational climate in the company, as well as the formation of such an element of information security as staff training. Implementation of the proposed methods will reduce the number of information security incidents and increase the competitiveness of the company.

Ключові слова – информационная безопасность; система безопасности; корпоративная культура; управление персоналом; мотивационный климат.

I. Вступ

Персонал компании является частью информационной системы (ИС). Система информационной безопасности (ИБ) компании является подсистемой ИС, таким образом можно сделать вывод о том, что персонал компании является частью системы ИБ компании [1, 2]. Причиной инцидентов в области ИБ часто является «человеческий фактор». В настоящее время, персонал — это ключевой ресурс компании. Важно получить сотрудника, который сможет полностью удовлетворить функциональный запрос нанимателя [3] и избегать работать с сотрудником, который не сможет его удовлетворить.

II. Актуальность

На наш взгляд, корпоративная культура и мотивационный климат в компании также важны для управления ИБ, как и другие факторы, непосредственно связанные с информационными технологиями. Эти инструменты управления могут обеспечить элементы ИБ, которые невозможно или неэффективно обеспечивать другими способами. И наоборот, корпоративная культура и мотивационный климат могут существенно усилить информационную безопасность компании и, соответственно, повысить конкурентоспособность компании. Таким образом, актуальную задачу повышения уровня ИБ компании, предлагается решить посредством интеграции инструментов управления персоналом, таких как, формирование корпоративной культуры и мотивационного климата компании в систему ИБ. Кроме этого, предлагается дополнить систему ИБ подсистемой обучения персонала в области ИБ.

III. Основная часть исследования

Цель любого предприятия в отношении персонала - «безубыточные» для компании отношения. Из распространенных правовых инструментов, с помощью которых обеспечивается отсутствие или минимизация ущерба фирме, применяются такие инструменты как:

1. NDA (Non-disclosure agreement) - соглашение о неразглашении конфиденциальной информации.
2. NCA (Non-competition agreement) - соглашение о неконкуренции.

Однако, эти документы не согласуются с украинским законодательством и не могут в достаточной мере обеспечить те функции, для которых их оформляют (Рис.1).

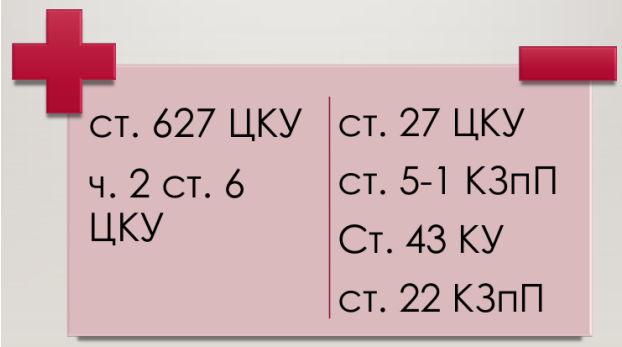

Рис.1. Статьи украинского законодательства, которые применимы к договорам NDA, NCA [4].

Это не значит, что их не нужно оформлять, так как подписанные NDA и NCA могут применяться для дополнительной мотивации сотрудников, как дополнительный психологический фактор обеспечения безопасности.

Роль корпоративной культуры в системе безопасности (СБ) должна быть отражена в политике ИБ, принципах построения и развития компании, в функциях системы безопасности.

Принципы системы безопасности (Рис.2):

1. Законность.
2. Соответствие корпоративной культуре.
3. Своевременность и активность (упреждающий характер мер обеспечения безопасности).
4. Экономическая целесообразность (сопоставимость возможного ущерба и затрат на обеспечение безопасности).
5. Специализация.

Например, некоторые пункты в функциях системы безопасности напрямую связаны с персоналом (п. 1, 2, 7, 8):

– Защита законных интересов компании и ее сотрудников.

– Обучение сотрудников по вопросам безопасности.

– Оперативное реагирование на угрозы безопасности компании.

– Защита коммерческой тайны компании.

– Инженерно-техническая защита зданий, сооружений компании.

– Обеспечение физической охраны собственности компании.

– Защита жизни, здоровья, достоинства сотрудников, прав сотрудников.

– Контроль выполнения сотрудниками правил безопасности.

– Разработка нормативной и методической документации по направлениям безопасности.

Рис. 2. Принципы построения и развития системы безопасности.

При подготовке персонала, с точки зрения ИБ, необходимо:

1. Добиться, чтобы выполнение правил безопасности стало частью корпоративной культуры компании (Рис.3).

Рис. 3. Корпоративная культура, как часть системы обучения правилам ИБ и контроля их выполнения.

2. Обеспечить мотивацию сотрудников на выполнение правил безопасности.

3. Обучить работающих в настоящее время сотрудников.

4. Обучать правилам безопасности сотрудников, принимаемых на работу.

5. Регулярно напоминать сотрудникам о правилах безопасности, проводить тренировки.

6. Организовать обучение руководителей (руководители должны быть подготовлены по более сложной программе, так как им придется обучать сотрудников и контролировать выполнение правил безопасности).

Выводы

На практике данный подход был реализован в ряде торговых компаний, например: ООО «Хот-Велл», ООО «Горизонт», ООО «Атлантик-Гейзер.

Особое внимание было уделено интеграции корпоративной культуры и мотивационного климата компаний с системой ИБ. Все сотрудники этих компаний прошли обучение в области ИБ. Кроме этого, регулярно проводятся занятия по ИБ, которые позволяют сотрудникам актуализировать свои знания. Внедрение данного подхода к управлению персоналом позволило существенно повысить информационную безопасность, эффективность и конкурентоспособность компаний. Количество инцидентов в области информационной безопасности снизилось и, в случаях их возникновения, благодаря подготовке персонала, действия сотрудников были эффективными и слаженными, что позволило минимизировать ущерб для компании.

Дальнейшее изучении этого подхода состоит в разработке соответствующих моделей и более глубокой интеграцией с бизнес-процессами компаний.

Литература

[1] Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. — К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. — 716 с.

[2] Грайворонський, М.В. Безпека інформаційно-комунікативних систем / М.В. Гайворонський, О.М. Новиков. – BHV, 2009. – 608 с.

[3] Кобрин М.В. К вопросу об обеспечении эффективности и безопасности индивидуальной информационной системы пользователя / М.В. Кобрин // 22-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI столетии». Зб. Материалов форума. Т.9. – Харьков: ХНУРЭ. 2018. – С.85-86.

[4] NON-COMPETE В УКРАЇНІ. Гаркуша Андрій [Электронный ресурс]. – Режим доступа: www/URL: https://uba.ua/documents/NON-COMPETE В УКРАЇНІ. Гаркуша Андрій.pdf